



# **Feasibility Study for a European Travel Information and Authorisation System (ETIAS)**

Final Report

16 November 2016



Written by PwC

*November – 2016*

**EUROPEAN COMMISSION**

Directorate-General for Migration and Home Affairs

Directorate B— Migration and Mobility

Unit B.3 — Information Systems for Borders and Security

*Contact: Marc SULON*

*E-mail: HOME-SMART-BORDERS@ec.europa.eu*

*European Commission*

*B-1049 Brussels*

***Europe Direct is a service to help you find answers  
to your questions about the European Union.***

**Freephone number (\*):**

**00 800 6 7 8 9 10 11**

(\* ) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

#### **LEGAL NOTICE**

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2016

ISBN: 978-92-79-63511-3

doi: 10.2837/36503

catalogue number: DR-06-16-239-EN-N

© European Union, 2016

Reproduction is authorised provided the source is acknowledged.



# Table of contents

<b>1 INTRODUCTION .....</b>	<b>8</b>
1.1 CONTEXT .....	8
1.2 WHAT IS THE ISSUE? .....	9
1.2.1 Information gap .....	9
1.2.2 Increasing traveller flows .....	9
1.2.3 Pressure at sea and land borders .....	10
1.2.4 Increasing return costs .....	10
1.3 WHY ETIAS? .....	11
<b>2 ETIAS HIGH-LEVEL DESIGN.....</b>	<b>12</b>
2.1 DESIGN PRINCIPLES .....	12
2.1.1 System objectives .....	12
2.1.2 System scope .....	13
2.1.3 Authorisation model.....	15
2.1.4 Validity period .....	15
2.1.5 Application fee.....	16
2.1.6 User perspective .....	17
2.2 DATA .....	18
2.2.1 Context .....	18
2.2.2 Approach .....	18
2.2.3 Purpose.....	19
2.2.4 Risks.....	19
2.2.5 Risk assessment.....	20
2.2.6 Data to be collected .....	23
2.2.7 Data set .....	28
2.2.8 Data retention .....	29
2.2.9 Access management and data ownership.....	30
2.3 BUSINESS PROCESSES .....	33
2.3.1 Context .....	33
2.3.2 Approach .....	33
2.3.3 Stakeholders involved.....	34
2.3.4 Four main processes.....	34
2.3.5 Process overview at the different border types.....	44
2.3.6 Support processes.....	48
2.4 ARCHITECTURE.....	52
2.4.1 Context .....	52
2.4.2 Approach .....	52
2.4.3 Architectural requirements .....	52
2.4.4 General architecture.....	53
2.4.5 ETIAS key IT architectural blocks .....	55
2.4.6 Interoperability with other systems.....	59
2.5 USER INTERACTIONS.....	63
2.5.1 Interacting with travellers .....	63
2.5.2 Interacting with carriers .....	67
2.6 SYSTEM SECURITY .....	72
2.6.1 Context .....	72
2.6.2 Purpose.....	72
2.6.3 Approach .....	73
2.6.4 Threat agents .....	73
2.6.5 Risk scenarios .....	73
2.6.6 Safeguards.....	78

2.7	IMPLEMENTATION APPROACH .....	84
2.7.1	<i>Roll-out options</i> .....	84
2.7.2	<i>Examples of large-scale IT systems roll-out</i> .....	85
2.7.3	<i>ETIAS implementation</i> .....	86
2.8	FUTURE TECHNOLOGY OPTIONS .....	88
2.8.1	<i>Mobile application</i> .....	88
2.8.2	<i>Shared infrastructure and private cloud services</i> .....	90
<b>3</b>	<b>EVALUATION OF IMPACT .....</b>	<b>91</b>
3.1	LEGAL .....	91
3.1.1	<i>Context</i> .....	91
3.1.2	<i>Legal consequences</i> .....	91
3.2	DATA PROTECTION.....	96
3.2.1	<i>Context</i> .....	96
3.2.2	<i>Approach</i> .....	96
3.2.3	<i>Data protection principles</i> .....	97
3.2.4	<i>Overview of safeguards</i> .....	97
3.2.5	<i>Points of attention for ETIAS</i> .....	97
<b>4</b>	<b>COST-BENEFIT ANALYSIS (CBA) .....</b>	<b>100</b>
4.1	COST MODEL .....	101
4.2	BENEFITS MODEL.....	104
4.3	CBA OUTCOME.....	105
4.4	SENSITIVITY ANALYSIS .....	105
4.5	OTHER IMPACTS.....	106
<b>5</b>	<b>CONCLUSIONS.....</b>	<b>107</b>
5.1	MAIN FINDINGS .....	107
5.1.1	<i>Design principles</i> .....	107
5.1.2	<i>Data</i> .....	108
5.1.3	<i>Business processes</i> .....	110
5.1.4	<i>Architecture</i> .....	111
5.1.5	<i>User interactions</i> .....	112
5.1.6	<i>System security</i> .....	113
5.1.7	<i>Implementation approach</i> .....	113
5.1.8	<i>Data protection</i> .....	114
5.1.9	<i>Cost-benefit analysis (CBA)</i> .....	115
5.2	CRITICAL SUCCESS FACTORS .....	115
<b>ANNEXES</b> .....	<b>117</b>	
ANNEX 1. – ACRONYMS AND ABBREVIATIONS .....	118	
ANNEX 2. – STUDY APPROACH.....	120	
<i>Objectives</i> .....	120	
<i>Scope</i> .....	120	
<i>Tasks</i> .....	120	
<i>Stakeholders</i> .....	123	
ANNEX 3. – DESIGN PRINCIPLES .....	124	
<i>Authorisation model</i> .....	124	
ANNEX 4. – DATA .....	126	
<i>Purpose</i> .....	126	
<i>Risks</i> .....	127	
<i>Current or upcoming relevant IT systems and databases</i> .....	133	
<i>Database checks</i> .....	141	
<i>ETIAS data fields assessment</i> .....	149	

<i>Definition of serious crime</i> .....	153
<i>Data collected by benchmark systems</i> .....	154
<i>Possible data collected by ETIAS</i> .....	157
<i>Data collected for visa</i> .....	158
<i>Data retention</i> .....	160
<i>Law enforcement access</i> .....	161
<i>Data model</i> .....	162
ANNEX 5. – BUSINESS PROCESSES .....	163
<i>Decision-making process options</i> .....	163
<i>Processing times</i> .....	164
<i>Field validation</i> .....	165
<i>Case-handling</i> .....	166
<i>Re-check of granted travel authorisations</i> .....	168
<i>Exemptions</i> .....	170
ANNEX 6. – ARCHITECTURE.....	175
<i>Architectural options</i> .....	175
ANNEX 7. – USER INTERACTIONS.....	184
<i>Interacting with travellers</i> .....	184
<i>Interacting with carriers</i> .....	192
ANNEX 8. – SYSTEM SECURITY .....	195
<i>Risk Assessment as per ISO 31000</i> .....	195
<i>Risk identification as per ISO 31000</i> .....	195
<i>Risk analysis as per ISO 31000</i> .....	196
<i>Risk evaluation as per ISO 31000</i> .....	196
<i>ETIAS Risk assessment</i> .....	197
<i>Safeguards</i> .....	223
ANNEX 9. – IMPLEMENTATION APPROACH .....	231
ANNEX 10. – DATA PROTECTION IMPACT.....	237
<i>Legal framework</i> .....	237
<i>ETIAS necessity and proportionality</i> .....	238
<i>Breakdown of safeguards by data protection principle</i> .....	238
<i>Overview of data protection safeguards for ETIAS</i> .....	249
ANNEX 11. – DETAILED COST-BENEFIT ANALYSIS .....	253
<i>Methodology</i> .....	253
<i>Cost model</i> .....	256
<i>Benefits valuation</i> .....	273
<i>Sensitivity analysis</i> .....	276
ANNEX 12. – ETIAS SIZING PARAMETERS .....	278

# 1 Introduction

## 1.1 Context

In February 2013, the European Commission (EC) tabled a package of legislative proposals on **Smart Borders**<sup>1</sup> aimed at modernising the Schengen Area's external border management. On 6 April 2016, a revised legislative proposal for Smart Borders was adopted by the Commission, including a Regulation for the establishment of an **Entry/Exit System** and a proposed amendment to the Schengen Borders Code (SBC) to integrate the technical changes needed for the Entry/Exit System (EES)<sup>2</sup>.

As part of an accompanying Communication to the European Parliament and the Council<sup>3</sup>, the EC also suggested assessing the possibility of establishing an **EU Travel Information and Authorisation System (ETIAS)**, in which **visa-exempt travellers would register relevant information** regarding their intended journey prior to departure. Similar systems have been put in place in other countries where bona-fide travellers have access to an online procedure allowing **migration and security risk assessments** to be performed before travelling to the border.

The initiative for a **European travel-authorisation system** is not new. In a communication from April 2008 on "preparing the next steps in border management in the EU"<sup>4</sup> the EC stated its intention to "examine the possibility of introducing an electronic system of travel authorisation at EU level". A year later, on 10 March 2009, the European Parliament adopted a resolution on the next steps in border management in the European Union and similar experiences in third countries, asking for a thorough explanation of the rationale for creating such a system<sup>5</sup>.

A study was subsequently carried out by PricewaterhouseCoopers in 2011, assessing options for establishing a travel-authorisation system for the EU<sup>6</sup>. In its conclusion, the study considered that at that time the conditions were not met for justifying such a system. In particular, only the SIS database was available to connect to and check entry conditions in advance. The study suggested following technical, political and legal developments at EU level to reconsider the conclusion reached. Five years have now passed and the context has changed. Increased global mobility, new migration and security challenges, the successful implementation of SIS II and VIS, and EU-wide momentum for safer and smarter borders embodied by the EES legislative proposal provide an **opportunity to revisit the conclusion on ETIAS**.

In light of this information gap for visa-exempt travellers, of the changed context, the need for a travel authorisation system was clearly identified by Member States and by the European Commission. This study describes solutions that would address the information gap, while minimising the negative impacts on stakeholders (including travellers, carriers, border guards and Member States' administrations).

---

<sup>1</sup> See: [http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228\\_01\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm) (accessed 10/2016).

<sup>2</sup> See: <https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-196-EN-F1-1.PDF> (accessed 10/2016).

<sup>3</sup> See: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication\\_on\\_stronger\\_and\\_smart\\_borders\\_20160406\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication_on_stronger_and_smart_borders_20160406_en.pdf) (accessed 10/2016).

<sup>4</sup> See: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008DC0069&from=EN>, p. 9.

<sup>5</sup> See: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009IP0085&from=EN>, p. 4.

<sup>6</sup> See: [http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/esta\\_annexes\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/esta_annexes_en.pdf) (accessed 06/2016).



## 1.2 What is the issue?

There are a number of pressing internal-security concerns faced by the EU that require an efficient response and justify the need for reassessing the feasibility of a travel-authorisation system.

### 1.2.1 Information gap

Progress has been made in recent years with a number of border-management systems, such as the full roll-out of the Visa Information System (VIS), the further development of the Schengen Information System (SIS), the Passenger Name Record (PNR) Directive, etc. However, the EU's IT landscape in the Migration and Home Affairs area still **lacks a system specifically covering visa-exempt third-country nationals (VE-TCNs)**. There is no advance information on this part of the population travelling to the Schengen Area. This group of travellers are **not subject to prior checks** and their individual entry conditions are not verified until they arrive at a border-crossing point to the Schengen Area. Today, over **1.2 billion people** from 61 countries fall into this category<sup>7</sup>. The following figure shows the countries of origin of visa-exempt third-country nationals (as at October 2016).

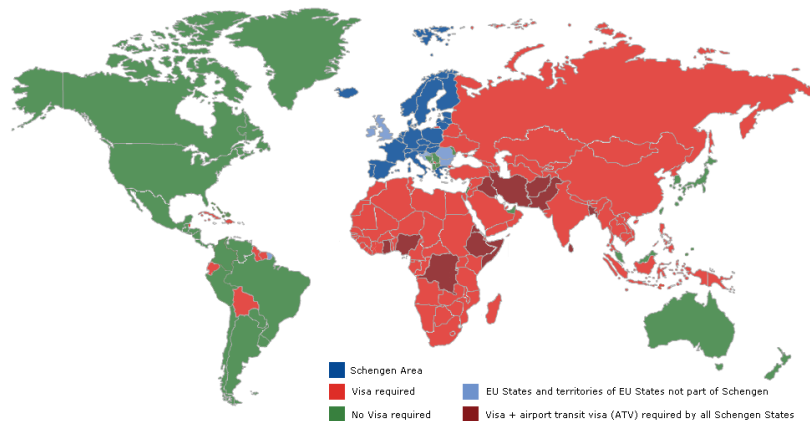


Figure 1: Countries of origin of visa-exempt third-country nationals

### 1.2.2 Increasing traveller flows

Global travel projections forecast a **major increase in border crossings** by air, land and sea in the next ten years. The total number of regular EU border crossings is expected to rise to **887 million** by 2025<sup>8</sup>, of which around **one-third would be by third-country nationals** traveling to Schengen countries for a short visit.

The completion of **visa-liberalisation negotiations** at EU level will contribute to the increase in border crossings by third-country nationals. The following figure illustrates the fast growth of the visa-liberalised population over the last 15 years – an increase of over 30%.

---

<sup>7</sup> Regulation No 539/2:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001R0539:20140609:EN:PDF> (accessed 06/2016).

<sup>8</sup> Technical Study on Smart Borders (2014), European Commission, p. 21, available at: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart\\_borders\\_technical\\_study\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf) (accessed 08/2016).

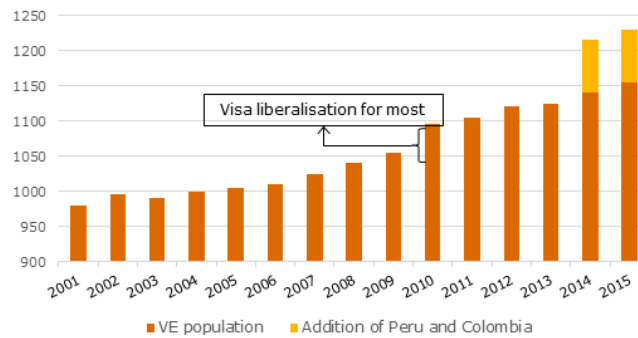


Figure 2: Growth in the visa-exempt (VE) population between 2001 and 2015 (in millions)<sup>9</sup>

### 1.2.3 Pressure at sea and land borders

Air borders will likely remain the major border-crossing point for VE-TCNs travelling to the Schengen Area in the future, though **sea and land will gain in importance**. Further progress with visa-liberalisation negotiations will impact on land borders in particular, posing **specific challenges** not faced today. And while Advance Passenger Information (API), and for some countries Passenger Name Records (PNR), are available at air borders, there is no equivalent at sea and land borders. They will face pressure from increasing VE-TCN flows and have no prior information on these travellers for the purpose of timely and efficient checks and risk assessment.

The following figure show the projected number of (entry and exit) border crossings for the Schengen Area in 2025 by visa-exempt travellers.

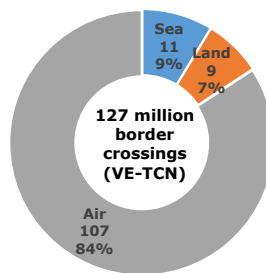


Figure 3: Projected number of entry and exit border crossings in 2025<sup>1011</sup>(in million) for visa-exempt travellers

### 1.2.4 Increasing return costs

The absence of information on, and pre-border-check screenings of, VE-TCNs poses further challenges, notably a **high rate of refusal of entry**, which results in **significant return costs**. The situation at land borders is particularly challenging in terms of refusal of entry. 56% of all **refusals of entry of third-country nationals** (both visa-exempt and visa holders)<sup>12</sup> at the border of the Schengen Area in 2015 were issued at land borders<sup>13</sup>.

<sup>9</sup> Frontex Risk Analysis for 2016, p. 22, available at:

[http://frontex.europa.eu/assets/Publications/Risk\\_Analysis/Annula\\_Risk\\_Analysis\\_2016.pdf](http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf) (accessed 09/2016).

<sup>10</sup> Estimation done assuming no change of visa regime in the period.

<sup>11</sup> Technical study on Smart Borders (2014), p. 23.

<sup>12</sup> Reliable information distinguishing between visa-holder and visa-exempt third-country nationals is not available.

<sup>13</sup> Frontex Risk Analysis for 2016, p. 66-68.

## 1.3 Why ETIAS?

A European Travel Information and Authorisation System is a comprehensive and effective response to the issues presented above. By **recording relevant information** regarding intended journeys by VE-TCNs prior to their departure and by carrying out **migration and security risk assessments** on them before they reach the border, the system would have the following benefits:

*Table 1: Main benefits of ETIAS*

<b>Issue</b>	<b>What ETIAS can offer</b>
<b>Information gap</b>	Stronger information position regarding VE-TCNs: who is coming to the border? Do they meet entry conditions? Do they pose any risk?
<b>Security concerns</b>	Enhanced security controls by making advance checks against watchlists.
<b>Increasing traveller flows</b>	Better management of traveller flows, in particular of visa-exempt traveller flows.
<b>Pressure at sea and land borders</b>	Enhanced border controls at the challenging border types: land and sea.
<b>Increasing return costs</b>	Cost-efficiency: reduced number of refusals of entry at the border by notifying travellers in advance of a refusal to pass the border.

The following chapter of the study, “**ETIAS high-level design**”, will explain in greater detail how ETIAS would work. Where deemed relevant, the study will provide a comparison with the three major electronic travel authorisation systems, which will be referred to as the “**benchmark systems**”<sup>14</sup>. Although the intention is not merely to transpose what has been done elsewhere into the EU, a comparative analysis can be an interesting tool to observe which solutions work well and which less so, which elements could inspire ETIAS implementation, and what pitfalls these systems have faced.

---

<sup>14</sup> The Australian eVisitor, the Canadian eTA and the American ESTA.

## 2 ETIAS high-level design

This chapter describes how ETIAS would work and be implemented and operated. More specifically, it looks into the following topics: **design principles; data; business processes; architecture; user interactions; security** and **implementation approach**.

The chapter identifies the preferred design of ETIAS, providing a high-level description of the system and its main components.

### 2.1 Design principles

This section aims at giving an overview of the main topics developed in this “ETIAS high-level design” chapter.

#### 2.1.1 System objectives

ETIAS should be an automated system used to determine the eligibility of visa-exempt third-country nationals to cross the external borders of the Member States and, in particular, whether their presence in the Schengen Area would represent a security threat. The system would aim at gathering information on these travellers prior to the start of their travel, in order to:

- perform a security risk assessment;
- perform a migration risk assessment;
- pre-assess part of the Schengen Borders Code entry conditions, informing the traveller whether he/she would be eligible to travel to the Schengen Area, and reducing the number of refusals at the border, thus creating benefits for both travellers and carriers;
- support border guards in their decision-making; and
- obtain advance information for all border types, as opposed to the current situation where API/PNR cover only air borders.

In addition to the above objectives, which are necessary to meet the system’s purpose, there are other objectives linked to each of the system’s stakeholders:

*Table 2: ETIAS main objectives per stakeholder*

Stakeholders	Current situation	ETIAS objectives
<b>1. Visa-exempt travellers (already visa-exempt)</b>	<ul style="list-style-type: none"> <li>• No previous knowledge of their eligibility to enter the Schengen Area before travelling to the border</li> <li>• Subject to different assessments depending on the MS of first entry</li> </ul>	<ul style="list-style-type: none"> <li>• Know in advance their eligibility to travel to the border</li> <li>• Reduce refusals of entry at the border</li> <li>• Harmonise the risk assessment: all VE-TCNs would go through the same process</li> </ul>
<b>2. Future visa-exempt travellers (currently visa holders)</b>	<ul style="list-style-type: none"> <li>• Currently subject to the visa procedure</li> </ul>	<ul style="list-style-type: none"> <li>• Know in advance their eligibility to travel to the border</li> <li>• Fewer refusals of entry at the border</li> <li>• Harmonised assessment: all VE-TCNs would go through the same process</li> </ul>
<b>3. National authorities (migration, security)</b>	<ul style="list-style-type: none"> <li>• No information collected on VE-TCNs</li> <li>• No risk assessment performed on VE-TCNs (security and migratory risks)</li> </ul>	<ul style="list-style-type: none"> <li>• Use the pre-screenings and the possibility of assessing security and migratory risks prior to arrival at the border</li> <li>• Obtain statistics/generate information on legal migration flows and other items of interest</li> </ul>

Stakeholders	Current situation	ETIAS objectives
<b>4. Law enforcement authorities<sup>15</sup></b>	<ul style="list-style-type: none"> <li>• Movements of VE-TCNs involved in illegal activities cannot be traced for investigations.</li> </ul>	<ul style="list-style-type: none"> <li>• Provide access to VE-TCN application information when duly justified</li> <li>• Enhance internal security</li> </ul>
<b>5. Border guards</b>	<ul style="list-style-type: none"> <li>• No information collected on VE-TCNs prior to their arrival at the border</li> <li>• Increasing traveller flows</li> <li>• Refusals of entry at the border are time-consuming to handle.</li> </ul>	<ul style="list-style-type: none"> <li>• Perform more effective and harmonised border controls</li> <li>• Pre-assess the conditions for entering the Schengen Area, set out in the Schengen Borders Code (Article 6)</li> <li>• Use this pre-assessment of the risks posed by an individual in deciding to allow/refuse entry, and possibly focus time and resources</li> <li>• Decrease the number of refusals of entry at the border and the time to handle them.</li> </ul>
<b>6. EU policy makers</b>	<ul style="list-style-type: none"> <li>• No systematic and comparable information on border management policy results/legal migration.</li> </ul>	<ul style="list-style-type: none"> <li>• Better implement an integrated management of external borders</li> <li>• More effective management of traveller flows</li> <li>• Possibility to obtain statistics/generate information on legal migration flows and other items of interest</li> </ul>
<b>7. EU citizens</b>		<ul style="list-style-type: none"> <li>• Better internal security in the Schengen Area</li> </ul>
<b>8. Carriers</b>	<ul style="list-style-type: none"> <li>• Non-admissible travellers are returned at the carrier's expense.</li> </ul>	<ul style="list-style-type: none"> <li>• Knowledge that the passenger transported has gone through a risk assessment prior to boarding</li> <li>• Fewer refusals of entry and lower associated return costs</li> </ul>

These objectives have shaped the design of ETIAS as described in the following sections.

#### Decision to grant or refuse entry to the Schengen Area

It is important to clarify that ETIAS would not guarantee entry to the Schengen Area: it would only grant authorisations to travel to the border. This new requirement does not change the nature of the border controls performed, and border guards would still have the final say as to whether to allow a VE-TCN to enter the Schengen Area. Having a travel authorisation does not guarantee entry into the Schengen Area; however, not having a travel authorisation would always result in a refusal of entry<sup>16</sup>.

## 2.1.2 System scope

### Geography

The geographical scope of ETIAS is the **Schengen Area**: 22 EU Member States (Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain and Sweden) and four associated countries (Iceland, Liechtenstein, Norway and Switzerland). In addition, four EU Member States do not yet fully implement the Schengen acquis (Bulgaria, Croatia, Cyprus and Romania) but their complete accession is expected in the next few years<sup>17</sup>. Consequently, in this study, the term "Member States" will encompass these 30 Schengen States. ETIAS would apply to **VE-TCNs travelling to any of these countries for a stay of no more than 90 days in any 180-day period**<sup>18</sup>. The **61 countries**

<sup>15</sup> Law enforcement authorities is used in this study to refer to the authorities within Member States in charge of criminal investigations. National authorities is used to refer to the authorities within Member States in charge of assessing the security and migration risks travellers could pose. While the two roles are distinct, they may, in practice and in some Member States, be fulfilled by the same authorities.

<sup>16</sup> "Having a valid travel authorisation" should thus be added to the list of entry conditions in the SBC. See section 3.1 "Legal".

<sup>17</sup> See: [http://ec.europa.eu/dqs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index\\_en.htm](http://ec.europa.eu/dqs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm) (accessed 08/2016).

<sup>18</sup> Regulation No 810/2009:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0810&from=EN> (accessed 07/2016).

(approximately 1.2 billion people) on the list drawn up by Regulation (EC) No 539/2001<sup>19</sup> would be subject to the travel-authorisation requirement.

### Size

The following figure gives an estimation of the proportion of visa-exempt travellers expected to cross Schengen borders in the next ten years.

Table 3: Number of VE-TCNs expected to cross the Schengen borders by 2025<sup>20</sup>

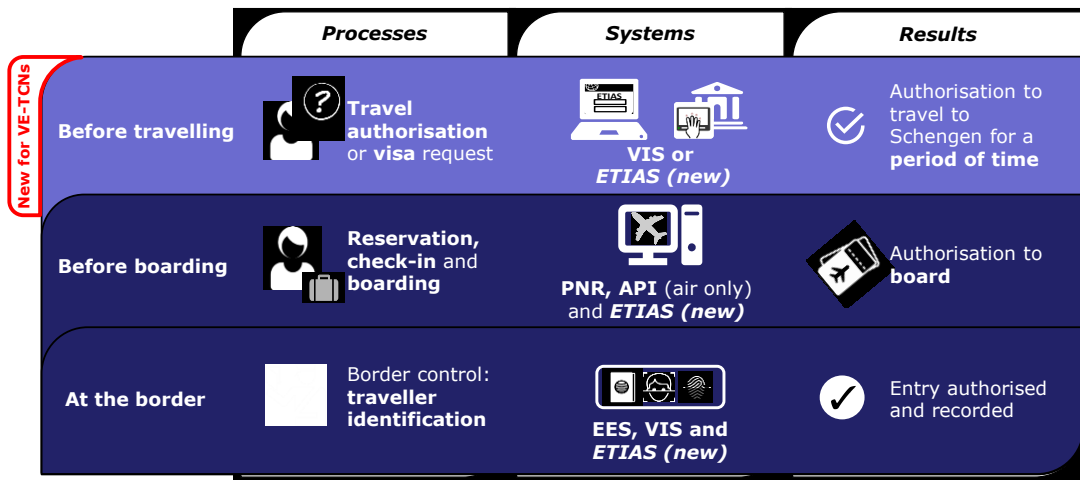
	2014	2020	2025
<b>Border crossings (entry + exit in millions)</b>	81	104	127
<b>Number of travellers (in millions)</b>	<b>30</b>	39	47

It can be estimated that if ETIAS were available today, it would process approximately **30 million applications** per year (depending on the length of the authorisation granted).

### Border type

ETIAS would apply to all border types: air, sea and land. It would complement and strengthen the current border management’s IT landscape in the Migration and Home Affairs area by adding a **new, pre-travel layer for VE-TCNs** to the overall border-management process. Similar set-ups are already in use in Australia, Canada and the US, where travellers’ data is checked and processed at several steps along the journey – before and during travel as well as at the border – in order to facilitate the travel experience on the one hand and ensure a high level of security on the other. The step-up of this **layered approach to border management** is illustrated in the figure below.

Figure 4: Layered approach to border management<sup>21</sup>



<sup>19</sup> Opcit.

<sup>20</sup> Technical Study on Smart Borders (2014), p. 21.

<sup>21</sup> The layer “during travel” does not apply to land and sea travel, as API and PNR data are collected only from air carriers.

### 2.1.3 Authorisation model

The choice of authorisation model (length of the validity of a granted travel authorisation) is of particular importance, as the entire design of ETIAS rests on this choice. Three authorisation models have been considered in the course of the analysis:

- 1) A travel authorisation valid for a **period of time**;
- 2) A travel authorisation valid for a **single trip**;
- 3) A **combination of 1 and 2**: a travel authorisation valid for a period of time with an obligation for the traveller to notify the authorities before each new trip. This would be a simple/"light" notification, as most of the data would have already been provided when requesting the authorisation for a period of time.

It is important to note here that as ETIAS is a "person- and document-centric system", a new travel authorisation would have to be requested when the travel-document information changes (for instance, when a new passport is issued).

The following table summarises the assessment of each authorisation model according to three main criteria:

1. **convenience** for travellers;
2. **workload** for the national authorities processing incoming applications; and
3. The relevance of the **data collected** to the risk assessment.

A full explanation of the advantages and disadvantages of these models and of the criteria is available in Annex 3 – "Design principles".

*Table 4: Comparative table of authorisation models*

Model	Convenience for travellers	Workload for national authorities	Relevance of the data for risk assessment	Consistency with the benchmark systems	
1. Travel authorisation valid for a period of time	++	++	+	✓	Preferred option
2. Travel authorisation valid for a single trip	--	--	++	×	
3. A combination of 1 and 2	--	--	++	×	

The countries using the benchmark systems (the US, Canada and Australia) have chosen to implement systems delivering travel authorisations valid for a period of time (option 1)<sup>22</sup>. However, unlike ETIAS, none of these systems is used at land borders, where no API or PNR (at air) or passenger manifestos (at sea) are available prior to traveller arrival. In light of its distinct advantages and of the existing practices in other countries, an authorisation valid for a period of time is preferred for ETIAS and will serve as an assumption throughout the study. Consultations with Member States' experts have also supported this choice as being the most feasible.

### 2.1.4 Validity period

Convenience for travellers advocates for the longest period possible: frequent travellers in particular would not have to submit a new application for each new trip. Costs and workload related to application management would also benefit from the longest period possible. However, these advantages are counterbalanced by the added value in terms of risk assessment: with time, the risk assessment

<sup>22</sup> The Australian eVisitor is valid for up to one year (<http://www.visabureau.com/australia/evisitor-visa.aspx>), the Canadian eTA is valid for five years (<http://www.cic.gc.ca/english/resources/tools/temp/eta/>) and the US ESTA is valid for two years ([https://help.cbp.gov/app/answers/detail/a\\_id/1126/~/esta---length-of-approval](https://help.cbp.gov/app/answers/detail/a_id/1126/~/esta---length-of-approval)). All three are valid for a defined period of time, or until the traveller's passport expires.

performed after the application is submitted loses relevance as the person’s situation may change<sup>23</sup> (a five-year validity period, for instance, would become the longest acceptable from this point of view). In light of these elements, **an authorisation valid for two to five years** (or up to the expiry date of the passport, whichever comes first) **seems to be the most appropriate solution**, in line with existing best practices in the benchmark systems.

A short (e.g. two years) validity period offers the closest alternative to an authorisation per trip. However, the longer the validity period, the more it will limit the cost, workload and administrative burden on the authorities involved in risk assessment as well as increase convenience for travellers, especially frequent travellers. The preferred validity period can be reviewed a few years after the system goes live, in order to re-assess whether the option meets the purpose and objectives of ETIAS. Finally the automatic re-assessment of the risk for existing travel authorisations also reduces the relevance of the discussion on the duration of the validity period: whether valid for two or five years, the travel authorisations are re-assessed once the system is notified of any relevant change.

### 2.1.5 Application fee

**The collection of a fee is envisaged** in order to finalise the travel-authorisation application process. Although the Australian system is free of charge for EU citizens, the Canadian and American systems collect a fee from the applicant at the end of the process (seven Canadian dollars for the Canadian system and 14 US dollars for the American one). From the perspective of a European system, the main benefit of a fee is to deter the submission of fake applications. However, the amount should not be too high, so as not to deter tourism, and certainly should not be set for the purpose of generating a profit; rather, the fee would cover ETIAS’s running costs only. The fee could be collected for each application lodged as the final step of the travel-authorisation form. It would be managed by an EU institution, which would also be in charge of its allocation. A third-party could collect the chosen amount. Specific questions on how much the fee should be and how it should be used are further detailed in the cost-benefit analysis.

*Table 5: Advantages and disadvantages of having a fee*

<b>Benefits of having a fee</b>	<ul style="list-style-type: none"> <li>• <b>Filter</b> Could act as a filter, as it would deter the submission of a very high number of applications (e.g. for the purpose of bypassing or crashing the system) and fake applications. Serve as a “proof of intent” to travel</li> <li>• <b>Contribution to the system</b> Makes a substantial contribution to ETIAS’s running costs</li> <li>• <b>Means of subsistence</b> Offers some indication that the traveller possesses means of subsistence</li> </ul>
<b>Possible pitfalls</b>	<ul style="list-style-type: none"> <li>• <b>Burden</b> Could be seen as an additional burden and inconvenience for travellers</li> <li>• <b>Diplomatic tension</b> Could create issues concerning visa reciprocity with countries that do not ask for a fee for obtaining a travel authorisation (the Australian eVisitor, designed especially for EU citizens, is free of charge)</li> <li>• <b>Deterrence of travel</b> Depending on the amount chosen, it could deter bona-fide travellers with limited means to travel to the Schengen Area. It could then be seen as discriminatory.</li> </ul>

In order to address the above-mentioned disadvantages, some mitigation measures could be anticipated. Most notably, the fee should be set at a reasonable price (the average fee of the benchmark systems is

<sup>23</sup> To counter this issue, granted authorisations could be reviewed periodically in light of the new information entered in EU and international databases. For more information, see section 2.3.6 “Support processes”.



around ten dollars<sup>24</sup>). More details about the proposed fee can be found in Chapter "4 Cost-benefit analysis (CBA)" and its accompanying annexes.

### 2.1.6 User perspective

To limit the burden that the ETIAS application could represent, the objective is set from the outset that the form should take **no more than ten minutes to fill in**. Indeed, the information requested should be well known to the applicants and they should **not need more than their passport, a credit card and a valid email address** (in line with the validity period of the authorisation) when applying for a travel authorisation. ETIAS would process the majority of applications **automatically**, carrying out an automatic risk assessment and delivering the granted authorisation **within minutes**. If the outcome of the automatic risk assessment is not positive (i.e. the applicant appears to pose a risk) and the application needs to be escalated for an additional manual risk assessment, **feedback should be provided to the applicant within 72 hours**<sup>25</sup>. A full explanation of the decision-making process, including automatic and manual risk assessments, is available in section 2.3 "Business processes". Finally, the system should ensure to the highest possible extent that travellers' privacy is respected.

---

<sup>24</sup> Free of charge for the Australian eVisitor, 14 dollars for the US ESTA and 7 dollars for the Canadian eTA.

<sup>25</sup> For a justification of this processing time, see Annex 5. – "Business processes".

## 2.2 Data

This section of the study presents an **overview of the data to be collected** by ETIAS. The section further assesses **data-retention, access-management and data-ownership** issues. It also includes the **data model** for ETIAS.

### 2.2.1 Context

Currently, any risk that a visa-exempt traveller may pose as regards the entry conditions set out in the **Schengen Borders Code** is assessed by border guards at border-crossing points<sup>26</sup>. The assessment carried out is constrained by time, the increasing number of travellers to be handled at the busy border-crossing points and the fact that the Member State of entry decides alone on authorising entry to the Schengen Area (as a comparison, before granting a visa, a consultation mechanism with other Member States exists in some cases). These three constraints limit the information and the depth of the first-line risk assessment. They constitute the "information gap" on VE-TCNs referred to in this study.

The future **Entry/Exit System** (EES) proposal has been drafted partly to remedy two of the above-mentioned issues: limited time and increasing traveller flows<sup>27</sup>. However, travellers' data collected through EES would only be available *after* the person has entered the Schengen Area (as suggested by its name, the system only collects data on, and at the time of, a traveller's entry and exit).

**Advance Passenger Information** (API) and subsequently **Passenger Name Record Directives** (PNR) have been designed to remedy, to some extent, the lack of what is referred to as "advance information" – traveller information that could be used before the person presents himself/herself at the Schengen border. However, the data collected as part of the API and PNR framework can only be collected for travellers coming to the Schengen Area by air. Information is still lacking regarding visa-exempt travellers coming through land and sea borders (see section "2.3 Business processes).

It is into this context that ETIAS would have to fit. To ensure that the new system **complement** and is **consistent** with the existing EU IT landscape<sup>28</sup>, it is particularly important to define with precision:

- which **purpose** ETIAS would fulfil;
- which **risks it** could better assess and mitigate;
- which database **checks** would need to be conducted to mitigate these risks and achieve the purpose(s); and, finally,
- which **data** should be collected for the check to be carried out, the risk to be mitigated and the purpose to be achieved?

### 2.2.2 Approach

A four-step approach is followed to define the ETIAS data set.

- Firstly, the **purpose** of the system is outlined;
- Secondly, the **risks** related to the purpose are identified<sup>29</sup>;

---

<sup>26</sup> For visa holders, these risks are also assessed through the visa application.

<sup>27</sup> See Article 5 of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation\\_proposal\\_entryexit\\_system\\_borders\\_package\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation_proposal_entryexit_system_borders_package_en.pdf) (accessed 09/2016).

<sup>28</sup> As highlighted by the communication from the Commission, the "fragmented architecture of data management" and the complexity of the landscape of systems governed differently are repeatedly identified as main shortcomings of information systems at EU level for border control and security. It is thus of particular importance to ensure, as much as possible, coherence and complementarity of ETIAS with other - existing and upcoming - systems. See "Stronger and Smarter Information Systems for Borders and Security", COM (2016) 205 final, European Commission, 06 April 2016: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication\\_on\\_stronger\\_and\\_smarter\\_borders\\_20160406\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication_on_stronger_and_smarter_borders_20160406_en.pdf) (accessed 09/2016).

<sup>29</sup> In line with current EU law, information should be processed only on the basis of concrete security needs - see Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit

- In the third step, a **risk assessment** approach is defined, including which **databases** would be queried;
- As a final, fourth step, **data to be collected** from the traveller is identified, allowing necessary database queries to take place.

This approach is illustrated below.



Figure 5: Approach to ETIAS data set identification

The approach allows to obtain the ETIAS data set for risk-assessment purposes. In addition to this data set, a number of data items would need to be collected for application-management and disambiguation purposes (defined below in section 2.2.6 “Data to be collected”).

### 2.2.3 Purpose

In light of the information gap concerning VE-TCN travellers as described earlier in the Introduction chapter, the purpose of ETIAS could be summarised as:

- a) **security risk assessment;**
- b) **migration risk assessment;**<sup>30</sup>
- c) pre-assessment of visa-exempt travellers with regards to at least part of the **entry conditions set out in the SBC.**

The system should aim to contribute to both internal security and the efficient management of migration flows.

### 2.2.4 Risks

The following criteria were applied in order to arrive at a shortlist of risks that ETIAS should assess and help to address:

- 1. Significance:** the risks identified would need to be prioritised at operational level (validated through consultations with Member States’ experts and EU agencies) and be prominent amongst the ETIAS target group (visa-exempt travellers) to justify the use of ETIAS to mitigate them. In addition, the use of ETIAS would only be justifiable for risks/threats that require a coordinated response at EU level and thus satisfy the principle of subsidiarity.
- 2. Compliance with the entry conditions set out in the SBC:** this criterion indicates whether the risk assessed is linked to the entry conditions set in the SBC.

The following table illustrates the risks ETIAS should assess and mitigate. A detailed analysis is contained in Annex 4. – “Data”.

---

System (EES) and a Regulation establishing a Registered Traveller Programme (RTP): [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18\\_Smart\\_borders\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf) (accessed 07/2016). In the case of ETIAS, concrete security - and, to a smaller extent, migration - needs were mapped in the study in the form of security and migration risks.

<sup>30</sup> Other, ancillary, purposes of the system, such as convenience for travellers and carriers, and border control facilitation are further discussed in Annex 4. – “Data”.

Table 6: Risks that ETIAS should assess and mitigate

Risk category	Risk	Significance	Compliance with SBC entry conditions
<b>Security</b>	<i>Terrorism</i>	+	++
	<i>Serious and cross-border organised crime</i>	++	++
	➤ <i>Document and identity fraud</i>	++	++
	➤ <i>Trafficking in human being</i>	++	++
	➤ <i>Drug trafficking</i>	++	++
	➤ <i>Illicit firearms trafficking</i>	++	++
<b>Migration</b>	<i>Irregular stay (overstay)</i>	++	+
<b>Public health</b>	<i>Threat to public health</i>	+	++

### 2.2.5 Risk assessment

The risks listed above can be evaluated via ETIAS using three methods:

- 1. Direct hit:** looking for known entities based on information (specific values) available in databases;
- 2. Network analysis:** looking for unknown entities in connection with a known entity based on information/specific values available in databases (whether the person has a connection with a known person of interest – e.g. through a phone number, email address, etc.);
- 3. Data analytics:** setting risk-assessment rules and identifying patterns on the basis of risk indicators/risk profiles, looking for aggregations of stand-alone risk indicators or matches against risk profiles. This also includes outlier discovery: looking for suspicious anomalies or deviations<sup>31</sup>.

Two first two tools rely on access to databases. This section will identify the necessary databases to be checked/queried by ETIAS for the purpose of assessing the risks previously identified and taking into account the following criteria:

- 1. Relevance:** how relevant is the data stored in this database for adequately assessing the identified risks?
- 2. Privacy and data protection:** how much data is accessed and is it sensitive data?
- 3. Implementation complexity:** is the necessary secure interface to the database easy to set up? Can the database cope with a large volume of queries?

All databases that receive a combined score greater than 0 sufficiently meet the criteria to be suggested for interfacing with ETIAS. The following table summarises the results of the assessment. More detailed explanation and justification is available in Annex 4. – “Data”.

<sup>31</sup> Applying the data analytics method would never result in the denial of a travel authorisation even if it obtains a high risk score or does not follow “normal”/“standard” patterns; rather, the case would be escalated for manual processing and likely involve obtaining additional information before a decision is taken.

Table 7: Databases to be checked for the purpose of ETIAS risk assessment

	Risk assessment						Selection criteria		
	Security		Migration			Public health			
	Terrorism	Serious and cross-border crime	Irregular stay (overstay)	Entry bans/return decisions	Refusal of entry	Threat to public health	Relevance	Privacy and data protection	Implementation complexity
<b>Databases</b>									
SIS	✓	✓		✓ <sup>32</sup>			++	+	+
VIS			✓				++	+	+
SLTD	✓	✓					++	++	++
TDAWN <sup>33</sup>	✓	✓					+	+	++
EES			✓		✓		++	+	++
<b>ETIAS components</b>									
ETIAS IT application	✓	✓					++	-	++
Screening rules	✓	✓					++	-	++
<b>Candidate databases for future integration</b>									
ECRIS	✓	✓					_ <sup>34</sup>	--	--
EIS <sup>35</sup>	✓	✓					++	-	--
EURODAC			✓				-- <sup>36</sup>	--	--

Three **candidate databases** are mentioned above as their integration with ETIAS could be reassessed at a later stage.

- **ECRIS** currently only contains convictions of EU citizens and therefore is not relevant for ETIAS. However, in future ECRIS could also contain convictions (in the EU Member States) of third-country nationals, thus becoming a source of valuable information for ETIAS.
- **Europol data:** while access to Europol data as a source of information on "persons of interest" would be worthwhile, EIS would need to be considerably upgraded in light of the existing limitations of its capacity and processing.
- As for EURODAC, both practical and privacy aspects suggest that using the database would not be feasible for now and would bring only limited added value. Its upcoming recast could cause this fingerprint database to evolve into a case-management system, also containing additional information. In this case, it would be interesting to reassess its added value.

At the same time, **Interpol databases** demonstrate added value and offer ease of technical implementation for connecting. TDAWN for instance contains a large volume of data, including a considerable amount on third-country nationals, while being easy to connect to and offering flexibility to the authority that gets a match in the system to act or not on the notice in question. A more detailed assessment can be found in Annex 4. – "Data".

<sup>32</sup> According to ongoing discussions, return decisions could be stored in the SIS in the future.

<sup>33</sup> Travel Documents Associated with Notices. For a description of the database, see Annex 4. – "Data".

<sup>34</sup> The assessment of ECRIS is based on the current situation. It should be revised should the system evolve and contain convictions of third-country nationals.

<sup>35</sup> Europol Information System. For a description of the database, see Annex 4. – "Data".

<sup>36</sup> The assessment of EURODAC is based on the current situation. It should be revised should the system evolve into a case-management system.

Among the databases, of particular importance are the ones potentially **contained in ETIAS itself**: the database of travel-authorisation applications (ETIAS IT application) and screening rules. These new databases are proposed/considered in order to enhance ETIAS's overall risk-assessment capability and in particular to allow for the data-analytics method to be applied. Moreover, they would fill an information gap regarding a complete pool of persons of interest from all Member States and would better inform migration risk assessments, which have fewer candidate databases to draw from for automatic risk assessment. Indeed, in the absence of a central migration database at EU level, ETIAS requires additional checks against Member States' information (available via the ETIAS screening rules) and against its own database of travel-authorisation applications in order to better fulfil its migration risk-assessment purpose.

### Screening rules

Although checking national databases may not be feasible, these systems could still bring significant added value to the ETIAS risk assessment, in particular since they contain information that cannot be entered into SIS (e.g. phone numbers or email addresses known to law enforcement). To increase the ETIAS risk assessment's added value and efficiently counter security risks, it is necessary to perform additional security checks and analysis by pooling all the available sources and data to transform data into useful information. This can be performed by implementing "screening rules" as part of ETIAS. The screening rules would be populated by Member States and would include:

- "investigation triggers", i.e. specific values (e.g. phone numbers, email addresses, etc.) that would automatically trigger manual processing if these values are entered into a newly submitted application; and
- data analytics rules, i.e. common risk indicators and patterns.

Member States and other stakeholders involved in the risk assessment would be able to propose changes to the data-analytics rules or to add specific investigation triggers, so as to ensure that the rules applied can be adapted and that they are always relevant and up to date. As threats evolve, the risk assessment will follow.

The screening rules would:

- use valuable information for the risk assessment by applying screening rules to incoming applications;
- harmonise this risk assessment. During current border controls different databases are consulted and each Member State consults its own national databases with limited possibilities to exploit information from other Member States;
- provide the possibility to add/modify or delete screening rules to adapt to the latest threats (a specific governance and review process would apply); and
- ensure that the investigation triggers inserted by each Member State stay confidential – the values would be encrypted and visible only to the Member State that creates them (if the Member State so wishes) (see section 2.6 "System security" for more information regarding encryption and other ETIAS security safeguards).

Although the repository of screening rules would be a new system in the EU, a similar set-up has been put in place in the US, where all relevant agencies (law enforcement, migration, border-management, intelligence) input data into a central system used in the ESTA automatic risk assessment. If there is a match, an officer forwards the case to the national authority that entered the investigation trigger into the system.

### Disambiguation

Disambiguation is the action of differentiating between two or several similar data for the purpose of identification. Disambiguation in the context of an electronic travel-authorisation system implies two types of actions:

- a) Differentiating between two or more applicants/applications with very similar data:
  - Two applications with very similar data (same name, surname, place of birth, etc.);
  - A child who is registered on the parents' passport;

- Change of surname (and first name in some cases) or other biographical data;
- Every time a passport expires (new passport number and issuing country):
- Positive match with any of the ETIAS components.

**b)** In the event of a positive match in any other database (e.g. the data appears in an alert or an investigation trigger). The first step for the Central Manual Processing Entity (CMPE) is to verify the applicant’s identity. This case has no impact on the data to collect, as these situations would always be managed manually (a positive match in a database or against ETIAS screening rules always requires manual processing, see section 2.3 “Business processes”).

For the purpose of efficiency, automation and workload for the CMPE, the study has identified the following two principles that should drive disambiguation:

- cases of disambiguation would have to be solved **centrally** and/or
- **automatically**, as far as possible.

Therefore, for disambiguation action (a), it is preferred to perform a large part of these tasks automatically at central level, which justifies the collection of additional data (as illustrated in the table below).

*Table 8: Impact of disambiguation*

	<b>Data</b>	<b>Applicant</b>	<b>CMPE</b>	<b>Automation</b>
<b>Action a)</b>	Collection of additional data	Collection of additional data. Low impact: - the data is well known by the applicant; - no data protection issue	Less workload	More automation
<b>Action b)</b>	No impact	No impact	Manual processing	Manual processing

## 2.2.6 Data to be collected

The approach used to define the data to be collected to perform the risk assessment is the following:

- 1) Listing the data collected by the comparable systems<sup>37</sup>** (ESTA, eTA, eVisitor) and by other European databases (i.e. VIS, EES and SIS). A detailed comparison is available in Annex 4. – “Data”.
- 2) Scoring each possible data**, against the following four criteria<sup>38</sup>:
  - 1. Ease of collection and automation:** is this data easy to provide, remember, write down? Can it be used for automated checks? Requesting long explanations or a piece of information that the person would have to look for in a document other than the passport or a credit card should be avoided – see section 2.5 “User interactions”. Similarly, there should be a limited amount of data collected that cannot be used for checks in other databases;
  - 2. Relevance:** how relevant is this data for achieving the purpose(s), assessing and mitigating the identified risks?
  - 3. Reliability:** to what extent can the data be trusted? Although the data collected is only declarative (the documents’ authenticity is not verified), some elements can be more or less trustworthy. The background questions, for instance, tend to have a low level of

<sup>37</sup> EIS is presented despite being currently not technically feasible, in light of possible future connections. On the other hand, EUODAC and ECRIS are not considered as at the time of writing of this report, they do not contain yet data relevant for ETIAS (see Annex 4. – “Data” for further details).

<sup>38</sup> The metrics used for the criteria are explained in Annex 4. – “Data”.

reliability. However, it has been noted in the benchmark systems, that travellers tend to answer more truthfully and provide more than is asked;

**4. Privacy:** how intrusive is it for a person's privacy to request and store this data?

**3) Removing and disregarding data elements that scored poorly** (i.e. the sum of the criteria was  $<$  or  $= 0$ ). Moreover, data elements for which proportionality and necessity were clearly insufficient have also been disregarded (independently from the scoring).

The table below presents the outcome of the selection and includes data required for risk assessment (based on the considerations above), as well as data required for application management and disambiguation purposes. The full assessment is available in Annex 4. – "Data". A "\*" beneath the data element means that the information is available in the passport.



Table 9: List of the data collected from the applicant through the online ETIAS form

Traveller data to be collected	Purpose					Data availability							Selection criteria				Benchmark			Data contained in the passport
	Security	Migration	Public health	Application management	Disambiguation	SIS	EES	EIS	VIS	SLTD	TDAWN	ETIAS (screening rules)	Ease of collection/ automation	Relevance	Reliability	Privacy	eVisitor	eTA	ESTA	
<b>Biographical data</b>																				
First name	√	√		√	√	√	√	√	√		√	√	++	++	+	++	√	√	√	√
Surname	√	√		√	√	√	√	√	√		√	√	++	++	+	++	√	√	√	√
Name at birth	√	√			√	√	√	√				√	++	++	+	++	√		√	√
Other name	√	√			√	√		√				√	+	++	+	++	√		√	
Parents' first names					√			√					+	+	<b>0</b> <sup>39</sup>	+			√	
Date of birth	√	√			√	√	√	√	√				++	++	+	++	√	√	√	√
Place of birth					√	√		√	√				++	++	+	++		√	√	√
Nationality	√	√		√	√	√	√	√	√				++	++	+	++	√	√	√	√
Additional nationalities	√	√		√	√			√					+	++	+	++	√	√	√	
Gender	√	√			√	√	√	√	√				++	++	+	++	√	√	√	√
<b>Passport data</b>																				
Passport number	√	√		√	√	√	√		√	√	√	√	++	++	+	++	√	√	√	√
Country of issuance	√	√		√		√	√	√	√	√	√		++	++	+	++	√	√	√	√
Passport expiry date	√	√		√			√		√				++	++	+	++	√	√	√	√

<sup>39</sup> Cannot be checked against any other source/database.

Traveller data to be collected	Purpose					Data availability							Selection criteria				Benchmark			Data contained in the passport
	Security	Migration	Public health	Application management	Disambiguation	SIS	EES	EIS	VIS	SLTD	TDawn	ETIAS (screening rules)	Ease of collection/ automation	Relevance	Reliability	Privacy and data protection	eVisitor	eTA	ESTA	
<b>Contact details</b>																				
Email address	✓			✓				✓				✓	++	++	+	+	✓	✓	✓	
Address (residence)	✓	✓			✓			✓					+	+	0	- <sup>40</sup>	✓	✓	✓	
Phone number	✓			✓				✓				✓	++	++	+	+	✓		✓	
<b>Intended travel</b>																				
MS of intended first entry				✓									++	-	+	+				
<b>Background questions</b>																				
Education and occupation		✓											+	++	-	-		✓	✓	
Convicted of a serious crime	✓							✓					+	++	-	-		✓	✓	
Previously been refused entry/visa, ordered to leave		✓				✓	✓		✓				+	++	+ <sup>41</sup>	-		✓		
Been recently present in a war zone	✓												+	++	-	-			✓	
Threat to public health: infectious disease <sup>42</sup> (e.g. tuberculosis)			✓										+	++	-	-		✓	✓	

<sup>40</sup> The address of residence of a person could indirectly reveal a lot of additional information on a person and his/her private life.

<sup>41</sup> It is currently under discussion whether return decisions will be stored in the SIS. Should it be the case, this could allow the verification of this information.

<sup>42</sup> According to Article 2(19) of the SBC, a "threat to public health" means "any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States."

Additional explanations and justifications for certain data fields are provided below:

- *Name at birth*: this data is collected for disambiguation purposes.
- *Other name*: this non-mandatory field aims at collecting any other name by which the person is known, be it an alias, an artistic name or a preferred name.
- *Parents' first names*: this data is collected for disambiguation purposes, and only the first name of both parents would be needed to fulfil this aim. Collecting both the parents' names and surnames would not be justified from a data-protection point of view. Indeed, this would entitle collecting data from subjects who are neither involved in nor aware of the procedure. In addition, collecting only the first names also offers more added value than the last names, as both parents and children often share the same family name.
- *Education and occupation information* could support a pre-assessment of the traveller's means of subsistence and inform a migration risk assessment (likelihood of overstay). It could also be used to check the ties with the country of origin, useful when assessing the migration risk.
- *Convicted of a serious crime*: this data could support a pre-assessment of the threat level that the traveller represents. Additional information would be required if the applicant declares having committed a serious offence<sup>43</sup>.
- *Recently been in a war zone*: this data could also support the threat level/security risk assessment and could assist in identifying potential foreign fighters. Additional information (where, why, supporting documents) would be required if the applicant declares having recently been in a war zone.
- *Threat to public health*: this question would only focus on the main communicable diseases with epidemic potential as defined by the World Health Organisation<sup>44</sup>. The European Centre for Disease Prevention and Control also lists the priority risks<sup>45</sup>. From these two sources, the following diseases have been considered a top priority: plague, tuberculosis, Nipah, Zika virus, coronaviruses, filovirus and dengue, Lassa and other haemorrhagic fevers.

The wording of the background questions should be as non-intrusive as possible. Supporting documents and additional explanations in writing would only be required for applicants answering "yes" to any of the background questions triggering manual follow-up to the application. Examples of possible wording and data-field formats can be found in Annex 7. – "User interactions".

### **Other types of data considered**

- **Payment information** could be useful from a security point of view. However, collecting the payment information of all visa-exempt travellers in a central EU database may not be considered proportionate for the purpose of a security risk assessment.

Therefore, ETIAS would follow the example of the benchmark countries: payment information would not be collected through the travel authorisation system nor stored in any database, but would be collected and stored by the bank contracted for this aim. In case of need, payment information can be traced and retrieved following strict, pre-defined conditions.

- **Meta-data** could be used to cross-check information. For ETIAS, relevant meta-data could be the IP addresses, the way a date is represented, the length of a field, etc.

In particular, the IP address could be used for:

- Determining the geographical location at the time of application;
- Confront it against lists of IP addresses known to be involved in malicious activity;
- Identify third-parties submitting application on behalf of travellers.

---

<sup>43</sup> The data field would either contain a list of offence (yes/no) or tick boxes. Whichever data collection method chosen, the field would be fully automated and no write-in field would be foreseen. The list of offences would derive from either the ones contained in Europol's mandate, which are aligned with the criminal acts that would enable a European Arrest Warrant, or the ones listed in Annex II of the PNR Directive. The full list of crimes is available in Annex 4. – "Data". See: <https://www.europol.europa.eu/content/page/mandate-119> (Article 4 and relevant annex) and [http://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC\\_1&format=PDF](http://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF) (Article 2) (accessed 09/2016).

<sup>44</sup> See: <http://www.who.int/csr/research-and-development/workstream1-prioritize-pathogens/en/> and <http://www.who.int/medicines/ebola-treatment/WHO-list-of-top-emerging-diseases/en/> (accessed 09/2016).

<sup>45</sup> See: [http://ecdc.europa.eu/en/publications/all\\_publications/Pages/index.aspx](http://ecdc.europa.eu/en/publications/all_publications/Pages/index.aspx) (accessed 09/2016).

However, IP addresses can change over time and be easily masked by using a proxy or VPN (although many of these services can also be detected). Moreover, people can apply while being connected to public hotspots, while travelling, while being abroad, further diminishing the usefulness of collecting them in a systematic manner.

The relevance and added value of other meta-data in the context of ETIAS should be further assessed before deciding in favour of collecting and processing it.

- **Social media** could be used in different ways:
  1. To cross-check data entered by the applicant (e.g. to check whether the year of birth entered in the ETIAS form corresponds to the year of birth declared by the applicant on Facebook) – however, information entered on social media is unreliable;
  2. To ensure that the person's social media identifiers (e.g. username on Facebook) are not included in a watchlist (this can also be done with phone numbers and email addresses);
  3. For conducting a manual, in-depth assessment of the person based on his/her online profiles;
  4. For conducting an automated check using software to detect keywords or images from the applicant's profile and to perform a network analysis;
  5. Social-media information could also be used to contact travellers.

If this idea is retained, social-media identifiers would be mandatory *to declare*, i.e. mandatory to fill-in if the traveller has an online presence; the field could be left blank if the person has no online presence. However, collecting and processing social-media information of applicants would be a significant intrusion in their private life. People recurrently publish personal information on social media, including political ideas, their religion or ideals. The request or the notion that social media would be checked within the assessment for a travel authorisation would likely be met with the opposition of many.

Overall the collection of social media identifiers, given its limited use, limited automation and strong privacy concerns, is assessed as not proportionate and therefore ETIAS should not collect them. This assessment could be revised once investigation techniques using social-media analysis are more mature, thus increasing the potential value for achieving ETIAS's objectives.

## 2.2.7 Data set

ETIAS's complete data set would comprise the data collected from the traveller with the addition of application specific data elements. These additional data elements would not be collected from external sources, but rather would result from the functioning of the system and of the ETIAS decision-making process.

The system would maintain an audit trail, recording the following elements:

- Application reference number;
- Date and time of the application;
- Date and time of the decision (authorisation granted or denied);
- Justification of the decision including the:
  - Log of the result of the automated screening (e.g. the risk score and whether any screening rules were logged);
  - If manual processing occurred, a short explanation/report would be filled in by the officer in charge of assessing the application.
- Date of the last re-check;
- Authority that took the decision (automatically granted, CMPE, Member State).

The figure below summarises the overall data set for ETIAS:

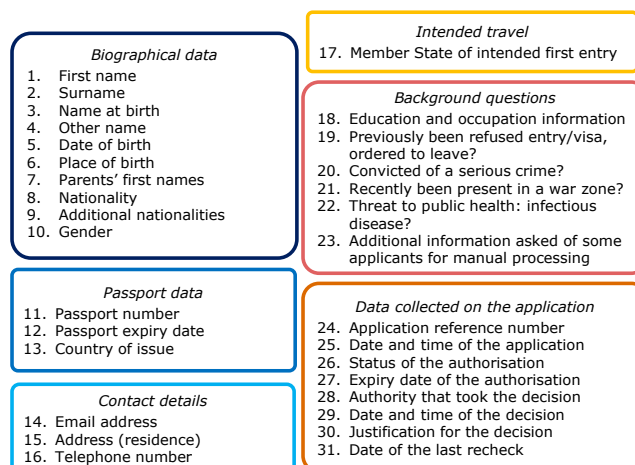


Figure 6: ETIAS data set

## 2.2.8 Data retention

The data retention period sets the amount of time for which information should be **retained in a database to fulfil a specified purpose**<sup>46</sup>.

The following table presents the retention periods for PNR, API and three relevant large-scale EU IT systems:

Table 10: Retention periods for EES, VIS, SIS, PNR and API

System	Data Retention
<b>EES proposal</b>	<ul style="list-style-type: none"> <li>• 5 years after the exit (or the refusal of entry) of the person</li> </ul>
<b>VIS</b>	<ul style="list-style-type: none"> <li>• 5 years from the expiry date of the visa,               <ul style="list-style-type: none"> <li>– or from the date on which the file was created in the VIS (application withdrawn, closed or discontinued),</li> <li>– or from the date of the visa authority's decision (visa refused, annulled, shortened or revoked)</li> </ul> </li> </ul>
<b>SIS</b>	<ul style="list-style-type: none"> <li>• 3 years<sup>47</sup> if not extended (review by Member State of the relevance of retaining the alert every 3 years)</li> </ul>
<b>PNR</b>	<ul style="list-style-type: none"> <li>• 5 years after transmission (depersonalised after 6 months)</li> </ul>
<b>API</b>	<ul style="list-style-type: none"> <li>• Deletion by carriers: 24 hours after arrival</li> <li>• By national authorities: 24 hours after transmission (unless the data is further necessary for the border guards' mandate).</li> </ul>

The preferred data retention period for ETIAS would be 5 years. This period is not only coherent with the retention period adopted for comparable systems (i.e. VIS), but would allow to maintain the link between the entry/exit records stored in EES and the travel authorisation associated with the travel document used. A shorter data retention could break this link before an entry/exit record is deleted (after 5 years).

<sup>46</sup> No information is publicly available regarding the retention of the eVisitor data in Australia or the Canadian eTA data. ESTA data is retained for three years in an active database (the two years validity of the travel authorisation and an additional one year after it expires). After that period, it is placed in a dormant database for 12 years, where inactive account information are unavailable for online access.

See: <https://www.cbp.gov/travel/international-visitors/frequently-asked-questions-about-visa-waiver-program-vwp-and-electronic-system-travel> (accessed 06/2016).

Additionally: "data linked at any time during the 15-year retention period (3 years active, 12 years archived), to active law enforcement lookout records, will be matched by DHS/CBP to enforcement activities, and/or investigations or cases, including ESTA applications that are denied authorisation to travel, will remain accessible for the life of the law enforcement activities to which they may become related". See ESTA Notice of Privacy 2016, p. 23-24.

<sup>47</sup> An extension to 5 years is being considered.

The retention period should start from the **end of the validity period** (either because of the elapse of time or because of a revocation). For denied travel authorisations, it would be five years from the moment of the decision.

At the end of the retention period, the data would be deleted automatically, as is currently the case for SIS alerts and VIS applications.

This approach could be strengthened by putting in place additional measures, such as placing certain data into a **dormant database** or **anonymising it**, taking into consideration that not all types of data are actively used over time. A detailed analysis of each of these options is available in section 3.2 "Data protection".

## 2.2.9 Access management and data ownership

Data retained in ETIAS would serve the following **main purposes**:

1. **Checking status**: including checks by carriers, border guards and travellers;
2. **Application processing**: including disambiguation, ongoing decision-making and risk assessment;
3. **Retrieval for law-enforcement purposes**: more specifically intelligence in the context of an investigation<sup>48</sup> (see next sub-section on access management);
4. **Reporting**: statistics, e.g. on VE-TCN traveller flows.

### Access management

Access to ETIAS data would be necessary for different stakeholders. Depending on their needs and tasks, and in line with privacy by design<sup>49</sup> principles, they would access some or all of the data for one of several explicit purposes, as summarised in the following table:

*Table 11: ETIAS data access by stakeholder*

Stakeholder <sup>50</sup>	Purpose	Data accessed
<b>Traveller</b>	Scheduling travel	Application status (ok/not ok) and end of validity period for granted authorisations
<b>Central Manual Processing Entity</b>	<ul style="list-style-type: none"> <li>• Application processing</li> <li>• Reporting</li> </ul>	All data <sup>51</sup>
<b>National authorities</b>	Application processing	Limited data (see below)
<b>Border guards</b>	Authorise or refuse border crossing	Application status (ok/not ok)
<b>Law enforcement authorities<sup>52</sup></b>	Retrieval for law enforcement purposes	Limited data (see below)
<b>Carriers</b>	Decide to board the traveller or not	Application status (ok/not ok)

The **CMPE** (the authority in charge of processing applications that have been flagged for further risk assessment) would need to have access to **all ETIAS data** for the purposes of ongoing decision-making, risk assessment, reporting and disambiguation. In contrast, **national authorities** (existing teams

<sup>48</sup> As ETIAS would not collect biometric data, it cannot be used for identification.

<sup>49</sup> Privacy by design means embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a proposed purpose and granting data access only to those entities that 'need to know.' See the Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union p.5, available at: [http://ec.europa.eu/dgs/home-affairs/doc\\_centre/borders/docs/1\\_en\\_impact\\_assessment\\_part1\\_v4.pdf](http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_impact_assessment_part1_v4.pdf) (accessed 09/2016).

<sup>50</sup> For more information on stakeholder tasks and role in ETIAS processes, see section 2.3 "Business processes."

<sup>51</sup> These access rights may change over time if a dormant database is implemented. For more information, see section 3.2 "Data protection".

<sup>52</sup> Law enforcement authorities is used in this study to refer to the authorities within Member States in charge of criminal investigations. National authorities is used to refer to the authorities within Member States in charge of assessing the security and migration risks travellers could pose. While the two roles are distinct, they may, in practice and in some Member States, be fulfilled by the same authorities.

involved in PNR/API processing) would only be able to access **data related to applications escalated to them by the CMPE. Travellers** would need access to their **application status** in order to check whether they have a valid travel authorisation and what is the authorisation's **end of validity date**. **Border guards and carriers** would only need to consult the **status of a travel authorisation**. It would be sufficient for these stakeholders to receive an "ok/not ok" message via their respective interfaces.

As demonstrated in section 2.2.4 "Risks", organised crime (notably trafficking in human beings, drug trafficking and firearms trafficking) can be linked to international travel – including visa-exempt travel. Information about travellers can thus be helpful in criminal investigations. This has been demonstrated by the use of the VIS for law enforcement purposes, which has allowed law enforcement authorities to make substantial progress in cases related to trafficking in human beings, drug trafficking and terrorism<sup>53</sup>.

Contrary to EES, ETIAS data cannot be used for identification purposes, as the system would not contain biometrics.

In the case of ETIAS, **law-enforcement authorities** would **not have access to information regarding health** (and the traveller's parents' first name, both of these type of information not being relevant for criminal investigations).

The following **conditions** should be met for a law enforcement authority to access ETIAS data:

- Access must be necessary for the aforementioned specific purposes;
- Access must be necessary for combatting terrorism or other serious crimes;
- Access must be necessary for an ongoing operational case (as opposed to general information-gathering for e.g. strategic-analysis purposes);
- There must be reasonable grounds to consider that accessing ETIAS data will substantially contribute to a criminal investigation;
- The law-enforcement authority must be one of the authorities designated by Member States as being entitled to access ETIAS data;
- A request for access must be submitted to and verified by a dedicated body checking whether the relevant conditions for accessing ETIAS data for law-enforcement purposes are fulfilled.

The same conditions would apply to access to travel authorisation **payment information** stored by a bank as well as to **meta-data** if collected by ETIAS.

The proposed approach to law-enforcement access is similar to what has been foreseen for EES<sup>54</sup> thus ensuring **coherence and consistency** of the EU legal framework.

### Data ownership

Data ownership is the way in which responsibility and accountability for the integrity<sup>55</sup> of data is distributed. Three data ownership models can be envisaged for ETIAS:

- **Member State ownership:** the Member State that entered the data is responsible and accountable for its integrity, including for keeping it up-to-date. This is the model used for VIS, SIS and EIS. This is not a viable alternative for ETIAS, as data would be entered into the system by travellers themselves.
- **Shared Member State ownership:** the Member State that obtained information relevant to the data is responsible and accountable for updating it. A Member State can update the data entered by another Member State. The EES proposal foresees shared data ownership between all participating Member States. This model is not viable for ETIAS, as the CMPE would be the entity obtaining information relevant to the data in most cases (it would be the entity contacted by travellers in the event of an issue, as it would be in charge of the helpdesk).
- **Shared CMPE and Member State ownership:** ETIAS data (data entered by travellers and any other data not entered by Member States) could be owned by the CMPE. Member States would only be responsible and accountable for the investigation triggers and other information that they entered into the system.

This last model emerges as the preferred solution for ETIAS, as it would:

- be consistent with the role foreseen for the CMPE, which would be in charge of the helpdesk; and

---

<sup>53</sup> See EES proposal, p. 6.

<sup>54</sup> See in particular Chapter IV of the EES proposal.

<sup>55</sup> Integrity addresses data completeness, accuracy and validity.

- provide clear-cut accountability for data entered by travellers. It would be difficult to choose the Member State responsible and accountable in the event of an issue with data entered by a traveller having no link to a specific Member State (e.g. in cases of automatically-granted authorisations).

In all cases, updates to applications made by the CMPE would have to be documented, and the history of the changes and the original data would have to be kept.



## 2.3 Business processes

This section identifies the ETIAS business processes. It provides an initial high-level description of how ETIAS would work: which activities would be carried out by the stakeholders involved and the system itself on a regular basis, from the application for a travel authorisation to the revocation of an already-granted authorisation.

### 2.3.1 Context

According to estimations made during the Smart Borders Technical Study<sup>56</sup>, 84% of border crossings by VE-TCNs take place at air borders, 9% at sea borders and only 7% at land borders. However, taking into consideration that the overall number of border crossings by VE-TCNs is expected to grow to 127 million by 2020, this means that up to 3 million VE-TCNs would be crossing into the Schengen Area at land borders.

Moreover, the possible visa liberalisation of any sizable countries sharing a land border with Europe may significantly increase the percentage of VE-TCNs entering the Schengen Area via land.

ETIAS processes will therefore have to demonstrate their feasibility at all border types and adapt to the VE countries concerned, taking into account their respective Internet and mobile penetration, among other things.

### 2.3.2 Approach

The business processes described hereafter have been designed and analysed leveraging on:

- consultations with Member States and EU agencies;
- consultations with carriers; and
- comparable systems worldwide, in particular the US ESTA and the Canadian eTA.

This section presents the results of the different options considered through the analysis, of which more details can be found in Annex 5. – “Business processes”.

#### **Assumptions**

- EES will be operational by the time that ETIAS is implemented;
- The travel authorisation will be valid for a fixed period of time. A period of two years is assumed for practical purposes;
- All border types will fall under the scope of ETIAS.

Should one of these assumptions prove not to be valid, the processes described below would have to be adapted accordingly.

---

<sup>56</sup> Technical Study on Smart Borders (2014).

### 2.3.3 Stakeholders involved

The below image summarises the main stakeholders involved in ETIAS business processes, which are then described in the following sections.

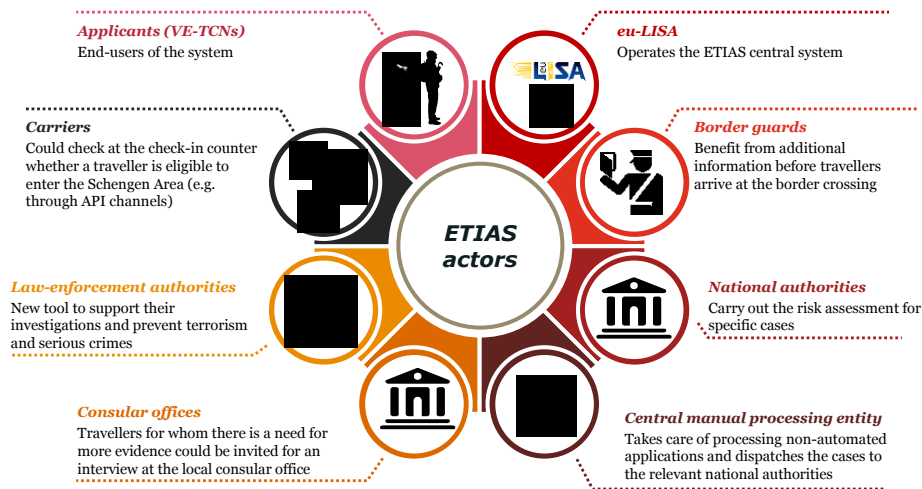


Figure 7: ETIAS stakeholders

Among them, of particular importance is the Central Manual Processing Entity (CMPE). Section 2.3.4 “Four main purposes” further details the CMPE’s role and responsibilities and the decision-making process. The possibility to grant law enforcement authorities’ access to ETIAS is discussed in section 2.2.9 “Access management and data ownership”; this stakeholder’s involvement is thus not mentioned below.

### 2.3.4 Four main processes

This section focuses on the four main processes related to the submission and handling of a new application for a travel authorisation, as these processes have the highest impact on ETIAS stakeholders, specifically on applicants and on the national authorities. Nevertheless, ETIAS support processes are also essential for it to meet all its goals and be a successful tool for border management and security. Relevant support processes are described in section 2.3.6 “Support processes”.

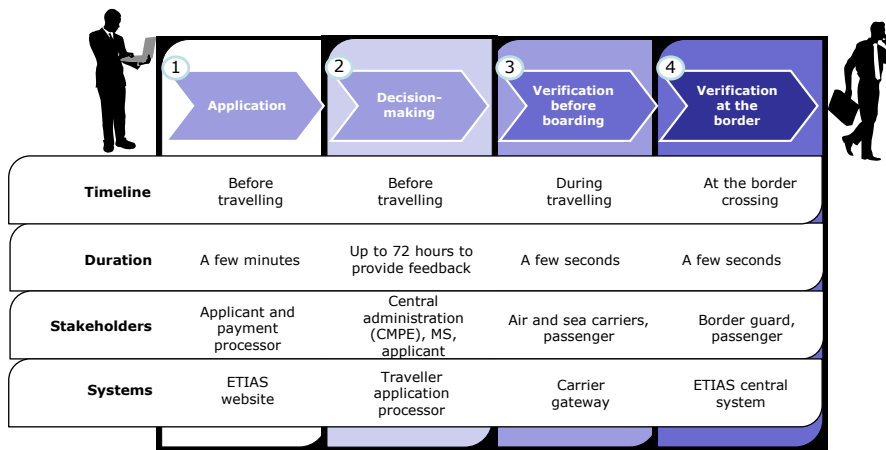


Figure 8: Overview of ETIAS business processes<sup>57</sup>

A new application would undergo four sequential steps:

<sup>57</sup> Process 3 “Verification before boarding” would only apply at air and sea borders.

1. **Application:** applicants request a travel authorisation by filling-in an online form. The authorisation would be electronic only and linked to the applicant's passport number and county of issuance<sup>58</sup>;
2. **Decision-making** (including the notification to applicants): depending on the case, the authorisation is automatically granted or the request is transferred for processing to the CMPE and possibly to national authorities;
3. **Verification before boarding:** carriers would be required to verify before boarding whether the traveller has a valid travel authorisation. If not, the carrier would incur the risk of having to bring the traveller back to the point of departure, if he/she is refused entry at the Schengen border. In practice, the carrier would not board the traveller onto the vessel. This would be possible only when a check-in process exists, and therefore would not apply in the case of land borders, where the traveller can arrive at the border without having gone through a check-in procedure;
4. **Verification at the border:** an automated query to the ETIAS system would allow border guards to swiftly verify whether a traveller has a valid travel authorisation. While a denied travel authorisation would always lead to a refusal of entry, having a travel authorisation would not give a "right of entry"; the decision on whether to authorise entry would still be taken by the border guard at the border-crossing point, in accordance with the Schengen Borders Code.

## 1) Application

*Table 12: Application process factsheet*

<b>Process</b>	Application
<b>Input</b>	Traveller's passport, credit card, valid email address, access to ETIAS website
<b>Trigger</b>	Planned trip to Schengen Area
<b>Stakeholders</b>	Applicant, payment processor
<b>Main activities</b>	Information entry, application review, fee payment, application submission
<b>Systems</b>	ETIAS Internet services
<b>Outcome</b>	Application complete

Travellers would be requested to apply for a travel authorisation 72 hours before starting their trip to the Schengen Area, as a swift answer (i.e. the automated "yes"), although likely, would not be guaranteed.

The application process can be divided into three steps, illustrated below:

1. **Enter information:** the applicant visits a secure website before their intended travel. The secure website can be accessed from the applicant's computer or mobile device, or possibly from an intermediary's computer (e.g. a travel agency's). He/she enters personal data. If necessary, an intermediary provides help to the applicant for inputting his/her personal data. Allowing third parties to fill-in the form for others would make it easier for people without an Internet connection or with disabilities, and would address other difficulties (e.g. language barriers). The web interface proceeds to simple field validations (e.g. "Are all mandatory fields filled-in?") before allowing any further step (for a detailed description of the field validations that could be carried out, see the "Field validation" subsection below). Possibly other personal data are collected (meta-data<sup>59</sup>).
2. **Review application:** before the final submission, a summary of the information provided would be displayed to the applicant, who would be asked to check and declare the accuracy of the information provided. The summary would also request the applicant to confirm his/her understanding of the fact that submitting inaccurate data could jeopardise the possibility to travel

<sup>58</sup> The same passport number can indeed be issued by different countries.

<sup>59</sup> Meta-data is "data about other data". In the case of ETIAS, this would be for example the way a date is represented, or the length of a field. See section 2.2.5 "Risk assessment".

to the Schengen Area as the travel authorisation could be denied, or revoked at a later stage, if inaccurate data is submitted.

3. **Pay fee:** the applicant might pay a fee to finalise the process. In this case, an intermediary (e.g. a bank) would perform the actual transaction and keep the respective records. A copy of the record would also be provided to the applicant.
4. **Submit application:** the application is sent securely to the ETIAS central system.

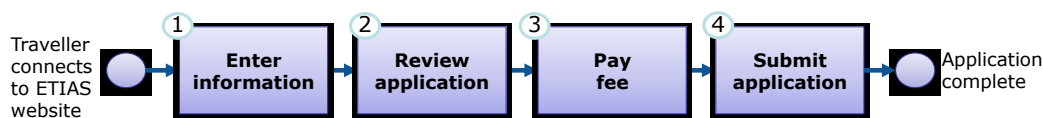


Figure 9: Application process

### Field validation

Field validation ensures that the data entered by applicants through the website or app is accurate and that no mistake complicates the decision-making process. As an example, field validation consists of ensuring that the phone-number field is filled-in only with numbers. This is done to increase data accuracy and help the applicant to notice and correct spelling mistakes and typing errors. However, field validation is limited as it can neither completely ensure the accuracy of the data entered, nor ensure the accuracy of all fields to the same extent (see Annex 5. – “Business processes”).

Additional details and considerations regarding the practical modalities of the application (time to fill-in an application, Internet access issues, application filled-in by third parties, possibilities for updating data, etc.) can be found in section 2.5 “User interactions”.

## 2) Decision-making

Table 13: Decision-making process factsheet

<b>Process</b>	Decision-making
<b>Input</b>	Access to relevant databases, connections between CMPE and MSs
<b>Trigger</b>	Application complete/incoming applications
<b>Stakeholders</b>	Applicant, CMPE, national authorities
<b>Main activities</b>	Automated processing, manual processing
<b>Systems</b>	ETIAS IT application, traveller application processor, search interface to other systems
<b>Outcome</b>	Notification of the decision to the applicant

The decision-making process is the process leading to an authorisation being either granted or denied. It is divided into steps, based on the assumption that if an authorisation is not automatically granted, it then has to be assessed manually. This safeguard is in line with EU Law<sup>60</sup>.

The process outlined hereafter was designed to:

- a) Have ≈95% of the incoming applications processed and granted automatically. This would be essential given the estimated number of incoming applications. There could be as many as 39 million VE-TCN applicants each year by 2020<sup>61</sup>, equivalent to ≈107,000 applications per day.
- b) Provide an expedited response to applicants through a harmonised process. Applicants applying through a European website would not expect to be treated differently (or potentially have a different appeal process) depending on the Member State processing their application.

<sup>60</sup> General Data Protection Regulation, Article 22 paragraphs 1 and 2: “The data subject shall have the right not to be subject to a decision based solely on automated processing (...) Paragraph 1 shall not apply if the decision: (...) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests (...)”. These safeguards include as a minimum the right to obtain human intervention, to express his/her point of view and to contest the decision.

<sup>61</sup> Technical Study on Smart Borders (2014).

- c) Allow Member States to be consulted when relevant and necessary for cases in which automated processing is not possible and Member States may possess intelligence concerning a specific applicant.

In light of these requirements, a cascade approach has been envisaged, divided into three steps to ensure a filtering and the coordination for the applications that would indeed require the assessment of a Member State:

- 1. Automated processing:** a central system (the traveller application processor), would process the applications by querying EU and international databases, applying additional checks and assigning a risk score to each application to determine whether an authorisation should be automatically granted.

The possible outcomes are:

- a. Authorisation granted;**
- b. Application escalated to manual processing** if a match/"hit"<sup>62</sup> or poor risk score exists<sup>63</sup>.

The traveller application processor is further described in section 2.4 "Architecture".

- 2. Manual processing by a central manual processing entity (CMPE):** will review applications coming from the automated assessment that require manual intervention.

The possible outcomes are:

- a. Authorisation granted** (e.g. in disambiguation cases in which it does not appear at first sight that the applicant is not the same person as the one on whom an alert or investigation trigger exists, a spelling mistake, etc.<sup>64</sup>);
- b. Application escalated to national authorities** for further processing<sup>65</sup>.

Whether the CMPE would be allowed to deny authorisations determines two variants that have been investigated in the study (see Annex 5. – "Business processes"). If the CMPE was entitled to do so, the outcome of its processing could also be:

- c. Authorisation denied** (e.g. if there is an alert for refusal of entry in the Schengen Information System (SIS));
  - d. Additional information requested from the applicant.** In some cases, the officer processing the application might notify the applicant of the need to provide further information. In such cases, similarly to what has been implemented by the Canadian eTA, the applicant would be invited to create an account on the ETIAS website to provide the requested information or scanned document.
- 3. Manual processing by one or several national authorities:** the responsible Member State assesses the case, which results in:
    - a. Authorisation granted;**
    - b. Authorisation denied;**
    - c. Additional information** requested from the applicant and/or **interview at consulate requested.**

The result of the manual processing by the CMPE and/or national authorities is then sent back to the ETIAS central system, where it is stored for a predefined period of time; the applicant is then notified of the decision.

This process is illustrated below:

---

<sup>62</sup> A search in the SIS can result in what is called a "hit". A hit means that an alert has been found on the person/object subject to the check.

<sup>63</sup> The risk score/outcome of the automated processing could be added to/part of the data field "justification for the decision" (see section 2.2.7 "Data set").

<sup>64</sup> The CMPE would not update ETIAS data as such; instead, it would add corrected data to the application file. This would allow keeping trace of the original data and of the correction made.

<sup>65</sup> This includes cases in which there is a match with an "investigation trigger". Part of these investigation triggers could be defined by Member States themselves. They would be contained in the "traveller application processor" (see sections 2.2 "Data" and 2.4 "Architecture").

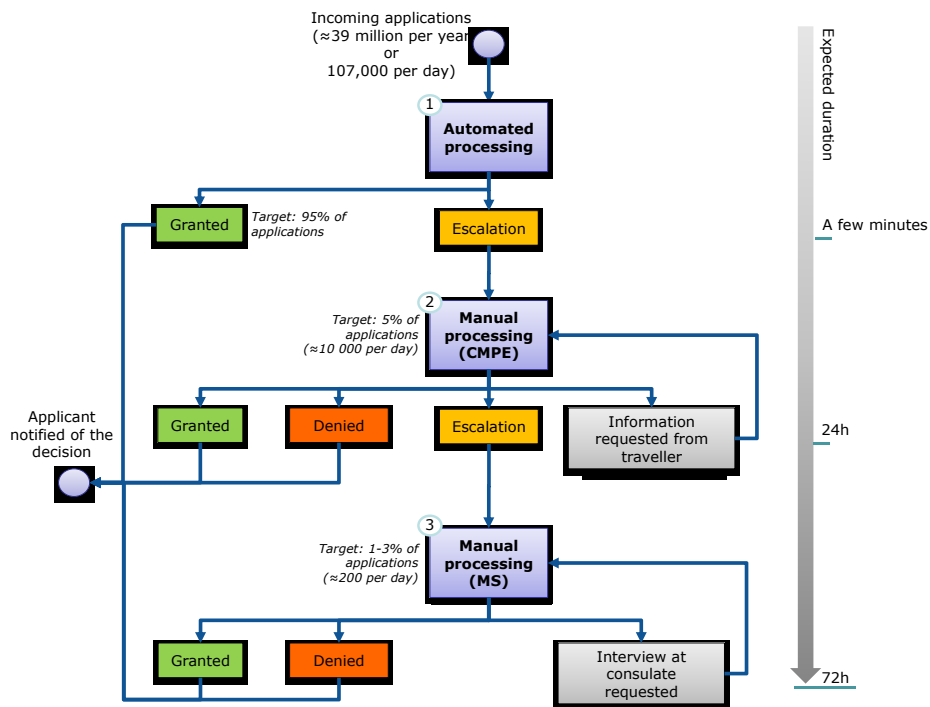


Figure 10: Decision-making process<sup>66</sup>

All comparable systems (US ESTA, Canadian eTA, Australian eVisitor) adopt a similar escalation mechanism, with applications being reviewed by a central administration, which includes experts of different grades and expertise, adapting different levels of complexity for issues that could be encountered with an application (e.g. whether it is for simple disambiguation or there is a security risk).

Rules would have to be defined for the three-step decision-making “cascade”, specifying in which cases an application would be fully handled centrally and in which cases it would be sent to one (or several) Member State(s) for further processing.

### Central Manual Processing Entity

#### Functions

This new entity would be a central administration for handling incoming applications requiring manual processing, seeking the support of Member States when relevant.

A central administration would need to be created to address the following requirements:

- Limiting the workload for Member States (to e.g. only 1-3% of all cases) and consulates as much as possible;
- Coordinating the decision-making process at European level; and
- Providing a uniform process/experience to travellers.

If no central administration were to be created, the entire burden of processing the applications would then fall on the Member States, compromising the overall feasibility of ETIAS given the volumes to be processed.

Whether an application identified for manual processing is handled by the CMPE or by one or more Member State(s) will depend upon detailed conditions established by the policy-maker. Nevertheless, the study has identified two possible variants for the allocation of responsibility:

1. The CMPE cannot deny an authorisation. Complex cases, i.e. cases that would lead to a **denial** or simply **require additional evidence**, are transferred to Member States;

<sup>66</sup> 107,000 applications per day is derived from a forecast of 39 million applications each year by 2020.

2. The CMPE can deny authorisations **in specific cases** (e.g. in case of an alert for refusal of entry in the SIS). Member States would be consulted **in cases for which they might have additional information** relevant to a specific application. As an example, this could be the case when a Member State has created a specific alert (e.g. in the SIS). For hits on alerts originating from a country not part of the Schengen Area, applications would be handled by the CMPE.

Independently of the variant chosen, the following principles could be provided for to increase the **efficiency** and **homogeneity** of the manual processing:

- a) The **CMPE will strive to reduce the workload of Member States**, doing the majority of the manual processing required whenever possible;
- b) The **CMPE could assume the role of process owner**, maintaining oversight even if the intervention of one or more Member State is required;
- c) The **CMPE could coordinate the processing** of the application if one or several Member State(s) need to be involved, to ensure that an answer is given to the applicant within 72 hours. Alternatively, a Member State "chef de file" could coordinate the processing;
- d) **Member States would have the possibility to create "investigation triggers" in the traveller application processor**, which would be specific values that would, if present in an application (either alone or combined) trigger manual processing. The application would then be taken out of the automatic process and sent to the CMPE<sup>67</sup> (see section 2.2 "Data").

A more detailed overview of the different cases and the expected results is presented in Annex 5. – "Business processes".

In addition to this **case-handling function**, the CMPE would have four additional functions:

- A **screening-rule-related function**. The CMPE would be in charge of defining the screening rules, but also refining them on the basis of statistics and with the help of Member States;
- An **audit function**. The CMPE would be in charge of monitoring its compliance with the EU legal framework. This would include verifying that the rules are correctly implemented and that they have no adverse consequences on Fundamental Rights;
- A **review function**, i.e. handling complaints brought by travellers concerning data protection, and complaints concerning the outcome of the decision-making process;
- A **helpdesk function**. The CMPE would be in charge of the helpdesk, i.e. a hotline that travellers would call to obtain support with their application for a travel authorisation or to report an issue with the website. The CMPE would answer travellers' queries and report website issues to eu-LISA.

### Organisation

The CMPE's role would be assumed by an EU agency. In order to efficiently perform both its case-handling and helpdesk functions, the CMPE would have to work 24/7. This would:

- Limit the backlog. Visa-exempt travellers are likely to apply for a travel authorisation outside Central European Time business hours, as they would apply from countries within a different time zone. If the CMPE were to work only during business hours, this would result in a significant number of applications awaiting processing at the beginning of the next CMPE shift;
- Ensure that the duration of the decision-making process is not exceeded. Should a significant backlog arise, the CMPE could find itself short of time to process applications;
- Increase convenience for travellers. They would be able to contact the helpdesk at any time;
- Ensure that any issue with the website (e.g. temporary unavailability) is known and reported to eu-LISA as soon as possible.

To carry out these four functions, the CMPE would be composed of:

- **Case-handling officers** working in shifts. The case-handling unit would be the largest in terms of

---

<sup>67</sup> It has been considered, in the course of the study, whether the forwarding of the application to the relevant Member State could be done automatically, via the system. However, in many cases the Member State to who would receive the application is not obvious (if several Member States are involved for instance – this would not be an issue if responsibility for a case would be allocated to the Member State of intended entry as declared by the traveller). Granting the CMPE the mandate to allocate the "complex" applications would allow it to perform a necessary monitoring and coordinating role.

the number of people. The unit's management would make sure that answers are provided on time to applicants;

- **Liaison officers from Member States** (one per Member State). Liaison officers would be physically present at the CMPE office(s) and assist in processing applications. They would also participate in defining and reviewing the screening rules. Depending on the needs, liaison officers could be present on a permanent or part-time basis;
- **Screening-rule officers** in charge of defining and refining screening rules;
- **Audit officers**, who would be in charge of verifying that the rules are correctly implemented and that they have no adverse consequences on Fundamental Rights;
- **Appeal officers**, who would deal with complaints concerning the outcome of the decision-making process. These officers would have to be independent from the case-handling unit;
- A **data-protection officer (DPO)**, who would:
  - monitor the compliance of the CMPE's data-processing activities with the EU legal framework on data protection; and
  - handle complaints from applicants relating to data protection (notably the right of correction and deletion).He/she could be assisted by national DPOs;
- **Helpdesk officers** working in shifts;
- **Support officers** (human resources, IT, security, procurement etc.).

### ***Duration of the decision-making process***

This three-step decision-making process should allow the system to automatically grant a travel authorisation to the vast majority of applicants (targeting 95% of applications) **within minutes**. Should the intervention of the central manual processing entity be required, an application could take up to **24 hours** to process. If the involvement of a Member State is necessary, the answer (authorisation denied or granted, or request for additional information or an interview) should be provided within **72 hours**<sup>68</sup> (for a detailed justification of these processing times, see Annex 5. – "Business processes").

If the Member State responsible for processing a case does not provide an answer within the processing time allowed (72 hours), the CMPE would consider that the authorisation can be granted. Exceptions to this rule could be foreseen for cases of a travel authorisation previously denied by a Member State for security reasons, for instance. Member States could also be given the possibility to request an extension of the allowed time in specific pre-defined circumstances.

These durations are aligned with the current practices of the other travel-authorisation systems: for instance, eVisitor automatically grants more than 80% of the applications lodged<sup>69</sup> within minutes and eTA is expected to grant 90% automatically<sup>70</sup>. In the event of a manual risk assessment, the processing time is 72 hours<sup>71</sup> for both Canada and the US, while the processing of the Australian eVisitor authorisations can take up to 10 working days<sup>72</sup>.

In specific situations (emergencies and possibly some cases of *force majeure*<sup>73</sup>), a dedicated field could be used to notify to the person in charge of the manual processing (if not already authorised automatically) of the urgency of the request.

---

<sup>68</sup> As the answer from the Member State may consist in requesting additional information or an interview, the *total* processing time of an application may be longer than 72 hours.

<sup>69</sup> See Reports from the European Commission on certain third countries' maintenance of visa requirements in breach of the principle of reciprocity: [http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/visa-policy/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/visa-policy/index_en.htm) (accessed 06/2016).

<sup>70</sup> See: <http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5839938> (accessed 06/2016).

<sup>71</sup> See for ESTA: [https://help.cbp.gov/app/answers/detail/a\\_id/1143/~how-do-i-know-if-my-esta-application-was-approved](https://help.cbp.gov/app/answers/detail/a_id/1143/~how-do-i-know-if-my-esta-application-was-approved) and for eTA: <http://www.cic.gc.ca/English/helpcentre/answer.asp?qnum=1084&top=16> (accessed 06/2016).

<sup>72</sup> See: [http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/visa-policy/docs/com\\_2012\\_681\\_final\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/visa-policy/docs/com_2012_681_final_en.pdf) (accessed 06/2016).

<sup>73</sup> See Annex 4. – "Data".



### ***MS manual procedure***

Within Member States, different set-ups could be envisaged for ETIAS application management. In light of the competencies and information required, Member States could reuse existing teams involved in API/PNR data processing rather than creating new administrative centres. As these teams are in the process of being created in many Member States, this also provides the opportunity to incorporate ETIAS application handling into their training.

Some level of harmonisation across Member States would most probably be beneficial, as the choice of different set-ups would impact negatively on ETIAS's overall efficiency. To prevent this issue, minimum standards for national set-ups could be put in place. They would aim to ensure that data is used and the relevant stakeholders are involved in a consistent and timely manner. For instance, it could be useful to ensure that Member States' processing units work seven days a week (given the limited number of applications with which Member States would be involved in processing, working 24 hours a day may not be necessary for all Member States' units; whether the unit needs to work 24 hours a day would need to be defined for each Member State and would depend on the number of applications).

In any case, an agreement would have to be reached on a national single point of contact to which the central manual processing authority would forward the relevant cases.

Rules concerning the interview at a consulate should also be defined. Such an interview should be a "last resort" measure and should be undertaken only when information from the application justifies it and no other check can provide an adequate answer to the pending questions of the authority in charge of manual processing. This would ensure that the additional workload for consular posts is limited and would curtail the inconvenience for travellers. Finally, to ensure that it is useful to ETIAS's risk assessment, the interview should specifically focus on the missing information, as opposed to being a generic interview.

### ***Request for additional information***

Should the CMPE or Member States need to request additional information, the applicant would first be asked to create a secure account. The additional information would be transmitted from this secure account to the ETIAS central system, where it would be accessed by the CMPE or the Member State having requested it.

If the applicant does not answer the request to provide more information within a pre-defined period of time (e.g. 30 days), the application processing would be closed. This would avoid retaining pending applications in the system for an indefinite period of time.

### ***Granting the travel authorisation***

When the travel authorisation is granted, the applicant would be notified by way of an email sent to the address provided in the application form.

### ***Denial of the travel authorisation***

Australia, Canada and the US have implemented different ways to handle cases in which the travel authorisation is denied:

- a) In Australia and the US, the person can still apply for a visa following the normal procedure;
- b) In Canada, case officers can determine that a more in-depth examination or an interview is required. If so, a referral to an overseas mission is made, where further assessments are conducted. Additional documentation can be requested if needed. Therefore, no authorisation is denied without human intervention and an in-depth examination of complex cases. As a result, a person who has been denied a travel authorisation cannot apply for a visa.

Providing the possibility for a traveller who has been denied a travel authorisation to apply for a visa may be difficult to propose in the EU context. In Australia, the universal visa-requirement approach threatens the eVisitor authorisation as a visa. A denied travel authorisation then leads to a visa application: a more cumbersome procedure with a mandatory interview at a consular office. In the US, ESTA determines the eligibility of visitors to travel to the country under the Visa Waiver Program<sup>74</sup>. In both cases, travellers are

---

<sup>74</sup> See: <https://www.cbp.gov/travel/international-visitors/esta> (accessed 07/2016).

not considered visa-exempt and it is thus acceptable that if they fail to obtain an authorisation through electronic channels and specific programmes, they can fall back on the normal visa procedure. It may, on the contrary, be diplomatically difficult for the EU to propose that citizens from visa-exempt countries must submit a visa application in some cases.

The Canadian model on this issue seems to be the most appropriate solution in the EU context: applicants for an authorisation to travel to the Schengen Area would not be redirected to the visa procedure. The interview would constitute the last possible step of the procedure to be eligible to cross the border. In cases in which the travel authorisation is denied, no application for a visa could be submitted by visa-exempt travellers; however they would still be able to appeal the decision (see section 3.2 “Data protection”).

When a travel authorisation is denied, the reason for the denial would be given to the applicant. This would be done in the notification email sent to the applicant to inform him/her of the result of the decision-making process. The reason for the denial would take the form of a text describing why the authorisation was denied (e.g. passport expired) and informing the applicant of the procedure for appealing the decision.

Finally, ETIAS’s legal basis should provide that the existence of a previously denied authorisation does not lead to the systematic denial of a new request for authorisation. The system would have to take into account that the conditions leading to a refusal could change over time.

### 3) Verification before boarding

*Table 14: Verification before boarding process factsheet*

<b>Process</b>	Verification before boarding
<b>Input</b>	Carrier obligation rules, connection to travel authorisation status
<b>Trigger</b>	Traveller initiates the trip
<b>Stakeholders</b>	Applicant, carrier
<b>Main activities</b>	Verifying the travel-authorisation status
<b>Systems</b>	ETIAS central system, carrier gateway
<b>Outcome</b>	Boarding allowed / Boarding denied

Carriers would verify whether a passenger has a valid travel authorisation **using a specific interface(s)** (see section 2.4 “Architecture”). The verification could take place from check-in (often done by travellers online at home) to no later than the time of boarding the vessel travelling to the Schengen Area.

This check aims at enforcing the travel-authorisation requirement by preventing travellers subject to this requirement from boarding if they do not possess a valid travel authorisation. To reach this objective, an **obligation to check** whether travellers have an authorisation could be imposed on carriers, in addition to the current obligations whereby they must check that travellers possess a valid travel document and, for visa holders, a valid visa (see section 3.1 “Legal”).

In future, according to the EES legislative proposal, with the implementation of EES and the abolition of passport and visa stamping, carriers would comply with their obligations (i.e. check whether a person holding a single- or double-entry visa has already used it) by connecting to EES. Therefore, to reduce the impact on carriers, the preferred solution would be to **integrate ETIAS verification with the consultation of EES**<sup>75</sup>. Should both processes be integrated, carriers would send the traveller’s API data<sup>76</sup>; this data would be used to query both the EES and ETIAS systems. An integrated response would then be sent back to the carrier (e.g. ok, not ok EES, not ok ETIAS, not ok EES and ETIAS<sup>77</sup>), based on

<sup>75</sup> EES legislative proposal, Article 12 paragraph 2, COM(2016) 194 final.

<sup>76</sup> See Article 3 of the API Directive.

<sup>77</sup> This would allow carriers to inform travellers about the issue.

whether the person has already used his/her visa (EES) and whether he/she has a valid travel authorisation (ETIAS) <sup>78</sup>.

An “ok” answer would not guarantee boarding, as the carrier would still, in line with current obligations, have to **check whether the person possesses a valid passport**. The boarding decision and responsibility would in fact remain with the carriers. Further details regarding the connection modalities for carriers are described in section 2.4 “Architecture” (the so called “carrier gateway”) and in section 2.5.2 “Interacting with carriers”.

This process is illustrated below.

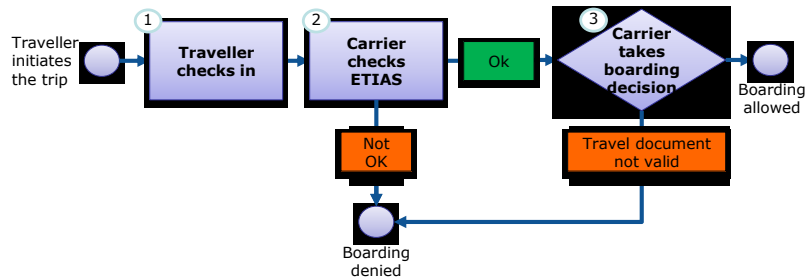


Figure 11: Verification before boarding process

**In event of denied boarding** a standard message with contact details (phone number/email address of hotline) should be made available for carriers to provide an answer to travellers who have been denied boarding. There is no carrier liability concerning passenger rights. Refusal of boarding on the basis of a refused or missing travel authorisation would not be grounds for passengers to request any reimbursement. Travellers would have to be responsible for complying with all the entry conditions, including having a travel authorisation.

The obligation to check ETIAS before boarding would **only apply to air and sea carriers**, as coaches and trains neither systematically check passengers’ identities nor usually have a check-in process. In fact, travellers can often purchase a train or bus ticket without a reservation. Therefore, the verification-before-boarding process would not apply to travellers coming by land to the Schengen border. It would also not apply to private boats and aircrafts as no carrier is involved in such cases. The travel authorisation would then be verified during the border-control process.

The absence of a valid travel authorisation would trigger the border guard to refuse entry, and thus even land carriers would be obliged to transport the passenger back, albeit without penalties. For this reason, land carriers would also have the possibility to connect to and consult ETIAS, if they wished, so as to minimise the number of people needing to be returned.

A more thorough assessment of this process’s impact on carriers transporting travellers to the Schengen Area would need to be performed.

#### 4) Verification at the border

Table 15: Verification at the border process factsheet

<b>Process</b>	Verification at the border
<b>Input</b>	SBC rules, connection to travel authorisation status
<b>Trigger</b>	Traveller arrives at the (Schengen) border
<b>Stakeholders</b>	Applicant, border guard

<sup>78</sup> All benchmark countries link their electronic travel authorisation systems to advance passenger information and their communication channels with air carriers. This setup allows carriers to receive information on the status of an authorisation in order to decide whether or not to authorise boarding. In Canada, the implementation of an interactive API was foreseen in the same action plan as the implementation of the eTA. See “Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness”: <http://canadagazette.gc.ca/rp-pr/p2/2015/2015-04-22/html/sor-dors77-eng.php> (accessed 06/2016).

<b>Main activities</b>	Verifying the travel document and authorisation status
<b>Systems</b>	ETIAS central system, border guard interface (National Uniform Interface)
<b>Outcome</b>	Entry / Refusal of entry (into Schengen Area)

The border guard would carry out the **usual border controls** as specified in the SBC, which include reading the visa-exempt traveller's passport data. The passport number and issuing country would be automatically used to query ETIAS and display an "ok"/"not ok" (existence (or not) of a valid travel authorisation) message on the border guards interface. The same operation could be used to query simultaneously EES. The system would then either perform the biometric verification of the traveller or proceed with the creation of the EES individual file. In this case, the EES file would be filled-in using information taken directly from the passport and **not** pre-filled with ETIAS data (declarative and thus less reliable).

At this stage, consistency checks between ETIAS and EES data could be performed. Any discrepancy could be pointed out to the border guard, who would have to allow or refuse entry taking into account this piece of information.

The discrepancy could then be notified to the CMPE and could potentially trigger a re-check of the application or the request to the traveller to submit a new application with correct data.

The following figure illustrates the verification at the border-crossing point.

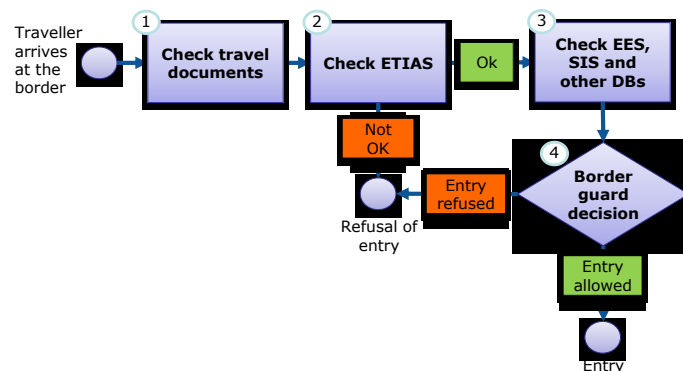


Figure 12: Verification at border-crossing process

### **Impact on border guards' work**

The impact for border guards of checking whether a valid travel authorisation exists, should be minimal. If properly integrated in the existing software, the check would simultaneously verify the SIS, EES and other national databases.

Despite the fact that ETIAS may have verified at least part of the entry conditions established by the Schengen Borders Code, the border guards would have to check them again, having the opportunity to see both traveller and document.

### **Exemptions**

A number of exemptions to the travel authorisation requirement would have to be foreseen. The full list of exemptions is presented in Annex 5. – "Business processes".

## 2.3.5 Process overview at the different border types

The figure below illustrates the entire process from the perspective of a traveller applying for a travel authorisation to him/her crossing the border, including the two cases where verification before boarding is possible (carriers have a role to play) or not possible (case without carriers).

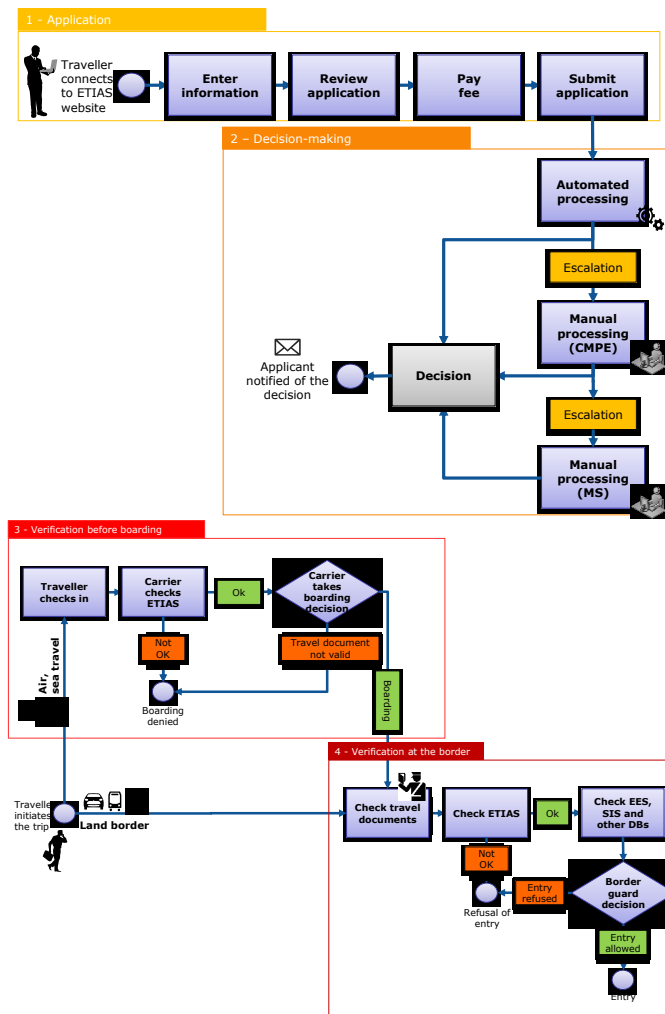


Figure 13: ETIAS process overview

## Land borders

### Context and current situation

ETIAS would be the only travel authorisation system that would apply to land borders in addition to air and sea ones – the Australian, Canadian and US systems do not include land borders. The situation at land differ greatly from that at air and sea. In the EU, although land travel currently represents around 5% of the VE-TCNs arriving at the Schengen borders<sup>79</sup>, this number is likely to increase dramatically given the current visa liberalisation discussions. This is why this border type merits further analysis.

Five main differences at land, affecting both carriers and travellers, would impact on the implementation of ETIAS.

### Role of carriers in light of ETIAS

**Absence of verification.** Although some carriers verify TCNs' travel documents before they board a train or bus, this practice is still not widespread. Carriers need means and resources to be able to perform a check on a visa, a travel authorisation or even just a passport (using a machine readable device). Due to the nature of land travel, these machines also need to be mobile and easy to use in a moving vessel, while air carriers usually perform the verification on the ground, at the check-in stage. Not all land carriers have acquired this type of equipment, which inevitably also comes at a cost. In addition, passengers are likely

<sup>79</sup> Technical study on Smart Borders (2014), p. 23. For a list of countries whose nationals do not require a visa, see Annex II of Regulation No 539/2001, available at: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-policy/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-policy/index_en.htm) (accessed 09/2016).

to board at different points in time (if the train/bus makes any additional stop between the cities of departure and arrival), which makes verifications prior to the boarding even more complex to implement<sup>80</sup>.

**Absence of advance information.** In 2004, the API Directive triggered the development of information-sharing practices for airlines, which are now equipped and connected to Passenger Information Units at Member-State level in order to send information about their passengers. Contrary to air travel, no advance passenger information is sent for travellers arriving by land. If one of the main objectives of ETIAS is filling an information gap on VE-TCNs, this gap is even greater at land borders.

**Heterogeneity.** The heterogeneity of the carriers' situations at land (small companies, different types of vessels, multiple stops before arriving at the Schengen Area, not all land carriers stop at the border, etc.) makes it very unlikely for now, and unrealistic for the EU, to require all carriers to verify their passengers' travel documents, visas and authorisations before embarking. The only type of carriers that could potentially verify ETIAS status prior to boarding would be the ones offering a direct link between a visa-exempt country and the Schengen Area, like certain trains for instance.

These differences would impact on the implementation of ETIAS, as only **three of the four main processes explained above would apply to land borders**: application, decision-making and verification at the border. Land carriers would not be involved in the verification process.

#### From a traveller's point of view

**Refusals of entry.** ETIAS would be an additional requirement for a population of travellers arriving using very different means at the Schengen border: by train, bus or in a private vehicle. In addition, more people travel privately by land than by air and sea. This heterogeneity makes it difficult to inform all VE-TCNs of the new requirement. If ETIAS is introduced without relevant preparatory measures designed for land borders, it is likely that the number of refusals of entry would increase due to the lack of travel authorisation. As a result, refusals of entry would rise slightly in the beginning before travellers become aware of ETIAS, before eventually decreasing<sup>81</sup>. For this reason, a grace period could be envisaged so that travellers get to know the new requirement before being refused them on the basis of a lack of valid travel authorisation.

**"On-the-spot" applications.** This also means that more VE-TCNs would try to make an application close to the border, or even once they arrive at the border. Indeed, travellers could try to apply on the spot using their own mobile devices, for instance, and would stand a good chance of receiving quickly a positive answer. This situation would probably lead to queues and people waiting at the border to receive the authorisation. In order to better manage the crowds and avoid potentially tense situations, computers with Internet access (which could be limited to the ETIAS website) or Internet hotspots could be made available at the border in order to let travellers apply on the spot from their mobile devices. As the large majority of applications are automatically granted within minutes, this option should not have a major impact on border-control procedures.

In practical terms, a traveller without a valid travel authorisation would be treated in a similar way to a person travelling without a valid visa: denial of entry.

#### ***Crossing a land border: four scenarios***

Four scenarios are possible when arriving at a Schengen land border. The differences of the three latter scenarios in comparison with scenario 1 are shown in bold and blue.

##### **1. Travelling on a train stopping at the border**

---

<sup>80</sup> This issue can be mitigated for a bus scenario as it is easier to identify newly embarked passengers on a bus. As a result, if the bus makes any additional stop in between the cities of departure and destination, checking the travel authorisation of these new passengers would be more feasible and have a less important impact on time management. However, whilst some train companies might have the means to pursue this type of equipment, it is very unlikely for buses to do so.

<sup>81</sup> For the year 2015, Member States reported approximately 118,500 refusals of entry of third-country nationals (visa-exempt and visa holders) at the border of the Schengen Area, mainly issued at land borders: 56%. Without any prior checks before arrival at the borders and without the filtering performed by air carriers, VE-TCN do not have any information on their likelihood of meeting the Schengen Borders Code entry conditions and actually crossing the borders. See Frontex Risk Analysis for 2016, p. 66-68.

The passenger embarks on the train. He/she only has to justify the validity of their travel ticket to the ticket inspector (either before boarding or whilst the train is already moving).

If the train makes other stops before arriving at the Schengen border, new passengers may board after the city of departure.

Before crossing the Schengen border, the train stops and the border guards perform a border check (including a verification of ETIAS status).

If the person is found not to meet the requirements set out in the SBC, including not possessing a valid travel authorisation, he/she will be required to disembark from the train.

## 2. Travelling on a train not stopping at the border

The passenger boards the train. He/she only has to justify the validity of their travel ticket to the ticket inspector (either before boarding or whilst the train is already moving)<sup>82</sup>.

If the train makes other stops before arriving at the Schengen border, new passengers may board after the city of departure.

The border checks are performed either:

- a) During the journey. ETIAS verification performed on a moving train would require the use of the mobile network required for EES checks and updates. This requirement is not simple to be fulfilled<sup>83</sup>; or
- b) When the train arrives at its final destination, already inside the Schengen Area.

If the person is found not to meet the requirements set out in the SBC, including not possessing a valid travel authorisation, he/she will be required to **re-board on a train returning to the country of origin**. This situation may be more difficult to handle and more time-consuming for border authorities as return is, in some cases, not immediately possible.

## 3. Travelling by bus

The passenger boards on the bus. He/she only has to justify the validity of their travel ticket to the ticket inspector or the driver, before boarding.

If the bus makes other stops before arriving at the Schengen border, new passengers may board after the city of departure.

**Unlike trains, buses will always stop at the land border, where the checks are performed by border guards.**

If the person is found not to meet the requirements set out in the SBC, including not possessing a valid travel authorisation, he/she will be required to disembark from the bus.

## 4. Individual travel (transport by personal means with no involvement of carriers, e.g. travelling by car)<sup>84</sup>

The passenger starts his/her journey and does not have to justify the validity of any ticket, passport or authorisation. When travelling without using a carrier, no verification by a third-party prior to arrival at the border is possible. If he/she makes other stops before arriving at the Schengen border, new passengers may board after the city of departure.

**Individual travellers will always stop at the land border, where the checks are performed by border guards.**

If the person is found not to meet the requirements set in the SBC, including not possessing a valid travel authorisation, he/she will have to return by his/her own means.

---

<sup>82</sup> The Eurostar and the Allegro trains are exceptions in that sense as they have a reservation system through which the verification of ETIAS status could be implemented in the future.

<sup>83</sup> See Technical study on Smart Borders (2014).

<sup>84</sup> This scenario also includes border crossings for commercial purposes by lorry drivers. From a commercial point a view, lorry drivers conveying goods to and from the Schengen Area for a business purpose would also need to apply for a travel authorisation. They could be exempted if they enter in any of the categories described in Annex 5. – “Business Processes”.

## Conclusion

The **heterogeneity** of travel means, the **absence of verifications** by carriers and the **absence of advance information** on TCNs before their arrival at the Schengen border makes the situation at land very particular and seemingly more difficult to handle. Although the denial or revocation of a travel authorisation will never (for individual travel) or very unlikely in the near future (for travel by bus or train) prevent a VE-TCN from travelling to the Schengen border, ETIAS would still limit the number of refusals of entry in the long run. Some **mitigation measures** could be put in place to limit the initial number of refusals of entry due to a lack of valid travel authorisation when the authorisation is put in place:

- Before ETIAS becomes mandatory
  - A widespread **communication campaign**, launched several months before the system goes live and focusing on the main roads and land communication routes in order to inform as many land travellers as possible;
  - Although carriers are not involved in verifying ETIAS status, they should also be included in this communication campaign as they could play an important role in informing their customers of the new requirement.
- When ETIAS becomes mandatory
  - ETIAS **kiosks, computers** with Internet access and/or **Internet hotspots** at the border-crossing points, allowing travellers to apply for an authorisation on the spot (This topic is further discussed in section 2.5.1 "Interacting with travellers");
  - A **grace period** in the implementation process (topic further discussed in section 2.7 "Implementation approach"). The heterogeneity of the population arriving by land (by bus, train, with or without a carrier, for different purposes, from different points of entry, etc.) makes the communication campaign trickier than for other border types. For this reason, the length of the grace period would mainly be determined by the situation at land borders.

### 2.3.6 Support processes

This section focuses on some key support processes.

#### Query of authorisation status

A travel-authorisation status can be verified by different end-users of the system and for different purposes:

*Table 16: Query of authorisation status by end-users*

End-user	Purpose of the action	Information needed
<i>Carriers</i>	To know at boarding whether a passenger holds a valid travel authorisation (topic addressed in section 2.5.2 "Interacting with carriers")	Application status: ok/not ok
<i>Border guards</i>	To verify at the border-crossing point whether a VE-TCN holds a valid travel authorisation	Application status: ok/not ok
<i>CMPE, national authorities, law enforcement</i>	For the purpose of the risk assessment or as part of an investigation (topic addressed in section 2.2.9. "Access management and data ownership")	Application status: ok/not ok, additional data
<i>Applicants</i>	To verify whether the travel authorisation is still valid, and to check its expiry date	Application status: ok/not ok, validity period, expiry date

The first three end-users listed in the table above would have special connections to ETIAS and would be able to verify the status of the authorisation through an interface. The applicants themselves, however,



would not have access to this type of interface<sup>85</sup>. It is then relevant to assess other possibilities for them to verify their authorisation status. Indeed, it can be assumed that after a certain period of time some applicants may have lost their confirmation email containing the status of their authorisation and its validity period.

The most secure and user-friendly solution is to establish a “retrieve status” option in the ETIAS website or app itself, through which travellers can request their authorisation details to be sent to them via the email address they used to submit the application. This query would require the passport number and issuing country, as the system will link it to the authorisation. The status is then retrieved and sent by email to the person<sup>86</sup>. The only requirement for the applicant is to have access to the same email address that they had at the time of the application. If this address has changed or is no longer operational, a new application would have to be submitted.

Lastly, the system could be designed with the functionality to send an automatic notification to applicants whose authorisation is reaching the end of their validity period (such as one month before expiry) in order to advise them to re-apply soon.

### Re-check of granted travel authorisations

As part of the decision-making process described above, once an application is submitted, ETIAS would run a risk assessment by querying the information present at that time in all the databases connected to it (SIS, VIS, EES, SLTD, TDAWN and ETIAS screening rules). If the authorisation is granted, it would undergo a **series of re-checks** as part of an ongoing risk assessment, in order to take into consideration any new information inserted in the above-mentioned databases. The re-check would therefore be performed against **newly-added alerts** or information and not against all data stored in the connected systems. The following table lists the databases that would be part of the re-check process as well as the frequency of the re-check. A more detailed assessment taking into consideration the technical capacity of the connected systems is available in Annex 5. – “Business processes”.

*Table 17: Databases present in the re-check process*

	Added value of the re-check	Possible frequency
<b>SIS</b>	Yes	Every 24 hours
<b>VIS</b>	No	N/A
<b>EES</b>	Yes	91 days after travel authorisation is granted and/or every 24 hours
<b>SLTD</b>	Yes	Every 24 hours
<b>TDAWN</b>	Yes	As a complement to SLTD – as often as SLTD
<b>Screening rules</b>	Yes	The frequency of the recheck would depend on how much Member States make use of this tool: if a lot of information is added every day, it would be beneficial to re-check it every 24 hours

The process should be **frequent** and a first assessment shows that a 24-hour re-check would be adequate. It would have to be performed at a convenient time in order not to overload the connected systems during peak hours; a **nightly** re-check should be considered, even though it would only be beneficial for the EU systems. Indeed, Interpol’s systems are accessed and populated by countries all around the world and are therefore used throughout the day and night. An application rechecked every 24 hours, with a two-year validity period and with no matches found, would go through the re-check process 730 times. This calls for the efficient technical implementation of the re-check process. It would be preferable to adapt the connected systems and databases to **transmit** new alerts/information to ETIAS<sup>87</sup>,

<sup>85</sup> As explained in section 2.5.1 “Interacting with travellers”, ETIAS would not be account-based due to high security standards required for the system. Indeed, this option would entail keeping a large amount of information from the traveller in a copied database accessible by the website or possibly the mobile application. As a result, there would not be any personalised webpage where the status of the application can be requested.

<sup>86</sup> More information on this database and how it links to ETIAS central system and the interfaces can be found in section 2.4 “Architecture”.

<sup>87</sup> This would be implemented more easily in EU databases.

rather than ETIAS querying all the systems and databases. The data transmitted would be compared to the application data within ETIAS<sup>88</sup>.

In the event of a match or a hit in any system, the application would be transferred to the CMPE (and possibly a Member State if need be) for **manual processing**, similarly to what happens at the moment when an application is submitted. If the CMPE (and the Member State contributing to the decision-making) deem it justified in light of the new information, an already-granted authorisation can be revoked.

### Revocation

Should the CMPE decide to revoke an already-granted authorisation, it would update the authorisation status in the ETIAS IT application. The traveller would be notified of the revocation by an email sent to the address provided in the application form. The notification email would contain the reason for the revocation. As for denied authorisations, the reason for the decision would take the form of a generic paragraph describing why the authorisation was revoked and informing the applicant of the procedure for appealing the decision.

### Appeal process

The appeal process would differ depending on the entity accountable for the decision (the CMPE or Member State(s)):

- For variant 1 (one or several **Member State(s) are accountable for the denial or revocation** of the authorisation), the appeal would have to be brought before the competent authority of the Member State that have denied or revoked the application;
- For variant 2 (the **CMPE is accountable for the denial or revocation**), the appeal would have to be brought before the Court of Justice of the European Union (CJEU)<sup>89</sup>.

However, for ETIAS, the study considered supplementing this judiciary appeal process by an administrative one, in order to provide more convenience for travellers and alleviate the potential workload for the Court/national competent authorities.

In cases of denied or revoked authorisation, the applicant would be provided with the possibility to appeal the decision through the following procedure:

- The applicant would have to send an email to a dedicated email address. This email address would have been provided to him/her in the email notifying the denial or revocation of the authorisation (and/or through the ETIAS website or app). The notification email would provide the application number and clearly state the importance of providing this number in any communication related to the appeal. The possibility to appeal would be provided for a pre-defined period of time (e.g. three months)<sup>90</sup>;
- The email would be received by the competent unit within the CMPE, which would have to handle the complaint;
- If the applicant disagrees with the conclusion of the competent unit, or if the unit would not have responded to the applicant in due time, the applicant would have the possibility to appeal to a court.

The following table summarises the advantages and disadvantages of creating a competent unit within the CMPE that would be in charge of handling complaints:

*Table 18: Advantages and disadvantages of complaint-handling by the CMPE*

Advantages	Disadvantages
------------	---------------

<sup>88</sup> This would allow ETIAS to recheck already-granted applications in light of these new pieces of information. Such a solution would be more proportionate in terms of privacy than ETIAS searching for a match between all the already-granted applications and all the refusal of entry alerts in SIS and overstay cases in EES (as only data of data subjects concerned are exchanged). It would also be less demanding in terms of processing capacity.

<sup>89</sup> Article 263 of the Treaty on the Functioning of the European Union.

<sup>90</sup> In cases in which the pre-defined period of time has passed, the person would still have the possibility to submit a new application.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>- <b>Convenience for travellers:</b> compared to an appeal before the court/national competent authorities, this first step would be:               <ul style="list-style-type: none"> <li>o less cumbersome in administrative terms;</li> <li>o less costly; and</li> <li>o less lengthy.</li> </ul> </li> <li>- <b>Workload for the CJEU/national competent authorities:</b> they would have to handle fewer complaints, than if no complaint-handling took place at the CMPE, as this first step would allow for a number of them to be resolved.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Total number of appeals:</b> as the first step of the process would be less cumbersome, less costly and less lengthy, the number of appeals may increase (compared with a process with no step before having to bring a complaint before the court).</li> </ul>

As demonstrated above, the complaint-handling by the CMPE as a first administrative appeal step would provide more advantages than disadvantages. It is thus the preferred solution regarding the ETIAS appeal process.

## 2.4 Architecture

This section of the study provides an overview of the **ETIAS architectural design**<sup>91</sup>, as determined by the purpose and objectives of the system, and its potential impact on connected applications and systems.

### 2.4.1 Context

The EU IT landscape in the area of Migration and Home Affairs, and the border management domain in particular, is composed of several systems and databases. As highlighted by the communication of the European Commission "**Stronger and Smarter Information Systems for Borders and Security**"<sup>92</sup>, it is essential to exploit all the existing tools to their full potential and to avoid an increase of complexity of the European systems landscape and fragmentation of the data collected. **Interoperability** is, therefore, a key requirements and an important objective. Any new system introduced in this ecosystem should be able to interface with the others, avoid redundancy of the data stored and should aim at building synergies with existing systems.

This is of particular importance in the case of ETIAS, which – by nature of its purpose – needs to **draw on information currently stored in a number of the existing EU large-scale IT systems** (as identified earlier in the section 2.2 "Data").

### 2.4.2 Approach

Our approach for the definition of ETIAS architecture stemmed from the business processes defined in section 2.3 "Business processes", and followed the four main steps:

- 1) Identification of **architectural requirements**;
- 2) Definition of the **general architecture**: on the basis of the requirements previously identified, different options are assessed regarding the overall architectural vision (central vs. decentralised system(s) and for the high availability)
- 3) **IT architectural building blocks**: all the main building blocks of the IT architecture, required to support the business processes, are then identified and described
- 4) **Interoperability with other systems**: finally, the study describes the possibilities to create synergies with other European systems with particular attention at the possible integration with EES.

The ETIAS architecture definition also included consultations with relevant stakeholders, balancing implementation complexity, security, privacy and data protection, and performance considerations.

### 2.4.3 Architectural requirements

The following high-level architectural requirements have been identified, taking into account the ETIAS four main processes described in detail in section 2.3 "Business processes" and related business requirements:

- **Privacy by design**: the system would collect and store the personal information of millions of travellers and for this reason it is essential to ensure its security. Both security and privacy must be part of the architectural design. Data minimisation, strong access control and encryption are crucial elements in this regard;
- **High availability**: prolonged outages would have a negative impact on travellers, carriers and the overall security and integrity of border management in the Schengen Area. It is assumed that ETIAS will have the same availability targets as the VIS and EES as they also support the same business process, i.e. verification at the border;

---

<sup>91</sup> While the section provides a high-level design of ETIAS, it should not be considered as architecture requirement specifications, which will only be defined during the system design. The focus of the analysis at hand is the functional architecture and how to ensure a smooth integration of a new system within the existing landscape of European IT systems already in use for border management and security.

<sup>92</sup> "Stronger and Smarter Information Systems for Borders and Security", COM (2016) 205 final.

- **Scalability:** the ever-increasing number of travellers to the Schengen Area, the advancing discussions on visa liberalisation and the seasonality of traveller flows require an architecture that could be further expanded rapidly in case of need, especially for handling application traffic via the ETIAS website or app (see below). The possibility to dynamically allocate system capacity would be crucial in this context;
- **Interoperability:** the system must be interoperable with other systems and in particular query other databases with high frequency. It should be possible for ETIAS building blocks to be used in the future by other systems as well;
- **Legal compliance and auditability:** compliance with the existing legal framework must be ensured and it should be possible to monitor it through audits and accurate logging functionalities. Given the high impact that the system might have on travellers, strong governance (including access control) and accountability must be ensured at all times;
- **Keeping it simple:** unnecessary complexity should be avoided. Having well-defined modules would allow for an easier development, implementation and operation.

#### 2.4.4 General architecture

Given the requirements identified above, various options for the ETIAS architecture have been considered – this analysis is included in Annex 6. – “Architecture”. The analysis concludes that the preferred option for ETIAS is a **central architecture**, with a system **hosted by eu-LISA** in Strasbourg and a **second site** in Austria (Sankt Johann im Pongau). This set-up emerges as the most fit-for-purpose for IT infrastructure that would need to support a pan-European system and service.

A central architecture option is also the most aligned to the current architectures of comparable systems (e.g. VIS and EES) and is considered the most viable. As opposed to a fully (or partially) de-centralised system, it has the following advantages:

- Reduced implementation complexity (single system vs. integration of up to 30 systems, one for each Member State);
- Reduced costs, stemming from both the simpler design and higher economies of scale;
- Higher level of oversight and control thanks to an easier auditability and simpler accountability and ownership.

In terms of **connections**, travellers and carriers would be served through the **public Internet** and Member States would be able to connect to ETIAS through the **existing TESTA-ng network**<sup>93</sup>. A standardised National Uniform Interface would be the interface for Member States to access to the services provided by ETIAS Central system.

The Central Manual Processing Entity would also connect to ETIAS through TESTA-ng network.

## High availability

An active-passive setup of the two ETIAS datacentres (with a production environment in each) appears to be insufficient to meet the high availability requirement for ETIAS. In this case ETIAS could have two production environments in the main site working in active-active configuration locally, thus increasing redundancy and reducing the likelihood of needing a full switch-over to the back-up site.

The below figure illustrates the possible set-up.

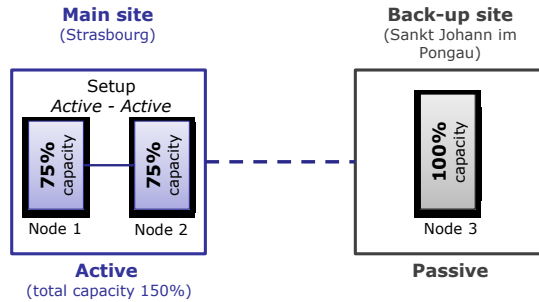


Figure 14: Possible configuration for ETIAS central system<sup>94</sup> to provide high availability

To avoid the deployment of an excessive overcapacity and to reduce costs, each instance would be sized at less than the required capacity (e.g. 75%). In fact, during normal operations the two instances, configured in “active-active” setup, would share the load and provide more than 100% of the capacity needed (e.g. 150% if each instance was 75%). If one of the two instances were to fail, then the system would still be able to provide services, although in “degraded mode” (as a single instance would be below the full capacity) with slower response times. This would last until either the system is fully restored or until the operations are switched to the back-up site.

While these measures are valid for the central system and database, the Internet-facing part of ETIAS, such as the access for travellers and carrier, might require additional measures aimed at mitigating possible DDoS<sup>95</sup> attacks. Such measures could range from using content delivery networks and other specific products to the replication of the website not only in Strasbourg and Austria but also within the DIGIT datacentre in Luxembourg or any other European Commission-operated data centre (further details regarding ETIAS security safeguards are described in section 2.6 “System security”).

Currently eu-LISA is carrying out specific studies aimed at increasing the availability of the current (and future) EU large-scale IT systems by exploring different set-ups for their respective two datacentres. For instance, by moving from the current active-passive setup to an active-active one or to a hybrid solution just like the one described above. ETIAS implementation and design should build on these results, leveraging on the lessons learned from other systems.

<sup>94</sup> The Internet-facing part of the system (e.g. the ETIAS website and app for travellers) would require specific measures for ensuring high availability, for the protection from possible DDoS attacks.

<sup>95</sup> Distributed Denial of Service.

## 2.4.5 ETIAS key IT architectural blocks

Two guiding principles have shaped the ETIAS key IT architectural blocks: (i) a central architecture and (ii) segregation between the public Internet and the ETIAS system. This results in a split between ETIAS central system and ETIAS Internet services as presented in the figure below:

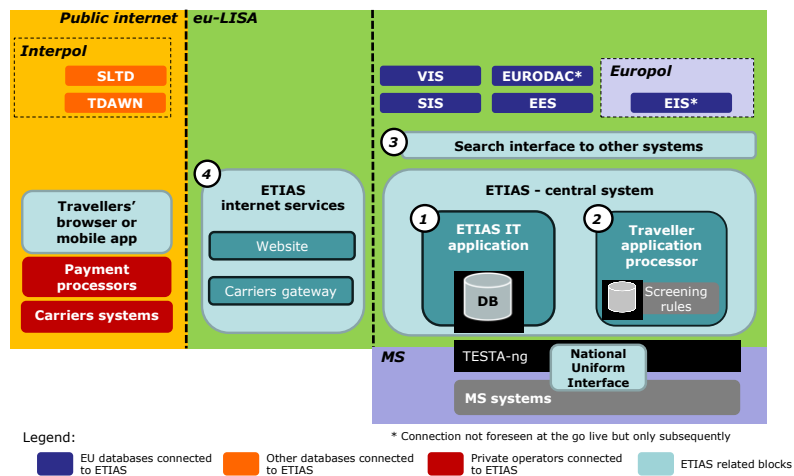


Figure 15: ETIAS high-level architecture

The main IT architectural blocks of ETIAS (as listed in the figure above) are:

1. **ETIAS IT application**, which would include a database of all the traveller applications lodged;
2. The **traveller application processor**, which would include a database of screening rules from Member States;
3. A **search interface to other systems**, which would allow querying other European and international databases as identified in section 2.2.5 "Risk assessment";
4. **ETIAS Internet services**, which would be the bridge between the ETIAS central system and travellers and carriers. They would include:
  - A **website** for travellers: the infrastructure supporting the ETIAS website or, possibly, mobile app to both submit a new application or to query the status of an existing travel authorisation without the risk of affecting the central system;
  - A **carrier gateway**: it would allow the connection of carriers and carriers' systems to ETIAS, to allow the check whether a passenger checking-in has or not a valid travel authorisation (see section 2.5.2 "Interacting with carriers" for more details about carriers' interaction with ETIAS).

ETIAS is then connected to Member States through a national interface. This interface provides services border systems and border guards. It also connects the relevant administration in charge of reviewing applications.

Table below illustrates the role of the ETIAS architectural blocks in each of the system’s four main business processes.

Table 19: Role of ETIAS building blocks in the ETIAS four main business processes<sup>96</sup>

ETIAS architectural blocks	1) ETIAS IT application	2) Traveller application processor	3) Search interface to other systems	4) ETIAS Internet services
<b>ETIAS main business processes</b>				
1) Application	✓			✓
2) Decision-making	✓	✓	✓	✓
3) Verification before boarding	✓			
4) Verification at the border	✓			

The remainder of this sub-section further details the main IT architectural building blocks.

### 1) ETIAS IT application

This module is the core of ETIAS and includes a **database containing all the applications lodged in the system** as well as the application layer encapsulating the database.

It provides all the services related to the management and update of applications, search services and ensures access control and logging. It is also connected to the ETIAS Internet services that interface with travellers.

Both Member States and the CMPE would be able to connect to the database, through the TESTA-ng network, for the purpose of manual processing. Member States would also be able to check if a traveller has/holds or not a valid travel authorisation by searching the system using passport data. They would access ETIAS services through the NUI, a standardised interface for national systems which was introduced within the Smart Borders Technical Study<sup>97</sup> as possible technical solution for EES.

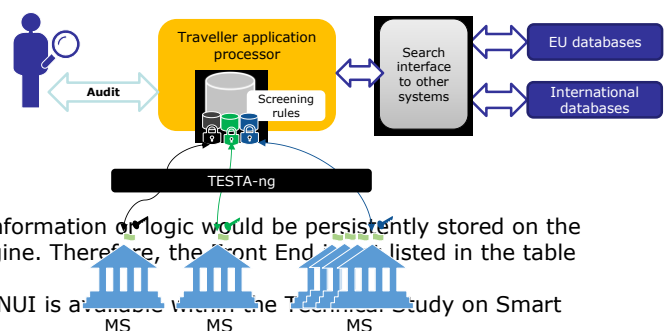
The database is expected to contain approximately 50 million of applications and respective decisions. With regards to the service level, the systems would have similar requirements as EES and the VIS, having to respond within few seconds to searches from border guards (the operation that requires the highest requirements for the SLA).

In addition to the main database, ETIAS IT application could also include a “dormant database” which would be used to store data not anymore needed for application processing (e.g. background questions or additional information requested to the traveller). The “dormant database”, as described in Section 3.2 “Data protection”, would be essential an archive for data with specific access rules for their access.

### 2) Traveller application processor

The traveller application processor would perform the **automated screening** of all applications lodged in the system. The use of a central traveller application processor would ensure a common approach in assessing the applications, at least for the first level of the decision-making process. The traveller application processor would:

- Query the pre-defined European and international systems for risk assessment purposes through the “Search interface to other systems”;
- Perform internal checks – e.g. check the presence of previously denied or revoked travel authorisations;



<sup>96</sup> Please note the assumption is made that no part of ETIAS information or logic would be persistently stored on the Front End. The Front End would only act as a presentation engine. Therefore, the Front End is not listed in the table above.

<sup>97</sup> A complete description of the possible functionalities of the NUI is available within the Technical Study on Smart Borders (2014), section 6.6.4.



- Apply screening rules to the incoming applications.
- Record an audit trail and allow for periodic audit of the system.

Moreover, Member States could potentially contribute to the screening rules, adding, for instance, investigation triggers (e.g. phone numbers, email addresses to be monitored) that would be stored encrypted, to ensure confidentiality, in the Travellers application processor.

*Figure 16: Traveller application processor*

### 3) Search interface to other systems

This component would provide a **single interface to search all the other European and international systems** that would need to be consulted within the decision-making process for a traveller application.

Having such a service provided by a separate component would increase the adaptability and re-usability of this service. New databases could be queried in the future simply by adding a new connection to the Search interface without interfering with the traveller application processor which would just consume the search services.

This component should therefore be easily **adaptable**, so that it could be updated in case of changes in any of the DBs consulted or if a new system is to be connected. An open solution, based on vendor-independent components would be preferable. Some Member States have developed comparable solutions that could be taken into consideration during the design phase or even reused if possible.

Having several systems involved in the decision-making process, which has severe constraints in terms of time and availability, will require putting in place SLAs and policies with other systems, defining clear **targets for response time and availability**. It will also be necessary to establish fall-back procedures in case one or more systems are unavailable, so as to limit the impact of outages of other systems on the overall availability and performances of ETIAS.

### 4) ETIAS Internet services

ETIAS Internet services would power the front-end of the system. Its objective is to provide services to travellers and carriers, through the public Internet, while saving ETIAS central system from the workload of the requests and also shielding it from possible cyber-attacks.

Services provided per user category:

- **Travellers:** ETIAS Internet services would support ETIAS website or mobile app (the section 2.5 “User interactions” elaborates further on user interactions) used by travellers to apply for a travel authorisation or to verify the status of their applications/authorisations. In addition, a notification or mail server would be used to notify the applicant of any changes of status.
- **Carriers** could connect to ETIAS to verify whether a person has a valid travel authorisation at check-in (further details on the interactions with carriers are also presented in section 2.5.2 “Interacting with carriers”).

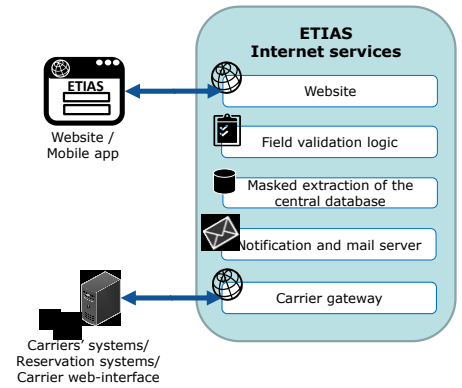


Figure 17: ETIAS Internet services building block

The components of ETIAS Internet services are the following:

- a. **Website:** ETIAS applications would be submitted online through a portal and possibly a mobile application. The ETIAS website would also be linked to a third-party payment processor that would provide the infrastructure for online payments. The requirements of the website are provided in section 2.5.1 “Interacting with travellers”.

Among the security features that would have to be adopted, it is expected that the web server will contain a security safeguard to protect it from injection attacks. In the case of an attack, additional executable code is injected in the field that is intended to enter traveller information. More details are provided in section 2.6 “System security”.

- b. **Field validation logic:** the information provided within the online application form is subject to some basic validation rules that would be essential to increase the data quality. See Annex 5. – “Business processes” for more information regarding the types of field validation.
- c. **Masked extraction of the central database:** in order to allow travellers and carriers to verify the status of a travel authorisation, ETIAS Internet services would include an extraction of the main database. This extraction would be a small sub-set of personal information (masked or encrypted), sufficient for identifying the traveller (e.g. application reference number, issuing country and passport number, name and surname) and the status of the related travel authorisation.
- d. **Notification and mail server:** once an application is approved, denied, revoked or in case a face-to-face meeting at a consular office is requested, a notification would be sent directly to the travellers using the contact details previously provided. The simplest option for the notification would be an email with a reference code that would identify the application submitted. Alternatively, the notification could be also sent to the mobile phone of the person. This channel could also be used to answer queries from the traveller regarding the status of his/her travel authorisation.

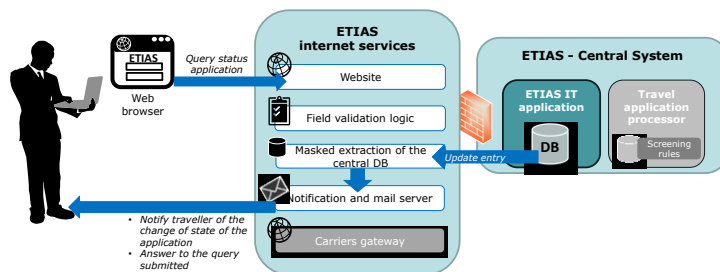


Figure 18: Information flow in case of: granting or denial of a traveller authorisation in the central system, or of query from the traveller

**e. Carrier gateway(s)**

Different channels and ways of connection should be provided by ETIAS to accommodate the different systems used by carriers according to their different technical capabilities usually linked to the carrier’s size or frequency of travels to the Schengen Area and that would have to connect to ETIAS.

The possible channels could be:

- i. **Dedicated “API-like” connection from accredited carriers to ETIAS Internet services.** Carriers, following an accreditation process, would have the possibility to connect directly their system(s) to an ETIAS server which, always on the basis of the masked extraction of the database would provide an answer within few seconds. This channel would allow carriers to reuse the infrastructure already developed for API transmission.
- ii. **Dedicated connection of the main reservation systems/networks to ETIAS Internet services.** Carriers often rely on dedicated IT systems to handle the reservation process. These systems could also be connected to ETIAS. The advantage would be for both carriers, that would not have to modify their own systems, and for ETIAS that would have to provide support to a reduced number of users.
- iii. **Web interface.** Smaller carriers could benefit from the possibility of using a web-interface to check the status of a travel authorisation. It would be an account-based website, carriers would have to first request credentials.
- iv. **Email channel.** As last resort, it could be envisaged that for special circumstances, the check could be performed by sending an email using a pre-agreed format and encryption. This channel could be used as fall back in case of issues with any of the above.

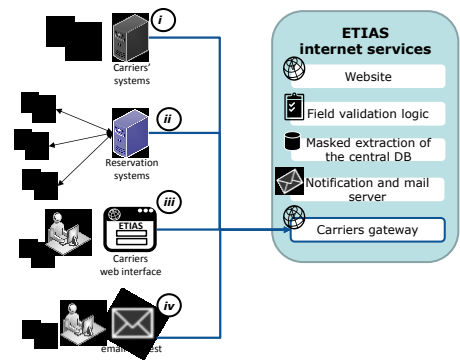


Figure 19: Possible communications channels with carriers

## 2.4.6 Interoperability with other systems

### ETIAS and the objectives for interoperability for European systems

The implementation of ETIAS could act as a catalyst for greater interoperability of information systems in the area of borders and security. It could support at least three of the four dimensions<sup>98</sup> identified by the European Commission’s April 2016 Communication on “Stronger and Smarter Information Systems for Borders and Security”<sup>99</sup>. Specifically, it would contribute to the following objectives for interoperability:

#### 1. Single search interface

The ETIAS “Search interface to other systems” would allow to query simultaneously all the relevant European systems in the field of border management and security and international databases. This component could be reused by Member States in the future, thus realising an occurrence of the “Single search interface” ambition of the Commission’s April 2016 Communication.

#### 2. Interconnectivity of information systems

Connecting ETIAS to other European (and international) databases would be an essential step to fully exploit information already available, particularly in the decision-making process. In this regard, ETIAS would be completely aligned with the objective of the communication, by automatically searching through other European databases for border management and law enforcement.

#### 3. Common repository of data

ETIAS could also become a constituent element of a “Common repository of data” – another aim expressed in the Commission’s April 2016 Communication<sup>100</sup>. More specifically, ETIAS data would be complementary to EES data which include data to identify the travellers, thus providing a source to cross-check: biographical data declared by the traveller could be compared with the data collected from the passport during the first enrolment within EES.

<sup>98</sup> a) Single search interface; b) Interconnectivity of information systems; c) Shared biometric matching service; d) Common repository of data.

<sup>99</sup> “Stronger and Smarter Information Systems for Borders and Security”, COM (2016) 205 final.

<sup>100</sup> Ibid.

## **Syntactic and semantic interoperability<sup>101</sup>**

Concerning existing systems, an important element to consider is the syntactic interoperability. Different fields might have a different encoding in different systems, using different representations, different conventions and even different alphabets.

ETIAS should adopt the same syntactic and data representation as EES in order to maximise the possible synergies between the two systems. ETIAS should also apply the same transliteration solutions as in the VIS and the SIS.

Moreover, the adoption of the **Universal Message Format (UMF)** should be considered in order to foster interoperability. The Universal Message Format proposed by Europol, is a standard XML-based data format and has been implemented for the main concepts used in law enforcement<sup>102</sup>. It allows mapping different databases to common concepts and data fields. While none of the European systems in scope (SIS, VIS or even EIS) is currently fully compliant with UMF, the adoption of a common model will be increasingly important in the future for the interoperability agenda.

Despite the best efforts of harmonisation and standardisation of the syntax of ETIAS, and given the high number of databases connected to it, it is likely some fields and codes will need to be translated by the system when interfacing with other systems.

With regards to the communication with carriers, in order to minimise the impact of this new system and to reduce the development required on their side it is recommended that the "carrier gateway" would follow the same standards and syntax as used for the transmission API/PNR. This would allow air carriers to reuse, at least partially, the infrastructure developed already.

## **Impact on other systems sizing**

Connecting ETIAS to European or international databases would necessarily increase the volume of requests and queries for these systems. Given the high volumes envisaged for ETIAS, this would most likely trigger specific investments.

The regular re-checks of the applications already granted could be particularly taxing for other systems as it could mean additional millions of queries. How and how often the re-check will be implemented (see section 2.3.6 "Support processes") will determine the magnitude of the impact. One scenario, the complete re-check of the entire database would imply between 40-100 million of queries done to other systems regularly. For comparison, the current capacity of the VIS is  $\approx$ 450 000 queries per hour.

An alternative option would have the databases transmitting new alerts to ETIAS, so that only these new elements would be re-checked. While this latter option would minimize the workload, it would entail specific development for all the databases involved (and amendments of the respective legal basis).

Given the number of variables to be considered (dependant on the final design of the system), specific impact assessments will have to be carried out before connecting to these systems, to precisely gauge the magnitude of the evolutions required, on the basis of the estimated volumes, on the re-check mechanism and on the agreed SLA for availability and response time.

## **Integration with EES**

Expected in 2020, EES will record biometric data and entry/exit history of third-country nationals travelling in and out of the Schengen Area. Given the nature of the data collected by EES (for identifying travellers) and the scope (about TCNs crossing Schengen borders), the possibilities of integration with EES are particularly interesting for ETIAS.

Below the study examines EES and ETIAS in order to identify and highlight possible synergies and interactions.

---

<sup>101</sup> Syntactic interoperability: two or more systems capable of communicating with each other by using specific data formats, communication protocols and standards.

Semantic interoperability: capability of two or more system to interpret the information exchanged meaningfully and accurately, for instance by using a common information exchange reference model or common ontologies.

<sup>102</sup> Universal Message Format, Europol, 2014: <http://bookshop.europa.eu/en/universal-message-format-pbQL0214410/> (accessed 08/2016).

### **1) Link between EES and ETIAS**

From a business point of view both EES and ETIAS support the same process (the border control) and there would be a strong interest in linking the declarative data provided by the traveller during the ETIAS application process, with the identification data contained in EES (the biometrics and the biographical data extracted from the passport).

The ETIAS and EES data sets could be linked (see Annex 4. – “Data”, section Data Model), just as it is currently foreseen between EES and VIS. This would allow creating a person-centric system, thus allowing the reconciliation of the data belonging to the same individual. The entry/exit data of a traveller would be linked to a passport, which would itself be linked to a travel authorisation (or a visa for visa holders). This would allow knowing which travel authorisation was used to enter the Schengen Area.

### **2) Integration of EES and ETIAS database**

ETIAS database could be implemented jointly with the EES database. Data belonging to one or the other system would be flagged accordingly so as to ensure each data is accessed by the authorised users of each system. Merging the two databases could create significant cost savings (less hardware, software, development, testing and operating costs) and as well be a step towards the creation of a common repository of data (see Commission Communication on “Stronger and Smarter Information Systems for Borders and Security”).

ETIAS data would not be used, however, to pre-fill EES’ individual files as ETIAS data is declarative, therefore inherently less reliable than the data EES would collect directly from the passport at the person’s first entry.

While in the case of VIS and EES the option of a full integration would have created significant risks of delaying EES as VIS is already a live system, in this case, the integration would be between two systems yet to be designed. EES design could then still be influenced and adapted before investments are done.

While the integration of the two systems could be highly advantageous in terms of costs and to reduce the overall complexity and fragmentation of the European systems, its viability will depend on the timing of the respective design phases (and ultimately on the respective legislative approval processes). Nevertheless the respective designs should allow for the possibility should both systems be approved.

### **3) Single web service for travellers and carriers**

Both systems foresee a web service for travellers and carriers, which would reply to simple queries using an extraction of the main database as a means to minimise the risks in case of breach. Hosting requirements and the competences needed would be the same. In light of this, the EES web service could be extended and enhanced to serve both systems. Moreover, it would be beneficial to present to travellers and carriers a single window to query the systems.

Before a new trip to the Schengen Area, a visa-exempt traveller would want to know whether his/her travel authorisation is still valid and if he/she has reached the maximum allowed number of days in the Schengen territory. The creation of two distinct web accesses would be only confusing for the traveller and potentially cumbersome for carriers that might need to connect their systems to another web service. Similarly, the “carrier gateway” should provide a single message answering for both ETIAS and for EES.

### **4) National Uniform Interface**

The National Uniform Interface (NUI) included in the current legal proposal for EES<sup>103</sup> could as well be extended to cover the functionalities of ETIAS. The NUI is the interface that would be used by Member States to access all the services provided by ETIAS (border checks, decision-making process and law enforcement access).

The multiplication of interfaces, systems and communication lines increases the complexity of the overall IT landscape. A common and standardised access point that would give access to all the services of the EU systems would reduce complexity and, in the long run, maintenance and testing costs.

---

<sup>103</sup> COM(2016) 194 final, “Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011”, European Commission, 06/04/2016

The NUI would orchestrate and route the messages received from the Member State to the right module (ETIAS or EES) providing a particular service, creating a European enterprise service bus, where even additional systems could be added in the future. Security and confidentiality would be still guaranteed by the access control and the encryption. It would be a step forward the creation of the "Single search interface"<sup>104</sup>.

Should the Single search interface already exist at the time of ETIAS implementation, then the NUI could just interface with it for the queries at the border and for the possible law enforcement access. It would still connect with ETIAS central system for the services related to the processing of travellers applications. The reuse of the NUI would be even more logical and necessary if ETIAS and EES were to be built within the same central database (as the NUI is part of EES), separated only at logical level, using different access rules.

### **5) Shared network**

EES and ETIAS could easily share the TESTA-ng network, avoiding the deployment of new access points and new lines. ETIAS traffic is expected to be much more limited compared to the traffic envisaged for EES, as no biometric information would be exchanged, but only few alphanumerical data.

A separation of the network level would in fact not yield any advantage in terms of security or data protection, and the traffic could still be separated at an application level.

---

<sup>104</sup> See "Stronger and Smarter Information Systems for Borders and Security", COM (2016) 205 final.

## 2.5 User interactions

This section analyses the different end-user requirements, looking at the ergonomics of the system for the travellers and the carriers.

### 2.5.1 Interacting with travellers

#### Benchmark analysis

A benchmark analysis on end-user considerations, summarised in the table below, is the foundation of the assessment performed, further developed taking into consideration the specificities of ETIAS.

*Table 20: Overview of end-user considerations in the benchmark countries*

	eVisitor	eTA	ESTA
<b>Number of webpages</b>	6	2	6
<b>Average time to fill-in the form</b>	10 minutes maximum	10 – 15 minutes minimum	20 minutes minimum
<b>Languages of the website</b>	Only English	2: French and English (explanatory forms available in 10 languages)	22
<b>Languages allowed for answering</b>	Only English	French and English	Only English
<b>Possibility for modification of data</b>	Yes	No	Yes
<b>Support for third parties</b>	Yes (only for some countries in the programme)	Yes	
<b>Fee</b>	Free	7\$	14\$ (free until 2010)
<b>Means of payment</b>	Non-applicable	Major credit cards	Major credit cards (inclusion of PayPal currently under discussions)
<b>Response time</b>	Automatically granted within minutes – 2 to 10 working days if manually processed	Automatically granted within minutes – 72 hours for feedback if manually processed	
<b>Request for additional information</b>	Yes		No
<b>Procedure if travel authorisation denied</b>	Visa	No visa, other possibilities	Visa
<b>Creation of an account</b>	Yes (before the application)	No (only if additional documents are needed)	No

## Time to fill-in the application

The time to fill-in a travel-authorisation application should be reasonable and not take more than **10-15 minutes** as the traveller should not need anything else than his/her passport, a credit card and an email address to apply. A lengthy application could negatively affect data quality and a cumbersome system could also deter travellers. The exact time would depend on:

- **the chosen dataset** (see section 2.2.6 “Data to be collected”);
- **the data-input method** (scroll-down menu, pop-up window or free field);
- **the user-friendliness and design of the website or mobile application.** For instance, while the US ESTA website is structured over six webpages including the payment, the Canadian eTA is only composed of two pages, giving the impression of being shorter than the American one for an almost similar data set.

It would also be important to inform upfront travellers of how long in advance they would need to apply and what would be the maximum period of time before receiving a feedback from the system. This would limit the number of late requests and avoid unnecessary uncertainty and stress for travellers. Overall maximum processing time for an application would have to be kept reasonably short to avoid being too constraining for travellers. As discussed in section 2.3 “Business processes”, ETIAS maximum feedback time could be up to 72 hours (although the final decision could take longer if an interview or more information is requested), aligned with the Canadian and US systems.

## Updating a submitted application

The study would recommend not having an account (i.e. no credentials), although this would limit the possibility to retrieve information afterwards, as it would increase the amount of data collected and increase the overall complexity for ETIAS that would have additional processes to manage.

Personal information should not, in fact, circulate by emails and the possibility to retrieve the entire application from the website or app would constitute a security threat if not protected with credentials. Updating information, after the submission of the application, would then be not allowed. The application should thus be filled-in and submitted in one attempt, adding importance to the user-friendliness of the website or mobile app which should be as simple as possible to minimise the number of errors from travellers.

An account could, however, be requested and created in case the applicant is asked to submit additional information as a part of the manual risk assessment.

*Table 21: Possibility to update an application: comparison of the benchmark systems*

Australia	Canada	US
<ul style="list-style-type: none"><li>• Update possible of some data</li><li>• Account based system to access them</li></ul>	<ul style="list-style-type: none"><li>• No update possible</li><li>• Account only in case further information are requested</li></ul>	<ul style="list-style-type: none"><li>• Update possible of some data</li><li>• Access using unique tracking number (or application number), the date of birth and the passport number<sup>105</sup></li></ul>

<sup>105</sup> If a traveller loses, forgets, or does not have access to his/her application number or travel status, he/she can retrieve the application number through the ESTA website or app by entering the name, date of birth, passport number and passport issuing country.



## Language requirements

Language availability plays an important role in the overall ergonomics of the systems. The lack of guidance alongside with a possible language barrier can lead to low data quality due to the increased risks of errors. The following tables shows the major language requirements that should be foreseen on the basis of the current 61 visa-liberalised countries:

Table 22: Top eleven languages spoken in the VE countries<sup>106</sup>

Top 11 languages	Volume
English	393,149,301
Spanish	358,803,804
Portuguese	210,779,165
Japanese	126,323,715
Korean	50,503,933
Malay	31,180,476
Mandarin	29,092,106
Serbian	9,438,806
Arabic	9,266,971
Hebrew	8,192,463
Cantonese	7,943,374
<b>Total</b>	<b>1,234,674,114</b>
<b>Total different alphabet</b>	<b>271,941,844</b>
<b>Total latin alphabet</b>	<b>962,732,270</b>

Handling multiple languages and alphabets would create a significant burden for the processing of the application and potentially even jeopardise the accuracy of the assessment. The Canadian system takes an interesting approach for this challenge. While the form is available only in French and English (and inputs are accepted only in these alphabets) the online help is available in several languages. Similarly ETIAS could be available in limited number of languages while maintaining an extensive multi-language support.

Moreover, the use of multiple-choice questions and/or drop-down boxes would mitigate the issue of supporting multiple languages. Not only it would be easier for travellers, but the possible answers could be encoded and translated in Member States' languages so as to facilitate the processing of the applications once received.

Lastly, allowing third-parties to fill-in the form on behalf of travellers could be a mitigation measure for a low number of languages available in the application form.

### Support to the travellers

The following services could be made available to applicants:

- **Self-service help portal** with an extensive Frequent Asked Questions (FAQ) page in order to limit the number of queries via email and phone. This service should also be available in different languages.
- **Email contact.** Travellers could also have the possibility to contact support in writing through embedded forms in the website or mobile application. This instead of a simple email address would help categorising the requests and possibly avoid the use of this channel to resolve claims and consequently transmit personal information on a potentially not secure channel.
- **A helpline 24/7.** For specific questions or issues not solved through the self-service help portal, a dedicated team would be available to support travellers. The CMPE could manage the support to travellers and exploit the feedback received to improve the website/app and identify possible IT issues.

For any of these services, a minimal set of languages should be available in order to cope with the majority of applicants. On the basis of the most spoken languages in VE countries, English, Spanish and Portuguese would already cover 77% of the visa-exempt population.

Lastly, and as highlighted in the architecture section, both EES and ETIAS foresee a web service for travellers. Before a new trip to the Schengen Area, a visa-exempt traveller could then receive an

---

<sup>106</sup> Source: PwC, 2016.

aggregated answer on both the validity of his/her travel authorisation (ETIAS) and on how many days is he/she allowed the stay in the Schengen Area (EES).

### Third-party data collection

All the benchmarked systems allow third parties such as travel agents to **apply on behalf of traveller** (Australia only allows some EU countries to also apply through a third party). Although it is expected that they might require an additional fee, this possibility would still be beneficial to counter issues some applicants may face, such as low access to an Internet connection, computer or credit card.

Specifically to Internet access, the most recent average Internet users' rate for the visa-exempt countries is 70%<sup>107</sup> (by comparison, the European Union's rate is 78.1%). While the US, which account for almost 26% of the VE population, has a very high rate (87.4%), this rate varies significantly across VE countries<sup>108</sup>. Given the growing numbers of phone subscriptions worldwide and Internet access on mobile platforms, making ETIAS available in both computer and mobile application could increase its reach and user friendliness.

### Conclusion

The following **guiding principles** should drive ETIAS user interactions with travellers:

- Data collection
  - There should be a single interface and an EU-wide application form;
  - Minimal manual input and as much automation as possible through the use of drop down menus, tick boxes, confirmation of data input, etc.;
  - The data fields should be explained and support material should be available for applicants;
  - The data should be known by the applicant and only a passport, a credit card and an email address should be necessary to apply;
  - A user-friendly website and possibly a mobile application will be key for limiting the number of errors. For instance, a good practice can be observed in the eTA system (Canada), where the website asks at the beginning of the application process for the applicant's nationality and the means of travel (air, sea or land).
- Languages
  - There is no need for the form to be translated into all the official EU languages;
  - ETIAS should only collect data in Latin alphabet;
  - However, limiting the language of data input should be compensated by help services and additional material being available in more languages (Spanish and Portuguese at least).
- Support
  - The more information is available on the website or via the app, the less workload the support services will have. A clear and user-friendly website/app would also increase data quality.
- Awareness
  - A communication campaign should be launched, similarly to what was done for the VIS roll-out, in order to inform travellers on the new requirement. Different institutions should be involved in this process: at EU level (Commission's website and communication channels) and at Member State level (especially with consular offices). In Canada, the Citizenship and Immigration Department displays a message briefly explaining the eTA on all its websites<sup>109</sup>.

---

<sup>107</sup> The average Internet users' rate for VE countries is 55.9%, and the data weighted on the total population is 70%. For details on the statistics, refer to Annex 7. – "User interactions". Source of the data: International Telecommunication Union, World Telecommunication/ICT Development Report and database and World Bank estimates. See: <http://data.worldbank.org/indicator/IT.NET.USER.P2> accessed 09/2016).

<sup>108</sup> The lowest value for internet penetration is East Timor: 1.1%.

<sup>109</sup> See: <http://www.cic.qc.ca/> (accessed 25/07/2016).

The table below summarises the possible issues applicants may encounter and suggests mitigating measures:

*Table 23: Applicants' possible issues and possible mitigating measures*

<b>Issues</b>	<b>Possible mitigation measures</b>
<b>Internet – computer access</b>	<ul style="list-style-type: none"> <li>• ETIAS kiosks in major airports worldwide;</li> <li>• ETIAS kiosks in major consular offices worldwide;</li> <li>• ETIAS kiosks and Internet hot-spots at land border-crossing points, with the possibility to pay by cash;</li> <li>• Allow third parties to lodge the application on behalf of the traveller;</li> <li>• Mobile ETIAS app to lodge application.</li> </ul>
<b>Access to a credit card</b>	Allow for other types of payment: <ul style="list-style-type: none"> <li>• PayPal;</li> <li>• Through third parties;</li> <li>• Cash (although it would create numerous logistic and organisational challenges, it could be an option to consider for specific circumstances);</li> <li>• Mobile phone payment means</li> </ul>
<b>Access to the consular office (in case of interview)</b>	Allow for uploading additional documents online.
<b>Language barrier</b>	If the system has limited language options, explanatory factsheets should be made available.
<b>Doubts about the system and outcome of the application</b>	Q&As, hotline (also useful to spot errors in the website/app through travellers' feedback).
<b>Knowledge of the new requirement</b>	<ul style="list-style-type: none"> <li>• Large-scale communication campaign, involving different stakeholders (European Commission, carriers, consular offices, etc.);</li> <li>• Grace period in the implementation period;</li> <li>• ETIAS kiosks to apply on the spot.</li> </ul>
<b>Last minute applications</b>	<ul style="list-style-type: none"> <li>• ESTA Internet kiosks are available worldwide (like in Schiphol airport for instance) which allow passengers to apply for a travel authorisation onsite, receive the confirmation, purchase the flight tickets and board on the plane. This solution could be interesting for ETIAS, including at land borders where people could arrive unaware of the requirement.</li> </ul>

## 2.5.2 Interacting with carriers





### Carriers obligations

Carriers are currently legally obliged to verify that the passengers hold a valid travel document and, if applicable, a valid visa<sup>110</sup>. If a traveller is refused at the border, the carrier bears the responsibility and the cost of return to the country of origin. In addition, if the person transported was refused due to a lack of necessary travel documents, the carriers also has to pay a penalty between a minimum of 3.000 and a maximum not inferior to 5.000€ per passenger. In the future, with the implementation of EES and the abolition of the passport and visa stamping, carriers will comply with their obligations by connecting with EES<sup>111</sup>. The table below summarises the main obligations currently expected.

<sup>110</sup> Article 26 of the Schengen Convention and Articles 2 to 6 of the Directive supplementing the Schengen Convention (2001/51).

<sup>111</sup> EES legislative proposal, Article 12 paragraph 2, COM (2016) 194 final.

Table 24: Summary of the obligations for carriers

Legislation	Carrier	Responsibility
<ul style="list-style-type: none"> <li>• Schengen Convention 1990</li> <li>• Directive supplementing the Schengen Convention (2001/51)</li> </ul>	 All types of carrier	<ul style="list-style-type: none"> <li>– Assume the responsibility and implement the necessary measures to ensure that passengers are in possession of a valid travel document</li> <li>– Carriers are obliged to return the aliens to the country of origin if the entry is refused.</li> <li>– Penalties to carriers can be applied by MS:                             <ul style="list-style-type: none"> <li>○ The maximum amount is not less than 5,000 euros</li> <li>○ The minimum amount is not less than 3,000 euros</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>• API Directive (2004/82)</li> </ul>	 Air carriers only	<ul style="list-style-type: none"> <li>– Carriers are obliged to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State.</li> </ul>
<ul style="list-style-type: none"> <li>• PNR Directive (2016/681)</li> </ul>	 Air carriers only	<ul style="list-style-type: none"> <li>– Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats and insuring an appropriate level of data security:                             <ul style="list-style-type: none"> <li>(a) 24 to 48 hours before the scheduled flight departure time; and</li> <li>(b) Immediately after flight closure</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>• EES (Legislative proposal not yet approved – Article 12 COM(2016) 194 final)</li> </ul>	 All types of carrier	<ul style="list-style-type: none"> <li>– Carriers may use the secure Internet access to the web service to verify whether or not TCN holding a single or double entry visa have already used the visa.</li> <li>– The carrier shall provide the following data:                             <ul style="list-style-type: none"> <li>○ The short stay visa sticker number, including the three letter code of the issuing MS,</li> <li>○ The type of visa,</li> <li>○ The date of end of maximum duration of the stay</li> </ul> </li> <li>– The web service shall on that basis provide the carriers with an OK/NO OK answer</li> </ul>

As described in section 2.3 “Business processes”, ETIAS would then add a new requirement for the carriers, which would have to verify whether a traveller has also a valid travel authorisation. Land carriers would not be required to perform a systematic check of their VE-TCN passengers which was assessed as not feasible and incompatible with the current way they operate: without a check-in process and with no verification of the identity of the passengers. Nevertheless, the possibility to connect to ETIAS would be available for all carriers, including for land carriers should they wish to perform the verification so to minimise the number of travellers that they would have to return in case of refusal of entry by the border guards.

Despite the new obligation ETIAS is expected to bring benefits for carriers. By pre-checking the Schengen Borders Code entry condition, ETIAS should help reducing the number of refusals of entry at the border, thus reducing costs for carriers which would have to bring the refused passengers back.

### Carriers requirements

Travel authorisation systems are not a novelty for many air carriers which had already to connect and comply with similar systems (e.g. US ESTA). As a result ETIAS can benefit from their lessons learned. IATA<sup>112</sup>, the International Air Transport Association, and ICAO<sup>113</sup> have issued some guidance regarding the best practises that could be adopted in order to minimise the impact on carriers. On the basis of IATA and

<sup>112</sup> “Best Practice for Electronic Travel Systems”, IATA/CONTROL Authorities Working Group, 27 October 2015, available at: [https://www.iata.org/iata/passenger-data-toolkit/assets/doc\\_library/03-interactive\\_api/IATA%20CAWG%20Best%20Practice%20for%20Electronic%20Travel%20Systems%20revised%202016\\_v1.pdf](https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/03-interactive_api/IATA%20CAWG%20Best%20Practice%20for%20Electronic%20Travel%20Systems%20revised%202016_v1.pdf) (accessed 09/2016).

<sup>113</sup> Working Paper – Facilitation Panel (FALP) Ninth meeting, ICAO, FALP/9-WP/12, 4-7 April 2016.

ICAO best practise documents and of the input received from carriers associations consulted during the preparation of the study, the following main requirements were identified:

*Table 25: Summary of carrier requirements for travel authorisation systems*

Requirement	Description	How ETIAS address it
API-like connection	Connection to ETIAS should be <b>harmonised to the existing interfaces/systems for API transmission</b> . Ideally, the verification of the travel authorisation should take place as answer to the transmission of API data, through an interactive API system.	ETIAS carrier gateway supports an API-like messaging type, delivering a clear, concise and fast answer. Further details on the communications with carriers are described below.
Regular re-check	<b>Travel authorisation should be re-checked regularly</b> to reduce the likelihood of a refusal of entry at the border despite a valid travel authorisation.	ETIAS includes regular automated re-checks of the travel authorisations (see section 2.3 "Business processes")
Minimise the impact for travellers	ETIAS should not deter passengers from travelling. This can be further broken down in the following aspects: <ul style="list-style-type: none"> <li>• <b>Limited cost for travellers.</b> Fees charged should only be for cost recovery and not serve as a source of revenue for other government programs.</li> <li>• <b>Validity for a period of time.</b> A one-time application per passenger, allowing for multiple entries over a set period of time.</li> <li>• <b>Robust and user-friendly electronic lodgement platform.</b> The online application should be easy to use for travellers. Tools should be built into the application to assist individuals to avoid errors when completing the application form.</li> <li>• <b>No Paper.</b> An electronic notification to the passenger should be sufficient and replace paper evidence of an individual's approval for travel.</li> </ul>	ETIAS design is fully aligned to the requirements.
Fall back procedures	<b>Back up procedures</b> in the event of a system outage should be put in place, such as the introduction of a 24/7 support line.	ETIAS includes a 24/7 support line for technical issues on top of a design ensuring high availability. Additional fall back procedures will have to be defined in the design phase.
Information campaign and implementation	<ul style="list-style-type: none"> <li>• ETIAS should develop <b>communication strategies</b> in <b>multiple languages</b> in cooperation with other governments, travel industry and airlines.</li> <li>• ETIAS should foresee a <b>grace period</b> of time after implementation where passengers are allowed entrance into the Schengen Area but informed of the new requirements.</li> </ul>	ETIAS implementation will be accompanied by an extensive information campaign for travellers. A voluntary to mandatory (including grace period) roll-out is the highest scoring option for the ETIAS implementation (see section 2.7 "Implementation approach").

### **ETIAS, API and PNR**

Air carriers already transmit data to Member States before departure: API and PNR data. Sea carriers transmit passenger manifests, which are equivalent to API for air transport. ETIAS checks would then be yet another submission. It is then clear that, from the carriers' perspective, ETIAS should be as integrated as possible with these systems. ETIAS should allow for the same messaging conventions, so that same message for API or PNR, could be transmitted to two systems at the same time, thus reducing the development necessary on carriers side. For similar reasons the future EES check (i.e. check via web service whether a person has or not consumed a single or double entry visa<sup>114</sup>) could also take place simultaneously with the ETIAS check. The figure below shows the possible timeline for data transmission for air carriers for the different systems.

<sup>114</sup> EES legislative proposal, Article 12 paragraph 2, COM (2016) 194 final.

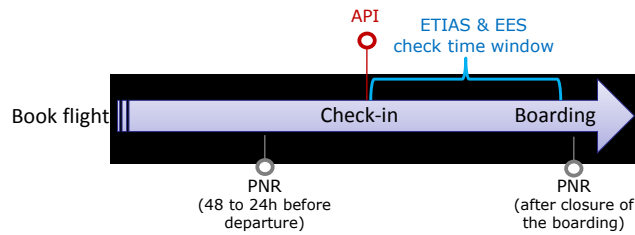


Figure 20: Timeline data transmission for air carriers

Differently from API and PNR, where carriers transmit several information, the verification of ETIAS would be done simply transmitting few data fields like passport number, issuing country and surname.

An increasing number of countries around the world are moving towards the implementation of interactive API, which, following the transmission of the API data, would provide to carriers with an ok/nok answer. This is, for instance, what will be also implemented in Canada to complement their eTA system.

However, the option of an interactive API system was assessed as not viable within the current European context. API is, in fact, not a central system, but rather data collected by Member States. ETIAS would not be able to answer to an API transmission. Updating all API infrastructures within Member States, to allow the retrieval of the ETIAS status, would be significantly more costly and increase uncertainties and the risk of delays due to the diversity of the national systems. Similarly, the recent PNR Directive established the PNR system as a decentralised system, therefore, the same considerations described above for API would also apply.

A revision of the API directive is currently being discussed. Such revision could bring new elements regarding the treatment of API data, for instance by centralising them. The option of an interactive API could then be re-assessed in light of the new possibilities.

### Carriers connections

Carriers would connect to ETIAS through the “carrier gateway” described earlier within the Architecture section, with different connection modalities designed to accommodate carriers needs depending on their size and infrastructure. This setup follows the design currently adopted by the Canadian system.

- a) Direct connection between carriers and ETIAS using an API format of messaging;
- b) Service provider/reservation systems connected to the central system. Most air carriers are connected to few specialised networks and reservation systems that could be used to offer ETIAS to carriers;
- c) Web-interface. A web-interface would allow for manual checks.
- d) Email using pre-formatted file.

Collaboration with both carriers and their service providers would be essential during the design phase, to ensure that the roll-out will be smooth.

To avoid a multiplication of interfaces to carriers the integration with the EES web service is considered to be the preferred option. That would, however, require that the EES design takes into consideration ETIAS requirements, especially considering the format used for the messages exchanged that would have to be compliant with API. Carriers would then receive a single message answer for both systems (e.g. ok, no ok EES, no ok ETIAS, not found, no ok).

The below table provide an overview of the different connection modalities in the benchmark systems:

Table 26: Overview of connection modalities in comparable systems

Country	Connection
Australia	Australia has a working in partnership with the Société Internationale de Télécommunications Aéronautiques. All requests from travel agents or airlines reservations systems, whether they are applications for ETAs or enquiries on visa status, pass through the host-based Request Capture system.

Canada	<p>Carriers can send API/PNR data to the Canada Border Services Agency (CBSA) using any of the following authorised method of transmission:</p> <ul style="list-style-type: none"> <li>○ Connecting directly to the CBSA data acquisition system</li> <li>○ Arranging for a service provider to connect on the carrier’s behalf</li> <li>○ Sending the data via email</li> <li>○ Using the CBSA Internet API Gateway.</li> </ul> <p>Canada foresees the implementation of an Interactive API system.</p>
US	<p>Carriers have dedicated connections to ESTA so that they can verify whether a passport has a valid ESTA and whether the person can obtain a boarding pass and embark on the plane. The data used to query the system comes from Advanced Passenger Information System, specifically the passport number, issuing country and country of citizenship. Airlines verify ESTA at check in.</p> <p>Carriers must register through an online procedure to receive the accreditation.</p>

### Support and testing

Before connecting to ETIAS carriers would have to obtain accreditation to connect to ETIAS. Although carriers would only connect to the carrier gateway within “ETIAS Internet services” and not to the main database (ETIAS IT application), they would still have the responsibility to ensure the security of their systems and to adopt appropriate security safeguards to prevent the misuse of the connection.

ETIAS would provide technical support for carriers with a 24/7 helpdesk, so to have a timely response in case of issues or outages. Carriers should have back-up systems or fall back procedures to ensure to be able to comply with the obligation even in case of system outage on their side.

The testing activities could be facilitated by providing a simulator of the ETIAS carrier gateway, which could be used by carriers during development. Moreover, a testing environment should be made available for carriers or service providers testing the direct connection to ETIAS. Allowing the connection of service providers and reservation systems could provide a simpler way for establishing the connection with ETIAS with very limited development activities for each carrier.

Carriers, or their industry partners, planning system changes that might affect their information transmission should notify the eu-LISA at least six months before the changes are implemented (only in the case of direct connection with ETIAS) to allow sufficient time for planning and performing testing activities..

## 2.6 System security

xxxThis section presents an **overview of the main security risks scenarios** and the **approaches suggested to mitigate them**, focusing on the security of data exchange rather than on infrastructure security. Hence, this section presents a risk assessment composed of the risk identification followed by a risk analysis according to different risk scenarios.

The security section is structured in three parts. The essential concepts are described here and a more detailed elaboration can be found in Annex 8. – “System security”.

### 2.6.1 Context

ETIAS would provide application services via the public Internet for visa-exempt third-country nationals, and would exchange and process sensitive data regarding the travellers, the application and its status. By providing these via the public Internet, ETIAS is exposed to different security threats, related to Confidentiality, Integrity, Availability and Privacy (CIAP). Studies<sup>115</sup> indicate a continuous and significant increase of cyber security threats; 33% per year.

Cyber threats can lead to consequences that directly affect a traveller’s application and the integrity of ETIAS infrastructure. For instance, a Distributed Denial of Service (DDoS) will make the system unavailable for the applicants and for other end-users (MS, border guards, and EU agencies). Other adversarial events such as hacking of content can affect the integrity of the data, and further compromise applicant’s information affecting ETIAS ability for correct verification of status. In addition, ETIAS application system relies on the travellers to perform their applications using independent platforms outside the control of ETIAS, which may be vulnerable to adversarial threats, such as malware on software.

At the same time, ETIAS processes and exchanges large amounts of sensitive data in a complex manner presenting challenges to data privacy. It is thus important to adopt the concept of privacy by design, and implement the correct security controls to address data privacy issues and be conformant with the new General Data Privacy Regulation, as described in section 3.2 “Data protection”.

### 2.6.2 Purpose

The purpose of the security risk management is to identify potential technical and security problems within ETIAS design so that risk-handling activities may be planned, invoked and implemented as needed in the system to mitigate adverse impacts.

ETIAS facilitates the application process for the travellers, EU agencies and the involved Member States, through a generalised and automated process. Therefore, it collects, transmits and processes large amounts of sensitive data, making security a crucial requirement to assure confidentiality and integrity of the exchanged and processed data.

Hence, it is important to ensure the confidentiality of the data through access control and encryption, protecting unauthorised entities and processes to access the data and avoid unwanted disclosures of information. Similarly, the integrity of the data exchanged and processed in ETIAS is very important, as travellers insert sensitive data in the system, which are then used to evaluate their application. However, if the data is tampered with (changed, corrupted) the traveller may see his/her authorisation denied, or the system may grant an authorisation from a fraudulent application.

The following sections elaborate on a security risk assessment covering possible security risk scenarios, following the **ISO 31000 standard**.

---

<sup>115</sup> The Global State of Information Security® Survey 2016, <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html> (accessed 07/2016).



### 2.6.3 Approach

The approach used for the risk assessment of the security aspects throughout this study follows the ISO 31000 standard. The underlying paradigm is summarised as:

- Threat agents describe concrete actors that have the capability to perform activities intended to negatively impact ETIAS processes. The latter are referred to as the assets at stake, as described in the section 2.3 "Business processes". Threat agents can belong to one or more threat groups such as Nation State, organised crime, hacktivists, and insiders;
- Risk scenarios describe such activities. For each risk scenario, probability and impact needs to be evaluated. In the present security risk analysis, impact is classified in two dimensions. The first dimension is the type of negative effect, distinguished between Confidentiality, Integrity, Availability and Privacy (CIAP). The second dimension is the party that undergoes this negative effect, distinguished between traveller, border guard, and competent authority<sup>116</sup>;
- The present analysis is part of a feasibility study, meaning that the analysed system is not in operation, has not been built, and has not been formally designed. Therefore the risk assessment focuses on potential impact rather than on probability. As ETIAS is not implemented and estimating probability is a function of how safeguards are implemented and operated, probability is left out of the current risk equation. It is assumed that the safeguards are correctly implemented following the good security practises to create a risk impact hypothesis. Risk scenarios also considered the privacy impact (dimension 1);
- Safeguards are security controls that have as objective to mitigate these negative effects. Such mitigation can be based on preventive, detective, and corrective controls, or a combination thereof.

### 2.6.4 Threat agents

The different threat agents considered along with the practical implications on the different actors are summarised in Annex 8. – "System security".

### 2.6.5 Risk scenarios

In total, 37 risk scenarios have been elaborated and documented in Annex 8. – "System security". From this set, a selection of the 13 scenarios that were evaluated to have the highest possible impact are presented in this section. These risk scenarios have been elaborated in terms of threat agents, storyline, and impact in the two dimensions (CIAP and impacted party). The following combinations were evaluated as having the greatest need for mitigating safeguards:

- **Confidentiality:** risks of disclosure of traveller's sensitive information to unauthorised entities or processes. (impact: **High**);
- **Integrity:** risks associated to possible modification or deletion of travellers' sensitive information stored, processed and transferred in ETIAS in an unauthorised and undetected way. (impact: **High**);
- **Availability:** risks of lack or block of the accessibility and use of ETIAS by authorised entities. (impact: **Moderate**);
- **Privacy:** risks to access and disclosure of any personal identifiable information (PII) of travellers by unwanted entities. (impact: **Moderate**);

The different risk scenarios include the practical impact on travellers, on competent authorities and on border guard authorities. This section summarises the most important scenarios along with the practical impacts, whereas a more descriptive overview of the set of scenarios is included in Annex 8. – "System Security". The impact of each scenario is classified according to the two dimensions ("type of effect" and "impacted party"). The first dimension is used to prioritise the risk scenarios. The scenarios related to confidentiality and integrity are classified to have a 'high' impact, whereas availability and privacy scenarios are classified to have a moderate impact.

---

<sup>116</sup> The competent authorities denomination considers the stakeholder's group composed by any EU agency and Member State authorities that connect and operate ETIAS.

Impact dimension 1 is described in the table below. Impact dimension 2 is described in the subsequent table.

Table 27: Risk scenarios overview – dimension 1

Risk Scenario	Impact dimension 1 Type of effect
<p><b>RS.01 Information Disclosure</b></p> <p>The threat agent obtains access to sensitive information of travellers or other ETIAS storage, exploring access control policies misuse, cryptographic flaws such as key misuse (private or secret key exposed by travellers) or software bugs and vulnerabilities.</p> <p><b>Threat Agent:</b> Hacker (Nation State, organised crime, Hacktivist)</p>	<p>Confidentiality</p> <p>Privacy</p> <p>A Nation State or a Hacktivist might try to discredit the ETIAS system and its responsible agency by divulging sensitive information on a sufficiently large scale. In this way the confidentiality of the VE-TCN will be impacted, and this might lead to reputational damage for ETIAS and its Agency.</p> <p>Organised crime actors might use this information to support ransom crimes.</p>
<p><b>RS.02 Eavesdrop</b></p> <p>The threat agent eavesdrops the communication between the traveller and ETIAS, or between ETIAS Central System and the Member State. The threat agent can retrieve full or partial traveller application information, and steal payment information or credentials.</p> <p><b>Threat Agent:</b> Hacker (Nation state or organised crime), or privileged employee/supplier/vendor/partner (organised crime)</p>	<p>Confidentiality</p> <p>Privacy</p> <p>Large scale sales of re-usable payment information such as credit card information</p> <p>Misuse of stolen credential to craft further attacks</p>
<p><b>RS.03 Cryptographic breach</b></p> <p>The threat agent performs attacks to the confidentiality and integrity information and data exchanged relying on cryptography protocols:</p> <ul style="list-style-type: none"> <li>• Algorithm breach (the algorithm is broken, this applies to one-way functions, symmetrical and asymmetrical encryption algorithms);</li> <li>• Key breach (the private or secret key is exposed or weak);</li> <li>• Key misuse (an authorised users uses a key for a non-authorised purpose);</li> <li>• Protocol or scheme breach (the protocol (e.g. mutual authentication) or scheme (e.g. encryption or signature scheme) is broken).</li> </ul> <p><b>Threat Agent:</b> Hacker (Nation state, organised crime, Hacktivist)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>A cryptographic breach may result in a lack of trust in the system</p>
<p><b>RS.04 Rerouting</b></p> <p>The threat agent reroutes the connection from VE-TCN to ETIAS, or from any ETIAS component connection to an adversarial component and channels that lack authentication. This may provide travellers to follow an invalid application process or the threat agent to perform man-in-the-middle attacks.</p> <p><b>Threat Agent:</b> Hacker/Privileged employee (organised crime or Hacktivist)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>Privacy</p> <p>This may result in a lack of trust in the system</p>

Risk Scenario	Impact dimension 1 Type of effect
<p><b>RS.05 Third-Party Communication</b></p> <p>The threat agent performs unauthorised monitoring and/or modification of communications to third-party components, while exploring existing vulnerabilities at the third-party components. This affects any interface with third-party components and web-services, such as:</p> <ul style="list-style-type: none"> <li>• External databases (EES, SIS, VIS, etc.);</li> <li>• External payment providers;</li> <li>• Traveller's communications.</li> </ul> <p><b>Threat Agent:</b> Hacker (Nation state, organised crime, Hacktivist)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>Privacy</p>
<p><b>RS.06 Software bugs/vulnerabilities</b></p> <p>The threat agent exploits coding bugs or design flaws (e.g. buffer overflows, improper validation of input) in ETIAS systems in order to gain unauthorised access to obtain or alter traveller information available databases of ETIAS.</p> <p><b>Threat Agent:</b> Hacker or privileged employee (Organised crime, Hacktivist)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>Privacy</p>
<p><b>RS.07 Authentication</b></p> <p>The threat agent performs integrity and access control attacks, exploring authentication and communication vulnerabilities among the different ETIAS components, travellers, and third-party services (payment providers, Member State interfaces, EES, SIS, VIS...). In this attack the threat agent could obtain unauthorised control (hijacks) of a pre-existing and legitimate network session between the ETIAS components, or between ETIAS and the travellers.</p> <p><b>Threat Agent:</b> Hacker or Privileged employee (Nation state, organised crime)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>Privacy</p> <p>Misuse of authentication failures to craft further attacks</p>
<p><b>RS.08 Credentials Forgery</b></p> <p>Credentials forgery (fraudulent alteration) to gain unauthorised access to ETIAS or to traveller personal information. This affects the systems and the traveller's online and personal credentials (ETIAS login credentials, ETIAS application information, identification documents).</p> <p><b>Threat Agent:</b> Hacker or Privileged employee (organised crime)</p>	<p>Integrity</p> <p>Privacy</p> <p>Misuse of authentication failures to craft further attacks</p>
<p><b>RS.09 Insider</b></p> <p>The threat agent performs adversarial or accidental internal actions that delete, block access to information and tamper with VE-TCN applications (e.g. altering sensitive information, granting unauthorised travelling, and denial of travelling). This threat agent is usually an employee of the ETIAS actors, such as EU agency, a Member State authority and Border Guards agency.</p> <p><b>Threat Agent:</b> Employee (Nation state, organised crime, Insider)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>Availability</p> <p>Privacy</p>

Risk Scenario	Impact dimension 1 Type of effect
<p><b>RS.10 Network communication attacks</b></p> <p>The threat agent explores network attacks to modify and tamper with ETIAS information, such as injections, botnets, exploit kits and web application attacks. These attacks deliberately make changes to compromise the integrity of information, by corrupting or deleting stored in ETIAS databases or transferred between ETIAS components. Risks related to the communication between the front- and back-end of the ETIAS and external components, including payment interfaces, external database and any logical communication.</p> <p><b>Threat Agent:</b> Hacker (Organised crime, Hacktivist) or Privileged employee (Insider, organised crime)</p>	<p>Integrity</p> <p>Availability</p> <p>Confidentiality</p> <p>For integrity refer also to RS.3</p> <p>For confidentiality, refer to RS.1 and RS.2</p>
<p><b>RS.11 Denial of Service</b></p> <p>The threat agent performs attacks tackling ETIAS availability, by exploring vulnerabilities to the ETIAS Web Service and user interface, through (D)DoS, injection, and network scans attacks. These attacks deliberately impair the availability and performance of the ETIAS Web Service, by flooding with fraudulent application requests and exploring vulnerabilities in the ETIAS user interface and Web Service.</p> <p><b>Threat Agent:</b> Hacker (Nation state, organised crime, Hacktivism)</p>	<p>Availability</p> <p>May discourage the use of ETIAS</p> <p>May cause reputational damage to ETIAS and its responsible agency</p>
<p><b>RS.12 Malware/Spyware</b></p> <p>This threat includes the adversarial or accidental installation of malicious software at ETIAS Central System or on employees' computers through phishing scam or website downloads, such as malware, botnets, virus, Trojan horses, ransomware and spyware. Such software is designed to deliberately compromise the integrity and confidentiality of data in ETIAS storage or at an employee computer.</p> <p><b>Threat Agent:</b> Hacker/Supplier/Partner (Nation state, organised crime, Hacktivism)</p>	<p>Confidentiality</p> <p>Integrity</p> <p>Availability</p> <p>Consequences of malware/spyware are particularly hard to predict since they often lead to bootstrapping other attacks</p>
<p><b>RS.13 Hardware malfunction, failure or fraudulent</b></p> <p>The threat agent explores risks of the used hardware, such as document readers, ETIAS application readers and network and storage infrastructure.</p> <ul style="list-style-type: none"> <li>• Hardware counterfeiting (illegal imitations)</li> <li>• Hardware forgery (illegal alteration)</li> <li>• Hardware malfunction or failure of information system hardware (e.g. hard disk drives, memory, routers, or network switches).</li> <li>• Hardware performance/efficiency</li> </ul> <p><b>Threat Agent:</b> Supplier/vendor/partner (organised crime) or employee (organised crime, Hacktivism)</p>	<p>Integrity</p> <p>Availability</p>

Table 28: Risk scenarios– dimension 2

Risk Scenario	Impact dimension 2 Impacted party
<b>Confidentiality</b>	<p><b>VE-TCN:</b></p> <ul style="list-style-type: none"> <li>• Misuse of traveller’s personal information, e.g. <ul style="list-style-type: none"> <li>○ By state agents that lack the right to have access to this information;</li> <li>○ By parties with an interest in the traveller’s plan in order to maximise their profit (e.g. travel agencies);</li> <li>○ By family members with diverging opinions or travel plans.</li> </ul> </li> <li>• Misuse of payment information (leaked information) resulting in subsequent financial/economic loss (e.g. use of credit card by hacker to pay hacker’s Card-Not-Present purchases on the Internet, sales of credit card details on Darknet);</li> <li>• Consequential identity theft by reusing the information.</li> </ul> <p><b>Border guard:</b></p> <ul style="list-style-type: none"> <li>• Extra workload to handle complaints, and to perform additional verifications.</li> </ul> <p><b>Competent authorities:</b></p> <ul style="list-style-type: none"> <li>• Disclosure of screening rules and Member States additional legal and decisional information.</li> </ul>
<b>Privacy</b>	<p><b>VE-TCN:</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage of PII.</li> </ul>
<b>Integrity</b>	<p><b>VE-TCN:</b></p> <ul style="list-style-type: none"> <li>• VE-TCN’s entry erroneously refused, resulting in extra work for both VE-TCN and Consulate/Competent Authority;</li> <li>• VE-TCN’s entry erroneously granted, resulting in incorrect travel authorisations with possible criminal consequences;</li> <li>• Increased duration at border crossing, requiring extra verifications with possible incorrect outcome;</li> <li>• Subsequent financial/economic loss by misuse of payment information (tampered information);</li> <li>• Extra application workload (manual process and interviews).</li> </ul> <p><b>Competent authorities:</b></p> <ul style="list-style-type: none"> <li>• Incorrect VE-TCN assessment and decision <ul style="list-style-type: none"> <li>○ Resulting in additional safety exposure in case of erroneous granting;</li> <li>○ Resulting in extra workload in case of erroneous denial.</li> </ul> </li> <li>• Loss of reputation.</li> </ul> <p><b>Border guard:</b></p> <ul style="list-style-type: none"> <li>• Incorrect decision due to tampered information.</li> </ul>
<b>Availability</b>	<p><b>VE-TCN:</b></p> <ul style="list-style-type: none"> <li>• VE-TCN’s entry delayed.</li> </ul> <p><b>Competent authorities:</b></p> <ul style="list-style-type: none"> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications;</li> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications;</li> <li>• Handle formal legal complaints.</li> </ul> <p><b>Border guard:</b></p> <ul style="list-style-type: none"> <li>• Incorrect decision due to pressure to make ad-hoc decision without availability of the ETIAS application.</li> </ul>

## 2.6.6 Safeguards

This section elaborates on the safeguards and how they mitigate the security risk scenarios previously described. The safeguards follow the structure of the **ISO 27002:2013** clauses.

### Introduction of safeguards

The following table summarises the seven main safeguards to mitigate the threats from the different risk scenarios identified. The security controls listed here protect particularly against the higher impact scenarios, with a focus on those impacting confidentiality and integrity of ETIAS data. A full description covering all fourteen ISO 27002:2013 clauses is provided in Annex 8. – “System security”.

The costs related to these safeguards are estimated to amount to approximately 4% of the budget for hardware, software and development, for each environment, thus cumulating if considering the redundant setup discussed within the Architecture section. The total cost is estimated to exceed two million EUR, just for the hardware and software dedicated to security.

*Table 29: Overall Safeguard description summary*

Safeguards identification	Safeguards description
SG.01 Human Resources	<p>Human Resources safeguards address the human factor:</p> <ul style="list-style-type: none"> <li>• Prior to employment;</li> <li>• During employment; and</li> <li>• At time of termination and change of employment</li> </ul> <p>It includes the recruitment, training and management of all staff involved in ETIAS design, implementation and operation. This includes staff from Member States and relevant competent authorities. All involved personnel should be educated about the risks related to information systems, and be trained on how to act, and which security controls to apply, in order to avert relevant threat events.</p> <p>HR safeguards are a foundation of security. Core ICT systems are protected by an increasing number of technical safeguards, including network segregation. Attackers respond by crafting new attack vectors, including infections of personal devices of users and ICT staff of the systems they intend to attack. Attacks e.g. via social media attempt to plant malware on such a personal device. Once the device is within reach of a business network, the malware attempts to open a communication path from the personal device onto the core system, or to inject malware into the core system. Therefore, selection of staff and staff awareness and training in the recognition of irregularities are a foundation of security.</p>
SG.02 Access Control	<p>Access control safeguards address:</p> <ul style="list-style-type: none"> <li>• Business requirements of access control;</li> <li>• User access management and user responsibilities;</li> <li>• System and application access control.</li> </ul> <p>ETIAS assets should be identified, classified and monitored for then implementing different levels of physical and logical access control among different ETIAS actors to the information stored, transferred and processed within ETIAS.</p> <p>Access control safeguards define and enforce a user’s right (e.g. read, write, create, delete, execute ...) over information. They are implemented through mechanisms such as Access Control Lists (ACL) or Role Based Access Control (RBAC). It is good practise to integrate the management of access control within an Identity and Access Management (IAM) solution.</p>
SG.03 Cryptography	<p>Cryptographic controls address the confidentiality and integrity of the ETIAS information assets, in accordance with the classification of that asset. Cryptographic controls should be in place for each component, particularly addressing entity and message authentication, as well as the protection of information in transfer/in storage.</p> <p>Cryptographic safeguards are used to protect the integrity, authenticity and confidentiality of information. They are implemented by using algorithms and the appropriate keys. The three basic families of algorithms are: key-less algorithms which do not use a key (e.g. hash algorithms such as the Secure Hash #3, SHA3), symmetrical algorithms which use a single key for all involved parties (e.g. the Advanced Encryption Standard, AES), and asymmetrical algorithms which use public/private key pairs (e.g. Rivest-Shamir-Adleman, RSA, or Elliptic Curve Cryptography, ECC). Many more sophisticated algorithms exist as well, including threshold algorithms (where a pre-defined number of parties need to collaborate to create a key).</p>
SG.04	Communications security addresses network security management and the security of information

Safeguards identification	Safeguards description
Communications Security	<p>transfers.</p> <p>Communication safeguards start from designing and managing the network itself in such a way that its components (routers, firewalls, wired and wireless access points, communication links, management stations, etc) are controlled in terms of hardware and software, including configurations and updates. This particularly includes integrity of the network itself, and protection of its cryptographic safeguards. Subsequently the services offered by the network can be created to offer security in the form of transport or network integrity, confidentiality and availability.</p>
SG.05 System acquisition, development and maintenance	<p>System acquisition, development and maintenance safeguards address security requirements of information systems, as well as security in development and support processes and for test data. System acquisition, development and maintenance safeguards cover the process and the people responsible for it, including training and knowledge aspects as well as the related risk management. Focal points are clear definitions of Responsible/Accountable/Consulted/Informed (RACI) for the security aspects of Software Development Life Cycle (SDLC), formal specification of security requirements, integration of the SDLC risks with the enterprise's overall Risk Management, secure coding guidelines and application penetration testing prior to go-life.</p>
SG.06 Information Security Incident Management	<p>Information Security Incident Management addresses the management of information security incidents and improvements resulting thereof. A formalised incident management process identifies, responds to, recovers from, and follows up on security incidents.</p> <p>Information Security Incident Management aims to report information security events and weaknesses, to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. It includes awareness, incident recognition, response and escalation procedures, as well as formal incident reporting.</p>
SG.07 Operations Security	<p>Operations security addresses:</p> <ul style="list-style-type: none"> <li>• Operational procedures and responsibilities;</li> <li>• Backup, as well as logging and monitoring;</li> <li>• Control of operational software;</li> <li>• Technical vulnerability management including protection from malware;</li> <li>• Information systems audit considerations;</li> <li>• Operations security safeguards include what is needed to keep the business (with underlying network, computer systems, applications and environment) up and running in a secure and protected way. It is situated after systems have been acquired, developed and deployed. Its activities are continuous in nature.</li> </ul>

## Safeguards mitigating risk scenarios

Risk scenarios are matched to safeguards, to ensure that every possible risk scenario is at least countered by one safeguard. This is marked by "X" in table below.

Table 30: Risk scenarios - safeguards matrix

	SG01 - Human Resources	SG02 - Access Control	SG03 - Cryptography	SG04 - Communications Security	SG05 - System acquisition, development and maintenance	SG06 - Incident management	SG07 - Operations security
RS01 - Access Disclosure		X	X	X	X	X	X
RS02 - Eavesdrop			X	X			
RS03 - Cryptographic breach			X				
RS04 - Rerouting			X	X			X
RS05 - Third-party communication		X	X	X	X		
RS06 - Software bugs/vulnerabilities					X	X	
RS07 - Authentication		X	X	X			
RS08 - Credentials Forgery			X			X	
RS09 - Insider	X	X					X
RS10 - Network and Interface interactions				X		X	X
RS12 - Denial of Service				X		X	X
RS13 - Malware/Spyware	X			X		X	
RS14 - Hardware malfunction, failure, or fraudulent					X		

### Human Resources safeguards

For ETIAS, HR safeguards should be implemented that address at least:

- Security vetting of all personnel, staff and subcontractors, covering central entity processing as well as Member State personnel involved in ETIAS. Member States' personnel should work in secure facilities;
- Development of an ETIAS Security Policy (which would include rules on professional secrecy and define responsibilities regarding data security), and inclusion thereof in the organisation's set of rules that need to be complied with. This Security Policy should be equally applicable to any party connecting to the system (including Member States);
- Initial security awareness training, including communication of ETIAS Security Policy;
- Annual continuous education session;
- Embedding of security policy compliance in HR procedures such as annual evaluation and exit procedure.

Insider attacks (RS09) and malware/spyware attacks (RS13) are particularly addressed through security awareness training and continuous education, resulting in vigilance of personnel.

### Access control safeguards

For ETIAS, access control safeguards should be implemented that address at least:



- Specification of the ETIAS Access Control policy covering the ETIAS Internet services and the central system, as well as the related management systems. This should be based on the rules set out in section 2.2.9 "Access management and data ownership".
- Allocation of responsibility for translation of the policy into practical measures such as Access Control Lists<sup>117</sup> (ACL), Role Based Access Control<sup>118</sup> (RBAC) or Attribute Based Access Control (ABAC), preferably as part of an Identity and Access Management<sup>119</sup> (IAM) solution. This should include a classification of the information assets, the creation of roles for parties that access the system, and the definition of which party can access what information, with the justification thereof. Appropriate segregation of duty should be addressed via the ACL group, RBAC role or ABAC attribute and rule management. Access for travellers will be limited to submitting an application via the ETIAS Internet services, and requesting the status of their application using a reference number.
- This should further include authentication of all users except travellers.
  - For travellers:
    - The submission of an application through the ETIAS Internet services will not require authentication. The authenticity of the application will be verified in the central system as part of its business logic;
    - Requesting the status of their application will not require authentication beyond the use of reference number<sup>120</sup>.
  - For all other parties that access ETIAS, as well as for system managers, authentication shall be based on 2 factor authentication. There should also be physical access control and authentication for accessing the facilities from where ETIAS will be reachable, so that only duly authorised staff has access.
- Monitoring and follow-up of access control violation attempts.
- From a communications perspective, an 'authorisation to connect' should be enforced. Such an authorisation would be granted by the ETIAS owner to parties that need access. One of the conditions for granting the authorisation is undergoing an audit in order to demonstrate that the party requesting the access operates all safeguards required, and complies with the ETIAS Security Policy.

Access disclosure (RS01), third-party communication attacks (RS05), and authentication attacks (RS07) should be mitigated by the combination of the mechanisms described here. Particularly insider attacks (RS09) should be mitigated via appropriate access control definitions and segregation of duty.

### **Cryptographic safeguards**

The various discussions held with stakeholders during the execution of the feasibility study indicated that encryption of the ETIAS database was in general regarded as being overly complex and having the potential to negatively impact system performance. For this reason, ETIAS cryptographic safeguards should be implemented that address:

- Selection including update of adequate algorithms and key lengths, including their key roll-over as a consequence of expiration or an incident;
- Authentication of the Internet Service towards applicants through a TLS (Transport Layer Security)<sup>121</sup> certificate, certified by an appropriate Trust Service Provider;

---

<sup>117</sup> An ACL solution grants permissions to users via group memberships, e.g. *John is a member of group Usergroup1*. The actual authorisations to the technical resources such as files are defined on the groups, e.g. *Group Usergroup1 has READ access to file1*.

<sup>118</sup> RBAC and ABAC are more recent solutions that grant permissions via role memberships and attribute values respectively.

<sup>119</sup> An IAM system combines authentication, access control and workflow to manage these in one integrated solution.

<sup>120</sup> Using name and passport number (or other similar data) would make the system more prone to attacks. Indeed, the structures of passport numbers are well known and names are easy to invent: it is thus possible to create a high number of requests that the system will recognise as genuine and have to process. Should this number be too important, the system would collapse.

<sup>121</sup> Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are both frequently referred to as "SSL". These are cryptographic protocols that provide communications security over a computer network.

- Authentication of the operators of the manual procedure and of the system managers, where at least one factor shall include a cryptographic algorithm challenge/response sufficiently strong for its purpose;
- Electronic sealing of application status confirmation emails (as per EU 910/2014, an electronic seal is an electronic signature issued by a legal entity);
- The randomness of the applicant's reference number, making it hard to guess for other parties than the original applicant;
- Encryption of network traffic between applicant and Internet Service, between Internet Service and Central System, and between Central System and other systems (EES, SIS, VIS and Member States' systems);
- Encryption of network traffic between Central System and the end points of the operators of the manual procedure and of the system managers;
- Selective encryption or hashing of parts of personnel data in reports intended for management or for any authority exercising oversight or audit, as to protect the privacy of applicants.

Attacks related to disclosure of information (RS01 Access disclosure attack, RS02 Eavesdropping, RS04 Rerouting and RS05 Third-party communication attacks) should be mitigated by encryption information. Breaches in cryptographic mechanisms (RS03) should be mitigated by the selection and update of algorithms and key roll-over. RS07 Authentication attacks and RS08 Credentials forgery should be mitigated by the selection of sufficiently strong cryptographic primitives in the authentication protocols.

### **Communication safeguards**

For ETIAS, communication safeguards should be implemented that address:

- Physical security of all ETIAS communications equipment, including access control and protection against power-cuts and power fluctuations;
- Protection against common attack scenarios such as Distributed Denial of Service (DDoS), by combining safeguards implemented at the Internet Service Provider (e.g. so-called 'clean pipes') and safeguards implemented at the ETIAS ingress point (e.g. load balancers and blacklists);
- Protection of the integrity of software updates of all ETIAS communication equipment (firewalls, routers, access points etc.);
- Firewalls that operate at application and network level of the protocol stack;
- Intrusion Detection/Prevention systems that automatically monitor network traffic, perform automated event analysis and can activate or propose to activate protection mechanisms such as temporary network disconnect and traffic rerouting to an externally hosted webpage that displays the message "Service temporary unavailable".

By making the ETIAS Internet Service and the Central System only available via strictly controlled access paths, communications safeguards should address RS01 Access disclosure attack, RS02 Eavesdropping, RS04 Rerouting and RS05 Third-party communication attacks. By enforcing appropriate authentication along the access path, they would mitigate against RS07 Authentication attacks, as well as RS10 Network and interface interaction attacks. RS12 Denial of Service attacks would be mitigated by the combination of ISP and internal protection, and RS13 Malware/spyware attacks would be mitigated by application level firewalls.

### **System acquisition, development and maintenance (SADM) safeguards**

For ETIAS, SADM safeguards should be implemented that address:

- Specification of detailed security requirements from a business process perspective, reflecting the applicant's point of view, as well as from an ETIAS management perspective, reflecting the operators of the manual procedure and of the system managers. These security requirements should include:
  - Identification and authentication;
  - Access and session management;
  - User data protection (access control, residual data protection, stored data integrity);
  - Communication (connectivity and non-repudiation of origin/receipt);
  - Cryptographic support (key management and operations);
  - Trusted path/channels;
  - Security management (management of safeguards, security management roles);

- Privacy and data protection (e.g. anonymisation);
- Resource utilisation (fault tolerance of Internet Service and Central System, priority of service, resource allocation)
- Security audit (security audit data generation, security audit analysis/review)
- Integration of these security requirements in the overall requirements, and allocation of accountability for their implementation;
- Development or acquisition of safeguards whose implementation will ensure the ETIAS operational system meets these requirements;
- The monitoring of these safeguards, in order to ensure adequate maintenance is applied preventively or on an as-needed basis.

By the implementation of SADM safeguards, controls would address RS01 Access disclosure attacks, as well as RS05 Third-party communication attacks and RS06 Software bugs/vulnerabilities. RS14 Hardware malfunction should be mitigated by appropriate testing and monitoring.

### **Incident management safeguards**

For ETIAS, incident management safeguards should be implemented that address:

- Roles, responsibilities and communication lines for reporting incidents as well as responding to them;
- Classification of incidents;
- Collection of evidence and the related 'chain of custody';
- Corrective and recovery actions;
- Escalation levels and the relationship to Business Continuity Management.

By the implementation of incident management safeguards, controls would address RS01 Access disclosure attacks, as well as any RS06 Software bugs/vulnerabilities that would surface. RS08 - Credentials forgery should be addressed by responding to users reporting incidents related to the use of their credentials. Also RS10 Network and interface interaction attacks, RS12 DOS attacks and attacks using Malware/Spyware (RS13) should trigger incidents upon which corrective and recovery actions are taken.

### **Operations security safeguards**

For ETIAS, operations security safeguards should be implemented that address:

- Documenting the Standard Operating Procedures and Processes;
- Segregation of duties for Operators;
- Separation of development, test and operational facilities;
- System hardening (Operating System installation and configuration, stripping of unnecessary components, patching, scanning);
- Follow-up of supplier/sub-contractor engagements and roles & responsibilities;
- Service Level Agreement and Reporting;
- Asset Management (evolution of equipment, hardware, software), including license management;
- Threat and Vulnerability Management.

By the implementation of operational safeguards, controls would address RS01 Access disclosure attacks, as well as RS04 Rerouting attacks, RS09 Insider attacks, RS10 Network and interface interaction attacks, and RS12 Denial of Service attacks.

## 2.7 Implementation approach

This section describes the different possibilities for implementing ETIAS. It first offers a brief overview of four options, then illustrates how some of them have been used for other systems and lastly analyses how these options can be adapted to ETIAS.

### 2.7.1 Roll-out options

The following potential options for ETIAS implementation have been identified on the basis of the experience of other large-scale IT systems, in the EU and worldwide, and on the basis of the nature of ETIAS:

- A. “Big-bang”:** ETIAS is operational in all the regions of the world and at all border types in one go. This option entails that all end-users, basic IT components, communication channels and procedures are targeted and ready at the same time.
- B. Gradual by border type:** ETIAS is implemented at one Member State border type at a time. It is also gradually implemented by carriers in their own systems. Given that the highest number of VE-TCNs arrive by air to the Schengen Area, ETIAS could be implemented first at air, then at sea borders and lastly at land borders<sup>122</sup>. Alternatively, roll-out at land borders first would leave more room for rectification of problems and would give more time for carriers to adapt to the new requirement. Indeed, an error at land border would affect less VE-TCN, less border guards and would not have an impact on carriers.
- C. Gradual per region:** the travel authorisation is first required for travellers with a nationality from a specific region x of the world, then from region y and finally from region z. As the Americas have the largest share of VE-TCN, prioritising this region would make ETIAS a requirement for the majority of the global VE-TCN population (75%). On the other hand, prioritising another region, for instance Europe and the Middle East, could also be beneficial as the workload would increase slowly and give more time to end-users to adapt. Another option is for future countries joining the visa-exempt programme to be taken as a region per se.
- D. From voluntary to mandatory:** holding a travel authorisation is voluntary in all regions and at all border types at first and then becomes mandatory after time, while allowing for an initial period of grace.

A number of implementation options can be combined, for instance **per border type** and **per region**. As the majority of VE-TCN from region Americas and Asia-Pacific would come to the Schengen Area by air, ETIAS roll-out could be combined with roll-out at air borders (or, for the same reason, a combination between implementation in the European region and with roll-out at land borders). Consequently, different combined options also exist:

- A combination of border type (air) and region (Americas and Asia-Pacific);
- A combination of border type (land) and region (Eastern Europe);
- A combination of border type and voluntary to mandatory.

It is important to differentiate between the *implementation option* (previously listed) and step-wise/phased implementation of ETIAS *functionalities*. Whilst the former is the way the system is rolled-out, with its basic components (carriers connected, webservice in place, stakeholders aware, trained and prepared), the latter are specific features of the system that can be added at a later stage and that do not prevent ETIAS from performing basic tasks. Some functionalities that can be considered for later implementation include:

- Connections with other systems and databases
  - *Connection/interoperability with EES*. This functionality would depend on the level of interconnectivity between the two systems. Indeed, if ETIAS is strongly integrated with EES, then both shall be rolled-out at the same time. If the connection can be done at a

---

<sup>122</sup> 107 million for air borders, followed by 11 million at sea and 5% at land. See: Technical study on Smart Borders (2014), p. 23.

- later stage, then the benefit would lay on the fact that neither of them would depend on the other one's implementation date.
- *Connection with EIS*. ETIAS could check the EIS database at a later stage, once the technical difficulties are overcome. The factors compromising the link between ETIAS and EIS are described in the section 2.2 "Data" and Annex 4. – "Data".
  - *Connection with VIS*. The connection to the VIS could be implemented at a later stage if no new visa-exempt country joins the programme in the next five years. Indeed, as VIS retains visa data for five years, the only use of its connection to ETIAS would be for the newly joined visa-exempt countries (for visa history and for refused visas).
  - *Connection with EURODAC*. At this stage the system does not seem relevant for a connection with ETIAS (see section 2.2 "Data" and Annex 4. – "Data"). However, as its evolution focuses on case management it could perfectly make sense to reassess its compatibility with a travel authorisation system in the future.
  - *Connection with ECRIS*. At this stage the system does not seem relevant for a connection with ETIAS (see section 2.2 "Data" and Annex 4. – "Data"). However, it might be interesting to reassess it if the system evolves and include data on third-country nationals.
- Screening rules. The repository of screening rules can be a check added at a later stage and its absence would not compromise ETIAS operability.
  - Collection of a fee
    - The system could be free of charge at first, although it is always a difficult step to request payment for a service that was initially free.
  - Change of data fields (e.g. background questions)

The implementation of ETIAS *functionalities* can be combined with any *implementation option*. A step-wise/phased approach would allow the system to go-live and be operational at a very early stage, give more time for stakeholders to experience functionalities, better adapt them to the system and prioritise the components to put in place first.

## 2.7.2 Examples of large-scale IT systems roll-out

### The example of the VIS roll-out

The Visa Information System has been implemented gradually and per region: visas were mandatorily recorded in VIS starting in North Africa on 11 October 2011, but visas were checked at all Schengen borders from the beginning. The biometric verification at the border became compulsory from 11 October 2013 onwards (two years after becoming operational). The VIS has been progressively rolled-out around the world over a four-year period, and finished its implementation in December 2015<sup>123</sup>.

The Commission Decision 2010/49/EC of 30 November 2009<sup>124</sup> determined the first regions for the start of operations of the VIS based on a country-specific migratory risk assessment and on expected workload:

*(3) "The Commission has made an assessment for the different regions as defined in 2005 by the Member States' experts for the progressive implementation of the VIS, and taking into account, notably for the first criterion, elements such as the average visa refusal and entry refusal rates for each of the regions concerned, and, for the third criterion, the fact that consular presence or representation should be increased in certain regions in order to efficiently implement the VIS in these regions".*

The following regions were determined at a later stage, based on the same assessment and on the experience gathered during the first roll-out (paragraph 9). VIS also needed to be implemented at the borders of the Member States, which consisted in a "region" per se, and some delays were observed in a few countries with a large amount of border-crossing points. *"To avoid a gap when fighting illegal immigration and protecting internal security, the Schengen border crossing points should be designated as*

<sup>123</sup> See: [http://ec.europa.eu/dqs/home-affairs/what-is-new/news/news/2015/20151202\\_2\\_en.htm](http://ec.europa.eu/dqs/home-affairs/what-is-new/news/news/2015/20151202_2_en.htm) (accessed 08/2016).

<sup>124</sup> See: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0049&from=EN> (accessed 08/2016).

a separate region for the roll-out in order to cover the visa applications lodged at the external borders” (Art.2).

As a conclusion, VIS was successfully rolled out combining a regional approach with an increase in functionality (the mandatory biometric verification).

### Roll-out of other electronic travel authorisation systems

While the Australian eVisitor has been rolled-out following a big bang approach (mandatory for all EU citizens at midnight on 27 October 2008), the eTA and ESTA have been rolled-out gradually. The Canadian system has experienced some delays and it is finally mandatory for all travellers since September 2016 (it first entered in operation in August 2015). In addition of also evolving from voluntary to mandatory, the American system also gradually established some of its elements: the fee was installed two years after the initial roll-out and the risk-assessment checks were adapted to the context. The data fields and background questions changed through time, adapting to a new global context (presence in a war zone), to new internal requirements (addition of diseases in the health-related question) or to different needs for risk assessment.

### 2.7.3 ETIAS implementation

The following table summarises the impact of choosing different options, which is assessed on the basis of the following criteria:

1. **Cost:** the total cost of the implementation on the day of the go-live and also the additional costs of any modification or delay.
2. **Level of technical complexity and risk:** the complexity of the system’s roll out from a technical and risk management point of view (availability of the system, business continuity and technical setup).
3. **Flexibility and adaptability:** the way the implementation can allow for adjustments and unforeseen modifications throughout its go-live phase.
4. **Preparatory measures:** end-user trainings, awareness campaigns, etc.
5. **End-user impact and involvement:** the implementation impact on the end-users (traveller, border guard and carrier).

A detailed assessment and additional information on the methodology are provided in Annex 9. – “Implementation approach”. The following table shows a summary of the analysis:

Table 31: Assessment of ETIAS implementation options

Option / Criteria	Cost	Technical complexity and risks	Flexibility and adaptability	Preparatory measures	Convenience for travellers	Convenience for border guards	Convenience for carriers
A. “Big bang”	€€	-	--	-	-	-	--
B. Gradual per border type	€	+	++	+	-	+	0
C. Gradual per region	€	-	++	--	--	-	-
D. From voluntary to mandatory	€	+	++	+	+	-	+

The **gradual** options are all more flexible than the big bang option, but this flexibility translates into higher costs. For this reason, and although it scores lower on flexibility and adaptability, the “**big-bang**” option is a preferred option from a technical, cost and end-user point of view. It would require more preparatory efforts as all the basic components of the system would have to be ready for the go-live date (border guard trained, system available for their interface, carriers connected and liable for the boarding of VE-TCN, travellers aware of the requirement, etc.). Gradual implementation options can also have a “big-bang” element. Indeed, in terms of preparatory measures, option C (gradual per region) has similar impacts as the “big-bang” option as all border crossing points would have to be ETIAS-ready at the same time.

Although the major stakeholders involved in the deployment of ETIAS at EU level have experience with gradual **per-region** types of roll-out (e.g. VIS), applying this option to ETIAS could have significant disadvantages not encountered in the case of VIS. Indeed, the visa system is a tool for harmonisation of short-stay visits whilst ETIAS would be an additional requirement imposed on individuals previously exempt from any administrative process prior to the arrival at a Schengen border. It could generate considerable confusion and extra workload among the end-users: carriers and border guards would need to pay extra attention to the nationality of the passenger in order to know whether or not to verify ETIAS status. Lastly, and from a VE-TCN point of view, this option can be perceived as a discriminatory tool for the citizens of the prioritised region(s).

The **voluntary to mandatory** option (e.g. over a 12-month period, similar to what has been done in Canada) obtains the highest score in the assessment.

Lastly, some of the negative impacts on users can be alleviated by similar mitigation measures, regardless of the option chosen:

- a) The establishment of a **grace period**. Without publicising this, and from the date of applicability of the mandatory requirement, travellers without a valid travel authorisation could be allowed one-off travel and (potentially) entry to the Schengen Area, during a fixed period of time, in order to give them time to adjust to the new system. This would be applicable to all visa-exempt travellers to avoid discrimination issues.
- b) **A testing phase in real conditions**. It would give the end-users the possibility to test the system with real data and spot any possible issue in advance in order to rectify it prior to the full roll-out date(it is important to mention that this testing phase would need to be included in the legal basis).

The implementation option for ETIAS can be "à la carte" drawing on different combinations of options and functionalities. It is important to note that the same type of implementation with the same set of chosen functionalities would apply to all Member States.

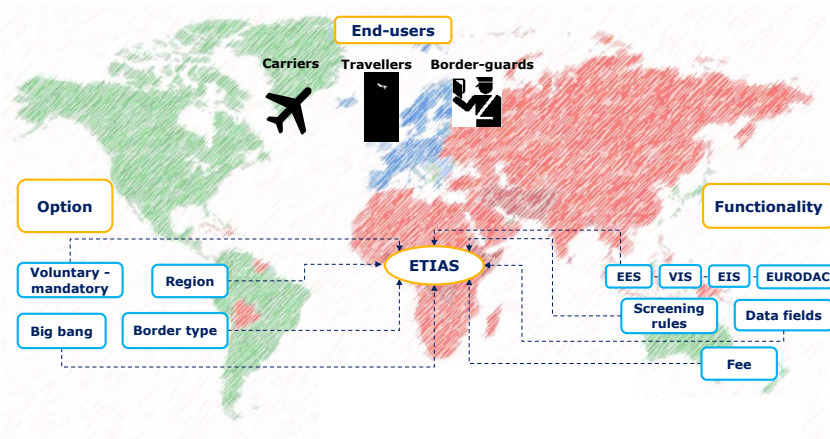


Figure 21: ETIAS implementation "à la carte"

Lastly, a large-scale technological change like the roll-out of ETIAS needs social acceptance from all its major stakeholders in order to be successful. Change management, communication campaigns and trainings are paramount to take into account for the ETIAS roll-out, given that the system is composed of different interfaces used by different end-users in order to perform different tasks. The human factor is the most crucial element in this context and it is advised to take into account all the heterogeneous end-users sensibilities and needs when analysing the preferred option, as well as foresee a significant communication and training effort regardless of the choice of implementation option.

## 2.8 Future technology options

ETIAS implementation is unlikely to be completed before year 2020/2021. By that time new technologies might have become viable options for ETIAS. This sections looks into promising technological options that might enhance the functionalities of ETIAS or the experience for users.

### 2.8.1 Mobile application

A dedicated mobile application supporting the most common mobile operating systems, could be used to allow travellers to request their travel authorisation. Exploiting the mobile channel is increasingly important and common.

The use of an ETIAS mobile application, beyond the simple use as portal for lodging application, could also have more advanced features by leveraging on hardware like cameras and near-field communication (NFC), which are becoming standard in modern smartphones. However, the low level of smartphone penetration in some visa-exempt countries (e.g. 41% in Brazil and 25% in Peru<sup>125</sup>) means that **requiring their use would not be a viable option for the time being**. The use of a mobile application can only be on a voluntary basis. The situation should be re-assessed close to the implementation date, as the diffusion of these devices might have changed significantly.

Below a description of possible features and use-cases that could be enabled by a mobile app.

#### 1) Photo of the biographical page of the passport

The traveller could be asked to take a picture of the biographical page of the passport within the application process.

Possible use-cases:

- **Evidence:** the image could be stored within ETIAS central system and used should manual processing be required. It could, for instance, support the disambiguation and be evidence of the identity declared within the application form. Moreover the passport page includes the photo of the traveller, which could be compared to existing databases such as EES, however, the comparison would be mostly done by an operator as the scanned picture is unlikely to be of sufficient quality to guarantee good results with an automated verification.
- **User convenience and data quality:** the mobile app could read the Machine Readable Zone (MRZ) (or the fields of the biographical page using an optical character recognition (OCR)) and compare the information acquired with the data inserted by the applicant. This consistency check could help reducing errors by spotting mismatches. The information scanned from the passport page could alternatively be used to pre-fill part of the form asking then for confirmation by the user.
- **Visible security feature:** having the image of the passport could allow verifying basic security features. The check could either be done by experts within the CMPE for applications that were sent for manual processing or even by the app although this would require templates for each type of passport to be loaded in the application and continuously updated. Collecting and storing images within ETIAS central system might create unintended consequences. Inappropriate or even illegal images could potentially be uploaded into a European database. Ad-hoc software and monitoring would then be required.

Commercially available mobile applications already provide the features listed above. For instance, the image below shows the mobile application from Easyjet which allows to capture data from the passport with a photo (although without verification of security features in this case); other apps (e.g. from United Airlines) offer the same functionality.

---

<sup>125</sup> Poushter, Jacob. "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies | Pew Research Center", [www.pewglobal.org](http://www.pewglobal.org) (accessed 10/2016).



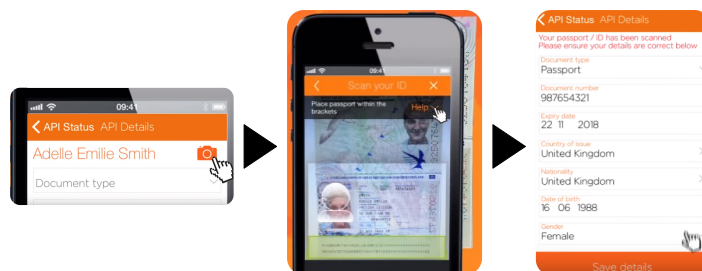


Figure 22: Easyjet mobile application allow the capture of passengers' data directly from a photo of the passport (source: Youtube Easyjet channel)

## 2) Chip reading of the passport

By using Near Field Communication (NFC) enabled smartphones the traveller could read the chip of his/her passport (valid only for applicant with an electronic passport or eMRTD<sup>126</sup>). Unfortunately, not all smartphones have such technical feature. For instance, Apple iPhones, one widespread brands of smartphones, would currently only have its most recent version able to read the passport.

Possible use-cases:

- **User convenience and data quality:** the application would be able to pre-fill part of the fields of the application form by acquiring them directly from the eMRTD itself. This would not only facilitate the user, but also reduce the likelihood of typos and errors in preparation of the application form. Reading data from the chip directly is also more reliable than using an OCR on the image of the passport.
- **Acquisition of the facial image:** having access to the passport chip would also allow the extraction of the facial image. The facial image from the passport would greatly enhance the identification of the travellers, facilitating the disambiguation when necessary and possibly creating a biometric link with EES which would also store the facial image of the travellers.
- **Facial image verification:** access to the facial image from the passport chip would also allow the biometric comparison with a live photo, a "selfie". This operation would verify the identity of the person filling-in the application form. A biometric verification can, however, fail, encounter errors and in any case increase the difficulty for the user of completing the application process. It might also require the adoption of liveness detection techniques to reduce the risk of frauds.

## 3) Acquisition of biometrics

Smartphones have an increasing number of sensors able to capture a variety of biometric characteristics. The most common ones are:

- Facial image
- Fingerprint
- Iris – the first commercial models are now starting to appear on the market.

Taking into consideration that European systems contain either fingerprints or the facial image, there is limited interest in capturing iris or any other biometric which would not have any reference to be compared with.

The facial image can be compared with the picture either on the document biographical page or in the passport chip, allowing for a local verification, as described earlier. This would not be possible for fingerprints, which cannot even be read from the passport chip without the appropriate country specific certificates, which are often not shared by countries. Moreover, common sensors used in smartphones are not adequate to capture a fingerprint for automated comparison with the existing databases (limited capture area and use of capacitive technology with different and unknown specifications/performances), nor is the fingerprint captured usually accessible by the application itself, hence this could not be transmitted or compared.

<sup>126</sup> electronic Machine Readable Travel Document. The vast majority of VE-TCN are likely to be equipped with an eMRTD at the time of go live of ETIAS.

Overall capturing biometrics remotely would pose significant challenges, not only from a technological point of view, but also in terms of user experience. The application process would be undoubtedly more complex. For this reason among the various possibilities, the most promising option would be the capture of the facial image from the passport chip, instead of live, which would only be possible with NFC equipped smartphones.

### **Conclusion**

A mobile application with the possibility to acquire either optically or from the chip information contained in the passport would be beneficial for users and increase data quality, by avoiding having the applicant manually typing in their biographical information. ETIAS should therefore consider the possibility to provide a mobile application for the passengers with smartphones and for this reason the development of a mobile app has also been included in the cost model of ETIAS (see Chapter 4 "Cost-benefit analysis (CBA)").

However, the current dissemination and diversity of smartphones hardware are reasons why the mobile application cannot be mandatory. Consequently **the capture of any image using travellers' devices would be unpractical and in practice rules out the capture of biometrics remotely and unsupervised.**

## 2.8.2 Shared infrastructure and private cloud services

eu-LISA is bringing forward initiatives aimed at establishing common shared infrastructures, however, the three main systems operated by eu-LISA were delivered as separate systems which limited the possibilities for reuse or synergies of any infrastructure. These systems were, in fact, originally requested to be designed as fully isolated systems. ETIAS should benefit from the results of the studies on common shared infrastructures and build further on them, so to increase its cost effectiveness.

Virtualisation of servers and cloud services are not new technologies, however, their use within the European IT landscape is still very limited. These technologies aim at separating the infrastructure layer from the application layer and at allocating dynamically resources when needed.

In the future European systems could be run on a private<sup>127</sup> cloud dedicated at the provision of government services simplifying issues of scalability and sizing of the systems before entering into production. Such shift would, however, require the re-engineering of several of the current application so that they could fully take advantage of the new paradigm. ETIAS, on the other hand, could be developed to be cloud-ready, adopting, for instance, a scalable and stateless design.

While cloud technology could help optimising the infrastructure deployed, it would not be likely to reduce the overall capacity required. eu-LISA operated systems are correlated as they support the various processes part of the European border management. This means that a sharp increase of travellers or a new security threat are likely to create peaks of workload for all the systems at the same time, at least to a certain degree. Therefore the infrastructure would still have to be sized to cope with the full load of all systems simultaneously.

---

<sup>127</sup> It is important to note that a "private cloud" does not assume that it is run by a private-sector company. In this case it would be a "cloud" at the level of eu-LISA, owned by that company and with storage located in the EU. The pursued benefit is to have "storage provided as a service".

## 3 Evaluation of impact

The present Chapter 3 describes the ETIAS impact on the current EU legal framework in the Migration and Home Affairs area, outlining **which legislation would need to be modified** in light of a new travel authorisation requirement. It also highlights **data protection implications**, identifying a number of relevant **safeguards** and **remedies**.

### 3.1 Legal

The following section focuses on the **legal impact** of the implementation of ETIAS. More specifically, it lists which **legal texts** in the relevant EU legal framework would have to be **modified** and how.

#### 3.1.1 Context

The implementation of ETIAS would impact the EU legal framework in three main ways:

- A **new Schengen Area entry condition** for visa-exempt travellers would have to be created, namely “possessing a travel authorisation”;
- **New connections** would have to be established between ETIAS and other EU and international systems. The legal bases of the EU systems to which ETIAS would connect would have to reflect this connection; agreement(s) between the EU and the international organisation(s) managing the international systems would have to be put in place;
- **New mandates for stakeholders** in charge of the operational management of the system or in charge of the processing of the applications for a travel authorisation would have to be defined.

The following paragraphs describe in detail these changes. For each **legal text** that would need to be amended, the **articles to be modified** as well as the **new articles to be added** are mentioned.

#### 3.1.2 Legal consequences

##### Schengen Borders Code<sup>128</sup>

- **Article 6(1)** should be modified to include a new condition to the list of entry conditions for third-country nationals. This new condition would only apply to visa-exempt third-country nationals, who would have to be “in possession of a valid travel authorisation”<sup>129</sup>.

A legal basis for a travel authorisation requirement for transit travellers would be needed as well in case they would not be exempted from the ETIAS requirement. It would have to be assessed further whether amending Article 6 of the SBC would be sufficient. The Code sets out entry conditions and rules governing border control of persons *crossing* the external border of the Schengen Area while air and sea transit travellers do not always cross the external border of the Schengen Area from a legal point of view. A different legal basis may therefore have to be foreseen that obliges all transit travellers to obtain a travel authorisation<sup>130</sup>.

In case only transit travellers *crossing* the Schengen border are required to possess a travel authorisation (travellers staying in the international zone of the airport would be exempted), the amendment to Article 6 of the SBC would be sufficient.

---

<sup>128</sup> Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

<sup>129</sup> The study considered whether the expression “valid travel document entitling the holder to cross the border” that is currently used in Article 6(1) could be interpreted extensively to include both the passport and, if required, the travel authorisation that would be electronically linked to it. Such interpretation would allow to introduce the new entry conditions “be in possession of a valid travel authorisation” without amending Article 6(1) of the SBC. However, it is clear that the expression “valid travel document” is strictly referring to the passport and cannot include other documents/authorisations linked to it, in particular because the need to possess a visa is mentioned as a separate entry condition. The need to possess a travel authorisation would thus have to be introduced as a separate entry condition as well.

<sup>130</sup> The requirement to possess a transit visa for visa holders transiting through the Schengen Area is mentioned in the Visa Code.

## Schengen Convention

- **Article 5(1)** should be modified to include a new condition specific to visa-exempt third-country nationals, who would have to be "in possession of a valid travel authorisation", to the list of Schengen Area entry conditions for third-country nationals.
- **Article 20** should be amended to include a cross-reference to the new condition specific to visa-exempt third-country nationals included in Article 5(1).
- **Article 26(1)(b)** should be modified to include the carrier's obligation to make sure that visa-exempt third-country nationals carried by sea or air are in possession of a "valid travel authorisation"<sup>131</sup>. It is important to note that Article 26(3) specifically extends this obligation to international coach carriers transporting groups, with the exception of local border traffic. The study does not provide that land carriers – including coaches – would be obliged to check whether their passengers have a travel authorisation. Article 26(3) may thus need to be modified to specify that the obligation to check whether travellers have a travel authorisation does not apply to coaches.
- **Article 101(2)** should be modified to reference the central manual processing entity (CMPE) as being an authority with access to the data entered in the SIS.

## Schengen Handbook<sup>132</sup>

- **Articles 1(1), 1(6) and 1(7)** should be modified to include being in possession of a "valid travel authorisation" as an entry condition.
- **Article 1(8)** might also be subject to amendment in the future, should the means of subsistence be checked as part of the ETIAS authorisation process. Currently the study does not foresee that means of subsistence would be checked as a travel authorisation would be valid for a period of time and the means of subsistence needed would depend on the length of the stay, which can only be known if an authorisation is requested for each trip.
- **Article 6(1)** would have to be modified to include the lack of valid travel authorisation as a cause for refusal of entry<sup>133</sup>.

## VIS Regulation<sup>134</sup>

- **Article 3** should be modified to include the CMPE as a designated authority for VIS consultation.
- A new article should be introduced in **Chapter III** (Access to data by other authorities) to provide for VIS consultation by the CMPE for the purpose of ETIAS applications processing. This new article could have the following title: "Access to data for processing the application for a travel authorisation".
- A detailed article providing for interoperability between ETIAS and VIS should be included.
- An addition should be made to **Article 34**, to ensure that a record of each consultation of the VIS by the CMPE or Member States for the purpose of processing ETIAS applications is kept.

---

<sup>131</sup> If carriers are required to check whether visa-exempt travellers have a valid travel authorisation before boarding on the vessel, a legal basis extending carriers' obligations would need to be foreseen. Provisions would also have to be created to give carriers the right to refuse boarding based on a lack of a travel authorisation.

<sup>132</sup> Commission Recommendation Establishing a common "Practical Handbook for Border Guards (Schengen Handbook)" to be used by Member States' competent authorities when carrying out the border control of persons.

<sup>133</sup> Entry would be systematically refused if a person under the requirement to have a valid authorisation presents himself/herself at the border without one.

<sup>134</sup> Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). The VIS Decision would most probably not need to be changed.

## Legislation related to the Schengen Information System

### SIS II Regulation<sup>135</sup>:

- **Article 27** should be modified to include the CMPE as a designated authority for SIS II consultation.
- An article providing for interoperability between ETIAS and SIS II should be included.
- An addition should be made to **Article 12** to ensure that a record of each consultation of the SIS by Member States for the purpose of processing ETIAS applications is kept.
- An addition should be made to **Article 18** to ensure that a record of each consultation of the SIS by the CMPE for the purpose of processing ETIAS applications is kept.

### SIS II Decision<sup>136</sup>:

- **Article 40** should be modified to include the CMPE as a designated authority for SIS II consultation.
- An addition should be made to **Article 12** to ensure that a record of each consultation of the SIS by Member States for the purpose of processing ETIAS applications is kept.
- An addition should be made to **Article 18** to ensure that a record of each consultation of the SIS by the CMPE for the purpose of processing ETIAS applications is kept.

### EES Proposed Regulation<sup>137</sup>

- An article should be added within **Chapter I** (General provisions on the interoperability with ETIAS). The article should be similar to Article 7 "Interoperability with the VIS".
- A detailed article would have to be added in **Chapter III** (Entry of data and use of EES by other authorities) on the use of the EES data for examining travel authorisation applications. This article should authorise the use, by the CMPE, of EES data.
- An addition would need to be made to **Article 41** to ensure that a record of each consultation of EES by the CMPE or Member States for the purpose of processing ETIAS applications is kept.
- Other changes related to the technical implementation of ETIAS would have to be made to the implementing acts for the development and technical implementation of EES<sup>138</sup>, to reflect ETIAS reuse of the architecture of EES.

A number of additional existing legal texts have been analysed where the study concludes that there would be no amendments required. These are listed below:

---

<sup>135</sup> Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

<sup>136</sup> Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

<sup>137</sup> Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011.

<sup>138</sup> Article 33 of the EES proposal.

- **Regulation on Visa Requirements and Exemptions**<sup>139</sup>;
- **Regulation on Local Border Traffic**<sup>140</sup>: the Regulation would not need to be amended, even if it is foreseen to exclude visa-exempt third-country nationals that are border residents and holders of a local border traffic permit from the requirement to possess a travel authorisation. Indeed, it would be sufficient to state this exemption in the ETIAS legal basis;
- **Visa Code**<sup>141</sup>;
- **PNR Directive**<sup>142</sup>;
- **API Directive**.

### Connection to SLTD and TDAWN

Depending on the EU agency chosen to take up the role of CMPE, a new cooperation agreement might need to be signed with Interpol<sup>143</sup>.

### ETIAS management

- A new or extended mandate would have to be included in the appropriate, existing or new, legal basis for the **CMPE**;
- **eu-LISA**'s mandate would have to be extended in the agency's legal basis<sup>144</sup>, as the EU agency would be in charge of the operational management of ETIAS:
  - **Article 1(2)** would have to include a reference to ETIAS, to provide for eu-LISA to be responsible for the operational management of the system;
  - A new article would have to be created within **Chapter II** (Tasks), to describe the tasks performed by eu-LISA in relation to ETIAS;
  - **Article 7(5)** and **7(6)** would have to include references to ETIAS, to ensure that any external network provider would not have access to ETIAS and that the management of encryption keys remains within the competence of the agency;
  - **Article 8(1)** would have to include a reference to ETIAS. This would provide for eu-LISA to monitor the developments in research relevant for the operational management of the system (as the agency currently has to do for other EU systems it is responsible for);
  - **Article 12(1) (s)(t)(v)(x)(z)** may have to be amended to reflect that the eu-LISA's Management Board:
    - (s) Adopts reports on the development of ETIAS;
    - (t) Adopts reports on the technical functioning of ETIAS;
    - (v) Makes comments on the European Data Protection Supervisor (EDPS)'s reports on ETIAS audits and ensures appropriate follow-up to these audits;
    - (x) Publishes statistics related to ETIAS;
    - (z) Ensures annual publication of the list of competent national authorities having access ETIAS data for law enforcement purposes<sup>145</sup>.
  - **Article 15(4)** could be amended to authorise (the agency that hosts) CMPE to attend the meetings of eu-LISA's Management Board as observer when a question concerning ETIAS is on the agenda.

<sup>139</sup> Council Regulation (EC) No 1932/2006 of 21 December 2006 amending Regulation (EC) No 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement.

<sup>140</sup> Council and European Parliament Regulation (EC) No 1931/2006 of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention.

<sup>141</sup> Council and European Parliament Regulation (EC) 810/2009 of 13 July 2009 establishing a Community Code on Visas.

<sup>142</sup> Directive (Eu) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

<sup>143</sup> The European Monitoring Center for Drugs and Drug Addiction (EMCDDA), Frontex, Europol, Ceuol and Eurojust have signed cooperation agreements with Interpol. See: <http://www.interpol.int/About-INTERPOL/Legal-materials/International-Cooperation-Agreements/Regional-Organizations> (accessed 09/2016).

<sup>144</sup> Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011R1077> (accessed 09/2016).

<sup>145</sup> This could also be done by the European Commission.

- **Article 17(5)(g)** would need to be amended to add a reference to ETIAS legal basis. This would ensure coherence of the EU legal framework by stating that eu-LISA's confidentiality requirements would also allow compliance with ETIAS's provisions on confidentiality.
- **Article 19(1)** could be amended to add an "ETIAS Advisory Group" to the list of groups that shall provide eu-LISA's Management Board with expertise relating to large-scale IT systems. **Article 19(3)** could be amended to provide that (the agency that hosts) CMPE may appoint a representative to the ETIAS Advisory Group.

## 3.2 Data protection

This section elaborates on **data protection** considerations for ETIAS and, in particular, the **data protection safeguards** that ought to be put in place to ensure ETIAS is compliant with EU data protection principles.

### 3.2.1 Context

ETIAS would be processing high volumes of personal data. Access to the data is expected to be provided for different stakeholders, including national law enforcement authorities. Therefore, it is of particular importance to ensure adequate levels of data protection through the implementation of appropriate safeguards, in line with the applicable **EU data protection legal framework**<sup>146</sup> and taking into account **privacy by design**<sup>147</sup> considerations.

### 3.2.2 Approach

The approach used by the study to define the appropriate ETIAS data protection safeguards follows three steps:

1. **Data protection principles:** each data protection principle as provided for in the EU data protection legal framework<sup>148</sup> is presented and explained.
2. **Overview of data protection safeguards:** possible safeguards are listed (see Annex. 10 – “Data protection impact”), drawing on the following sources:
  - a. Existing legislation in the area of EU large-scale IT systems and data sets (VIS and SIS Regulations and Decisions, PNR Directive<sup>149</sup>);
  - b. Upcoming legislation (the EES proposal).

The section assesses whether each safeguard is **appropriate for ETIAS**, considering the findings of the previous sections, in particular the system’s purpose(s), the travel authorisation model, the data model and the architecture. The rule of thumb applied is that any existing data protection safeguard that is compatible with ETIAS, given its purpose and design, and that would strengthen the system’s privacy and accountability should be included. Only safeguards that clearly do not fit with the purpose and design of ETIAS have been excluded.

---

<sup>146</sup> A detailed overview is available in Annex 10. – “Data protection impact”.

<sup>147</sup> Privacy by design is based on seven guiding principles:

1. *Proactive not Reactive; Preventative not Remedial:* anticipate data protection risks and include mitigating actions and safeguards to prevent violation of data protection and privacy rights;
2. *Privacy as the default setting:* introduce requirements that will be incorporated into processes and technologies including data minimisation, purpose specification and limitation, barriers to data linkages and differentiated access;
3. *Privacy embedded into the design:* embed privacy in the design and architecture of the IT systems;
4. *Full functionality:* positive sum not zero sum – ensure that both security and data protection requirements are met;
5. *End-to-end security:* comprise data protection and privacy safeguards throughout the entire data lifecycle, from collection to deletion;
6. *Visibility and transparency:* include independent verification mechanisms to ensure the lawful processing of personal data;
7. *Respect for the user:* make sure that appropriate information is provided to the user.

See Technical Study on Smart Borders (2014), p. 27-28.

<sup>148</sup> In particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. For a description of the applicable EU data protection legal framework, see Annex 10. – “Data protection impact”.

<sup>149</sup> The API Directive is older and much less precise than the PNR, VIS, SIS and EES legal bases. It thus contains a limited number of data protection safeguards, which is the reason why it is not part of the table and analysis below.



- 3. Points of attention for ETIAS:** specific safeguards are discussed, as whether or how they should be implemented for ETIAS is not straightforward.

### 3.2.3 Data protection principles

As mentioned in Annex 10. – “Data protection impact”, the EU legal framework on data protection provides a list of different principles to be respected in the course of data processing<sup>150</sup>:

- **Lawfulness, fairness and transparency**  
The processing of personal data should be based on consent or should be necessary for legitimate purposes. In addition, processing should be based on EU or Member States’ law.
- **Purpose limitation**  
Data shall be “collected for specified, explicit and legitimate” purposes. It should not be further processed in a manner that is incompatible with these purposes.
- **Data minimisation**  
Data shall be “adequate, relevant and limited” for the purpose(s) for which it is processed.
- **Accuracy**  
Data shall be accurate. This principle includes the obligation for the data controller (i.e. the entity defining the purpose(s) and means of the data collection) to keep data up-to-date and ensure deletion or rectification of inaccurate data.
- **Storage limitation**  
Data shall be kept “in a form that permits the identification” of persons for no longer than necessary for the purposes. Data can be kept in an anonymised form for archiving.
- **Integrity and confidentiality**  
The security of the data collected should be ensured.
- **Accountability**  
The data controller is responsible for compliance with the above-mentioned principles. It shall demonstrate this compliance.

These principles are implemented in the EU systems and data sets through a number of safeguards.

### 3.2.4 Overview of safeguards

As illustrated in Annex 10. – “Data protection impact”, most of the safeguards existing for other systems and data sets are applicable to ETIAS, as ETIAS data would be processed centrally (safeguards aiming at eu-LISA apply) as well as by Member States (safeguards aiming at Member States apply).

However, as some of ETIAS’s features would be unique, the system requires putting in place adapted safeguards. Four of them (the ones for which whether or how they should be implemented for ETIAS is not straightforward) are described in the following section.

### 3.2.5 Points of attention for ETIAS

#### **Right of information**

The right of information would be ensured as follows:

---

<sup>150</sup> See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). See also Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Table 32: Overview of main right of information safeguards

Right	Safeguard	Responsibility
Right of information	<ul style="list-style-type: none"> <li>Information campaign</li> <li>Instructions on the ETIAS website/app</li> <li>Email instructions</li> </ul>	The <b>ETIAS implementation team</b> would ensure sufficient information is provided via the proposed channels.

## Remedies

Remedies (ways to set right an undesirable situation, e.g. a right has been violated) should guarantee the **rights of persons** whose data is collected<sup>151152</sup>, as follows:

Table 33: Overview of data protection procedures and responsibilities for remedies

Remedy	Responsibility
<ul style="list-style-type: none"> <li>Set-up of a function responsible for correction and deletion of inaccurate and unlawfully recorded data.</li> <li>Procedure in place for appealing to a mandated body or court against the treatment of personal data<sup>153</sup>.</li> </ul>	<ul style="list-style-type: none"> <li>The <b>DPO of the CMPE</b> handles requests for access, correction or deletion<sup>154</sup>.</li> <li><b>EDPS and/or the Court of Justice of the European Union</b> handle complaints related to processing by the CMPE;</li> <li><b>national competent authorities</b> handle complaints related to processing by MS.</li> </ul>

## Storage limitation by design

In line with the privacy by design approach, the study analysed whether placing part of ETIAS data in a dormant database or anonymising it could strengthen storage limitation in the context of ETIAS.

The detailed analysis that can be found in Annex 10. – “Data protection impact” provides the following conclusions:

### a) Dormant database

A ‘dormant database’ is a database to which access is more **restricted** than in the main ‘active database’ and in which data is kept for a passive, more **limited use**.

For ETIAS, a dormant database would be used to restrict access by the CMPE and processing units within Member States to background questions while permitting access for **reporting and law enforcement purposes**. Indeed, the background questions would not anymore be of use for application processing purposes.

The assessment of this safeguard suggests that it would be **highly appropriate for ETIAS**, as it would ensure adequate treatment and protection of some data, especially sensitive data, contained in the background questions<sup>155</sup>.

<sup>151</sup> The EU legal framework on data protection enshrines two main ‘rights’:

- Right of information: each person from who data is collected should be informed, as a minimum, about the contact details of the data controller and of the data protection officer, the purposes of the processing, the recipients of the data, the criteria used to determine the retention period, his/her rights and the extent to which providing data is mandatory.
- Rights of access, correction and deletion: each person from who data is collected has the right to access the data, to obtain rectification of inaccurate data and to obtain deletion under certain conditions.

Other rights, such as the right to data portability, are also enshrined in the General Data Protection Regulation. However, these are less relevant in the context of ETIAS.

<sup>152</sup> Article 47 of Charter of Fundamental Rights of the European Union (2012/C 326/02) enshrines the right to an effective remedy before a tribunal.

<sup>153</sup> Applicants would be informed about this procedure in the email received on the outcome of the decision-making process. For a list of the information that would be provided to applicants, see Annex 10. – “Data protection impact”.

<sup>154</sup> Requests for access, correction and deletion could as well be allocated to Member States. Rules would have to be defined to allocate applications that have not been processed by Member States. As this alternative creates complexity and risk creating confusion for applicants, it has not been retained by the study.

## **b) Anonymisation**

Anonymisation is the **masking-out** or **removal** from a data set of data that can be used to identify a person; in effect, the data set is transformed into a form which makes it impossible to identify specific individuals.

Anonymising ETIAS data could be envisaged to facilitate:

- **Applications processing** (identifying risk profiles and patterns as part of risk assessment); and
- **Reporting** (gathering of statistics).

Access to anonymised data would be restricted to specific stakeholders for these specific purposes. Based on the analysis, the **use of anonymisation for ETIAS should be assessed further** to confirm its relevance and added value before embedding it in the design of the system.

---

<sup>155</sup> This result could be achieved by using different technical means (e.g. access control or masking out background questions, which could be “de-masked” in case of necessary – appeal or law enforcement purposes).

## 4 Cost-benefit analysis (CBA)

Cost-benefit Analysis (CBA) is one of the standard evaluation tools applied within the framework of European Commission impact assessments. The approach applied for ETIAS CBA also uses the **standard methodology of the Commission**<sup>156</sup>.

The broad purpose of CBA is to facilitate a more efficient allocation of resources, demonstrating the **added value for society** of a particular solution, as well as the **conditions for the investor to arrive at a positive cost-benefit balance**. In particular, the results of a CBA should provide evidence that the solution is desirable from a socio-economic point of view and that it is consistent with the underpinning overall policy goals by confirming that a project contributes to their achievement.

CBA is built on the following main assumptions:

- The CBA is conducted from the point of view of the infrastructure owner, i.e. it takes into account costs and benefits for the Member States, but excludes costs and benefits for VE-TCNs and carriers. The latter ones are further explained in section 4.5 "Other impacts".
- The CBA is done on the basis of conservative assumptions avoiding the accumulation of "reserve buckets" but at the same time making sure that numbers are always on the "safe side". As an example the current costs of technological components are applied over the whole time span while the trend is having a reduced cost for equivalent capacity or performance. This benefit was found too risky to quantify and the safe approach of keeping costs constant for equivalent performance was adopted. Other examples of specific assumptions that also follow a cautious costing approach include the implementation of the system ("big bang" as opposed to gradual) and the two-year travel authorisation validity period (as opposed to three, four or five years). In these cases there was uncertainty regarding a "best"/preferred option and the higher-cost option was chosen to safely cover any scenario.

In addition, the following specific assumptions frame the CBA:

- The current list of visa-exempt countries contains 61 countries. It is estimated that countries that are currently in visa liberalisation process might increase the number of ETIAS applications by approximately 2.3 million<sup>157</sup>. However, the CBA does not take this increase into account as it would have a marginal effect and also due to the uncertainty of the outcome of the visa liberalisation process,
- The assumption on the timeline is:
  - By the end of 2016, the Commission issues the ETIAS legal proposal;
  - By the end of 2017, the co-legislators will adopt the Commission proposal;
  - Development starts after this adoption, which means from 2018 onwards;
  - The development can be performed over a 3-year period,
- Schengen acquis and its future development will apply to 30 countries, i.e.:
  - Schengen EU countries (Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain and Sweden);
  - Schengen non-EU countries (Iceland, Liechtenstein, Norway and Switzerland);
  - Accession countries working to implement the Schengen rules (Bulgaria, Croatia, Cyprus and Romania).
- The analysis evaluates the costs and benefits over a ten-year period following the assumption that the legislative proposal for ETIAS will be adopted by the end of 2017 and that ETIAS implementation will start in 2018. Thus, the CBA reference period is 2018 to 2027 which fits into the next EU Multi-annual Financial Framework.
- The assumption is made that ETIAS will follow a "big-bang" or uniform implementation approach: the system starts being operational in all the regions of the world in one go, be it from voluntary to mandatory or not. In case of gradual approach per region or border type, the maintenance costs during the first years of operations would be lower depending on how progressively the system

---

<sup>156</sup> [http://ec.europa.eu/regional\\_policy/sources/docqener/studies/pdf/cba\\_guide.pdf](http://ec.europa.eu/regional_policy/sources/docqener/studies/pdf/cba_guide.pdf) (accessed 07/2016).

<sup>157</sup> Estimation is based on number of uniform visa applications.

would be rolled-out and the fee revenue would only be collected for travellers who are in the scope of application of ETIAS.

- Both the baseline and regulatory scenarios account for the historical based natural growth trend in foreign national arrivals. It is not anticipated that ETIAS fee will reduce demand for travel to Schengen Area.
- The assumption is made that ETIAS authorisation will be valid for two years, which is the most conservative approach out of the most favourable options proposed by Member States<sup>158</sup>. If the validity period of ETIAS authorisation was longer, the number of applications would be lower, as frequent travellers would have to re-apply for authorisation to enter less often. Lower number of ETIAS applications would result in lower revenues from ETIAS fee and lower operational costs because of e.g. smaller number of applications to be processed manually.
- The assumption is made that each ETIAS application will require the payment of a non-refundable amount of 5 euros. The amount is sufficiently small to avoid a lasting impact on tourism even coming from less affluent regions. Any change of this fee amount impacts benefits significantly.
- In order to ensure coherence and consistency of the EU legal framework it is envisaged that data entered in ETIAS would be retained for five years, as is the case for EES and VIS. In case of shorter data retention period, less storage would be required, but this would have a very marginal impact on hardware and software costs, because of overall low storage requirements (please see hardware costs estimation for further reference).
- It is assumed that some of the EES infrastructure components will be re-used, (TESTA-ng network and National Uniform Interface (NUI)), however the sizing of the database was performed as if it were built as a standalone database. This was considered as the most conservative approach as the way the EES will be implemented will only be known after its legal text is adopted and its design has started.

This chapter provides a summary of the ETIAS CBA results. Detailed explanations of the rationale for costs and benefits estimations as well as explanations regarding the precise scope/content of each of the cost and benefit item are provided in Annex 11. – “Detailed cost-benefit analysis”. This annex should be read together with the *Excel* with detailed calculations of all cost items, which is provided as a separate document.

## 4.1 Cost model

The cost model includes estimations of total investment and operational costs. The investment costs are the expenditures planned to develop ETIAS during the first three years of the project and any one-off expenses incurred in the operational phase, while operating costs include routine maintenance costs, as well as software updates and hardware update costs.

The investment and operational costs are divided into:

- 1) **DG Home expenses;**
- 2) **eu-LISA expenses;**
- 3) **Expenses of the EU body to be in charge of Central Manual Processing Entity;**
- 4) **National expenses to be funded via ISF;** and
- 5) **National expenses to be funded either by national budgets or national programmes in the ISF funds.**

Based on the assumptions listed above, ETIAS development costs are estimated at 224 million. The last year of the development will require most of the investment, because of the start of operations of CMPE, as well as seeing the main software and hardware investments. The average operational costs of the system, including costs for system evolution, are estimated at 79 million per year. Total costs throughout the period under review, i.e. throughout the 10 years between 2018 and 2027 are estimated at approximately 780 million.

The figures and the table below provides an overview of the main ETIAS cost items.

---

<sup>158</sup> During consultations Member States were mostly in favour of two to four years ETIAS validity period.

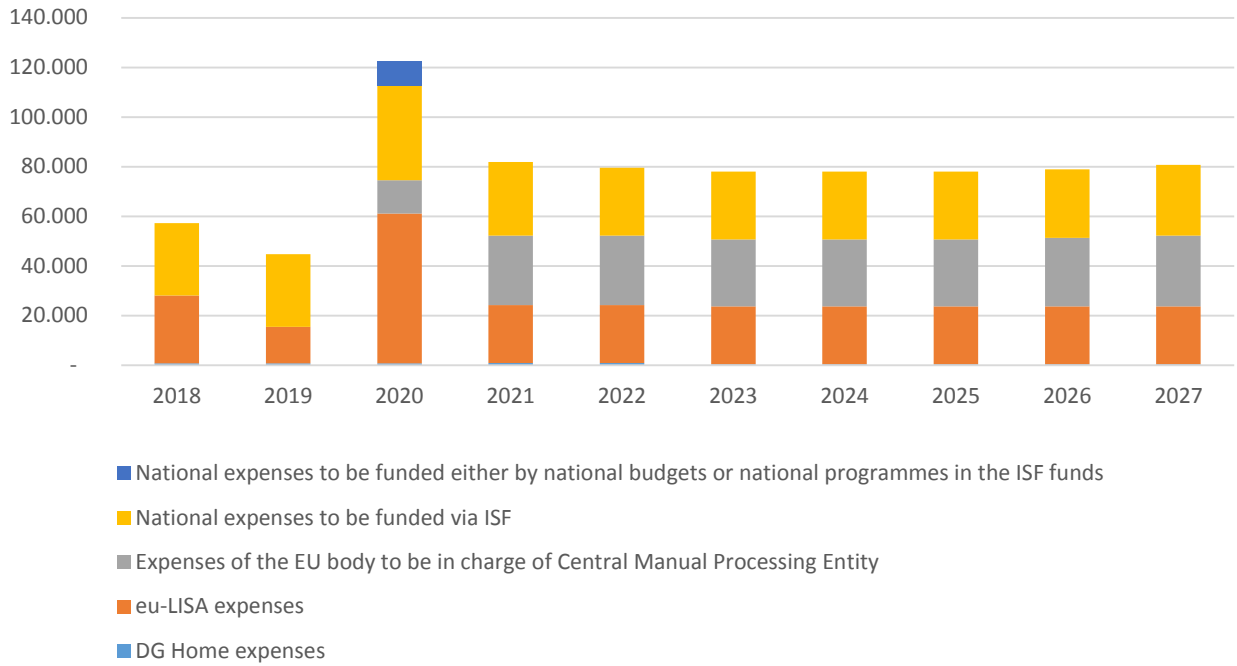


Figure 23: ETIAS costs structure per budget source ('000, EUR)

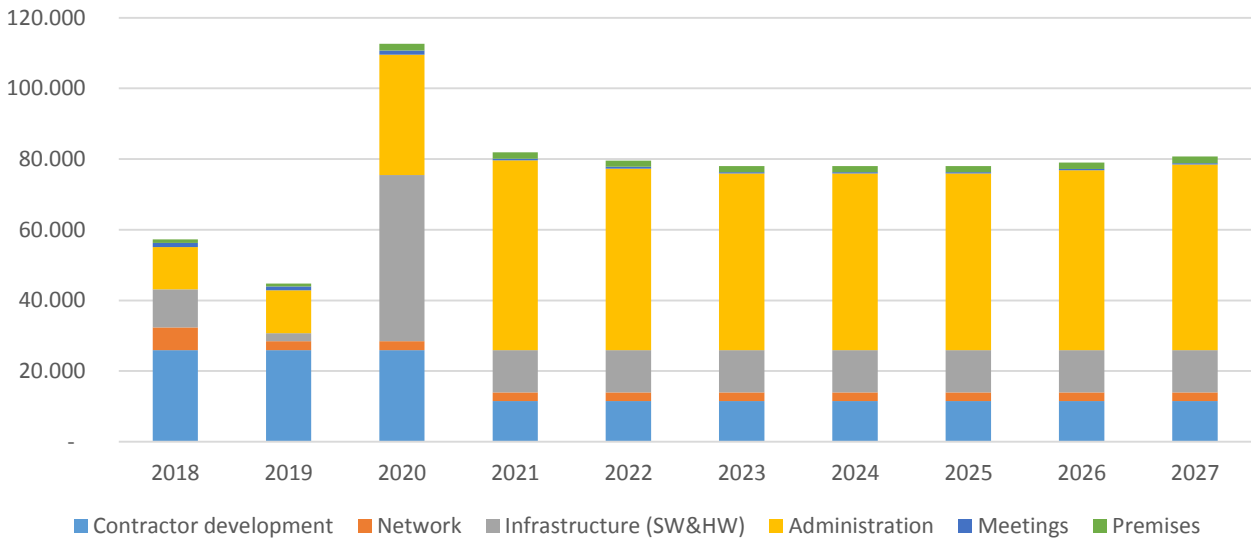


Figure 24: ETIAS costs structure per cost item ('000, EUR)

Table 34: The results of costs estimation ('000, EUR)

	Investment phase			Operational phase							TOTAL
	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	
<b>DG HOME expenses</b>	<b>725</b>	<b>725</b>	<b>725</b>	<b>859</b>	<b>859</b>	<b>334</b>	<b>334</b>	<b>334</b>	<b>334</b>	<b>334</b>	<b>5,563</b>
Administration (management of ISF; ETIAS fee distribution)	402	402	402	536	536	134	134	134	134	134	<b>2,948</b>
Meetings	323	323	323	323	323	200	200	200	200	200	<b>2,615</b>
<b>eu-LISA expenses</b>	<b>27,332</b>	<b>14,800</b>	<b>60,449</b>	<b>23,406</b>	<b>23,406</b>	<b>23,406</b>	<b>23,406</b>	<b>23,406</b>	<b>23,406</b>	<b>23,406</b>	<b>266,422</b>
Contractor development (Central System, interfaces, impact on other systems)	5,940	5,940	5,940	4,010	4,010	4,010	4,010	4,010	4,010	4,010	<b>45,887</b>
Software	8,862	1,974	38,352	10,075	10,075	10,075	10,075	10,075	10,075	10,075	<b>119,713</b>
Hardware	1,932	343	8,743	1,829	1,829	1,829	1,829	1,829	1,829	1,829	<b>23,822</b>
Network	6,441	2,472	2,472	2,472	2,472	2,472	2,472	2,472	2,472	2,472	<b>28,693</b>
Administration (development and operations team)	2,278	2,453	3,325	4,207	4,207	4,207	4,207	4,207	4,207	4,207	<b>37,507</b>
Meetings	819	819	819	168	168	168	168	168	168	168	<b>3,633</b>
Premises (office space for external contractors and additional staff, datacentre space)	1,061	798	798	644	644	644	644	644	644	644	<b>7,168</b>
<b>Expenses of the EU body to be in charge of Central Manual Processing Entity</b>	-	-	<b>13,422</b>	<b>28,026</b>	<b>28,026</b>	<b>27,006</b>	<b>27,006</b>	<b>27,006</b>	<b>27,543</b>	<b>28,534</b>	<b>206,568</b>
Administration (staff that will process ETIAS applications manually; managerial, support staff; information campaign)	-	-	12,294	26,897	26,897	25,877	25,877	25,877	26,392	27,341	<b>197,453</b>
Premises (office space)	-	-	1,129	1,129	1,129	1,129	1,129	1,129	1,151	1,193	<b>9,115</b>
<b>National expenses to be funded via ISF</b>	<b>29,240</b>	<b>29,240</b>	<b>38,047</b>	<b>29,603</b>	<b>27,293</b>	<b>27,293</b>	<b>27,293</b>	<b>27,293</b>	<b>27,688</b>	<b>28,418</b>	<b>291,405</b>
Contractor development (integration and operations of NUI)	20,000	20,000	20,000	7,500	7,500	7,500	7,500	7,500	7,500	7,500	<b>112,500</b>
Administration (teams in Member States, involved in PNR/ API processing, technical	9,240	9,240	18,047	22,103	19,793	19,793	19,793	19,793	20,188	20,918	<b>178,905</b>

	managers and other staff)											
NATIONAL BUDGETS	National expenses to be funded either by national budgets or national programmes in the ISF funds	-	-	10,000	-	-	-	-	-	-	-	10,000
	Training	-	-	10,000	-	-	-	-	-	-	-	10,000
	Total development and operational costs (in '000)	57,297	44,765	122,643	81,893	79,583	78,038	78,038	78,038	78,972	80,692	779,959

Total development costs (in '000)	224,705
Average yearly operational costs (in '000)	79,322

## 4.2 Benefits model

The benefits model covers estimations of tangible benefits, such as revenues coming from user fees, as well as intangible ones, such as time savings from process automation. The results of the benefits estimation are provided in the table below.

Estimation of the benefits relies on two main assumptions:

- ETIAS application will require the payment of a non-refundable amount of 5 euros;
- There will be around 40-43 million applications submitted each year.

Table 35: The results of benefits estimation ('000, EUR)

	Investment phase			Operational phase							TOTAL
	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	
ETIAS fee revenues	0	0	0	203,000	179,350	186,150	192,950	199,750	207,060	214,540	<b>1,382,800</b>
Time savings	0	0	0	989	1,014	1,114	1,219	1,329	1,446	1,568	<b>8,679</b>
<b>Total benefits</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>203,989</b>	<b>180,364</b>	<b>187,264</b>	<b>194,169</b>	<b>201,079</b>	<b>208,506</b>	<b>216,108</b>	<b>1,391,479</b>

The quantifiable benefits are dominated by the amount of the fee collected. The time saving for border guards to handle a lower amount of travellers refused at the border leads to a small benefit. This is due to the use of modest assumptions as regards the cost saving (estimate of 2 hours saved per case) and the use of a low cost per border guard hour (17 euro average). Employer's costs for first line border guards are in a range of 1 to 10 between the lowest and highest value among Member States considered.

The result of the computation shows that benefits accrue steeply: revenue (around € 200 million per year) is about 2,5 higher than the average operations costs (around € 80 million per year). Hence the initial investment of € 224 million is recovered within less than two years. The "benefit" is put as revenue to the EU budget and reduces each Member State contribution.



## 4.3 CBA outcome

Once all ETIAS costs and benefits are quantified and valued in monetary terms over the time period considered, it is possible to conclude on the CBA outcome, which is expressed via the following:

- **The Net Present Value (NPV)<sup>159</sup>** of ETIAS amounts to EUR 429 million which shows that the discounted total benefits are higher than the costs and the project is desirable;
- **The Internal Rate of Return (IRR)** is equal to 35%, which means that there will be a gain in investment;
- **The Benefit-Cost ratio (B/C ratio)<sup>160</sup>**, which amounts to 1.7, again indicates that discounted benefits are higher than the discounted costs and that the system is worth the investment.

The very positive figures need to be handled cautiously as despite all efforts, this is an exercise spanning over the long term (next 10 years) and is only as valid as long as the assumptions are met.

The CBA outcome essentially leads to the conclusion that even a small fee of 5 euros per application will be sufficient to have ETIAS running as a financially self-supporting system.

## 4.4 Sensitivity analysis

This section of the study provides the results of the sensitivity analysis, which identifies the critical variables of the project. Such variables are those whose variations, be they positive or negative, that have the largest impact on the costs and benefits of the project. In ETIAS case, the most critical variables are the following:

- **The number of VE travellers:** if the number of travellers was 10% lower than assumed in the estimations, the overall costs would be 5% lower and the benefits would be 10% lower. The investment rate of return (IRR) would amount to 29%, i.e. it would lower by 4 percentage points and cost-benefit ratio (B/C) would amount to approximately 1.5, i.e. it would be lower by 10 percentage points.
- **Percentage of the applications to be processed manually:** if 10% of all applications were processed manually, instead of 5% that are foreseen in the model, this would almost double the costs of the CMPE. This would also increase the total costs significantly – by 23%, as CMPE costs comprise very large share in the total costs. IRR would decrease to 23%, whereas B/C ratio would decline to 1.3.
- **Time needed to process 1 application manually at CMPE:** if it took 12 minutes, instead of anticipated 10 minutes, to process 1 application manually, the administrative and premises costs of CMPE would be 18% higher and total costs of ETIAS would be 5% higher. The total cost calculation is very sensitive for this parameter. The average 10 minutes per case is a conservative estimate compared to other benchmarks. An increase of the average time from 10 to 12 minutes looks small but is in fact very significant as it refers to an average over a large amount of cases.
- **ETIAS fee:** 1 EUR decrease in fee would result in 25% reduction of ETIAS fee revenues. If ETIAS was made available for free for children under 12 years old and if they account for a 15% share of all travellers, this potentially would lower the fee revenues by around 18%. IRR would decrease to 31%, whereas B/C ratio would decline to 1.53.
- **Maintenance costs of hardware and software:** if the percentage for the maintenance costs of hardware and software was increased to 25%, instead of 20%, this would result in 10%

---

<sup>159</sup> NPV is the sum of the discounted total benefits and costs of a project. The NPV is a very concise performance indicator: it represents the present amount of the net benefits (i.e. benefits less costs) flow generated by the project expressed in one single value.

<sup>160</sup> The B/C ratio is the present value of project benefits divided by the present value of project costs. When this ratio is greater than 1, the benefits are greater than the costs and the project is desirable.

increase of overall software costs and 8% increase in hardware costs. However the impact on total costs of ETIAS would be negligible. It would amount to only 2% increase.

- **Costs for ETIAS evolution:** if the evolution costs of ETIAS was estimated as 15% of the initial development, instead of 10%, this would result in IRR decrease by 1 percentage point and B/C ratio decrease by 5 percentage points.
- **Validity period of ETIAS application:** if the validity period for the ETIAS application was extended to 5 years (rather than 2 years in the current computation), the workload for CMPE and teams in Member States, involved in PNR/ API processing would decline gradually for the first 4 years of ETIAS operations, due to the declining number of new applications. Therefore administrative costs of CMPE would decrease by 13% and administrative costs of teams in Member States, involved in PNR/ API processing would decrease by 11%. The maximum storage requirements and processing power requirements could be lower in case of the longer validity period for ETIAS. This could result in an approximately 9% decrease of hardware costs, 2% decrease of software costs and 7% decrease of overall costs. Since a lower proportion of travellers would require ETIAS, the revenues would be also lower by 11 percentage points. At the end the revenue decrease (about EUR 154 million over 10 years) would be more important than the cost decrease (about EUR 52 million). At the end the IRR would decline to 33%, whereas B/C ratio would decrease to 1.6.
- **Transition period for ETIAS application:** in case of a 1-year transition from voluntary to mandatory, it is assumed that only 20% of travellers will use the application. This would have a significant impact (of around 13% decrease), on administrative costs, because less staff will be needed for CMPE and teams in Member States, involved in PNR/ API processing, technical managers and other staff at the first years of operations. Total cost would thus amount to approximately 735 million euros. The collected revenues from the ETIAS fee would be also by approximately 7 percentage points lower, because of lower number of applications.

## 4.5 Other impacts

As mentioned under the main assumptions, ETIAS CBA was conducted from the from the point of view of the infrastructure owner, i.e. the estimated balance takes into account costs and benefits for the Member States, but excludes costs and benefits for VE-TCNs and carriers. The latter ones are explained in more detail in the table below.

*Table 36: Costs and benefits for travellers and carriers*

	Costs	Benefits
For travellers	<ul style="list-style-type: none"> <li>• VE-TCNs will have to pay non-refundable fee for ETIAS application, which is assumed to amount to 5 Euros.</li> <li>• VE-TCNs will also bear the costs of additional time, needed to fill-in ETIAS application. It is estimated that this time should amount to approximately 10 minutes for each application.</li> </ul>	<ul style="list-style-type: none"> <li>• The main benefit for the travellers will be avoided trips to and back from the border in case of prior refusal via ETIAS.</li> </ul>
For carriers	<ul style="list-style-type: none"> <li>• Carriers will bear the costs of connecting their systems to ETIAS, so that they could check ETIAS application status before boarding the traveller. The amount of those costs will depend upon the existing carriers' infrastructure.</li> </ul>	<ul style="list-style-type: none"> <li>• Carriers will benefit from less costs for taking back travellers refused at the border ("inadmissible arrivals").</li> <li>• There will be less penalties as ETIAS allows also to check that the travellers has a passport whose expiry date meets the entry conditions.</li> </ul>

## 5 Conclusions

This chapter includes the **main findings** of the study and the **critical success factors** that are crucial to ETIAS successful implementation and functioning.

### 5.1 Main findings

The following main findings are derived from the analysis conducted in Chapters 2, 3 and 4. Each finding relates to one of the 11 topics<sup>161</sup> investigated in the study. For each topic, different options have been considered. The preferred ones were identified by applying assessment criteria and analysing different options' advantages and disadvantages. This allowed the identification and description of the ETIAS configuration that fits most with the purpose defined by different stakeholders and with the current context. The findings presented in this section relate to this preferred configuration, options that were ruled out are not mentioned below.

#### 5.1.1 Design principles

---

- Finding 1** ➤ **Purpose:** ETIAS main purpose would be an advance security and migration risk assessment of visa-exempt travellers with a view to grant an authorisation to travel to the Schengen Area.
- 

ETIAS would aim at checking whether visa-exempt travellers are eligible to enter the Schengen Area *before* they start travelling, allowing to reassure both travellers and carriers that a refusal of entry would be unlikely (although still possible).

---

- Finding 2** ➤ **Authorisation model and validity period:** once granted, an authorisation would be valid for a period of time that for practical purposes would best be comprised between two and five years (or the validity of the passport, whichever comes first).
- 

Three authorisation models have been considered in the course of the analysis:

- 4) A travel authorisation valid for a **period of time**;
- 5) A travel authorisation valid for a **single trip**;
- 6) A **combination of 1 & 2**: a travel authorisation valid for a period of time with an obligation for the traveller to notify authorities before each new trip.

Benchmark systems (from US, Canada and Australia) have chosen to implement systems delivering travel authorisations valid for a period of time. This model is indeed more convenient for travellers and would bring less workload for the authorities in charge of manually processing the applications, while still bringing added value in terms of assessing the risks posed by travellers.

A similar balance would have to be achieved for ETIAS with a travel authorisation longer than two years to accommodate frequent travellers but shorter than five years to ensure the relevance of the information collected (although the re-check process, i.e. periodic checks against new information or alerts entered into EU or Interpol's systems, would enable the travel authorisation to stay reliable throughout time).

---

- Finding 3** ➤ **Fee:** the collection of a fee in order to finalise the travel authorisation application process would be highly beneficial to ETIAS.
- 

---

<sup>161</sup> Design principles, data, business processes, architecture, user interactions, system security, implementation approach, future technology options, legal impacts, data protection and costs. There is no finding related to future technology options and legal impacts, as these two sections are not related to the ETIAS system per se but to future technology developments and the EU legal framework.

Collecting a fee would have the following advantages:

- **Filter:** a fee could act as a filter as it would deter the submission of a very high number of applications (e.g. for the purpose of bypassing the system or breaking it down) and fake applications and serve as a “proof of intent” to travel;
- **Contribution to the system:** it would make a substantial contribution to ETIAS running costs.

## 5.1.2 Data

---

**Finding 4** ➤ **Application form:** 22 data would be collected from each traveller.

---

The following categories of data would be collected:

- Biographical data (e.g. name, date of birth...);
- Passport data;
- Contact details;
- Information on the intended travel (Member State of intended first entry);
- The answer to 5 background questions (e.g. education and occupation data).

This dataset (maximum 26 data fields) is **smaller than what is being collected by a similar system** (ESTA) in the US (minimum 37 data fields), and also much **more limited than the information currently requested in the Schengen visa process** (minimum 44 data fields). ETIAS would also not collect biometric data as opposed to the Schengen visa process since the reliability of biometric data remotely collected cannot be ensured (it cannot be ensured that the biometric data belongs to the applicant).

---

**Finding 5** ➤ **Risk-assessment n°1:** cross-check would be done against the following databases: EES, VIS, SIS, SLTD and TDAWN. Access to Europol data would be worthwhile as well, pending systems capacity and relevant data volume increase. Similarly, access to ECRIS and EURODAC data could be foreseen in the future should data relevant for ETIAS purposes become available in these systems.

---

**EES** is the future Entry/Exit system recording the entries and exits in the Schengen Area of all third-country nationals (proposal currently under discussion). It would provide information on whether a person has overstayed or has been refused entry.

**VIS** (Visa Information System) would be used to check whether the person has been denied a visa and for what reason<sup>162</sup>.

**SIS** (Schengen Information System) contains information on objects and persons of interest. It would be used to check whether the person is subject to an entry ban or another alert (e.g. the person is a child reported as missing) or whether the person’s passport is sought for seizure or has been reported lost or stolen.

**SLTD** (Lost and Stolen Travel Document Database) would be used to check whether the applicant’s passport is lost or stolen, as reported by countries that do not enter alerts in SIS (other countries than Schengen countries and the United Kingdom).

**TDAWN** (Travel Documents Associated with Notices) contains records of genuine travel documents belonging to criminals. It would be used to check whether the applicant’s passport is reported as being of these.

---

<sup>162</sup> For those coming from a country which has just changed visa regime.

---

**Finding 6** ➤ **Risk-assessment n°2:** in addition to cross-checks against databases, background questions and screening rules would be used for the risk-assessment.

---

**Background questions** would relate to e.g. whether the person has previously been refused entry and would be used during manual processing for assessing whether the person poses a security or migration risk.

The **screening rules** would be created by the CMPE and Member States. They would include:

- “Investigation triggers”, i.e. specific values (e.g. phone numbers) that would trigger manual processing if these values are entered into a newly submitted application;
- Data analytics rules, i.e. common risk indicators and patterns.

These rules would be periodically reviewed to ensure that they are relevant and up-to-date.

They would allow to:

- Harmonise the risk assessment. During current border controls, other Member States’ databases than the one of entry are not consulted and hence the assessment can be different depending on the point of entry in the Schengen Area;
  - Enable confidentiality of the investigation triggers inserted by each Member State – the values would be encrypted and only visible to the Member State that creates them.
- 

**Finding 7** ➤ **Retention and access:** data would be retained for 5 years after the end of validity of the travel authorisation. They would be accessible for law enforcement purposes under specific and pre-determined conditions.

---

ETIAS data would become part of the EES individual file as a visa-exempt traveller is in almost all cases going to pass a Schengen border-crossing point (a small number of travellers may decide to cancel a trip after they applied and received a travel authorisation). The ETIAS data retention period would therefore be aligned with the one of EES and would be five years starting from the **end of the validity period** (either because of the elapse of time or because of a revocation). For denied travel authorisations, it would be five years from the moment of the decision.

**Law enforcement authorities** would **not have access to all ETIAS data**. Safeguards/conditions would have to be met. The approach proposed in the study to law enforcement access is similar to what has been proposed for EES.

### 5.1.3 Business processes

The process section described the main processes that support ETIAS in the different phases of the traveller's journey:

1. **Application:** applicants request a travel authorisation by filling-in an online form;
2. **Decision-making** (including notification to applicants): depending on the case, the authorisation is automatically granted (within minutes) or the request is transferred for manual processing to the competent authorities. In all cases, an answer to the applicant is provided 72 hours maximum after the application has been submitted<sup>163</sup>;
3. **Verification before boarding:** air and sea carriers would mandatorily verify before boarding whether the traveller has a travel authorisation. If not, the carrier would know that boarding the traveller exposes him to be liable to return him. For land carriers (railways, buses...), this verification would not be mandatory but their liability for taking the traveller back would remain;
4. **Verification at the border:** an automated query to ETIAS would allow border guards to swiftly verify whether a traveller has a travel authorisation. While a denied travel authorisation (or the absence of one) would always lead to a refusal of entry, having a travel authorisation would not give a "right of entry". The decision on whether or not to authorise entry would still be taken by the border guard at the border-crossing point.

The figure below illustrates the entire process.

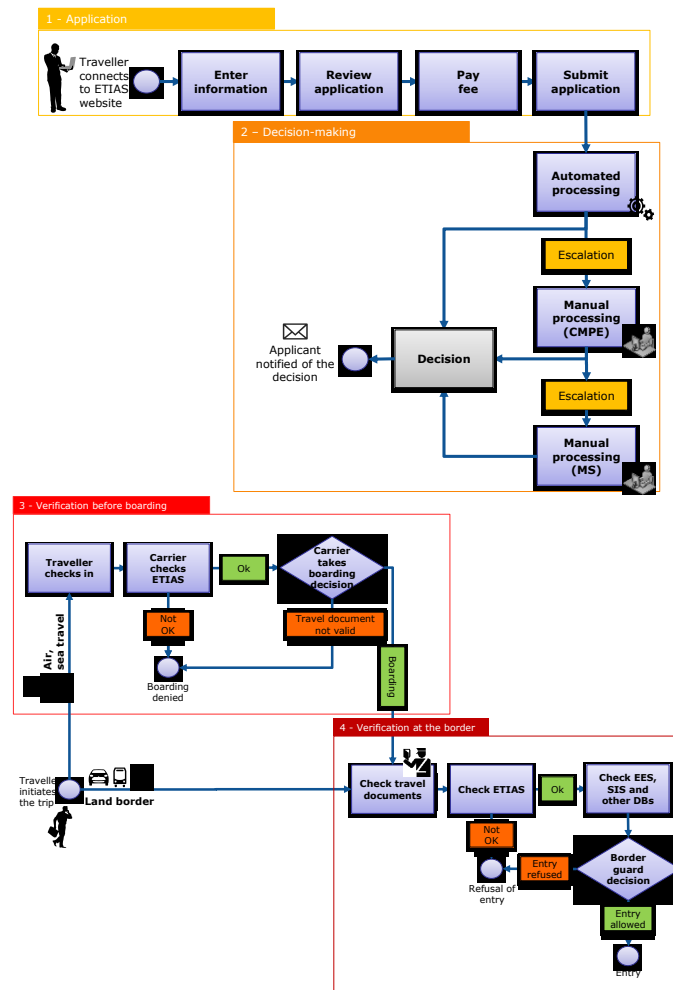


Figure 25: ETIAS process overview

<sup>163</sup> As the answer from the Member State may consist in requesting additional information or an interview, the total processing time of an application may be longer than 72 hours.

Additionally, four “support processes” have also been identified in the study: a) query of the authorisation status, b) re-check of granted travel authorisations (to regularly check whether there is any new piece of information or alert in the EU or Interpol’s systems that modifies the status of existing travel authorisations), c) revocation of an already-granted application, and d) appeal to the decision to deny or revoke an authorisation.

- 
- Finding 8** ➤ **Processing of application:** more homogeneous security and migration risk-assessment of VE-TCN requires a central role. A model exists which combines decision-making at central and national level. This model can be implemented with different variants on the split of responsibility between both.
- 

The creation of a central entity would be needed to address the following requirements:

- Handle the cases in which the consultation of the databases revealed a hit or that match a risk pattern;
- Lessen the workload for Member States (to only 1 to 3% of all cases) and consulates by transferring only the cases where there is a need for more analysis and that may lead to a denial;
- Coordinate the decision-making process at European level;
- Provide a uniform process/experience to travellers.

If no central administration were to be created the entire burden of processing the applications would then fall on Member States, compromising the overall feasibility of ETIAS given the volumes to be processed.

- 
- Finding 9** ➤ **Recheck:** SIS and EES should be adapted/built to notify ETIAS of new (or updates on) alerts on refusal of entry and new (or updates on) overstayer cases.
- 

This would allow ETIAS to recheck already-granted applications in light of these new pieces of information. Such a solution would be more proportionate in terms of privacy than ETIAS searching for a match between all the already-granted applications and all the refusal of entry alerts in SIS and overstay cases in EES (as only data of data subjects concerned are exchanged). It would also be less demanding in terms of processing capacity.

An efficient re-assessment process would diminish the need for a short validity period for the travel authorisation, which would be beneficial to travellers’ acceptance of the system.

#### 5.1.4 Architecture

---

- Finding 10** ➤ **Central vs decentralised system:** a central architecture would provide more benefits for ETIAS.
- 

A **central** architecture emerges as the most fit-for-purpose for ETIAS. As opposed to a fully (or partially) de-centralised system, it has the following advantages:

- Reduced implementation complexity (single system vs. integration of up to 30 systems, one for each Member State);
  - Reduced costs, stemming from both a simpler design and higher economies of scale;
  - Higher level of oversight and control thanks to an easier auditability and simpler accountability and ownership allocation.
- 

- Finding 11** ➤ **Reuse:** the EES architecture blocks could be used for ETIAS.
- 

The following building blocks of EES could be reused:

- Its communication network;
- The National Uniform Interfaces (NUI), i.e. standardised interfaces for national systems;
- The web service for carriers;
- The database.

### 5.1.5 User interactions

Travellers should not take more than ten minutes to fill in an ETIAS online form. The time spent on filling an application may negatively affect the data quality and a cumbersome system could also deter travellers from initiating the application process.

The time to fill-in the application is directly linked to the **website design**. For instance, while the US ESTA website contains six pages, the Canadian eTA is composed of two pages. From an applicant point of view, the Canadian system seems much shorter than the American for an almost similar data set.

---

**Finding 12** ➤ **Travellers website:** the website used by travellers to apply for a travel authorisation would need to take into account a number of parameters (including languages spoken by VE-TCN) to ease the application process.

---

While all EU languages would not be relevant for the ETIAS application form, a number of EU and non-EU languages are spoken by a large part of visa-exempt travellers (e.g. Spanish, Japanese). Should the application be only in English, support would need to be available in a number of other languages.

Another element to take into account is the data collection method (scroll-down menu, pop-up window or free field) as some could be seen as more cumbersome and complex to understand than others.

---

**Finding 13** ➤ **Helpdesk:** a helpdesk would be necessary to allow travellers to call in case of an issue with the application or the website.

---

The feedback received could be used to improve the website and spot possible IT issues, which would be crucial in ensuring the implementation of ETIAS does not impact tourism.

---

**Finding 14** ➤ **Application with the help of a third party:** authorising a third party (e.g. travel agency or a family member) to fill-in an application form on behalf of a traveller is crucial to ensure ETIAS accessibility.

---

This possibility would be very beneficial to counter issues some applicants may face: limited to no access to an Internet connection, a computer or a credit card, handicap etc...

---

**Finding 15** ➤ **Connection to carriers' systems:** carriers' connection to ETIAS should be harmonised with the interfaces/systems that are currently used for the transmission of API data.

---

Air carriers operating in the EU have implemented systems that allow them to transmit travellers' API data<sup>164</sup>. The verification of the travel authorisation status would thus take place as an answer to the transmission of API data using the same message formats. This would allow reducing costs and increasing convenience for carriers.

---

<sup>164</sup> API (Advance Passenger Information) are data transmitted by air carriers to national authorities for the purpose of combatting irregular migration.



## 5.1.6 System security

---

**Finding 16** ➤ **Safeguards:** 7 main types of safeguard are relevant for ETIAS.

---

ETIAS, as a system operating via Internet, would be exposed to much more security risks than any of the other EU large-scale IT systems, which function with a closed user group (only Member States' administrations can access them).

Nevertheless, a detailed examination of risks applied on the basis of the ISO 31000 risk assessment methodology allows to define a comprehensive set of safeguards.

Two key safeguards have been identified: 1) access for travellers would be limited to submitting an application via the ETIAS Internet services, and requesting the status of their application using a reference number. Applicants would not access the database itself; 2) similarly, carriers would not query the database itself but an extract of it.

Other safeguards consist in systematically applying high standards in the following areas:

- Human resources (e.g. training, security awareness);
- Access control (e.g. use of strong passwords, systematic changes, password protection...);
- Cryptography (e.g. encrypted communications between Member States and the ETIAS system) ;
- Communication security (i.e. ensuring networks are protected);
- System acquisition, development and maintenance (e.g. prior testing before go-live);
- Information security incident management (i.e. procedures are in place to follow-up on any security incident);
- Operation security (e.g. availability of the system is ensured).

## 5.1.7 Implementation approach

---

**Finding 17** ➤ **Options:** the conditions for a successful "big bang" approach are difficult to achieve as it requires multiple stakeholders (national systems, border control systems, carriers, etc.) to be ready on time by a precise date while they are not all accountable to the same authority. The preferred option would be to include a strongly monitored transition from "voluntary to mandatory".

---

The following options were examined:

- **"Big-bang"**: ETIAS is operational in all the regions of the world and at all border types in one go;
- **Gradual by border type**: ETIAS is implemented at one Member State border type at a time;
- **Gradual per region**: the travel authorisation is first required in region x of the world, then in region y and finally in region z;
- **From voluntary to mandatory**: holding a travel authorisation is voluntary in all regions and at all border types at first and then becomes mandatory after time, while allowing for an initial period of grace.

In addition, some functionalities could be considered for later implementation (e.g. connection with the VIS, etc.).

---

**Finding 18** ➤ **Grace period:** independently of the option(s) chosen for implementing ETIAS, the implementation would highly benefit from a grace period.

---

From the date of applicability of the mandatory requirement, travellers without a travel authorisation could be allowed one-off travel and (potentially) entry to the Schengen Area, during a fixed period of time, in order to give them time to adjust to the new system.

## 5.1.8 Data protection

Most of the safeguards existing for other systems and data sets are applicable to ETIAS; indeed, as ETIAS would possess central and decentralised components, safeguards related to centralised/semi-centralised systems (notably EES and VIS) and safeguards related to decentralised ones (PNR<sup>165</sup>) are both appropriate. However, as some of ETIAS's features would be unique, the system would also require putting in place adapted safeguards.

---

**Finding 19** ➤ **Safeguards n°1:** as some of ETIAS's features would be unique, the system would also require putting in place adapted safeguards.

---

In particular, the creation of the CMPE would require to adapt the allocation of accountability and responsibility concerning data accuracy, which is in other EU IT systems allocated to Member States.

---

**Finding 20** ➤ **Safeguards n°2:** the use of a dormant database should be foreseen to ensure adequate treatment and protection of some data.

---

To ensure access to data for **reporting purposes** and **law enforcement purposes** while increasing the level of protection of sensitive data contained in the background questions, an additional safeguard would be introduced, which consists in transferring **data which is not needed for applications processing** anymore into a dormant database<sup>166</sup>. It is one of the techniques in line with the privacy by design approach. Such data would be moved from the active database at the latest at end of validity period (in the range of two to five years) of the travel authorisation.

---

**Finding 21** ➤ **Rights of information and access:** the **ETIAS implementation team** would ensure sufficient information to travellers is provided via the proposed channels; the Data Protection Officer of the CMPE would handle request for access, correction or deletion.

---

If the Data Protection Officer would deny access, correction or deletion, or would not answer within the given lead time, the person would have the possibility to bring a complaint before the EDPS and/or the Court of Justice of the European Union.

---

<sup>165</sup> The PNR (Passenger Name Record) is a data set sent by airlines to Member States in order for them to conduct a risk assessment on passengers arriving to the Schengen Area by air.

<sup>166</sup> A 'dormant database' is a database to which access is more restricted than in the main 'active database' and in which data is kept for a passive, more limited use.

## 5.1.9 Cost-benefit analysis (CBA)

### Finding 22

- **Total cost and benefit:** Setting up ETIAS would cost 224 million euros while operating the system is estimated at 79 million annually. Therefore in total, cumulated over 10 years, ETIAS would cost 779 million euros to develop and run while the expected quantifiable benefits from having the system (time savings and fee revenue) would amount to 1.4 billion euros. The benefits remain volatile as they could be lower depending on the staff required to handle applications manually, but are sufficient to state that ETIAS can be managed financially as a zero-sum operation for the EU budget. It should be noted that the main benefits are not quantifiable as they concern an increased level of security.

The investment and operational costs would be divided between DG Home, eu-LISA, the central manual processing entity (CMPE) and Member States. More specifically, the costs would be divided into:

- DG Home expenses (5,6 million euros over 10 years);
- eu-LISA expenses (266,4 million euros);
- Expenses of the CMPE – this entity would be created to handle applications that would have to be processed manually, in order to alleviate Member States’ workload (206,6 million euros);
- National expenses to be funded via ISF<sup>167</sup> (291,4 million euros); and
- National expenses to be funded either by national budgets or national programmes in the ISF funds (10 million euros).

The most important part of the cost would be related to manual processing by the CMPE. Taking into account the foreseen number of visa-exempt travellers to the Schengen Area, a **5-euro fee** would be sufficient to cover ETIAS’s costs.

## 5.2 Critical success factors

The following critical success factors are crucial to ETIAS implementation and functioning.

Critical success factor	Proposed solution(s) identified in the study
<b>Added value for internal security and national authorities</b>	<ul style="list-style-type: none"> <li>– Use of information available in national, EU and international databases to maximise the efficiency of the risk assessment;</li> <li>– Harmonisation to carry out an homogenised risk-assessment: <ul style="list-style-type: none"> <li>○ A single interface (website or app) and unique EU-wide application form;</li> <li>○ Automatic processing by a central system;</li> <li>○ Coordination by a central processing unit.</li> </ul> </li> <li>– Large scope of ETIAS (it applies to all VE-TCNs with only thoroughly thought-through exceptions).</li> </ul>
<b>Security and data protection to:</b> <ul style="list-style-type: none"> <li>– Limit risks for the internal security of the EU;</li> <li>– Limit risks of unauthorised access to data;</li> <li>– Ensure legal compliance;</li> <li>– Embed privacy by design.</li> </ul>	<ul style="list-style-type: none"> <li>– Appropriate safeguards. This would require both the use of: <ul style="list-style-type: none"> <li>○ The data protection safeguards established for other EU systems; and</li> <li>○ Tailor-made solutions adapted to the specificities of ETIAS.</li> </ul> </li> </ul>
<b>Ease of implementation to:</b> <ul style="list-style-type: none"> <li>– Ensure a smooth, quick cost-effective transition;</li> <li>– Avoid delay in implementation;</li> <li>– Limit impact on the main stakeholders.</li> </ul>	<ul style="list-style-type: none"> <li>– Attention to existing carriers’ systems requirements and specificities during the implementation of these systems connection with ETIAS;</li> <li>– Extensive communication campaign to avoid a high number of travellers coming to the border without a</li> </ul>

<sup>167</sup> Internal Security Fund. The Fund promotes actions related to the management of the Schengen Area borders.

Critical success factor	Proposed solution(s) identified in the study
	travel authorisation.
<b>Ease of use</b> to: <ul style="list-style-type: none"> <li>- Limit impact on the main stakeholders;</li> <li>- Avoid negative impact on EU business/tourism.</li> </ul>	<ul style="list-style-type: none"> <li>- Integration with the EES web service for carriers;</li> <li>- Appropriate messaging system delivering a clear, concise and fast answer to carriers' queries on travel authorisation status;</li> <li>- Integration of the EES web service for travellers. The web service would provide a single traveller's virtual point of entry to Schengen;</li> <li>- Easy and fast application process;</li> <li>- Overall user-friendliness of the website.</li> </ul>
<b>Technical flexibility</b> to: <ul style="list-style-type: none"> <li>- Cope with the ever-increasing number of travellers;</li> <li>- Cope with future changes of the list of visa-exempt countries;</li> <li>- Facilitate re-use and interoperability to maximise the efficiency of the risk assessment.</li> </ul>	<ul style="list-style-type: none"> <li>- Scalability, i.e. a system that could be further expanded in case of need, especially for handling application traffic via the ETIAS website;</li> <li>- Interoperability, i.e. a system interoperable with other systems, capable of querying them with high frequency;</li> <li>- Possible integration with the EES to exploit synergies.</li> </ul>
<b>Moderate investment and running costs</b> for: <ul style="list-style-type: none"> <li>- ETIAS to remain a "financially zero-sum operation" for the EU budget while only requiring a small fee per application.</li> </ul>	<ul style="list-style-type: none"> <li>- Reuse of existing technical components;</li> <li>- CMPE hosted in an existing EU agency;</li> <li>- National teams hosted in existing entities handling passenger data;</li> <li>- Well-defined and efficient process.</li> </ul>
<b>Accessibility</b> to: <ul style="list-style-type: none"> <li>- Ensure access to the application form and other services by visa-exempt people, as the system would rely on applications made via Internet and mobile Internet access becomes more widespread than Internet access via fixed lines.</li> </ul>	<ul style="list-style-type: none"> <li>- Deployment of a mobile solution for the application website on top of the more classic Internet website.</li> </ul>

# Annexes

## Annex 1. – Acronyms and abbreviations

<b>ABAC</b>	Attribute Based Access Control
<b>ACL</b>	Access Control Lists
<b>API</b>	Advance Passenger Information
<b>Art.</b>	Article
<b>B/C</b>	Benefit-cost ratio
<b>BCP</b>	Border crossing point
<b>BCU</b>	Backup Central Unit
<b>CBA</b>	Cost/Benefit Analysis
<b>CBSA</b>	Canada Border Services Agency
<b>CIAP</b>	Confidentiality, Integrity, Availability and Privacy
<b>CJEU</b>	Court of Justice of the European Union
<b>CMPE</b>	Central Manual Processing Entity
<b>CU</b>	Central Unit
<b>DBT</b>	Design-Build-Test
<b>DDoS</b>	Distributed Denial of Service
<b>DPO</b>	Data Protection Officer
<b>EC</b>	European Commission
<b>ECRIS</b>	European Criminal Records Information System
<b>ECtHR</b>	European Court of Human Rights
<b>EDPS</b>	European Data Protection Supervisor
<b>EES</b>	Entry/Exit System
<b>EIS</b>	Europol Information System
<b>eMRTD</b>	electronic Machine Readable Travel Document
<b>ENISA</b>	European Union Agency for Network and Information Security
<b>EPRIS</b>	European Police Records Index System
<b>ESTA</b>	Electronic System for Travel Authorisation (US)
<b>ETA</b>	Electronic Travel Authorisation System (Australia)
<b>eTA</b>	Electronic Travel Authorisation System (Canada)
<b>ETIAS</b>	European Travel Information and Authorisation System
<b>EU</b>	European Union
<b>EURODAC</b>	European Dactyloscopy (EU fingerprint database for asylum seekers and some categories of irregular migrants)
<b>eu-LISA</b>	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
<b>eVisitor</b>	Electronic Travel Authorisation System (Australia)
<b>FRA</b>	EU Agency for Fundamental Rights
<b>FSS</b>	Functional System Specifications
<b>FTE</b>	Full-time equivalent
<b>IAM</b>	Identity and Access Management
<b>ICAO</b>	International Civil Aviation Organisation
<b>ICT</b>	Information and Communication Technology

<b>IRR</b>	Internal Rate of Return
<b>ISF</b>	Internal Security Fund
<b>IT</b>	Information Technology
<b>LEA</b>	Law enforcement authorities
<b>MS</b>	Member State(s)
<b>NFC</b>	Near-field communication
<b>NPV</b>	Net Present Value
<b>NUI</b>	National Uniform Interface
<b>OCR</b>	Optical character recognition
<b>PII</b>	Personally Identifiable Information
<b>PIU</b>	Passenger Information Unit
<b>PNR</b>	Passenger Name Record
<b>RBAC</b>	Role Based Access Control
<b>RTP</b>	Registered traveller programme
<b>SADM</b>	System Acquisition, Development and Maintenance
<b>SBC</b>	Schengen Borders Code
<b>SDLC</b>	Software development lifecycle
<b>SIS</b>	Schengen Information System
<b>SLA</b>	Service Level Agreement
<b>SLTD</b>	Interpol's Stolen/Lost Travel Document
<b>TLS</b>	Transport Layer Security
<b>VE</b>	Visa-exempt
<b>VE-TCN</b>	Visa-exempt third-country national
<b>VPN</b>	Virtual private network
<b>TESTA-ng</b>	Trans European Services for Telematics between Administrations (communication network to exchange data between European and Member States administrations)
<b>TCN</b>	Third-country national
<b>TDAWN</b>	Interpol's Travel Documents Associated with Notices database
<b>TSS</b>	Technical System Specifications
<b>UMF</b>	Universal Message Format
<b>US</b>	United States
<b>VIS</b>	Visa Information System

## Annex 2. – Study approach

### Objectives

The main objective of the study is to assess the feasibility of setting-up a European Travel Information and Authorisation System (ETIAS), especially looking at:

- a) Analysing the possible **contributions** of ETIAS to the implementation of EU policies, and
- b) Analysing the **impact** of this system on the EU migration, visa, internal security and border control processes and on stakeholders.

The analysis aims at answering the following key questions:

- Why should an electronic travel authorisation system for visa-exempt travellers be developed?
- What would be its impact on EU migration, visa and security?
- How would that system work?
- How would it best be implemented?
- What are the conditions for yielding a positive cost/benefit balance?

### Scope

The following table outlines the topics in scope and out of scope.

*Table 37: ETIAS study scope*

	In scope	Out of scope
<b>Contribution of ETIAS to the implementation of EU policies</b>	<ul style="list-style-type: none"> <li>• Migration</li> <li>• Visa</li> <li>• Internal Security</li> </ul>	<ul style="list-style-type: none"> <li>• Other options (e.g. a system for use by non-visa-exempt travellers; a system for use by certain countries only; use of existing systems for the purpose)</li> </ul>
<b>Impact of ETIAS</b>	<ul style="list-style-type: none"> <li>• Migration, Visa and Internal Security policies</li> <li>• Stakeholders involved</li> <li>• ETIAS legal consequences on existing instruments</li> </ul>	<ul style="list-style-type: none"> <li>• Detailed legal and fundamental rights analysis (high-level/principles only), i.e. recommendations on the choice of the ETIAS legal instrument</li> </ul>
<b>Border crossing processes (impact of an electronic travel authorisation)</b>	<ul style="list-style-type: none"> <li>• First line border checks               <ul style="list-style-type: none"> <li>◦ Benefit at first entry</li> <li>◦ Benefit in case of subsequent entry within the data retention</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Second line border checks</li> </ul>
<b>Differences of border control</b>	<ul style="list-style-type: none"> <li>• Air border</li> <li>• Land border               <ul style="list-style-type: none"> <li>◦ Roads</li> <li>◦ Trains</li> </ul> </li> <li>• Sea border               <ul style="list-style-type: none"> <li>◦ Ferries</li> <li>◦ Cruise ships</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Differences of controls for specific border-crossing points</li> </ul>
<b>Advantages and disadvantages for stakeholders</b>	<ul style="list-style-type: none"> <li>• Travellers</li> <li>• Border control authorities</li> <li>• National authorities</li> <li>• Law enforcement authorities</li> </ul>	<ul style="list-style-type: none"> <li>• MS-by-MS impact</li> </ul>

### Tasks

In order to reach the study's objectives, the following tasks have been performed:



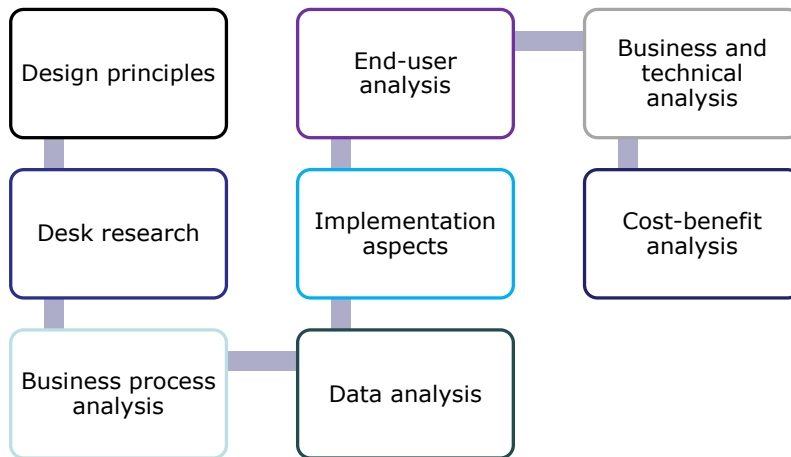


Figure 26: ETIAS study tasks

The following figure outlines the four main phases of the study:



Figure 27: ETIAS study phases

## Relevant legislation

The following table lists the main legislative acts analysed during the data collection phase of the study. They consist of a solid background in order to understand the topic.

*Table 38: Relevant legislation*

<b>Visa Policy</b>	<ul style="list-style-type: none"> <li>• Council Regulation (EC) No 1683/95, laying down a uniform format for visas</li> <li>• <b>Council Regulation (EC) No 539/2001</b>, listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement</li> <li>• Decision no 1105/2011, on the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa and on setting up a mechanism for establishing this list</li> <li>• Any upcoming modifications of the list of countries whose citizens become visa-exempt</li> <li>• Reports from the Commission on visa reciprocity</li> <li>• Regulation (EC) No 767/2008 (VIS Regulation)</li> <li>• Communication from the Commission on the "State of play and the possible ways forward as regards the situation of non-reciprocity with certain third countries in the area of visa policy", April 2016</li> </ul>
<b>Data Protection</b>	<ul style="list-style-type: none"> <li>• Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data</li> <li>• Upcoming <b>General Data Protection Regulation</b></li> <li>• Upcoming Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data</li> <li>• Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data</li> </ul>
<b>Border Management</b>	<ul style="list-style-type: none"> <li>• Regulation (EC) No 562/2006 (Schengen Borders Code)</li> <li>• Revised proposal for a <b>Regulation amending the Schengen Borders Code</b> to integrate the technical changes that result from the new proposal for the EES Regulation establishing an EES</li> </ul>
<b>Other relevant systems</b>	<ul style="list-style-type: none"> <li>• Revised proposal for a <b>Regulation establishing an EES</b></li> <li>• Commission Impact assessment accompanying the document revised proposal for a Regulation establishing an EES</li> <li>• SIS II Decision</li> <li>• SIS II Regulation</li> <li>• <b>Directive 2004/82/EC</b> of 29 April 2004 on the obligation of carriers to communicate passenger data</li> <li>• <b>Directive 2016/681</b> of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime</li> </ul>

## Stakeholders

The study understands the following entities as the main stakeholders of ETIAS:

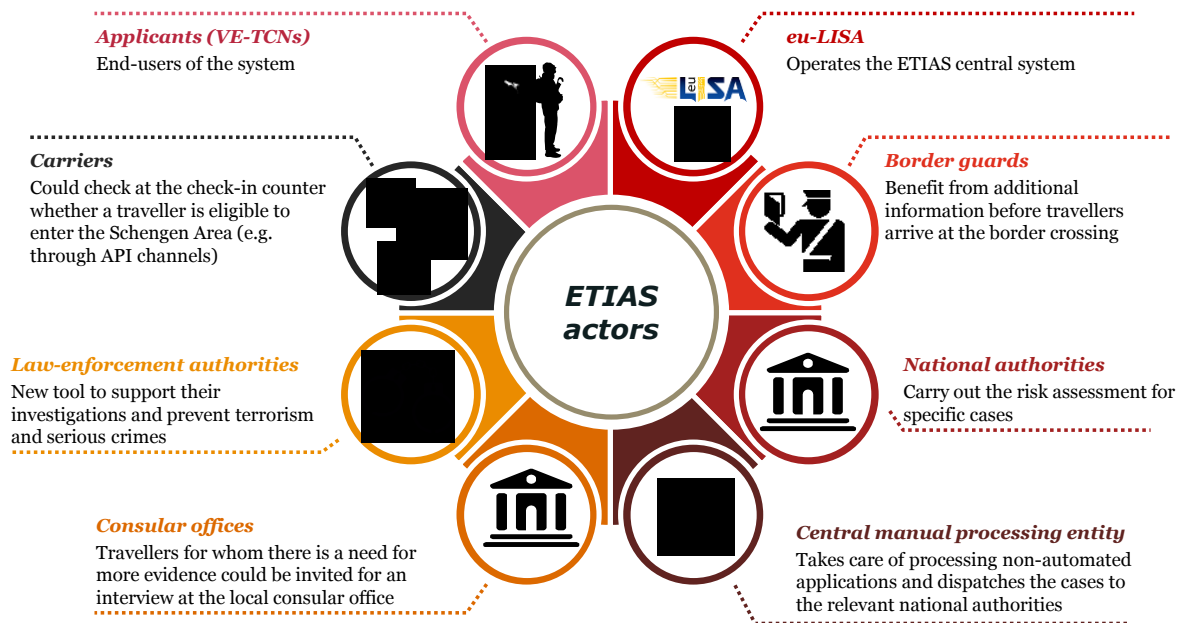


Figure 28: ETIAS stakeholders

During the study, interviews and workshops have been organised with DG Home, the Members States, EU agencies (eu-LISA, Frontex and Europol), Interpol and with carriers' interest group representatives.

## Annex 3. – Design principles

### Authorisation model

Each of the criteria is assessed using the following metrics:

Legend	Convenience for travellers	Workload for national authorities	Relevance of the data to the risk assessment	Consistency with the benchmark systems
++	The travel authorisation is very convenient for travellers	The authorisation model lessens the workload of national authorities	The data collected is very relevant to and useful for the risk assessment	✓: All the benchmark systems follow this approach
+	The travel authorisation is convenient for travellers	The authorisation model lessens the workload of national authorities to a certain extent	The data collected is relevant to and useful for the risk assessment	N.A.
-	The travel authorisation is inconvenient for travellers	The authorisation model has a negative impact on workload for national authorities	The data collected is only relevant to the risk assessment to a limited extent	N.A.
--	The travel authorisation is a burden on travellers	The authorisation model adds a significant amount of workload for national authorities	The data collected is neither relevant to nor useful for the risk assessment	✗: None of the benchmark systems follow this approach
0	The criterion is not applicable	The criterion is not applicable	The criterion is not applicable	The criterion is not applicable

Table 39: Authorisation model comparative table

Model	Advantages	Disadvantages
<b>1. Travel authorisation valid for a period of time</b>	<ul style="list-style-type: none"> <li>- <b>Convenience for travellers:</b> <ul style="list-style-type: none"> <li>▪ Allows travellers to use a travel authorisation to enter the Schengen Area during a set period of time without having to submit a new application for each new entry;</li> <li>▪ A potentially more limited data set, as data related to specific trips would not be collected and stored.</li> </ul> </li> <li>- <b>Reduced impact on carriers and tourism:</b> <ul style="list-style-type: none"> <li>▪ Thus represents less risks of tourism reduction compared with models 2 and 3<sup>168</sup>;</li> <li>▪ And less risks of competitive disadvantage for companies relying on transit through the Schengen Area<sup>169</sup>.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- <b>Reduced data collection and relevant assessment:</b> <ul style="list-style-type: none"> <li>▪ Does not allow re-assessment of the situation of the traveller for each trip;</li> <li>▪ Would not allow collecting data specific to each trip (e.g. first point of entry, place of stay, plate of the car, name of hotel etc.);</li> <li>▪ Would not allow informing in advance land borders of incoming travellers. Contrary to air and sea borders, at land borders the incoming traffic is mostly unknown;</li> <li>▪ Would not be able to alert the traveller whether he/she has remaining days to spend within Schengen (from EES) as the application would not be linked to a</li> </ul> </li> </ul>

<sup>168</sup> The long-term impact on tourism appears to be negligible in the US and in Australia, which both choose a travel authorisation valid for a period of time. See Regulatory Impact Analysis Statement, Regulations Amending the Immigration and Refugee Protection Regulation: <http://www.gazette.gc.ca/rp-pr/p1/2014/2014-06-21/html/reg1-eng.php> (accessed 06/2016).

<sup>169</sup> As an example, in 2015, 6,022,359 passengers transited through Copenhagen airports. See: <https://www.cph.dk/globalassets/om-cph/investor/koncernsrapporter/group-annual-report-2015.pdf>, p. 110

Model	Advantages	Disadvantages
	<ul style="list-style-type: none"> <li>- <b>Reduced administrative burden:</b> eases the workload related to application handling for administration(s) (as a lower number of applications would be submitted).</li> </ul>	<ul style="list-style-type: none"> <li>- specific trip.</li> </ul>
<b>2. Travel authorisation valid for a single trip</b>	<ul style="list-style-type: none"> <li>- <b>Enriched and relevant data collection and assessment:</b> <ul style="list-style-type: none"> <li>▪ Allows the collections of trip specific information that could be used for the risk assessment;</li> <li>▪ Allows re-assessment of the situation of the traveller for each travel, thus, allows taking into account parameters that might have changed since his/her last entry;</li> <li>▪ Allows the possibility to link to EES, informing the travellers and the administration(s) performing the risk assessment on whether the person has days left to spend in the Schengen Area. This option would therefore be beneficial for migration risk assessments;</li> <li>▪ Allows providing advance notice of the incoming travellers at all types of borders.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- <b>Inconvenient for travellers:</b> <ul style="list-style-type: none"> <li>▪ Travellers would have to submit a new notification for each new entry. This would be particularly impactful for frequent travellers<sup>170</sup>;</li> <li>▪ More data would be collected (a set for each trip).</li> </ul> </li> <li>- <b>Higher impact on carriers and tourism:</b> <ul style="list-style-type: none"> <li>▪ Represents a higher risk of tourism reduction compared with model 1;</li> <li>▪ Competitive disadvantage for companies relying on transit through the Schengen Area (air carriers, cruise industry).</li> </ul> </li> <li>- <b>Increased administrative burden:</b> this option would create more burden for the assessment of the applications lodged than model 1 and model 3.</li> </ul>
<b>3. A combination of 1 &amp; 2</b>	<ul style="list-style-type: none"> <li>- <b>Enriched and relevant data collection and assessment:</b> <ul style="list-style-type: none"> <li>▪ Allows to perform an assessment per trip and to function as advance notice of the arrival of the travellers, just like model 2;</li> <li>▪ Allows the connection to EES for the purpose of checking the remaining days to be spent in the Schengen Area as described for model 2. This model would therefore be beneficial for migration risk assessments.</li> </ul> </li> <li>- <b>Reduced administrative burden:</b> allows having a simplified assessment for each trip notification (as it would be a complement to the risk assessment done previously), thus reducing the workload per trip for the administrations, compared to option 2.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Inconvenient for travellers:</b> this option would bring the highest inconvenience to travellers which would have to have two authorisation (one for the period and one for the trip) potentially creating confusion and errors.</li> <li>- <b>Increased administrative burden:</b> the administration(s) processing the applications lodged could have potentially an even higher workload than for model 2 (authorisation for a single trip), due to the necessity to handle any possible issue with a new submission either for a period or per trip.</li> </ul>

(accessed 09/2016). In case the travel authorisation is also required for travellers in transit, the case where its validity is for a duration of time is easier to manage for travellers and carriers.

<sup>170</sup> This could potentially be solved using frequent traveller programmes.

## Annex 4. – Data

### Purpose

In addition to the main ETIAS purpose, it can also be expected that ETIAS would aim to provide advantages in the areas of **convenience for travellers and carriers**, and **border control facilitation**. **Convenience for travellers and carriers** is certainly of importance to avoid ETIAS negative impact on tourism and competitive disadvantage for companies relying on transit through the Schengen Area. **Border control facilitation** – understood, in this study, as facilitation for border guards in their daily work – and its importance have been highlighted by discussions surrounding the EES proposal<sup>171</sup> that notably aims to remedy difficulties linked to the increasing pressure at the border, limited time allocated to carry out border controls and increasing flow of travellers.

**Convenience for travellers and carriers** may conflict with both security and migration purposes. As these two are the *raison d'être* of ETIAS, and more generally of the EU policy on asylum, migration and external border control, it is expected that they would take precedence over convenience for travellers and carriers to a reasonable extent. For this reason, convenience for travellers and carriers should be considered a **secondary purpose**. This purpose would be met by ETIAS mainly through the following:

- The procedure to obtain a travel authorisation would be lighter than the one for obtaining a visa – the contrary would go against both the principle of visa exemption and the rationale of visa liberalisation. It is indeed provided that travellers would fill-in an online form and would not have to go to a consulate to request the travel authorisation;
- Travellers would be able to get reassurance that they meet the entry requirements set out in the SBC (having a travel authorisation would however not guarantee entry in the Schengen Area; the decision on entry would be taken by a border guard at a border-crossing point);
- Carriers would be able to get reassurance that they are transporting a passenger whose compliance with the SBC entry conditions has been pre-assessed;
- Carriers would be able to decrease the number of passengers they have to return on their own resources from the Schengen border to the country of origin.

**Border control facilitation** should, similarly to convenience for travellers and carriers, be considered as an ancillary purpose. Border control facilitation would be limited by the fact that the implementation of ETIAS would not lighten border controls. Indeed, relaxing checks on the basis of the implementation of the system is not considered appropriate at the operational level for the following reasons:

- Border controls would provide another layer of protection;
- They would allow checking the travellers' identity using biometric data when EES will be implemented (identity checks would be limited for ETIAS);
- Border controls present high added value due to the visual contact - and if necessary additional interactions - that is possible with the traveller.

For these reasons, border controls would be complementary to ETIAS instead of being partially replaced by it. While this constraint limits border control facilitation, this purpose should be met to some extent through ETIAS's mid- to long- term impact on the number of travellers being refused entry at the border: this number should decrease with time, as travellers who do not meet the entry conditions set out in the SBC would be notified in advance through the denial of a travel authorisation.

Convenience for travellers and carriers, and border control facilitation are thus ancillary purposes that would be met through the implementation of specific features of the system (notifications to travellers that a travel

---

<sup>171</sup> See Article 5 of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation\\_proposal\\_entryexit\\_system\\_borders\\_package\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation_proposal_entryexit_system_borders_package_en.pdf) (accessed 09/2016).

authorisation has been granted or denied, limited time necessary to fill-in an application etc.) rather than through the collection of data.

## Risks

Compliance with the entry conditions set in the SBC and significance were applied in order to arrive at a shortlist of risks that ETIAS should assess and help address. Each of these criteria is assessed using the following metrics:

*Table 40: Criteria legend*

<b>Legend</b>	<b>Compliance with the entry conditions set out in the SBC</b>	<b>Significance</b>
<b>++</b>	The risk is directly linked to at least one of the entry conditions set in the SBC	The risk has recently been clearly highlighted as a top priority for the EU and there is an established link to VE-TCNs
<b>+</b>	The risk is linked to the overall entry conditions set out in the SBC	The risk has recently been highlighted as a priority for the EU and there is a limited link to VE-TCNs
<b>-</b>	The risk is not directly linked to the entry conditions set out in the SBC	The risk has not been recently highlighted as a top priority for the EU and there is no evidence of a link to VE-TCNs
<b>--</b>	The risk lies outside the scope of the entry conditions set out in the SBC	The risk is not a top priority for the EU and there is evidence of lack of involvement of VE-TCNs
<b>0</b>	The criterion is not applicable	The criterion is not applicable

Risks that receive a combined score greater than 0 can be assessed and addressed by ETIAS most efficiently.

From Europol's Serious and Organised Crime Threat Assessment (SOCTA) and the Frontex analysis of the main border threats<sup>172</sup>, the following risks have been identified and analysed in light of the criteria defined in section 2.2.4 "Risks":

Table 41: Analysis of the risks that ETIAS could assess and mitigate

Risk category	Risk	Compliance with SBC entry conditions	Significance	Explanation of significance
Security	Terrorism	++: "Not be considered as a threat to public policy, internal security"	+	<ul style="list-style-type: none"> <li>The attacks in Paris, Brussels and Nice have highlighted the importance of this risk;</li> <li>Priority in The European Agenda on Security of April 2015<sup>173</sup>;</li> <li>Priority in the Communication by the European Commission on "delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union";</li> <li>PNR Directive is a first step in harmonising responses at EU level, however PNR data is sent at check-in: limited time for authorities to conduct the assessment;</li> <li>PNR data processing is de-centralised, and the data is used differently depending on MS national contexts;</li> <li>PNR data are only collected for passengers arriving by air;</li> <li>ETIAS <u>individual</u> risk assessment can cover risks of terrorism.</li> </ul>
	Serious and cross-border organised crime	++: "Not be considered as a threat to public policy, internal security"	++	<ul style="list-style-type: none"> <li>Priority in the European Agenda on Security of April 2015<sup>174</sup>.</li> </ul>
	➤ Document fraud and identity fraud	++: "Possessing a valid passport"	++	<ul style="list-style-type: none"> <li>In 2015, MS reported 8,373 document fraudsters at entry border-crossing points from third countries<sup>175</sup>;</li> <li>Countries in the process of negotiations with the EU for visa liberalisation feature among the most commonly-detected document fraudsters<sup>176</sup>.</li> </ul>

<sup>172</sup> Frontex Risk Analysis for 2016, available at: [http://frontex.europa.eu/assets/Publications/Risk\\_Analysis/Annula\\_Risk\\_Analysis\\_2016.pdf](http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf) (accessed 06/2016).

<sup>173</sup> See: [http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu\\_agenda\\_on\\_security\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf) (accessed 09/2016).

<sup>174</sup> See: [http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu\\_agenda\\_on\\_security\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf) (accessed 09/2016).

<sup>175</sup> Frontex Risk Analysis for 2016, p. 14 and p. 24. This number remains low in view of the large movements across the borders and were mainly reported at air borders (which generally allow better conditions for border controls). Both of these factors point to vulnerabilities in the travel document inspection process, which is supported by the observations collected during an exercise carried out under Frontex umbrella. In particular, it was reported that the equipment's performance "shows a degree of variability, indecision and inconsistency", which results in false documents being accepted as genuine. Time pressure at the border was also reported as negatively impacting border guards' performance. Vulnerabilities related to technical issues were finally highlighted in the recent communication from the Commission (SLTD checks are not systematically conducted as some connections to the database are still missing. See "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final, European Commission, 06/04/2016, p.10 [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication\\_on\\_stronger\\_and\\_smart\\_borders\\_20160406\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication_on_stronger_and_smart_borders_20160406_en.pdf) (accessed 09/2016).

<sup>176</sup> Frontex Risk Analysis for 2016, p. 24.



Risk category	Risk	Compliance with SBC entry conditions	Significance	Explanation of significance
	➤ <i>Cybercrime</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>Priority in The European Agenda on Security of April 2015<sup>177</sup>;</li> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Trafficking in human being</i>	++: "Not be considered as a threat to public policy, internal security"	++	<ul style="list-style-type: none"> <li>Drug trafficking and trafficking in human beings are risks that have been highlighted as potentially arising from visa-exempt countries<sup>178</sup>.</li> </ul>
	➤ <i>Counterfeiting goods</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Excise and Missing Trader Intra-Community (MTIC) Fraud</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Drug trafficking (including synthetic drugs, cocaine and heroin)</i>	++: "Not be considered as a threat to public policy, internal security"	++	<ul style="list-style-type: none"> <li>Drug is trafficked into the EU through a variety of means, including by individual travellers, air couriers on commercial flights and private aircraft in addition to postal services and freight<sup>179</sup>;</li> <li>Relevance of a system that would aim at travellers for assessing and mitigating risks related to drug trafficking.</li> </ul>
	➤ <i>Illicit firearms trafficking</i>	++: "Not be considered as a threat to public policy, internal security"	++	<ul style="list-style-type: none"> <li>Many firearms are trafficked from former conflict regions, notably the Western Balkans where a number of visa-exempt countries are<sup>180</sup>.</li> </ul>
	➤ <i>Organised Property Crime</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Crime connected with nuclear and radioactive substances</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Illegal money laundering</i>	+: "Not be considered as a threat to public policy,	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>

<sup>177</sup> See: [http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu\\_agenda\\_on\\_security\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf) (accessed 09/2016).

<sup>178</sup> Frontex Risk Analysis for 2016, p. 22 (Peru and Colombia).

<sup>179</sup> Frontex Risk Analysis for 2016, p. 28 and European Drug Report 2016, p. 24: Trends and Developments, available at: <http://www.emcdda.europa.eu/system/files/publications/2637/TDAT16001ENN.pdf> (accessed 09/2016).

<sup>180</sup> Frontex Risk Analysis for 2016, p. 29. See also Europol, TE-SAT 2016, p. 8.

Risk category	Risk	Compliance with SBC entry conditions	Significance	Explanation of significance
	<i>activities</i>	internal security"		
	➤ <i>Motor vehicle crime</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Murder, grievous bodily injury</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Illicit trade in human organs and tissue</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Kidnapping, illegal restraint and hostage taking</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Racism and xenophobia</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Organised robbery</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Illicit trafficking in cultural goods, including antiquities and works of art</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Illicit trafficking in endangered animal species</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Illicit trafficking in endangered plant species and varieties</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Swindling and fraud</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Racketeering and</i>	+: "Not be considered as a threat to public policy,	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>

Risk category	Risk	Compliance with SBC entry conditions	Significance	Explanation of significance
	<i>extortion</i>	internal security"		
	➤ <i>Forgery of administrative documents and trafficking therein</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Forgery of money and means of payment</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Corruption</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	➤ <i>Environmental crime</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
<b>Migration</b>	<i>Irregular stay</i>	+: "Not be considered as a threat to public policy, internal security"	++	<ul style="list-style-type: none"> <li>Link between visa-exempt travel and this risk through the risk of irregular stay.</li> </ul>
	➤ <i>Overstay</i>	+: "Justifying the purpose of the intended stay and have sufficient means of subsistence" "Not be considered as a threat to public policy, internal security"	++	<ul style="list-style-type: none"> <li>In 2015, 67 316 cases of overstay were detected on exit<sup>181</sup>;</li> <li>The majority were nationals from countries in the process of negotiations with the EU for visa liberalisation.</li> </ul>
	<i>Clandestine entry</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	<i>Facilitation of irregular stay</i>	+: "Not be considered as a threat to public policy, internal security"	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>
	<i>Facilitation of clandestine entry</i>	+: "Not be considered as a threat to public policy,	-	<ul style="list-style-type: none"> <li>No evidence of link between visa-exempt travel and this risk.</li> </ul>

<sup>181</sup> Frontex Risk Analysis for 2016, p. 27.

Risk category	Risk	Compliance with SBC entry conditions	Significance	Explanation of significance
		internal security"		
<b>Public health</b>	<i>Threat for public health</i>	++: "Not be considered as a threat to (...) public health" <sup>182</sup>	+	<ul style="list-style-type: none"> <li>• Eliminate tuberculosis as a public health problem is a target of the Millennium Development Goals; Eastern Europe is identified as a challenging region for meeting this goal<sup>183</sup>. The region includes countries in the process of negotiations with the EU for visa liberalisation.</li> <li>• Medical tourism has been identified as an important risk the Canadian system should mitigate. However, from a European perspective, this risk is not present as the practice is more regulated and brings added value to the health care systems.</li> </ul>

<sup>182</sup> See Article 2(19) of the Schengen Borders Code: " 'threat to public health' means any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States".

<sup>183</sup> World Health Organization, "Background information about tuberculosis":  
[http://www.euro.who.int/\\_data/assets/pdf\\_file/0003/68970/fs01E\\_TBbackground.pdf?ua=1](http://www.euro.who.int/_data/assets/pdf_file/0003/68970/fs01E_TBbackground.pdf?ua=1) (accessed 09/2016).

## Current or upcoming relevant IT systems and databases

This section gives additional information about systems and databases that could potentially be connected to ETIAS.

*Table 42: Scope and description of the relevant systems and databases*

System	Scope	Purpose	Target	Description
<b>SIS</b>	EU – Schengen	Security and irregular migration	Persons subject to an alert	Currently used by 24 EU MS and four non-EU countries, the Schengen Information System supports operational cooperation between police, border and judicial authorities in criminal matters. It is both a police cooperation and a border control system. Data can be searched on a 24/7 basis, at border-crossing points and within national territory and consulates. The database contains information on objects and persons and works on a "hit/no-hit" basis. A hit on a person triggers an action (discreet check or refuse entry...). Under "objects", the database notably contains information on stolen documents.
<b>VIS</b>	EU – Schengen	Immigration control	TCNs applying for short-stay visas	The Visa Information System stores the visa-application and visas status for all short-stay Schengen visas. The visa-application process includes a consultation mechanism between Member States for specific cases. As per the SBC at entry into the Schengen area the border guard checks whether the travel document and visa are genuine and belong to the traveller. Designated authorities (police, consular posts, border and immigration authorities and Europol) are allowed to consult it for the purpose of prevention, detection and investigation of terrorist and serious criminal offences.
<b>SLTD</b>	Worldwide	Security, irregular migration	Travel documents reported stolen or lost	The Lost and Stolen Travel Document Database contains information on 63 million travel documents reported lost or stolen by 166 countries around the world (around 50% of the database concern TCN). It supports Interpol and other national law enforcement, immigration and border control authorities to assess the validity of a travel document.
<b>TDWAN</b>	Worldwide	Security	Travel documents associated with notices	This database contains records of genuine travel documents belonging to criminals and associated with Interpol notices. TDAWN is an extension of SLTD that contains the same type of information, but related to a criminals.
<b>EES</b>	EU - Schengen	Immigration control and security	TCNs entering the Schengen Area	Future Entry/Exit system recording the border-crossing point of entry, entry dates and authorising authority as well as the border-crossing point of exit and exit date of all TCNs entering or leaving the Schengen Area as well as the data that identify the traveller (proposal currently under discussion).
<b>EIS</b>	EU - Schengen	Security	Persons and other information related to crimes	The Europol Information System contains information on serious international crimes, suspected and convicted persons, criminal structures and offences. It is a reference system that can be used to check whether information on a certain person or an object of interest (such as a car, a telephone or an e-mail

				message) is available beyond national or organisational jurisdictions.
<b>ECRIS</b>	EU - Schengen	Security	Persons having a criminal record	The European Criminal Records Information System is a decentralised system: criminal records data is stored solely in national databases and exchanged electronically between the central authorities of the Member States upon request.
<b>EURODAC</b>	EU - Schengen	Immigration control	TCNs seeking international protection and of some categories of irregular migrants	EURODAC is used to compare the fingerprints of a person applying for international protection with the ones contained in the system. It aims to facilitate the application of the Dublin Regulation by determining which Member State is responsible for examining the claim for international protection.

Table 43: Data contained in relevant systems and databases

System	Collected data	Law enforcement access	Data retention period
<b>SIS</b>	<ul style="list-style-type: none"> <li>– Surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately;</li> <li>– Any specific, objective, physical characteristics not subject to change;</li> <li>– Place and date of birth;</li> <li>– Sex;</li> <li>– Photographs;</li> <li>– Fingerprints;</li> <li>– Nationality(ies);</li> <li>– Whether the person concerned is armed, violent or has escaped;</li> <li>– Reason for the alert;</li> <li>– Authority issuing the alert;</li> <li>– Reference to the decision giving rise to the alert;</li> <li>– Action to be taken;</li> <li>– Link(s) to other alerts issued in SIS II pursuant to Article 52;</li> <li>– Type of offence.</li> </ul>	<p>Yes (police checks carried out within the MS + national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge)</p>	<p>Review by MS of the relevance of retaining the alert every 3 years</p>
<b>VIS</b>	<ul style="list-style-type: none"> <li>– Application number;</li> <li>– Status information;</li> <li>– Authority with which the application has been lodged;</li> <li>– Surname, surname at birth (former surname(s));</li> <li>– First name;</li> <li>– Sex;</li> <li>– Date of birth;</li> <li>– Place and country of birth;</li> <li>– Current nationality and nationality at birth;</li> <li>– Type of travel document;</li> <li>– Number of travel document;</li> <li>– Authority which issued the travel document;</li> <li>– Document date of issuance;</li> <li>– Document date of expiry;</li> </ul>	<p>Yes</p>	<p>5 years from the expiry date of the visa,</p> <ul style="list-style-type: none"> <li>– or from the date of the creation of the file in the VIS (application withdrawn, closed or discontinued),</li> <li>– or from the date of the decision of the visa authority (visa refused, annulled, shortened or revoked)</li> </ul>

System	Collected data	Law enforcement access	Data retention period
	<ul style="list-style-type: none"> <li>– Date and place of the application;</li> <li>– Type of visa requested;</li> <li>– Surname, first name and address of the person issuing an invitation;</li> <li>– Name and address of the company/org. issuing an invitation, surname and first name of the contact person in the company/org.;</li> <li>– Destination of the intended stay;</li> <li>– Its duration;</li> <li>– Purpose of the travel;</li> <li>– Intended date of arrival and departure;</li> <li>– Intended border of first entry and transit route;</li> <li>– Residence;</li> <li>– Current occupation and employer; name of school for students;</li> <li>– For minors, surnames and first names of mother and father;</li> <li>– Photo;</li> <li>– Fingerprints;</li> <li>– Links to other applications.</li> </ul>		
<b>STLD</b>	<p><u>At least:</u></p> <ul style="list-style-type: none"> <li>– Issuing country;</li> <li>– Document type;</li> <li>– Document number;</li> <li>– Date of theft/loss;</li> <li>– Information related to the circumstances of the theft or loss;</li> <li>– Country who reported the lost or stolen document.</li> </ul> <p>...of a particular travel document (authorised users query specific passport numbers).</p> <p><u>No names, no personal data</u></p> <p>The searches are based on three data: type of document, number of document and country of issuance.</p>	Yes	<p>5 years</p> <ul style="list-style-type: none"> <li>– Or less (if purpose fulfilled or national, international entity or National Bureaux decide less)</li> <li>– Unless extended by the Executive Committee if necessary and database does not contain personal data</li> </ul>
<b>TDAWN</b>	Same data set as SLTD, but also including personal data.	<p>Yes</p> <p>Important to note that there is no obligation for the officers to act on a match.</p>	<p>5 years</p> <ul style="list-style-type: none"> <li>– Or less (if purpose fulfilled or national, international entity or National Bureaux decide less)</li> </ul>



System	Collected data	Law enforcement access	Data retention period
EES	<ul style="list-style-type: none"> <li>– Surname (family name); – First name(s) (given names);</li> <li>– Date of birth;</li> <li>– Nationality or nationalities;</li> <li>– Sex;</li> <li>– Type, number and three letter code of the issuing country of the travel document or documents;</li> <li>– Date of expiry of the validity of the travel document(s);</li> <li>– Facial image, where possible extracted electronically from the eMRTD, and where this is not possible, taken live.</li> </ul> <p><u>In addition for visa holders:</u></p> <ul style="list-style-type: none"> <li>– Short stay visa sticker number, including the three letter code of the issuing Member State, the type of visa, the date of end of maximum duration of the stay as authorised by the visa which needs to be updated at each entry and the date of expiry of the validity of the visa, if applicable;</li> <li>– At the first entry on the basis of the short stay visa, the number of entries and the authorised period of stay as indicated on the visa sticker;</li> <li>– Visa sticker number of the touring visa, the type of visa and the date of expiry of the validity of the visa.</li> </ul> <p><u>In addition for visa-exempt:</u></p> <ul style="list-style-type: none"> <li>– 4 fingerprints.</li> </ul> <p><u>In addition for each entry and exit:</u></p> <ul style="list-style-type: none"> <li>– Date and time of the entry;</li> <li>– Border crossing point and authority that authorised the entry;</li> <li>– Date and time of the exit;</li> <li>– Border crossing point of the exit.</li> </ul>	Yes	5 years after the exit (or the refusal of entry) of the person
EIS	<p><u>For cross-checking purposes:</u></p> <ul style="list-style-type: none"> <li>– Surname, maiden name, given names, alias or assumed name;</li> <li>– Date and place of birth;</li> <li>– Nationality;</li> <li>– Sex;</li> <li>– Place of residence, profession and whereabouts;</li> <li>– Social security numbers, driving licences, identification documents and passport data;</li> <li>– Other characteristics, including objective physical characteristics not subject</li> </ul>	Yes	Review by Europol of the relevance of retaining the data every 3 years

System	Collected data	Law enforcement access	Data retention period
	<p>to change such as dactyloscopic data and DNA profile</p> <ul style="list-style-type: none"> <li>– Criminal offences, alleged criminal offences, when, where and how they were (allegedly committed);</li> <li>– Means which were/may have been used to commit criminal offences, including information concerning legal persons;</li> <li>– Departments handling the case;</li> <li>– Suspected membership of a criminal organisation;</li> <li>– Convictions, where they relate to criminal offences in respect of which Europol is competent;</li> <li>– Inputting party.</li> </ul> <p><u>In addition, for informants:</u></p> <ul style="list-style-type: none"> <li>– Coded personal details;</li> <li>– Type of information supplied;</li> <li>– Whether anonymity is to be guaranteed;</li> <li>– Whether protection is to be guaranteed and by whom;</li> <li>– New identity;</li> <li>– Whether participation in a court hearing is possible;</li> <li>– Negative experiences;</li> <li>– Rewards.</li> </ul> <p><u>For strategic analysis purpose:</u></p> <ul style="list-style-type: none"> <li>– Personal details;</li> <li>– Physical description;</li> <li>– Means of identification;</li> <li>– Occupation and skills;</li> <li>– Economic and financial information;</li> <li>– Behavioural data;</li> <li>– Contacts and associates;</li> <li>– Means of communication used;</li> <li>– Means of transport used;</li> <li>– Information relating to criminal conduct;</li> <li>– Reference to other information systems in which information on the person is stored;</li> <li>– Information on legal persons associated with economic and financial information or criminal conduct.</li> </ul>		

System	Collected data	Law enforcement access	Data retention period
	<p><u>For victims:</u></p> <ul style="list-style-type: none"> <li>– Personal details;</li> <li>– Physical description;</li> <li>– Means of identification;</li> <li>– Victim identification data;</li> <li>– Reason for victimisation;</li> <li>– Damage;</li> <li>– Whether anonymity is to be guaranteed;</li> <li>– Whether participation in a court hearing is possible;</li> <li>– Crime-related information.</li> </ul> <p><u>For persons that might be called to testify:</u></p> <ul style="list-style-type: none"> <li>– Personal details;</li> <li>– Physical description;</li> <li>– Means of identification;</li> <li>– Crime-related information;</li> <li>– Whether anonymity is to be guaranteed;</li> <li>– Whether protection is to be guaranteed and by whom;</li> <li>– New identity;</li> <li>– Whether participation in a court hearing is possible.</li> </ul>		
<b>ECRIS</b>	Criminal records	Yes	N/A (depends on Member States' retention periods for criminal records)
<b>EURODAC</b>	<ul style="list-style-type: none"> <li>– Fingerprints;</li> <li>– Member State that transmits the information to EURODAC;</li> <li>– Place and date of the application for international protection;</li> <li>– Sex;</li> <li>– Reference number;</li> <li>– Date on which the fingerprints were taken;</li> <li>– Date on which the data were transmitted to the Central System;</li> <li>– Operator user ID.</li> </ul> <p><u>In addition, where applicable:</u></p> <ul style="list-style-type: none"> <li>– The date of the arrival of the person after a transfer;</li> </ul>	Yes	10 years after the date on which the fingerprints were taken

System	Collected data	Law enforcement access	Data retention period
	<ul style="list-style-type: none"> <li>– The date when the person left the territory of the Member State;</li> <li>– The date when the person was removed from the territory of the Member State;</li> <li>– The date when the decision to examine the application was taken.</li> </ul>		

## Database checks

Based on the table below, the following section (1) describes the added value of the databases retained for ETIAS and (2) gives an explanation on why others were not selected as relevant for ETIAS.

The assessment was performed according to the following metrics:

<b>Legend</b>	<b>Relevance</b>	<b>Privacy and data protection</b>	<b>Implementation complexity</b>
<b>++</b>	The database is essential to ETIAS risk assessment	The amount of data accessed from the database is very limited in quantity and is not sensitive	Connecting to the database is not technically complex; the database has sufficient capacity to support a large number of frequent queries
<b>+</b>	The database brings added value to ETIAS risk assessment	The amount of data accessed from the database is limited in quantity and/or is not sensitive	Connecting to the database poses some technical complexity; capacity issues are possible but unlikely
<b>-</b>	The database does not bring clear added value to ETIAS risk assessment	The amount of data accessed from the database is significant in quantity and/or is sensitive	Connecting to the database involves high technical complexity; capacity issues are very likely
<b>--</b>	The database does not bring any added value to ETIAS risk assessment	The amount of data accessed from the database is extensive in quantity and/or is sensitive	Connecting to the database given its current (technical) set-up and capacity is not possible
<b>0</b>	The impact is null or the criteria is not applicable	The impact is null or the criteria is not applicable	The impact is null or the criteria is not applicable

Databases	Risks						Assessment criteria		
	Security		Migration			Public health	Relevance	Privacy and data protection	Implementation complexity
	Terrorism	Serious and cross-border crime	Irregular stay (overstay)	Entry bans/return decisions	Refusal of entry	Threat to public health			
<b>Existing databases</b>									
National databases	✓	✓	✓	✓	✓		++	--	--
SIS	✓	✓		✓			++	+	+
VIS			✓				++	+	+
EURODAC			✓				--	--	--
EIS	✓	✓					++	-	--
ECRIS	✓	✓					-	--	--
SLTD	✓	✓					++	++	++
TDAWN	✓	✓					+	+	++
<b>Future databases</b>									
EES			✓		✓		++	+	++
<b>ETIAS components</b>									
ETIAS IT application	✓	✓					++	-	++
Screening rules	✓	✓					++	-	++

### Security and migratory risks

- National databases**

Relevance	Privacy and data protection	Implementation complexity
ETIAS checking national databases may provide information on a traveller useful for security or migration risk assessment. However, it would introduce discrepancies in application management: the checks would be different depending on the Schengen State responsible for the application.	The amount of data accessed would potentially be extensive in quantity and be sensitive (e.g. data revealing ethnic origin).	Direct checks of national databases raise issues from a technical point of view. In particular, it would lead to a high number of queries to national systems (a workload unforeseen at the time of their implementation). It would also be problematic from a confidentiality and legal point of view.

Access to Member States' national databases is therefore not deemed feasible for ETIAS. A mitigation measure is provided with the creation of the ETIAS central repository of screening rules.

- **SIS**

Relevance	Privacy and data protection	Implementation complexity
<p>Improvements were made to the system in 2015, to enable better information sharing on persons suspected of terrorist offences and on travel documents of persons suspected of wanting to join terrorist groups outside the EU<sup>184</sup>. While an important number of alerts in the SIS concerns EU citizens and documents issued by EU countries, this does not impact the relevance of checking the system for visa-exempt travellers, notably as a large part of the fraudulent passports detected in 2015 were issued by EU countries<sup>185</sup>. Moreover, SIS alerts for refusal of entry are not systematically checked at all border-crossing points, for practical reasons. A pre-check through ETIAS would diminish risks that a person subject to an alert for refusal of entry enters the EU<sup>186</sup>.</p>	<p>The amount of data that would be accessed from the database would be limited in quantity (a SIS alert contains only a limited number of data fields ).</p>	<p>Connection to this database is technically feasible and SIS has sufficient capacity to support a large number of frequent queries.</p>

Access to SIS meets the assessment criteria.

---

<sup>184</sup> Agenda on migration p5, available at: <https://www.cepola.europa.eu/sites/default/files/european-agenda-security.pdf> (accessed 09/2016).

<sup>185</sup> Frontex Risk Analysis for 2016, p. 24.

<sup>186</sup> However, a check in SIS would not be sufficient to assess and mitigate the security risks identified above. The Frontex Risk Analysis for 2016 indeed highlights that "[t]he number of persons refused entry due to an alert in the SIS system represented only about 8.2% of the total, with 9,762 refusals issued in 2015", which calls for the use of additional methods to pre-assess compliance with entry conditions. As a conclusion, this database meets the assessment criteria but should not be the only one consulted. See:

- **VIS**

Relevance	Privacy and data protection	Implementation complexity
VIS could be used to verify whether the traveller has previously been refused a visa. This would only deliver results on nationals from countries that were previously visa-holder in the last five years (data retention of the VIS). Access to this database is then relevant for newly joined visa-exempt countries.	The amount of data that would be accessed from the database would be limited in quantity (name, surname and possibly date of birth would be accessed to ensure accurate match; in the event of a match, status of the visa application and, in the event the visa has been refused, grounds for the refusal would be accessed).	Connection to the database is technically feasible and the database has sufficient capacity to support a large number of frequent queries (query would have to be done on the basis of the passport number instead of the visa sticker number as currently done).

Access to VIS meets the assessment criteria.

- **EURODAC**

Relevance	Privacy and data protection	Implementation complexity
The system could be used to check if the person has previously been refused asylum. However, EURODAC would for now bring only limited added value: as only a very limited number of citizens from visa-exempt countries should have been in a position to request asylum <sup>187</sup> , the costs related to checking EURODAC for granting travel authorisations may not be justified.	The amount of data accessed from the database would be extensive in quantity and sensitive (EURODAC can only be checked on the basis of fingerprints, which would require ETIAS to collect those to check them against EURODAC). In addition, checking EURODAC in the process of delivering authorisations for travelling to the Schengen Area could deter persons to apply for asylum.	EURODAC is currently functioning on the basis of fingerprints only: checks are done using fingerprints and the database contains little other data (gender mainly). It is not anticipated for ETIAS to collect fingerprints. For ETIAS to query EURODAC, a change to the latter would thus be necessary: the system would need to accept searches on the basis of biographical or passport data and store such data. The 2016 EURODAC legislative proposal (recast) plans modifications to the system in this direction <sup>188</sup> .

EURODAC, in its current set-up and in the current situation, does not meet the assessment criteria.

<sup>187</sup> See [http://ec.europa.eu/eurostat/statistics-explained/index.php/File:First\\_time\\_asylum\\_applicants\\_in\\_the\\_EU-28\\_by\\_citizenship\\_Q1\\_2015\\_%E2%80%93\\_Q1\\_2016.png](http://ec.europa.eu/eurostat/statistics-explained/index.php/File:First_time_asylum_applicants_in_the_EU-28_by_citizenship_Q1_2015_%E2%80%93_Q1_2016.png) (accessed 09/2016).

<sup>188</sup> Article 12 of the Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person], for identifying an illegally staying third country national or stateless person and on requests for the comparison with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), available at: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160504/eurodac\\_proposal\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160504/eurodac_proposal_en.pdf) (accessed 09/2016).



- **EIS (Europol Information System)**

Relevance	Privacy and data protection	Implementation complexity
<p>The system currently contains around 100,000 suspected/convicted criminals<sup>189</sup>, and 10% of them are TCNs. While an important part of the information contained in the EIS would also be in the SIS and national databases, EIS allows links to be created between different MS information. This system further retains historical data, while the SIS alerts are deleted when the case is resolved. This could provide useful information for the manual processing of the case.</p>	<p>The amount of data accessed from the database would be significant in quantity and would be sensitive (EIS data set is particularly extensive and includes sensitive data, such as whether the persons are informants or victims or alleged crimes, that could be used for the risk assessment).</p>	<p>The system is currently not available for border management as it primarily aims at supporting law enforcement cooperation<sup>190</sup>. Moreover, currently the EIS is technically not ready to be queried as much as ETIAS would need. Significant upgrades would be needed to ensure sufficient capacity to serve ETIAS purposes. Indeed, 100,000 searches per month are currently performed on the database (the estimate is 2,460,000 searches per month would be necessary for ETIAS). While the upgrade would be significant it would not be technically impossible.</p>

Although it could be interesting to re-evaluate the possible links between the EIS and ETIAS at a later stage, the database does not currently meet the assessment criteria.

- **SLTD (Stolen and Lost Travel Documents )**

Relevance	Privacy and data protection	Implementation complexity
<p>Fuller use of Interpol's SLTD has been recommended in the Agenda on Migration<sup>191</sup>. The added value of SLTD over the SIS can however be contested. Indeed, documents reported lost or stolen by countries participating in the SIS are entered both in SLTD and the SIS. Nevertheless, two main arguments point to the relevance of SLTD:</p> <ul style="list-style-type: none"> <li>- SLTD also contains data entered by countries that are not participating in the SIS (Ireland, Croatia, Cyprus and third countries);</li> <li>- Integrating SLTD to ETIAS would help harmonising the use of this database by MS, as some connections to it are currently still to be implemented<sup>192</sup>.</li> </ul> <p>Lastly, currently contains 63 million records, of which around half of them concern TCN citizens.</p>	<p>The amount of data that would be accessed is very limited in quantity and would not be sensitive (SLTD does not contain personal data but only travel-document data).</p>	<p>Connection to the database is technically feasible and the database has sufficient capacity to support a large number of frequent queries.</p>

<sup>189</sup> See: <https://www.europol.europa.eu/content/page/europol-information-system-eis-1850> (accessed 09/2016)

<sup>190</sup> "Stronger and Smarter Information Systems for Borders and Security", COM (2016) 205 final.

<sup>191</sup> Agenda on migration p5, available at: <https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf> (accessed 09/2016).

<sup>192</sup> "Stronger and Smarter Information Systems for Borders and Security", COM (2016) 205 final.

Access to SLTD meets the assessment criteria.

- **TDAWN (Travel Documents Associated With Notices)**

Relevance	Privacy and data protection	Implementation complexity
The system's notices concern individuals wanted for serious crimes and thus would be of particular relevance regarding security risk assessment, especially serious crime. It would then be relevant for ETIAS risk assessment.	The amount of data accessed from the database would be limited in quantity (TDAWN contains mostly travel-document data, biographical data, the description of the notice and reason for the inclusion of the person in the database). It is important to note that, as the country that reports the case is the entity deciding about the gravity of the crime, the reported case might not all meet EU standards and legal requirements concerning the definition of crime. However, there is no obligation to act on a match as the decision is always at the discretion of the officer).	Connection to the database is not technically complex; the database has sufficient capacity to support a large number of frequent queries.  In addition, connections to TDAWN are implemented via a VPN/secure Internet link, making the link to ETIAS seamless/one of the least technically complex to implement.

Access to TDAWN meets the assessment criteria.

- **EES**

Relevance	Privacy and data protection	Implementation complexity
The Entry/Exit System would provide information on TCNs who overstayed. It would also record refusals of entry on third-country nationals <sup>193</sup> . Although this information would only be available if the applicant for a travel authorisation has previously entered the Schengen Area, is it definitely relevant for ETIAS to check the future system.	The amount of data accessed from the database would be limited in quantity (name, surname and possibly date of birth would be accessed to ensure accurate match). Only the persons on the list of overstayers or having been refused entry would be searched for. Finally ETIAS would not access biometric data.	The complexity of implementing a link between ETIAS and EES is assessed as being low, as both systems are still to enter into their design phase. Being a database not yet implemented and live, changes can more easily accommodated.

---

<sup>193</sup> See Articles 10 and 11 of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation\\_proposal\\_entryexit\\_system\\_borders\\_package\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation_proposal_entryexit_system_borders_package_en.pdf) (accessed 09/2016).

The possible interactions between EES and ETIAS are developed in the Architecture section. Access to EES meets the assessment criteria.

- **ECRIS**

Relevance	Privacy and data protection	Implementation complexity
<p>The European Criminal Records Information System provides the electronic means for conviction information to be exchanged between MS in a standardised format. ECRIS is used to notify MS about convictions of their nationals and to send requests for conviction information for criminal proceedings or administrative or employment purposes. Nevertheless, the information system currently only concerns EU nationals although there are plans to extend it to third-country nationals. This system is in its current implementation not relevant for ETIAS.</p>	<p>The amount of data accessed would depend on the data in MS criminal records. It would potentially be extensive in quantity and be sensitive (e.g. criminal records and ancillary information).</p>	<p>As ECRIS does not store data itself, it is not possible for ETIAS to connect to it in the current set-up of the system.</p>

Access to ECRIS does not meet the assessment criteria in its current configuration and content. It is worth mentioning that a similar initiative is being discussed for a European Police Records Index System (**EPRI**). At the moment there is no concrete implementation plan, but this system would be interesting to reassess at a later stage.

- **ETIAS IT application**

Relevance	Privacy and data protection	Implementation complexity
<p>It may be envisaged to retain lodged ETIAS applications, for a pre-defined period of time, in order for them to be searched for each newly submitted application. Upon a match between the new application and a denied application stored in this database, the case would be automatically transferred for manual processing (see section "2.3 Business processes"). This would allow the processing entity to take a decision while having an overview of the person's history of travel applications. Such a database could also allow retrieving data submitted by "persons of interest" who have applied for a travel authorisation (e.g. for law enforcement purposes).</p>	<p>The quantity of data accessed would not be significant (ETIAS data set is limited) but would include sensitive information (i.e. background information).</p>	<p>Connection to the database is technically feasible as it will be part of the Central System.</p>

Access to ETIAS IT application meets the assessment criteria.

## Public health

Relevance	Privacy and data protection	Implementation complexity
No system related to this risk exists as such. If assessed, risks related to public health should be performed by other means than database checks.	To be justifiable, the data collected on health should be limited and focus on the major communicable diseases.	Not applicable, as no databases are available for this risk.

## Conclusion

On the basis of the above considerations, the table below summaries the preferred database checks that ETIAS would do.

*Table 44: Databases to be searched for ETIAS*

Systems	Aim	Commonly used at border crossing
<b>SIS</b>	Check applicants against alerts on persons.	✓
<b>VIS</b>	Check whether applicants have previously been rejected a visa.	✓
<b>SLTD</b>	Check applicants' passport details against stolen and lost travel documents.	✓
<b>TDAWN</b>	Check applicants against international notices.	
<b>EES</b>	Check whether applicants have previously overstayed.	✓ (will be in the future)
<b>ETIAS IT application</b>	Check whether applicants have previously obtained or were denied a travel authorisation.	
<b>ETIAS screening rules</b>	Check pre-determined fields of the application form against investigation triggers proposed by MS.	
Possible future connections		
<b>ECRIS</b>	Check whether the person has criminal records in Europe	
<b>EIS</b>	Check whether the person is involved in an ongoing criminal investigation	
<b>EURODAC</b>	Check previous requests for asylum	

## ETIAS data fields assessment

Each possible data was assessed against the following four criteria<sup>194</sup>:

1. **Ease of collection and automation:** is this data easy to provide, remember, write? Can it be used for automated checks? Requesting long explanations or a piece of information that the person would have to look for in another document than the passport or a credit card should be avoided. Similarly, there should be a limited amount of data collected that cannot be used for checks in other databases;
2. **Relevance:** how relevant is this data for achieving the purpose(s), assess and mitigate the identified risks?
3. **Reliability:** to what extent can the data be trusted? Although the data collected is only declarative (no verification of documents authenticity), some elements can be more or less trustworthy. The background questions, for instance, tend to have a low level of reliability. However, it has been noted in benchmark systems, that travellers tend to answer more truthfully and provide more than is asked;
4. **Privacy:** how intrusive is it for a person's privacy to request and store this data?

Each of these criteria is assessed using the following metrics:

Legend	Ease of collection and automation	Relevance	Reliability	Privacy
++	The data can be very easily provided by the applicant and can very easily be automatically processed by the system	The data is very useful for mitigating the risks previously defined	Although it is declarative, the data can be relied upon	The intrusion in the private life of the person is very limited. Data could already be provided to authorities at the border crossing or through API/PNR.
+	The data can be easily provided by the applicant and can easily be manually processed by the system	The data is useful for mitigating the risks previously defined	Although it is declarative, the data could possibly be relied upon	The intrusion in the private life of the person is limited.
-	The data cannot be easily provided by the applicant and/or cannot be fully manually processed by the system	The data is useful for the purpose of the assessment but is not useful for mitigating the risks previously defined	The data is not very reliable	The intrusion in the private life of the person is significant.
--	The data can be neither easily provided by the applicant nor be manually processed by the system	The data is not useful for mitigating the risks previously defined	The data is completely unreliable	Major intrusion in the private life of the person.
0	The impact is null or the criteria is not applicable	The impact is null or the criteria is not applicable	The impact is null or the criteria is not applicable	The impact is null or the criteria is not applicable

<sup>194</sup> The metrics used for the criteria are explained in Annex 4. – "Data".

Table 45: Overview of all data fields envisaged

Traveller data to be collected	Reason of the collection						Data in other DBs						Assessment criteria				Benchmark			Data contained in the passport	
	Security	Migration	Other SBC entry condition	Filtering / risk score	Application management	Disambiguation	SIS	EES	EIS	VIS	SLTD	TDAWN	ETIAS screening rules	Ease of collection/ automation	Relevance	Reliability	Privacy	eVisitor	eTA		ESTA
<b>Biographical data</b>																					
First name	✓	✓			✓	✓	✓	✓	✓	✓		✓		++	++	+	++	✓	✓	✓	✓
Surname	✓	✓			✓	✓	✓	✓	✓	✓		✓		++	++	+	++	✓	✓	✓	✓
Name at birth	✓	✓			✓		✓		✓					++	++	+	++	✓	✓	✓	✓
Other name	✓	✓			✓		✓		✓					+	++	+	++	✓		✓	
Parents' first names					✓				✓					+	+	0	+			✓	
Date of birth	✓	✓			✓		✓	✓	✓	✓				++	++	+	++	✓	✓	✓	✓
Place of birth					✓		✓		✓	✓				++	++	+	++	✓	✓	✓	✓
Nationality	✓	✓			✓		✓	✓	✓	✓				++	++	+	++	✓	✓	✓	✓
Additional nationalities	✓	✓			✓		✓		✓					+	++	+	++	✓	✓	✓	
Gender	✓	✓		✓	✓		✓	✓	✓	✓				++	++	+	++	✓	✓	✓	✓
Marital status									✓					+	-	0	-		✓		
<b>Passport data</b>																					
Passport number	✓	✓			✓	✓	✓	✓		✓	✓	✓		++	++	+	++	✓	✓	✓	✓
Country of issuance	✓	✓		✓			✓			✓	✓			++	++	+	++	✓	✓	✓	✓
City of issuance	✓	✓		✓										-	-	0	-			✓	✓
Issuing authority	✓	✓		✓										-	-	0	-	✓			✓
Passport expiry date	✓	✓			✓			✓		✓				++	++	+	++	✓	✓	✓	✓
Passport issuance date	✓	✓							✓					++	++	+	++	✓	✓	✓	✓
<b>Contact details</b>																					
Email address	✓				✓				✓			✓		++	++	+	+	✓	✓	✓	
Address (residence)	✓	✓			✓				✓					+	+	+	-	✓	✓	✓	

Traveller data to be collected	Reason of the collection						Data in other DBs						Assessment criteria				Benchmark			Data contained in the passport
	Security	Migration	Other SBC entry condition	Filtering / risk score	Application management	Disambiguation	SIS	EES	EIS	VIS	SLTD	TDAWN	ETIAS screening rules	Ease of collection / automation	Relevance	Reliability	Privacy	eVisitor	eTA	
Phone number	✓				✓			✓				✓	++	++	+	+	✓		✓	
<b>Intended travel</b>																				
MS of intended first entry					✓								++	-	+	+				
<b>Background questions</b>																				
Education and occupation		✓		✓									+	++	-	-		✓	✓	
Convicted of a serious crime	✓			✓				✓					+	++	-	-		✓	✓	
Been recently present in a war zone				✓									+	++	-	-			✓	
Threat to public health: infectious disease (e.g. tuberculosis)			✓										+	++	-	-			✓	
Seek work in the destination country													++	-	--	+			✓	
Previously been refused entry/visa, ordered to leave							✓	✓	✓				+	-	+	+		✓	✓	
Overstay <sup>195</sup>								✓					++	+	--	+			✓	
Seek to engage in serious organised/terrorism activity													++	-	--	+			✓	
Fraud and visa misappropriation <sup>196</sup>													+	+	--	+			✓	

<sup>195</sup> This is going to be checked automatically with EES.

<sup>196</sup> Already covered by questions related to the serious crime.

Traveller data to be collected	Reason of the collection						Data in other DBs						Assessment criteria				Benchmark				
	Security	Migration	Other SBC entry condition	Filtering / risk score	Application management	Disambiguation	SIS	EES	EIS	VIS	SLTD	TDAWN	ETIAS screening rules	Ease of collection/ automation	Relevance	Reliability	Privacy	eVisitor	eTA	ESTA	Data contained in the passport
<b>Intended travel and travel history</b>																					
Previously applied to visit the country								√		√				-	-	+	+		√		
Address of destination														0	-	-	--			√	
<b>Financial means</b>																					
Funds available to travel to the country		√												+	++	-	-		√		
<b>Other</b>																					
Social media														+	+	--	--			√	
Biometrics (facial image)														--	++	+	--				
Image of the passport														--	++	+	--				√

Other fields can be added in the future if it is demonstrated that they could bring an added value for the risk assessment: passport issuance date, city and authority of issuance.



## Definition of serious crime

With regards to the definition of serious crime, the possible reference lists can be:

- a) the European arrest warrant;
- b) Annex II of the PNR Directive. Terrorism is not listed as it is considered in another category (according to Articles 1 to 4 of Framework Decision 2002/475/JHA).

Both lists could be used for ETIAS and are largely similar, however, the PNR definition is the latest approved by European Parliament and therefore the most likely candidate to be used (with the addition of terrorism).

*Table 46: Comparison of the definitions of serious crimes*

PNR (Annex II PNR Directive, 2016)	European arrest warrant <sup>197</sup>
<ol style="list-style-type: none"> <li>1. participation in a criminal organisation,</li> <li>2. trafficking in human beings,</li> <li>3. sexual exploitation of children and child pornography,</li> <li>4. illicit trafficking in narcotic drugs and psychotropic substances,</li> <li>5. illicit trafficking in weapons, munitions and explosives,</li> <li>6. corruption,</li> <li>7. fraud, including that against the financial interests of the Union,</li> <li>8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,</li> <li>9. computer-related crime/cybercrime,</li> <li>10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,</li> <li>11. facilitation of unauthorised entry and residence,</li> <li>12. murder, grievous bodily injury,</li> <li>13. illicit trade in human organs and tissue,</li> <li>14. kidnapping, illegal restraint and hostage-taking,</li> <li>15. organised and armed robbery,</li> <li>16. illicit trafficking in cultural goods, including antiques and works of art,</li> <li>17. counterfeiting and piracy of products,</li> <li>18. forgery of administrative documents and trafficking therein,</li> <li>19. illicit trafficking in hormonal substances and other growth promoters,</li> <li>20. illicit trafficking in nuclear or radioactive materials,</li> <li>21. rape,</li> <li>22. crimes within the jurisdiction of the International Criminal Court,</li> <li>23. unlawful seizure of aircraft/ships,</li> <li>24. sabotage,</li> <li>25. trafficking in stolen vehicles,</li> <li>26. industrial espionage.</li> </ol>	<ol style="list-style-type: none"> <li>1. participation in a criminal organisation,</li> <li>2. <b>terrorism,</b></li> <li>3. trafficking in human beings,</li> <li>4. sexual exploitation of children and child pornography,</li> <li>5. illicit trafficking in narcotic drugs and psychotropic substances,</li> <li>6. illicit trafficking in weapons, munitions and explosives,</li> <li>7. corruption,</li> <li>8. fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,</li> <li>9. laundering of the proceeds of crime, counterfeiting currency, including of the euro,</li> <li>10. computer-related crime,</li> <li>11. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,</li> <li>12. facilitation of unauthorised entry and residence,</li> <li>13. murder, grievous bodily injury,</li> <li>14. illicit trade in human organs and tissue,</li> <li>15. kidnapping, illegal restraint and hostage-taking,</li> <li>16. <b>racism and xenophobia,</b></li> <li>17. organised or armed robbery,</li> <li>18. illicit trafficking in cultural goods, including antiques and works of art,</li> <li>19. <b>swindling,</b></li> <li>20. <b>racketeering and extortion,</b></li> <li>21. counterfeiting and piracy of products,</li> <li>22. forgery of administrative documents and trafficking therein,</li> <li>23. <b>forgery of means of payment,</b></li> <li>24. illicit trafficking in hormonal substances and other growth promoters,</li> <li>25. illicit trafficking in nuclear or radioactive</li> </ol>

<sup>197</sup> In red are highlighted the crimes that are not included in the PNR definition of serious crime.

PNR (Annex II PNR Directive, 2016)	European arrest warrant <sup>197</sup>
	materials, 26. trafficking in stolen vehicles, 27. rape, 28. arson, 29. crimes within the jurisdiction of the International Criminal Court, 30. unlawful seizure of aircraft/ships, 31. sabotage.

## Data collected by benchmark systems

The following table shows a comparison of data collected by similar systems in Australia (eVisitor), Canada (eTA) and the US (ESTA).

Table 47: Comparison of the data collected by the three benchmark systems

	eVisitor	eTA	ESTA
<b>Biographical data</b>			
Name, surname	✓	✓	✓
Other names	✓	x	✓
Date of birth	✓	✓	✓
Country of birth	✓	✓	✓
City of birth	x	✓	✓
Nationality / country of citizenship	✓	✓	✓
Additional nationalities	✓	✓	✓
Gender	✓ (male, female)	✓ (male, female, other)	✓ (male, female)
Marital status	x	✓	x
Country of residence	✓	x	x
Parents names	x	x	✓
Membership to the CBP Global Entry Programme	x	x	✓
Approximate number of data fields	Minimum 6 – maximum 7	Minimum 9 – maximum 11	Minimum 12 – maximum 14
<b>Passport data</b>			
Passport number	✓	✓	✓
Issue and expiration dates	✓	✓	✓
Country of issue	✓	✓	✓
City of issue	x	x	✓

	<b>eVisitor</b>	<b>eTA</b>	<b>ESTA</b>
Issuing authority	√	×	×
National identification number	×	×	√ (for some countries)
Personal identification number	×	×	√ (for some countries)
Visa number (if applicable)	√	√	×
Approximate number of data fields	Minimum 7 - maximum 9	5	Minimum 8 – maximum 16
<b>Contact details</b>			
Preferred language for communications	×	√	×
Email address	√	√	√
Residential address	√	√	√
Telephone number	√ (Immi Account)	×	√
Approximate number of data fields	Minimum 4 - maximum 5	5	Minimum 7 and maximum 8 (personal) and maximum 13 (contact details while in the US)
<b>Background questions</b>			
Education and occupation information	×	√	√ (not all fields are mandatory)
Seek work in the destination country	×	×	√
Fraud and visa misappropriation	×	×	√
Health related questions	×	√	√
Criminal records	×	√	√
Seek to engage in serious organised/terrorism activity	×	×	√
Urgent need for travel and other comments field	×	√	×
Previously been refused entry/visa, ordered to leave	×	√	√
Overstay	×	×	√
Been recently present in a war zone	×	×	√
Approximate number of	1	Minimum 6 –	Minimum 10 –

	eVisitor	eTA	ESTA
data fields for all background questions		maximum 12	maximum +20
<b><i>Intended travel and travel history</i></b>			
Previously applied to visit the country	x	√	x
Dates of intended stay	x	x	x
Intent to enter in more than one occasion	x	x	x
Address of destination	x	x	√
Point of contact information	x	x	√
Emergency contact information	x	x	√
Purpose of stay (business or tourism)	√	x	x
<b><i>Financial means</i></b>			
Funds available to travel to the country	x	√	x
Total approximate number of data fields	Minimum 18 – maximum 22	Minimum 25 – maximum 33	Minimum 37 – maximum +70

## Possible data collected by ETIAS

The following table shows the minimum and maximum numbers of data fields in the ETIAS application form:

*Table 48: Number of data fields for ETIAS*

	<b>Minimum number of data fields</b>	<b>Maximum number of data fields</b>
Biographical data <sup>198</sup>	9	11
Passport data	3	
Contact details <sup>199</sup>	5	
Intended travel	1	
Background questions <sup>200</sup>	6	7
<b>Total</b>	<b>24</b>	<b>27</b>

---

<sup>198</sup> "Other name" and "Additional nationalities" would not be applicable to all applicants. "Parents' first names" would require two data fields ("mother" and "father").

<sup>199</sup> "Address (residence)" would require three data fields ("address", "postcode" and "country").

<sup>200</sup> "Additional information" would not be applicable to all applicants.

## Data collected for visa

The data set collected for the purpose of granting a visa can be found in Annex I of the Visa Code<sup>201</sup>. It contains the following data:

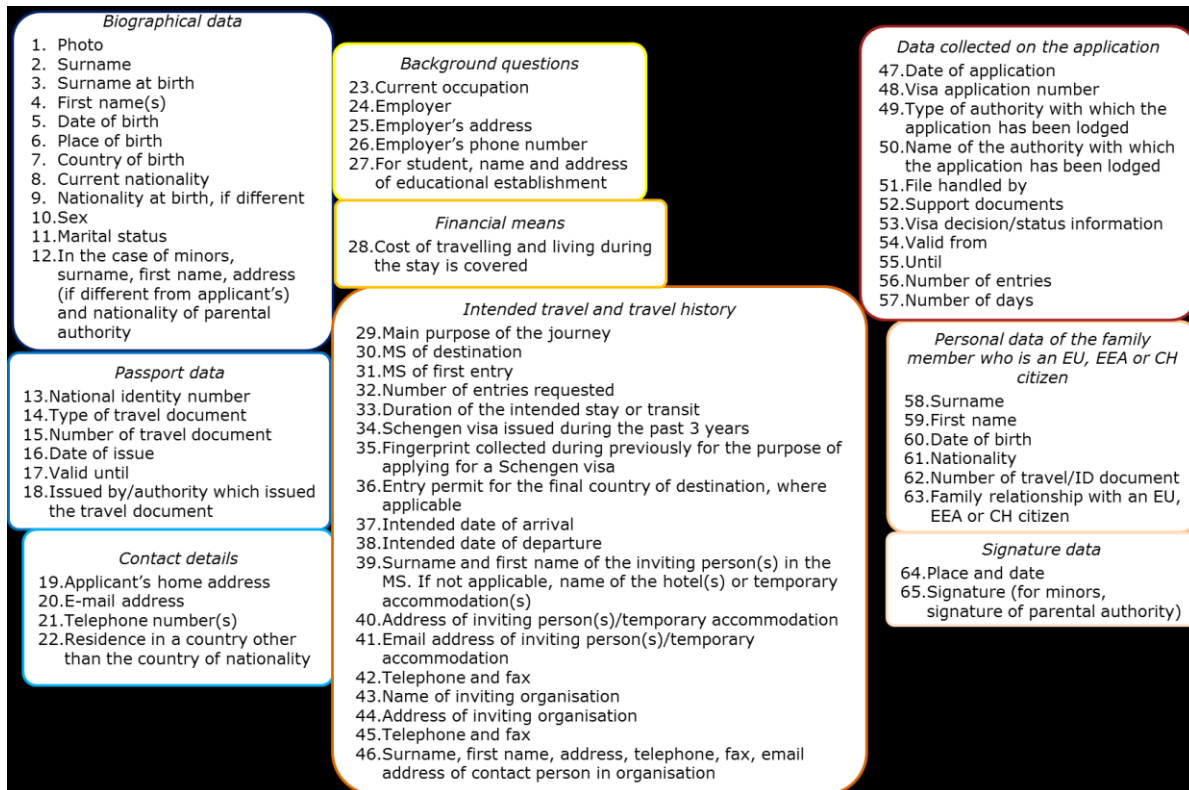


Figure 29: Data collected for the purpose of granting a visa

<sup>201</sup> Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code).

Table 49: Data collected for the purpose of granting a visa compared to ETIAS data set

Data collected for the purpose of granting a visa	ETIAS data set
<b>Biographical information</b>	
Photo	X
Surname	√
Surname at birth	√
First name(s)	√
Date of birth	√
Place of birth	√
Country of birth	√
Current nationality	√
Nationality at birth if different	X
Gender	√
Marital status	X
In the case of minors: surname, first name, address if different from the applicant's and nationality of parental authority	X
<b>Passport information</b>	
Nationality identity number	X
Type of travel document	X
Number of travel document	√
Date of issue	X
Valid until	√
Issued by/authority which issued the travel document	√
<b>Contact details</b>	
Applicant's home address	√
Email address	√
Telephone number(s)	√
Residence in a country other than the country of nationality	X
<b>Background questions</b>	
Current occupation	√
Employer	X
Employer's address	X
Employer's phone number	X
For students: name and address of educational establishment	X
Cost of travelling and living during the stay is covered	X
<b>Other data collected</b>	
Data on intended travel and travel history (18 fields)	X
Data on the application (11 fields)	X
Data on the family member who is an EU, EEA or CH citizen (6 fields)	X
<b>Additional steps of the process</b>	
Interview at a consular post	X not mandatory
Additional documents	X not mandatory
Processing fee	√
<b>Data collected in ETIAS</b>	
<b>Data collected for the purpose of granting a visa</b>	
Convicted of a serious crime	X
Been recently present in a war zone	X
Threat to public health: infectious disease (e.g. tuberculosis)	X

Overall, ETIAS data set (24 to 27 data fields) is smaller than the visa procedure data set (minimum 44 data fields, maximum 65 data fields). However, the system collects three additional data due to the absence of an interview prior to arrival at the borders: if the applicant has ever been convicted of serious crime, if the applicant has been recently present in a war zone and if the applicant is a threat to public health.

## Data retention

The study considered starting the 5-year retention period from the last exit of the traveller from the Schengen Area, as is currently proposed for the EES data. The table below summarises the advantages and disadvantages of this approach.

*Table 50: Advantages and disadvantages of starting the retention at the exit from the Schengen Area*

<b>Advantages</b>	<b>Disadvantages</b>
<p><b>Consistency</b> – Avoid having an EES record with no corresponding ETIAS data, and vice-versa</p>	<p><b>Limits to consistency</b> - Impossibility to always have a corresponding EES and ETIAS: travellers may submit an ETIAS application but decide not to travel (ETIAS but no EES) or come to the border without having applied for an authorisation (EES but no ETIAS).</p>
<p><b>Law enforcement</b> – Law enforcement authorities would have access to the ETIAS data on top of the EES data for a longer period of time</p>	<p><b>Purpose</b> – The data retention period cannot be extended for law enforcement purposes, as it is not the primary purpose of the system</p> <p><b>Limited additional data</b> – ETIAS would provide law enforcement authorities with limited additional data compared to EES; data would be of lower reliability as it is declarative<sup>202</sup>.</p>
	<p><b>Complexity</b> – Increased overall complexity of the system: the 5-year retention period would start either:</p> <ol style="list-style-type: none"> <li>a) from the exit of the traveller from the Schengen Area;</li> <li>b) from the last day of authorised stay if the traveller does not exit;</li> <li>c) from the attempt at entering the Schengen Area if entry was refused;</li> <li>d) from the moment of the decision (grant, deny, revoke) if the traveller does not come to the border.</li> </ol>

In light of the analysis, it appears that starting the 5-year retention period from the last exit of the traveller from the Schengen Area provides both advantages and disadvantages and should be further analysed.

<sup>202</sup> The following data would be provided by ETIAS on top of the EES data and would be accessible to law enforcement authorities: name at birth, other name, place of birth, parents' first name, email address, address, telephone number, answers to education and occupation, refused visa, serious crime and war zone background questions.



## Law enforcement access

In the case of ETIAS, **law enforcement authorities** would **not have access to all ETIAS data**. The following table illustrates which data could be accessed:

Table 51: Data accessible by law enforcement authorities

Data	Specific purpose
	Investigation
<b>Biographic data</b>	
<i>First name</i>	✓
<i>Surname</i>	✓
<i>Name at birth</i>	✓
<i>Other name</i>	✓
<i>Date of birth</i>	✓
<i>Place of birth</i>	✓
<i>Parents' first names</i>	
<i>Nationality</i>	✓
<i>Additional nationalities</i>	✓
<i>Gender</i>	✓
<b>Passport data</b>	
<i>Passport number</i>	✓
<i>Passport expiry date</i>	✓
<i>Country of issue</i>	✓
<b>Contact details</b>	
<i>Email address</i>	✓
<i>Address (residence)</i>	✓
<i>Phone number</i>	✓
<b>Intended travel</b>	
<i>MS of intended first entry</i>	✓
<b>Background information</b>	
<i>Education and occupation information</i>	✓
<i>Convicted of serious crime</i>	✓
<i>Recently been present in a war zone</i>	✓
<i>Threat to public health: infectious disease (e.g. tuberculosis)</i>	
<i>Additional information provided by the applicant at the request of the CMPE and/or the MS for the purpose of manual processing</i>	✓

## Data model

This section illustrates a possible data model for the ETIAS database. The data model would be linked to the EES database, so as to allow associating a recorded entry into the Schengen territory to the corresponding travel authorisation. Moreover, this would also allow linking a travel authorisation to an individual file in EES, thus benefiting of the EES identification services (provided by the biometric identifiers).

Once the link is established between the two systems it would be possible to cross-check the information provided in declarative form during the ETIAS application and the information on the passport, checked by a border guard at the time of border-crossing.

The link between EES and ETIAS would be similar to what is currently suggested by the EES legislative proposal for the VIS. Each entry/exit record would contain the reference to the corresponding travel authorisation. This reference would be automatically retrieved by the system when a new passport is presented at the border. It would then be added in the EES file. The retrieval would use the passport data (e.g. passport number, issuing country and date of birth) to query ETIAS.

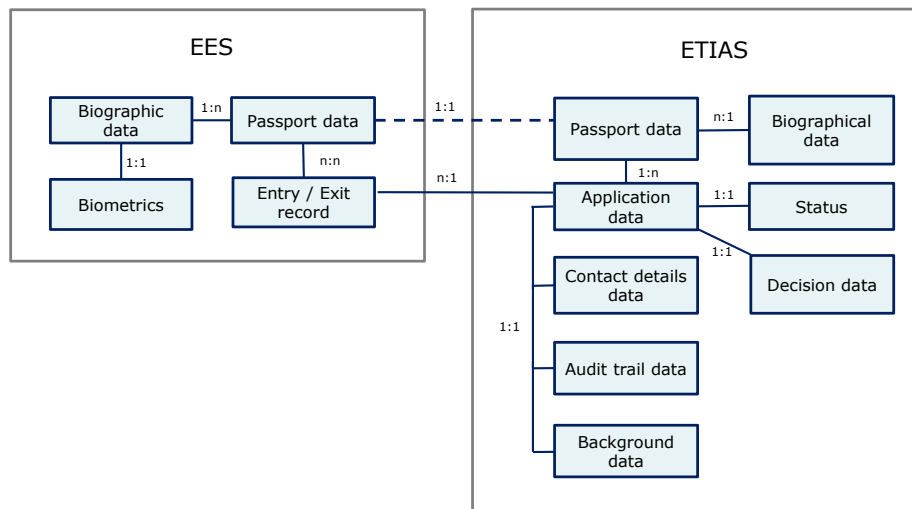


Figure 30: ETIAS high-level data model<sup>203</sup>

### <sup>203</sup> Entities

In the context of a data model, "entities" are real-world objects or persons. An "entity-set" is a set of entities that constitutes a group.

In the context of the ETIAS data model, an entity would be a traveller from a non-Schengen country. The entity-set would be "travellers from non-Schengen countries".

### Attributes

"Attributes" are the properties of the entities.

In the context of the ETIAS data model, the entity "travellers" would have as attributes "first name", "last name" etc.

### Cardinalities

"Cardinalities" describe the relationships between entities or between entities and their attributes. A cardinality between an entity and one of its attribute can be:

- One-to-one (1:1): one entity from entity set A can be associated with at most one entity of entity set B and vice versa;
- One-to-many (1:n): one entity from entity set A can be associated with more than one entities of entity set B however an entity from entity set B, can be associated with at most one entity;
- Many-to-one (n:1): more than one entities from entity set A can be associated with at most one entity of entity set B, however an entity from entity set B can be associated with more than one entity from entity set A;
- Many-to-many (N:n): one entity from A can be associated with more than one entity from B and vice versa.

## Annex 5. – Business processes

### Decision-making process options

The study analysed the following three options for the manual processing of applications:

1. **By Member States only.** The responsibility for each application would be allocated to one Member State according to pre-determined rules (in the case of an authorisation per trip, the first Member State of entry could be considered responsible for the application. In the case of an authorisation granted for a period of time, a mechanism to assign responsibility to Member States would have to be identified).  
Each Member State would have to assess the applications under its responsibility using the IT services provided by a European traveller application processor complemented with a search in its own databases. In case the search using the European traveller application processor reveals an alert/information from another Member State, the responsibility to follow-up would be on the Member State processing that specific application.  
There would not be any manual processing of applications at central level (a central entity could however provide support to Member States and travellers). Complaints from travellers would be redirected to the Member State which processed the related applications.  
This option possesses the major inconvenience of representing a significant workload for Member States. The workload would require additional staff at Member State level. This option is thus considered as **not viable** by the study;
2. **By the Central Manual Processing Entity (CMPE) only.** The CMPE would be responsible for all applications. Member States would not take part in their processing. This option would require the CMPE to connect to Member States' databases (to access or collect information from all Member States to assess security risks - not doing so would result in a lack of information; in case of a match with a case known by Member States, requesting the information to the national authorities would result in delays). However, this connection is deemed unfeasible due to technical and legal issues. This option is thus considered as **not viable** by the study;
3. **By both Member States and the CMPE.** The CMPE would be responsible for some applications and seek the help of Member States for others. It would coordinate the decision-making process when Member States are involved. This option is the preferred solution for ETIAS, as it would allow limiting the workload for Member States while involving them in manual processing, thus leveraging on the information they possess.

This option possesses itself two main variants:

- a) The CMPE cannot deny an authorisation. Complex cases, i.e. cases that would lead to a **denial** or simply **require additional evidence**, are transferred to Member States;
- b) The CMPE can deny authorisations **in specific cases** (e.g. in case of an alert for refusal of entry in the SIS). Member States would be consulted **in cases for which they might have additional information** relevant to a specific application, this could be for instance the case when a Member State has created a specific alert (e.g. in the SIS). In cases of hits on alerts originated from a country not part of the Schengen Area, the applications would be handled by the CMPE.

The following table summarises the advantages and disadvantages of two main identified variants.

Table 52: Comparison of the two main variants

	Advantages	Disadvantages
CMPE cannot deny an authorisation	<ul style="list-style-type: none"> <li>- Clear-cut <b>accountability in case of appeal</b> to the decision: the MS that dealt with the application handles the appeal.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>More workload for MS</b> that would have to handle all cases requiring additional evidence;</li> <li>- <b>More heterogeneous risk assessments;</b></li> <li>- Responsibility rule complicated in case of a match in an <b>international database</b> (SLTD and TDAWN) as the data is not owned by any MS.</li> </ul>
CMPE can deny authorisations in specific cases	<ul style="list-style-type: none"> <li>- <b>Less workload for MS;</b></li> <li>- <b>More harmonised risk assessment;</b></li> <li>- Central processing of matches in <b>international databases</b> (SLTD and TDAWN), in particular when the data has not been entered by a MS but by a third country.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Shared accountability in case of appeal</b> to the decision, depending on which entity dealt with the case.</li> </ul>

As demonstrated in the table, variant 2 (CMPE can deny authorisations) possesses more advantages and less disadvantages than variant 1 (CMPE cannot deny authorisations). It is thus used as the baseline in the study.

## Processing times

The lead times for application processing defined in 2.3.4 “Four main processes” are coherent with the ones of the Australian, Canadian and US systems. The three systems provide in the majority of cases – when the application can be handled automatically – an answer within minutes. When manual processing is required, the Canadian eTA and the US ESTA provide an answer within 72 hours. The Australian eVisitor provides an answer between two (48 hours) to ten working days after the application has been submitted.

ETIAS cases requiring disambiguation should be performed within 24 hours. However risk assessment<sup>204</sup> would require more than 24 hours – an assumption validated through consultations with EU agencies. Indeed, it would possibly involve critical thinking and contacts with other national services (considering that denying a travel authorisation to a person subject to a SIS alert for refusal of entry is not risk assessment *per se*, and can thus be done by the central manual processing entity within 24 hours). Both of these processing times have been confirmed through consultations with EU agencies.

The proposed processing time would allow travellers to receive an authorisation even in cases in which the trip to the EU would have been planned a relatively short time in advance, in coherence with the objective of remaining convenient for travellers. Risks of tourism reduction and related impacts on business (carriers) would also increase with an extended processing time.

The study also considered the pros and cons of having a longer response time (maximum 72 hours) for providing an answer to all applications independently of whether they would be processed automatically, by the CMPE or by Member States, in order to avoid the person to know that his/her application is

<sup>204</sup> Risk assessment is used, throughout this study, to describe the assessment carried out on each visa-exempt traveller. It would mainly involve database-searching, i.e. looking for known entities based on information available in databases. It could involve elements of “network analysis”, i.e. looking for unknown entities in connection with a known entity (whether the person has a connection with a known person of interest – through phone number or physical address etc.). “Filtering” (looking for accumulations of stand-alone risk indicators or looking for matches against risk profile) would only be possible in a very limited way. “Outliers discovery” (looking for suspicious abnormalities and deviations) would not be possible and is, in the case of ETIAS, out of scope.

“problematic”. A different approach is used in Australia: the government’s website publishes processing times for “low risk” and “high risk” travellers; the two groups being differentiated based on the nationality of the traveller<sup>205</sup>. The Canadian website on eTA explicitly states that most applications are approved within minutes but that “some applications can take several days to process”<sup>206</sup>. The US ESTA governmental website recommends to apply “at least 72 hours before travel”, and adds on the same page that “[i]n most cases, a response is received within seconds of submitting an application”<sup>207</sup>. None of the three systems from the benchmark is designed or advertised to prevent an applicant from knowing that his/her application is problematic. This thus does not appear as a necessary option for ETIAS, in particular considering the significant impact it would have on convenience for travellers.

## Field validation

The following accuracy checks could be enforced by the travellers’ web-interface:

- Are all the fields that apply for the given application filled-in?
- Are the phone number and/or email address formats valid? (e.g. a phone number field should only be filled by numbers; an email address should be composed of an “@”. More detailed format checks would be particularly difficult to implement and would require heavy workload for both generating them and monitoring their relevance over time. Formats of phone numbers and email addresses are indeed different across countries and can change. More detailed format checks are thus not recommended)
- Are the phone number and/or email address existing?
  - This could be verified by the sending of a code to the number/email address entered by the applicant; the application would only be valid after the traveller has entered the code received into the web-interface.
- Is the passport number format valid (e.g. are numbers and letters used in a consistent way compared to how number and letters should be used for an actual passport)?

More precisely:

- Number and type of characters by nationality could be known by the interface, that would display an error message when the number and type of characters entered by the applicant in the “identity document number” field would not match the requirements of typical identity documents for the given nationality (this presupposes that the field “nationality” would exist, and that it would be placed before the field “identity document number” in the application form). For example, the interface would know that a Belgian document starts with 2 letters. An application in which it would be indicated “Belgian” in the nationality field and “124653465412” in the identity document number field would display an error message. However, one could express reservations as to whether this would be possible in all cases. Indeed, exact information on the way passport numbers are designed in each visa-exempt country would have to be transmitted to the EU; this information would have to be updated with each change and immediately, so as not to prevent travellers from the country changing its passport-number design to apply and thus come to the Schengen Area. This information would as well need to be stored, which could generate security and practical issues;
- Rules could be implemented to ensure that there is no mixing up of the letter “o” and the number “0”;
- Following the Canadian model, it could be requested to enter the identity document number twice, while not allowing pasting information in the second field. The 2 fields would be compared by the interface; an error message would be displayed in case they are not matching.

---

<sup>205</sup> <https://www.border.gov.au/about/access-accountability/service-standards/visitor-visa-processing-times> (accessed 06/2016).

<sup>206</sup> <http://www.cic.gc.ca/english/visit/eta.asp> (accessed 06/2016).

<sup>207</sup> <https://esta.cbp.dhs.gov/esta/application.html?execution=e1s1> (accessed 06/2016).

- Is the passport still valid or has it expired?
- Is the application form filled-in with the appropriate alphabet letters?

This could as well be done through the design of ETIAS’s form itself: it could follow the Canadian model, which favours drop-down lists over free-text fields<sup>208</sup> – less reliable and less comparable - for, e.g. questions about the traveller’s current occupation.

In addition, after completion of all fields and before the payment, a page should allow applicants to check the accuracy of the data entered. The page would present all the data entered and would allow applicants to go back and change the data or to validate the application. Errors could be pointed out to applicants.

## Case-handling

The following table presents a detailed overview of the different cases that would lead to manual processing. For each case, an allocation of tasks between Member States and the CMPE is proposed, based on the principles described in “2.3.4 Four main processes”.

*Table 53: Tasks allocation for case handling (non-exhaustive)*

<b>Case</b>	<b>CMPE</b>	<b>MS</b>
	<b>Process the case</b>	<b>Coordinate the response from MS, ensure a response is given on time</b>
		<b>Contribute to the processing of the case</b>
<b>1. Disambiguation</b>	√	
<b>2. Hit against an alert/match with information in a EU system</b>		
– Alert for refusal of entry in the SIS	√ (deny authorisation <sup>209</sup> )	
– Other alert in the SIS		√
– Visa previously been rejected in the VIS		√
– Previous overstay in EES		√
– Hit against the EIS		√
<b>3. Match with an</b>		√

<sup>208</sup> By contrast, the US ESTA uses free-text fields.

<sup>209</sup> This systematic denial is coherent with the rules currently applied by border guards at the external borders of the Schengen Area as defined in the Annex to the SIRENE Manual. Indeed no other action is requested from border guards but to refuse admission when having a hit on an alert for refusal of entry. Stopping the person or carrying out a discreet check is only foreseen for other types of alert. See Annex to the Commission Implementing Decision replacing the Annex to Commission Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II), document C(2015) 326 final, Annex 3, Appendix 2: The SIS II Tables.

<b>Case</b>	<b>CMPE</b>	<b>MS</b>
<b>investigation trigger in the ETIAS screening rules</b>		
<b>4. Match with an international database</b>		
- Stolen and Lost Travel Documents database (SLTD); no MS involved	√ (process the case)	
- Travel Documents Associated With Notices (TDAWN); MS involved		√
- Travel Documents Associated With Notices (TDAWN); no MS involved	√ (process the case)	
- Travel Documents Associated With Notices (TDAWN); MS involved		√
<b>5. Match with a previously denied travel authorisation</b>		
- Authorisation denied by a MS		√
- Authorisation denied by CMPE	√ (process the case)	
<b>6. Match with one or several risk indicator(s) or a risk profile</b>	√ (process the case)	

## Re-check of granted travel authorisations

An efficient re-assessment process would diminish the need for a short validity period for the travel authorisation, which would be beneficial to travellers' acceptance of the system.

The table below provides a detailed analysis of 1) which databases should be used in the re-check process; 2) what should be the frequency of the re-check for each of them.

*Table 54: Justification for the databases present in the re-check process*

	Added value of the re-check	Justification
<b>SIS</b>	Yes	<p>The Second generation of the Schengen Information System entered into operations on 9 April 2013, replacing the former SIS I.</p> <p>No information is publicly available on how frequently the alerts are inserted in the system. But taking into account the last yearly increase of the number of alerts and regardless of the average three year data retention period, it can be roughly estimated that 20,580 alerts are inserted every day.</p> <p>Given the overall high number of alerts, their importance and their constant increase through time, as shown in the table above, re-checking SIS for new alerts every 24 hours can prove to have a significant added value.</p>
<b>VIS</b>	No	<p>VIS would be checked at the first application for a travel authorisation submitted by a citizen of a new visa-exempt country. Indeed it would not be relevant for all applications: the data it contains is only interesting to check for citizens of countries that became visa-exempt country in the last five years as the data in VIS is retained for five years maximum. In addition, VIS data gives an overview of previously refused visas for former visa holders. As these individuals are now VE-TCN, no additional information can be added to their VIS profile. As a conclusion, VIS only offers an added value for the risk assessment at the first application for a travel authorisation.</p>
<b>EES</b>	Yes	<p>The system would generate new and updated information on the entries and exits of VE-TCN on a daily basis and is therefore a useful tool to identify overstay.</p> <p>It would be useful to check each granted application:</p> <ol style="list-style-type: none"> <li>1. During the decision-making process, to check whether the person has previously overstayed;</li> <li>2. 91 days (short stay of 90 days in the Schengen Area + one day of overstay) after the submission of the application, as a traveller would have the right to stay within the Schengen Area for this period of time and thus cannot overstay before its end;</li> <li>3. Each day after this date, as the EES list of overstayers is updated daily.</li> </ol> <p>Re-checking EES after 91 days of validity period and every 24 hours since that date is then considered relevant for the risk assessment.</p>
<b>SLTD</b>	Yes	<p>Given that ETIAS is an individual and document-centric system, and as SLTD data is related to the passport information, it is clearly relevant to re-check it every day. The system receives an average of 10 million queries per day, which can go up to 30 million at peak times. In this sense, there will be no major technical difficulties querying SLTD every 24 hours.</p>
<b>TDAWN</b>	Yes	<p>As a component of SLTD, TDAWN would then be an interesting database to re-check as often as SLTD.</p>
<b>Screening rules</b>	Yes	<p>The screening rules are a new tool put in place in the context of ETIAS. They would contain both specific values inserted by MS and data analytics rules, i.e. common risk indicators and patterns. A match of an application with a screening rule would not lead to automatic denial, but would trigger the application to be manually processed. The frequency of the re-check would depend on the use MS do of this tool. Indeed, if many new pieces of information are added every day, it would be</p>



	beneficial to re-check it every 24 hours.
--	---

The following table shows the evolution of the number of SIS alerts over time (since the implementation of SIS II). This evolution has been used in the above table to demonstrate the need for frequent re-checks of the already-granted ETIAS authorisations against the new alerts entered into SIS.

*Table 55: Evolution of SIS alerts*

	9 <sup>th</sup> April 2013	31 <sup>st</sup> December 2013	31 <sup>st</sup> December 2014	31 <sup>st</sup> December 2015
Total number of alerts in SIS	46,921,344	50,279,389	55,970,029	63,481,889
Increase of number of alerts	N.A	+3,358,045 +6.7%	+5,690,640 +10.2%	+7,511,860 +11.9%
Total number of alerts on persons	N.A	861,900	797,764	793,318
Alerts for refusal of entry of a TCN	N.A	623,203 72%	547,492 68.6%	492,655 62%

## Exemptions

The exemptions define which category of persons would be exempt from a requirement (border controls, visa, travel authorisation). The following table presents the exemptions for the SBC, EES, VIS and the three benchmark systems.

Table 56: Exemptions in other EU and benchmark systems

<b>Exemption</b>	<b>SBC<sup>210</sup></b>	<b>EES proposal<sup>211</sup></b>	<b>Visa<sup>212</sup></b>	<b>eVisitor<sup>213</sup></b>	<b>eTA</b>	<b>ESTA</b>
Heads of State and the members of their delegation(s)	√				√ (the Royal Family)	
Holders of diplomatic, official/duty passports	√		√		√	√
Officials from international organisations	√		√ (holders of laissez-passer)			
Flight crew members	√		√ (civilian)		√	
Sea crew members	√		√ (civilian)	N.A	N.A	
Flight safety, accident investigators					√	
School pupils during school excursion			√			
Minors						
Holders of a long-stay visa/residence permit/ /residence card		√	√	√	√	√

<sup>210</sup> Article 20 of the Schengen Borders Code lists the categories of persons for whom specific rules for border checks should be applied. Exemptions that Member States may put in place are in not-bold blue in the table.

<sup>211</sup> Article 2 of the EES proposal (6 April 2016).

<sup>212</sup> The exemptions from the visa requirement are not fully harmonised at Schengen level. Article 4 of the Council Regulation (EC) No 539/2001 of 15 March 2001 lists the persons who *may* be exempt from the visa requirement: they are in not-bold blue in the table. Article 3 (5) of the Visa Code Regulation lists the categories of persons exempted from the requirement to possess a transit visa.

<sup>213</sup> As Australia follows a universal visa requirement, there is no exemption regime as such. Instead of being exempted from the eVisitor, some categories of travellers are required to apply for another visa outside the programme's scope. For example, a State Representative visiting Australia needs to apply for a Diplomatic Visa regardless of his/her nationality.

<b>Exemption</b>	<b>SBC<sup>214</sup></b>	<b>EES proposal<sup>215</sup></b>	<b>Visa<sup>216</sup></b>	<b>eVisitor<sup>217</sup></b>	<b>eTA</b>	<b>ESTA</b>
Cross-border workers/ People carrying out paid activities during their stay	✓		✓			
Local border traffic permit holders			✓			✓
Passengers in transit			✓ (some exemptions )		✓ (some exemptions )	
Last-minute/emergency travel				Case-by- case	Case-by- case	Case-by- case
Helpers in the event of disaster or accident, emergency/rescue flights	✓		✓			
Force majeure					✓	
Agreements with specific countries		✓ (Andorra, Monaco and San Marino)			✓ (US and St Pierre et Miquelon)	✓ (Canada and Bermuda)

In the case of ETIAS, the exemptions would define which persons are **exempted from the requirement to possess a travel authorisation**.

As mentioned in the introduction, ETIAS would apply to visa-exempt third-country nationals (VE-TCN) coming to the Schengen Area for a short stay. The following categories of person would thus be outside the scope of ETIAS:

1. **EU nationals**, including persons having a double-nationality, one of these being an EU nationality<sup>218</sup>;
2. **TCN visa holders**;
3. **VE-TCN having a right to long-term residence in the EU** (holders of a long-stay visa/residence permit/residence card<sup>219</sup> etc.), including students and workers.

<sup>214</sup> Article 20 of the Schengen Borders Code lists the categories of persons for whom specific rules for border checks should be applied. Exemptions that Member States may put in place are in not-bold blue in the table.

<sup>215</sup> Article 2 of the EES proposal (6 April 2016).

<sup>216</sup> The exemptions from the visa requirement are not fully harmonised at Schengen level. Article 4 of the Council Regulation (EC) No 539/2001 of 15 March 2001 lists the persons who *may* be exempt from the visa requirement: they are in not-bold blue in the table. Article 3 (5) of the Visa Code Regulation lists the categories of persons exempted from the requirement to possess a transit visa.

<sup>217</sup> As Australia follows a universal visa requirement, there is no exemption regime as such. Instead of being exempted from the eVisitor, some categories of travellers are required to apply for another visa outside the programme's scope. For example, a State Representative visiting Australia needs to apply for a Diplomatic Visa regardless of his/her nationality.

<sup>218</sup> Applications of the persons acquiring EU nationality would have to be deleted.

<sup>219</sup> This includes VE-TCN family members of EU citizens. See Articles 5 and 7 of Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and

Among VE-TCN coming for a short stay, the following persons would have to be exempted:

4. **Flight crew members.** In line with international law, no fees should be imposed on flight crew members. Moreover, countries must facilitate air traffic and prevent delays<sup>220</sup>. Exempting flight crew members from the requirement to possess a travel authorisation would allow EU law to be in line with these two provisions. Alternatively, flight crew members could be exempted from the fee – however this would be complex to implement; moreover, not providing flight crews with the full exemption would be difficult to justify in light of Schengen States’ commitment to facilitate air traffic;
5. **Sea crew members.** International law limits the requirements that can be imposed on sea crew members<sup>221</sup>. Moreover, countries must facilitate maritime traffic and prevent delays<sup>222</sup>. Exempting sea crew members from the requirement to possess a travel authorisation would allow EU law to be in line with international law; not exempting sea crew members would be difficult to justify in light of Schengen States’ commitments;
6. **Turkish self-employed persons and providers of services.** Turkish self-employed persons and providers of services would need to be exempted from the requirement to possess a travel authorisation. An agreement signed between the EU and Turkey indeed prevents the imposition of new (compared to what existed at the time of the agreement signature) and more stringent procedural or financial requirements on them<sup>223</sup>. This has been confirmed on numerous occasions by the European courts<sup>224</sup>. As no visa requirement (including the Schengen visa, which was not existing at the time of the agreement) should be imposed on this category of Turkish nationals, ETIAS cannot be considered as an alleviation of the visa/requiring less<sup>225</sup>;
7. Other nationals of countries with which the EU will sign **specific agreements**. They would have to be exempt should the agreement foresee it.
8. Persons involved in **emergency/rescue** (this may include flight safety, accident investigators, helpers in the event of disaster or accident etc.). Countries should establish measures for authorizing temporary entry for passengers who do not possess the required travel authorisation prior to arrival, due to exceptional diversion or delay of a flight<sup>226</sup>. Indeed conditions may not allow the filling-in of a

---

reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (Citizens Rights Directive), available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:158:0077:0123:en:PDF> (accessed 09/2016).

<sup>220</sup> See Convention on International Civil Aviation, Articles 15 and 22, available at: [http://www.icao.int/publications/Documents/7300\\_cons.pdf](http://www.icao.int/publications/Documents/7300_cons.pdf) (accessed 09/2016). All Schengen States have signed the Convention. See also Annex 9 to the Convention, Chapter 2, available at: <http://www.ifrc.org/docs/IDRL/Chicago%20Convention%20Annex%20209.pdf> (accessed 09/2016).

<sup>221</sup> In line with the Geneva Convention, countries must permit entry to sea crew members holding a passport and their appropriate “seafarer identity document”. Refusing entry to sea crew members who would not be in possession of a travel authorisation would contradict this commitment. As five Schengen States and Croatia are applying the Convention, not exempting sea crew members would place them in a difficult situation, as they would be in breach of their international commitment whenever entry would be refused by their border guards to a sea crew member on the basis that they do not possess a travel authorisation. See Article 6 of the Geneva Convention of 19 June 2003 (No 185), available at: [http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100\\_INSTRUMENT\\_ID:312330](http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312330) (accessed 09/2016).

<sup>222</sup> See Article 1 of the London Convention of 9 April 1965. All Schengen States have signed the Convention but Liechtenstein.

<sup>223</sup> Article 41 of the Additional Protocol to the Ankara Agreement, available at: [http://ec.europa.eu/enlargement/pdf/turkey/association\\_agreement\\_1964\\_en.pdf](http://ec.europa.eu/enlargement/pdf/turkey/association_agreement_1964_en.pdf) (accessed 09/2016).

<sup>224</sup> See European Agency for Fundamental Rights, Handbook on European law relating to asylum, borders and migration, 2014, p. 53.

<sup>225</sup> ECJ, C-228/06 [2009] ECR I-01031, *Mehmet Soysal and Ibrahim Savatli v. Bundesrepublik Deutschland*, 19 February 2009, available at <http://curia.europa.eu/juris/celex.jsf?celex=62006CJ0228&lang1=en&type=NOT&ancre=> (accessed 10/2016).

<sup>226</sup> This would also be in line with similar recommendations made regarding passengers who do not possess the required entry visa prior to arrival but would need entry following e.g. flight diversion. See Recommended Practice 3.75 (P.) of Annex 9 to the Convention on International Civil Aviation, October 2015, Chapter 3.

travel authorisation (i.e. passengers have no Internet access); this would be the case in flight diversion situations. The lack of foreseen exemption for these cases may lead to difficulties, e.g. an important number of travellers having to apply in the international area of an airport, just before the border-crossing points. This would be particularly problematic if some travellers do not receive the application within minutes. Alternatively, it can be envisaged to process these travellers' applications within a shortened processing time. Similarly, issues would arise for helpers in cases of rescue if time needs to be spent filling-in an application form.

In addition, the following exemptions *could* be foreseen for VE-TCNs coming for a short-stay:

9. **Holders of a local border traffic permit.** The local border traffic regime sets the conditions for residents of border areas, living up to 30 km from the border (50 km in exceptional situations) on both sides, to apply for a permit that allows them to cross the Schengen border without visa or passport. The permit is limited to the border area and valid for 1 and 5 years<sup>227</sup>. Exempting these travellers from the requirement to possess a travel authorisation would be coherent with the purpose of convenience for travellers and the current EU visa policy. Alternatively, the local border traffic regime could potentially be replaced by ETIAS (although the legal context is radically different: the local border traffic regime is an exception to the Schengen convention while ETIAS builds further on the Schengen acquis. Moreover, visa holders are excluded from ETIAS's scope while the local border traffic regime include them);
10. **Cross-border workers/people carrying out paid activities during their stay (including train/bus drivers and other staff, and lorry drivers)** could be exempt, so as to avoid ETIAS' negative impact on businesses relying on passengers or merchandises transport through the Schengen borders, which would otherwise have to pay the submission and renewal of their employees' ETIAS applications. However, this exemption would be particularly complex to implement as it would require the creation of a way to ensure it is not abused – currently, cross-border workers are not subject to specific measures;
11. **Family members of EU citizens** who do not have the right to long-term residence but are partner, dependant or member of the household of the EU citizen, or require care by the EU citizen for health reasons. Indeed EU law require Member States to facilitate the entry of these persons, to undertake an extensive examination of the personal circumstances and to justify any denial of entry to them<sup>228</sup>. If it is decided not to exempt them, responsibility for these cases could not be given to the CMPE and their applications would have to be systematically forwarded to the Member State where the EU citizen resides;
12. **Passengers in transit.** Contrary to Australia and Canada (and to some extent to the US), Europe is an important transfer hub (as opposed to being only an end destination). Thus there may be a significant commercial impact (European airports and ports may suffer a loss of competitiveness) if travellers transiting through the Schengen Area were not exempted from the ETIAS requirement. It has been mentioned, during the consultations with Member States, that exempting passengers in transit could create a security issue to the extent these travellers have sometimes the possibility to exit the airport/port and enter the Schengen Area; a transit flight/cruise could thus be used by persons seeking to avoid the ETIAS requirement. The person would exit instead of taking the second flight/return to the cruise ship. This difficulty may be circumvented by exempting only passengers in transit that would not enter the Schengen Area but stay in the airport's transit zone. Member States shall indeed, in accordance with the Annex 9 to the Convention on International Civil Aviation, allow as much as possible for passengers in transit to remain "within the airport of arrival without undergoing border control formalities to enter the State of transit" before their second flight<sup>229</sup>. In all

---

<sup>227</sup> Regulation (EC) No 1931/2006 of 20 December 2006 laying down the rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:405:0001:0022:EN:PDF> (accessed 09/2016).

<sup>228</sup> Article 3 of the Citizens Rights Directive.

<sup>229</sup> Annex 9 to the Convention on International Civil Aviation, Fourteenth Edition, October 2015, Chapter 3 (L.) (3.57).

those cases in which passengers do not enter the Schengen Area, whether the traveller possesses a travel authorisation would in any case not be checked by border guards – and the added value for the security of the Area would be non-existent;

13. **Heads of State** (and possibly, the members of their delegations, some **holders of diplomatic, official/duty passports** or certain official from **international organisations**). ETIAS's added value for these persons would be limited, as the probability that they would not comply with the Schengen entry conditions or pose a security or migration risk is particularly low. It could be assumed that their function would provide sufficient assurance on these points;
14. **Infants** or **children below a certain age**. Since the main purpose of the system is pre-travel security and migration risk-assessment of the threat a person could represent, infants or children below a certain age (e.g. 6 years old) could be exempt, as due to their age they could not represent any meaningful threat;
15. **School pupils** during school excursion. They could be exempt for similar reasons as infants would be;
16. **Persons participating in national frequent traveller programmes**. Exempting persons participating in national frequent traveller programmes would create a number of complications:
  - o The assessment conducted on these travellers to include them in the programmes would be similar, but not equivalent, to the one conducted for ETIAS. In particular, the Member State granting access to the programme would not have access to other Member States' information/databases;
  - o As a result of this limited access to other Member States' information, the risk-assessment would slightly differ from one programme to the other. Exempting frequent travellers from the ETIAS requirement could thus introduce discrepancies in the pre-assessment of travellers coming to the Schengen Area, which would diminish one of ETIAS' main added value – the harmonisation of VE-TCN pre-assessment.

Exempting these travellers is thus not a preferred solution for ETIAS.

Whether to provide for these exemptions would need to be further assessed in light of the possible security holes and additional complications they may create. An ETIAS with a few exemptions may provide more added value from a security perspective.

## Annex 6. – Architecture

### Architectural options

The ETIAS architecture is made of four main blocks (ETIAS IT Application, traveller application processor, Search Interface to other systems and ETIAS Internet Services), plus the Front End for the traveller, that provide the required services.

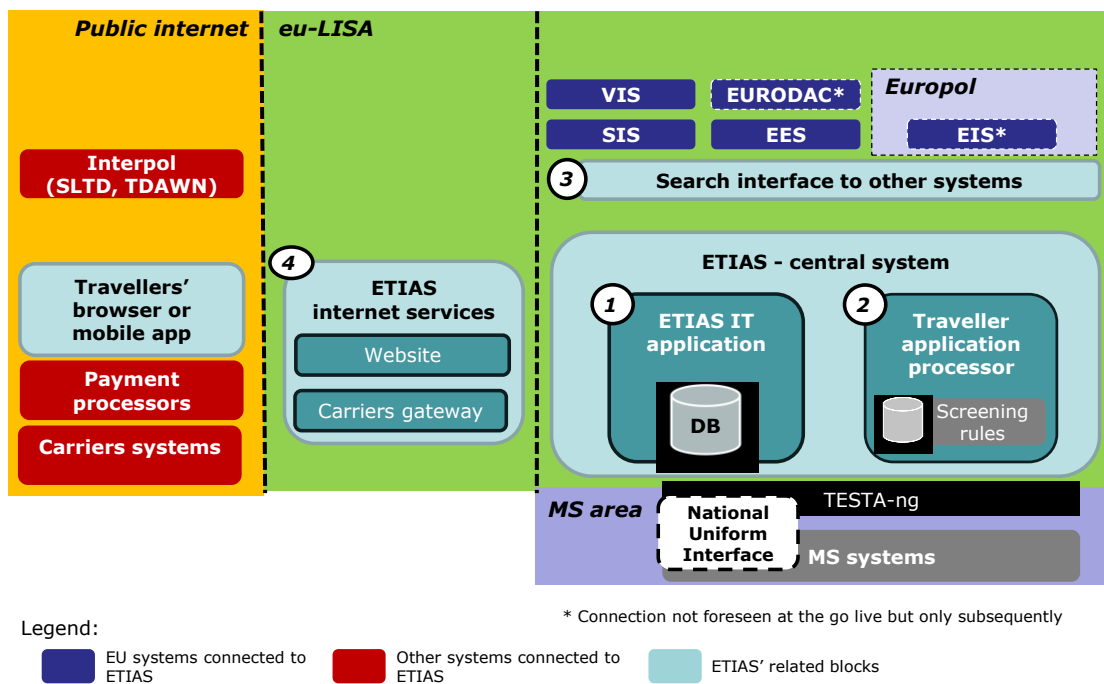


Figure 31: ETIAS main IT architectural building blocks

Assuming that ETIAS would be developed according to a modular design, where each of these architectural building blocks would provide a catalogue of services, each of these blocks could be developed following different architectural options.

The impact of the technical choices for one architectural block should have only limited impact on the others, hence their respective architectural options are considered independent.

An application could be either stored centrally or in national databases, and then be passed to the traveller application processor for processing. This would not make any difference for the decision-making process itself. Similarly, the fact that the assessment is done either centrally or by consulting national databases should not impact the ETIAS IT Application which would just store the result of the decision-making. However, there might be differences for performance and availability of the overall system.

A consistent approach across blocks (e.g. with all the building blocks being centralised) would be likely beneficial for the overall system, as it would reduce the complexity of implementation and maintenance.

Different architectural options have been considered and assessed according to the following criteria:

1. **Implementation complexity;**
2. **Cost:** both investment and operational costs;
3. **Privacy and data protection;**
4. **Performance and availability;**

Each of these criteria is assessed using the following metric:

Legend	
+	positive limited impact;
-	negative limited impact;
++	positive significant impact;
--	negative significant impact;
0	impact is null or the criteria is not applicable

### Architectural options for the ETIAS IT Application

	Option A: centralised architecture
Description	<p>All the traveller applications submitted through the ETIAS website/app would be lodged in a central database accessible by Member States and by the CMPE.</p> <p>The ETIAS IT application would not only store applications to be processed, but as well granted or refused authorisation and the respective history. ETIAS IT application would act as a central case-management system, ensuring coherence in how traveller applications are treated and recording a clear audit trail.</p> <p>The system would also allow the simultaneous manual processing of an application by multiple Member States at the same time. The CMPE would maintain an oversight of the entire process.</p> <p>This option would require to:</p> <ul style="list-style-type: none"> <li>• establish a central database for traveller application;</li> <li>• establish a central IT application for data entry by the traveller, and the management of these applications;</li> <li>• establish a governance model for the interactions between the CMPE and the MS.</li> </ul>
Implementation complexity	<p><b>+</b>: Positive impact on the technical complexity</p> <p>The technical complexity would be comparable to existing systems, such as the VIS. Establishing a central database and the application layer around it, does not pose major technical challenges.</p> <p>Having an architecture similar to the EES' architecture could also simplify the reuse of modules and functions (e.g. the interface to carriers).</p> <p>It would also be easier to establish a modular approach with building blocks that could potentially be reused by other applications, as there would be a stronger control over such building blocks.</p> <p>Integration of security safeguards would be easier, since the assets to be protected would be mainly centralised.</p>
Cost	<p><b>+</b>: Cost efficient</p> <p>A central system would be likely to benefit from economies of scales, such as volume discounts for licenses and avoid the replication of costs. For instance, maintenance costs would only occur centrally, at eu-LISA, rather than distributed in 26 MS (Schengen countries). It would likely have a shorter development, implementation and testing phases, as the architecture itself would be simpler.</p> <p>Finally, the interface between the central system and the Member States could be standardised, which would contribute to the consistency regarding how Member State rules are interacting with the traveller application processor.</p>
Privacy and data protection	<p><b>+</b>: Positive impact on data protection.</p>



	<p>A single repository of data would mean:</p> <ul style="list-style-type: none"> <li>• Avoidance of duplication of data</li> <li>• Better and easier auditability</li> </ul>
Performance and availability	<p>+: Positive impact on the performances and availability</p> <p>A central system deployed in Strasbourg with a back-up site in Austria would ensure high availability and allow a close monitoring of the level of performances delivered</p>

Option B: de-centralised architecture	
Description	<p>A de-centralised architecture would foresee a minimal central application that would act as dispatcher of the applications received through the public website/app to a decentralised application in a Member State.</p> <p>This option would require to:</p> <ul style="list-style-type: none"> <li>• Establish a central application for the dispatching of the traveller applications;</li> <li>• Establish a national application for each MS to manage the traveller application workflow;</li> <li>• Establish a central index/ search engine, to allow to search and retrieve the application stored in MS databases;</li> <li>• Establish a central repository for extracting statistics and reporting;</li> <li>• Establish governance to ensure a consistent behaviour when processing an application across 26 MS.</li> </ul>
Implementation complexity	<p>--: The technical complexity would be very high.</p> <p>The creation of a geographically distributed database with sufficient response time would be significantly more complex than having a single database to maintain.</p> <p>Information would be fragmented across different locations making harder to extract patterns, statistics or complex searches.</p> <p>The data relative to a certain person could be disseminated across several databases if the person had multiple applications processed by different MS.</p> <p>Finally, MS might have constraints in terms of technologies that can be deployed within their environments, thus increasing the heterogeneity of the IT systems that would need to work together.</p>
Cost	<p>--: a distributed system would not be cost efficient.</p> <p>This option would require the procurement of 26 databases deployed in 26 different locations. This would mean that certain assets would have to be acquired 26 times (e.g. software licenses and hardware platforms). At the same time, the administrative resources to maintain and operate such databases would have to be multiplied as well.</p> <p>Moreover, the central application would have to be developed and to be tested to work smoothly with all these systems, thus increasing the development and testing time.</p>
Privacy and data protection	<p>-: the impact on protection of personal data would be negative.</p> <p>A geographically distributed database would, in fact, mean fragmentation and possibly the redundancy of the information stored in it. The fragmentation across numerous databases would also increase the difficulty to audit ETIAS.</p>
Performance and availability	<p>--: the impact on the performance and availability would be significantly negative.</p> <p>The performance and availability of the overall system would depend on the performances and availability of national applications. An SLA would have to be agreed with all the MS and the disaster recovery plans would have to be tested, so to ensure an appropriate level of safeguard for the data stored in the system.</p>

Option C: centralised architecture with local copies at MS level	
Description	This option would be like option A, but would also allow for the creation of national copies of the ETIAS database. This option could be used to support potentially any of the process options, from a fully centralised process to a fully de-centralised process. It would potentially give MS more control over the data collected in ETIAS, which could be integrated fully with national systems.
Implementation complexity	-: the impact of this option on technical complexity would be negative. National copies of the database would have in fact to be synchronised with the central database, and eventual inconsistencies would have to be addressed. National copies would bring little to no advantage from a business point of view, while increasing the complexity of the development of the central system and of the testing with the MS.
Cost	-: this option would not be cost efficient. To allow national copies would likely imply: <ul style="list-style-type: none"> <li>• Increased development costs;</li> <li>• Increased maintenance costs;</li> <li>• Increased testing costs.</li> </ul> This is also corroborated by the lessons learned from the SIS development which does allow national copies.
Privacy and data protection	-: the impact of this option on the protection of personal data would be negative. Data would have to be replicated and consequently secured, in different locations.
Performances and availability	+ : Positive impact for performances and availability. National copies of the central database could be used in cases of outages of the central database. They could also help reducing the workload for the central systems thus being beneficial in terms of performance such as response time.

### Conclusion for the ETIAS IT Application

The centralised architecture appears to be advantageous and more fitting to the purpose of the system and to its business processes. As it can be seen in the table below, which summarises the assessment of the options considered, a centralised architecture appears to score higher in each of the criteria considered.

Table 57: Assessment of the options for the ETIAS IT Applications

	Option A: Centralised architecture	Option B: de-centralised architecture	Option C: centralised with local copies in MS
Implementation complexity	+	--	-
Cost	+	--	-
Privacy and data protection	+	-	-
Performances and availability	+	--	+
	<b>Best option</b>		

## Architectural options for the traveller application processor

Option A: centralised architecture	
Description	<p>The traveller application processor would itself be a central system, connected to all the relevant (both European and Interpol's) databases.</p> <p>It would include screening rules that would also allow MS to add specific investigation triggers. MS investigation triggers would be encrypted for additional confidentiality. Investigation triggers would be used as part of the decision-making process and risk assessment made on each application. This solution would allow MS to connect to the system and upload their investigation triggers, instead of gathering information from MS' systems.</p> <p>This option would require:</p> <ul style="list-style-type: none"> <li>• A central application connected to multiple databases, the traveller application processor would connect to SIS, EES, VIS, SLTD, TDAWN;</li> <li>• Screening rules that would allow MS to upload investigation triggers.</li> </ul>
Implementation complexity	<p><b>0</b>: the impact on data protection is assessed to be null.</p> <p>The implementation of screening rules to which MS could connect and where they could upload investigation triggers is in itself challenging given the sensitivity of the content of the possible negative impacts on travellers in case of malfunction. The requirement that the investigation triggers of each MS would be visible only to that MS is an additional layer of complexity.</p> <p>The implementation of a centralised architecture for this module would be aligned with the preferred choice for the ETIAS IT Application.</p>
Cost	<p><b>+</b>: The impact of this option on the cost is positive.</p> <p>A central architecture would achieve economies of scale.</p>
Privacy and data protection	<p><b>0</b>: the impact on data protection is assessed to be null.</p> <p>While the creation of screening rules might lead to the duplication of personal information already contained in national databases, the centralisation would allow a tighter control on the functioning of the traveller application processor.</p>
Performance and availability	<p><b>+</b>: the impact on performance is considered positive.</p> <p>A central system would simplify the scalability and reduce the scope of the evolution necessary in case of an increase of capacity.</p> <p>Moreover, the availability of the system would be less dependent on other systems, thus likely increasing the overall uptime.</p>

Option B: de-centralised architecture (Ma <sup>3</sup> tch <sup>230</sup> like – based solution)	
Description	<p>The de-centralised setup option for the traveller application processor would still have a central application connecting to European and international databases, but instead of having MS adding investigation triggers in the central repository of screening rules, it would connect directly to the national systems.</p> <p>The goal of this option is to exploit the information that MS have, to search for possible matches with the travellers applying for an ETIAS.</p> <p>The system would be based on a Ma<sup>3</sup>tch-like technology. In short this technology would allow performing the match without sharing personal data. However it would require deploying and integrating an additional layer for each of the systems connected. This layer would allow the</p>

<sup>230</sup> For further information on the Ma<sup>3</sup>tch technology see: "Ma<sup>3</sup>tch: Privacy and knowledge: 'Dynamic networked collective intelligence'", Udo Kroon FIU.NET, Minist. of Security & Justice, The Hague, Netherlands, 2013.

	<p>query by hashing the personal information and by translating the different data representations in the different systems.</p> <p>This option would require:</p> <ul style="list-style-type: none"> <li>• A central application connected to multiple databases;</li> <li>• The integration of an additional application layer for all the systems to be connected in all the 26 MS.</li> </ul>
Implementation complexity	<p>--: the impact on the technical complexity would be significantly negative.</p> <p>The Ma<sup>3</sup>tch technology applied to a high number of different national systems would pose significant challenges. An integration and impact assessment would have to be carried out for each of the systems involved, taking time and resources.</p>
Cost	<p>--: the impact on cost would be significantly negative.</p> <p>The integration of the Ma<sup>3</sup>tch technology would add a significant overhead in terms of costs. Moreover, the national systems might have to be upgraded in order to cope with the additional workload, hence additional investments might be required.</p>
Privacy and data protection	<p>+: the impact on the protection of personal data would be positive.</p> <p>The Ma<sup>3</sup>tch technology would allow avoiding redundancy of data, while still allowing to perform queries and to search databases. Personal information would not be shared, only their hash.</p> <p>It is worth to note, however, that the legal basis of the national systems might not allow such connection.</p>
Performance and availability	<p>--: the impact on the performances and availability would be significantly negative.</p> <p>The performances of the traveller application processor would be dependent on the performances of a number of national systems, whose SLA and availability requirements might differ from the ones identified for ETIAS.</p> <p>National systems would not be able to handle the additional workload without specific investment to upgrade the capacity to cope with the additional millions of queries that ETIAS would launch each year.</p>

### **Conclusion for the traveller application processor**

The screening rules seem to be the best way to exploit the information and intelligence that Member States might have to counter terrorism or other serious crimes. In the absence of screening rules the system would have to query each Member State' national database(s). A direct connection to 30 different sets of Member States' systems would be impractical and overall not feasible, as emerged from a consultation with Member States' experts.

*Table 58: Assessment of the options for the traveller application processor*

	Option A: Centralised architecture	Option B: de-centralised architecture (Ma <sup>3</sup> tch)
Implementation complexity	<b>0</b>	<b>--</b>
Cost	<b>+</b>	<b>--</b>
Privacy and data protection	<b>0</b>	<b>+</b>
Performances and availability	<b>+</b>	<b>--</b>
	<b>Best option</b>	

## Architectural options for the website

	Option A: Central website without any content delivery network
Description	<p>The ETIAS website would be a single European website, able to provide the same experience to all the VE-TCN connecting to it.</p> <p>This website could be hosted by eu-LISA. The entire website infrastructure and capacity would be provided internally.</p> <p>The website would be hosted both in both operation centres of eu-LISA (Strasbourg, France and Sankt Johann im Pongau, Austria). Additional hosting sites could be considered as additional protection against DDoS attacks (e.g. within the DIGIT datacentre in Luxembourg).</p> <p>This option would require:</p> <ul style="list-style-type: none"> <li>• The creation of an application entry point for travellers in the form of a website available on the public Internet. Via the website travellers can perform their data entry for the application, consult the status of their application and initiate interactions regarding refused applications. This application entry point would need to communicate securely with the ETIAS IT application;</li> <li>• Support for all current browser and device combinations;</li> <li>• Large bandwidth available;</li> <li>• Easily scalable architecture.</li> </ul>
Implementation complexity	<p>+: the impact on technical complexity would be positive.</p> <p>This option would not transfer assets (e.g. traveller data) to an external player and systems. All the data and applications necessary for powering the ETIAS website would remain within eu-LISA. However, eu-LISA would have to deploy the infrastructure and connectivity to support a website that would be used by millions of people each year.</p>
Cost	<p> -: the impact on the cost is assessed as negative.</p> <p>eu-LISA would have to build the infrastructure for the ETIAS website sizing it to support possible traffic peaks, as opposed to scale capacity when needed using cloud based solutions. Purchasing the extra capacity on the market through specialised operators is estimated to cost less than to build it.</p>
Privacy and data protection	<p>+: the impact on the protection of personal data would be positive.</p> <p>By keeping everything within eu-LISA, the personal data would be exposed to a smaller attack surface. Moreover, there would be the guarantee that the data would not leave the EU territory, providing more certainties regarding the legal framework that would protect personal data to be stored in ETIAS.</p>
Performance and availability	<p> -: the impact on the performances and availability would be negative.</p> <p>The use of content delivery networks and specialised cloud solutions would give more assurance in terms of flexibility to respond to surges of requests or outages. eu-LISA could have to look for additional locations for the website, so to increase its redundancy and resilience against attacks.</p>

Option B: Central website supported by a content delivery network	
Description	<p>This option would still require for the same as option A. However, it would add the support of content delivery networks, to replicate the ETIAS website (or parts of it) closer to the final users.</p> <p>This option would require:</p> <ul style="list-style-type: none"> <li>• Similar to option A, the creation of an application entry point for travellers in the form of a website available on the public Internet. Via the website travellers can perform their data entry for the application, consult the status of their application and initiate interaction regarding refused applications. This application entry point would need to communicate security with the ETIAS IT application;</li> <li>• Large bandwidth available;</li> <li>• Establishing a partnership with a trusted provider of delivery networks;</li> <li>• Developing additional security measures to ensure that any data transferred or even transiting through external providers would be fully protected (both confidentiality and integrity).</li> </ul>
Implementation complexity	<p>-: the impact on the technical complexity is assessed as significantly negative.</p> <p>The development and implementation would have to consider an additional layer. Ensuring high standards of security could lead to specific development.</p>
Cost	<p>+ : the impact on the cost is assessed as positive.</p> <p>The use of external operators would avoid to have an oversized ETIAS website in eu-LISA (to be able to absorb peaks), and therefore yield cost savings.</p>
Privacy and data protection	<p>-: the impact on data protection would be negative.</p> <p>A careful assessment of the solutions on the market should include whether personal data would be accessible by the company providing the service and what would be the jurisdiction under which such company operates. The usage of end-to-end encryption could mitigate concerns regarding the confidentiality of the information provided by the traveller to ETIAS even if through a Content Delivery Network (CDN) of a private company.</p> <p>However, at this stage there are concerns regarding the compliance of such solutions with the European data protection framework as most of the solutions identified were operating under other jurisdictions, outside Europe.</p>
Performance and availability	<p>+ : the impact on the performance and availability would be positive.</p> <p>Content delivery network are built with the purpose of improving availability and performances. However, considering the type of content and data transmitted with the ETIAS website (mostly text and simple web pages), the gains are likely to be limited.</p>

**Conclusion for the website**

In light of the data protection obligations to which ETIAS would be subject to, the option to build the entire capacity in house, seems to be the preferred choice. However, a more in-depth assessment should be carried out once the final specification will be available, especially to assess accurately the costs of building the required capacity vs. using an external operator.

If sufficient safeguards could be deployed to ensure confidentiality of the data, content delivery networks and cloud solutions should then be re-considered as they provide cost savings (purchasing this service from the market is generally cheaper than building the capacity in house) as well as better performances.

*Table 59: Assessment of the options for the webservice*

	Option A: Central website without any content delivery network	Option B: Central website supported by a content delivery network
Implementation complexity	+	-
Cost	-	+
Privacy and data protection	++	-
Performances and availability	-	+
	<b>Best option</b>	

## Annex 7. – User interactions

### Interacting with travellers

The present annex aims at giving statistical information on end-users in order to better grasp their specificities and requirements (languages, size of the country and Internet penetration rate). The following table gives an overview of the languages that are the most spoken in the current visa-exempt countries<sup>231</sup>:

*Figure 32: Top 11 most spoken languages in the visa-exempt countries*

<b>Top 11 languages</b>	<b>Volume</b>
English	393,149,301
Spanish	358,803,804
Portuguese	210,779,165
Japanese	126,323,715
Korean	50,503,933
Malay	31,180,476
Mandarin	29,092,106
Serbian	9,438,806
Arabic	9,266,971
Hebrew	8,192,463
Cantonese	7,943,374
<b>Total</b>	<b>1,234,674,114</b>
<b>Total different alphabet</b>	<b>271,941,844</b>
<b>Total latin alphabet</b>	<b>962,732,270</b>

---

<sup>231</sup> For these tables the “main language” per country is understood as the major language spoken and/or the official language of the country.



The following table shows the main language spoken in each visa-exempt country.

Table 60: Main language spoken in the visa-exempt countries<sup>232</sup>

VE country	Population	Main language	EU language
United States of America	324,118,787	English	Yes
Brazil	209,567,920	Portuguese	Yes
Mexico	128,632,004	Spanish	Yes
Japan	126,323,715	Japanese	No
South Korea	50,503,933	Korean	No
Colombia	48,654,392	Spanish	Yes
Argentina	43,847,277	Spanish	Yes
Canada	36,286,378	English	Yes
Peru	31,774,225	Spanish	Yes
Venezuela	31,518,855	Spanish	Yes
Malaysia	30,751,602	Malay	No
Australia	24,309,330	English	Yes
Taiwan	23,395,600	Mandarin	No
Chile	18,131,850	Spanish	Yes
Guatemala	16,672,956	Spanish	Yes
the United Arab Emirates	9,266,971	Arabic	No
Serbia	8,812,705	Serbian	No
Israel	8,192,463	Hebrew	No
Honduras	8,189,501	Spanish	Yes
Hong Kong	7,346,248	Cantonese	No
Paraguay	6,725,430	Spanish	Yes
Nicaragua	6,150,035	Spanish	Yes
Salvador	6,146,419	Spanish	Yes
Singapore	5,696,506	Mandarin	No
Costa Rica	4,857,218	Spanish	Yes
New Zealand	4,565,185	English	Yes
Republic of Moldova	4,062,862	Moldovan (Romanian)	Yes
Panama	3,990,406	Spanish	Yes
Bosnia and Herzegovina	3,802,134	Bosnian	No
Uruguay	3,444,071	Spanish	Yes
Albania	2,903,700	Albanian	No
former Yugoslav Republic of Macedonia	2,081,012	Macedonian	No
Trinidad and Tobago	1,364,973	English	Yes
Mauritius	1,277,459	Creole	No
Timor-Leste	1,211,245	Portuguese	Yes
Montenegro	626,101	Serbian	No

<sup>232</sup> PwC elaboration, from the CIA factbook, available at: <https://www.cia.gov/library/publications/the-world-factbook/fields/2098.html> (accessed 07/2016).

<b>VE country</b>	<b>Population</b>	<b>Main language</b>	<b>EU language</b>
Macao	597,126	Cantonese	No
Solomon Islands	594,934	English	Yes
Brunei Darussalam	428,874	Malay	No
Bahamas	392,718	English	Yes
Barbados	285,006	English	Yes
Vanuatu	270,470	English	Yes
Samoa	194,523	Polynesian	No
Saint Lucia	186,383	English	Yes
Kiribati	114,405	English	Yes
Saint Vincent and the Grenadines	109,644	English	Yes
Grenada	107,327	English	Yes
Tonga	106,915	English	Yes
Micronesia	104,966	English	Yes
Seychelles	97,026	Creole	No
Antigua and Barbuda	92,738	English	Yes
Dominica	73,016	English	Yes
Andorra	69,165	Spanish	Yes
Saint Kitts and Nevis	56,183	English	Yes
Marshall Islands	53,069	Marshallese	No
Monaco	37,863	French	Yes
San Marino	31,950	Italian	Yes
Palau	21,501	Palauan	No
Nauru	10,263	Nauruan	No
Tuvalu	9,943	English	Yes
Holy See	801	Italian	Yes

<b>Total population</b>	<b>1,249,248,277</b>
-------------------------	----------------------

The following table illustrates the average percentage of Internet users and mobile users in visa-exempt countries compared to the average in the European Union:

*Table 61: Internet users in the visa-exempt countries*

VE country	Population	Internet users	Mobile cellular subscriptions	Weighted on population
Albania	2,903,700	60.1%	106%	0.23%
Andorra	69,165	95.9%	88%	0.01%
Antigua and Barbuda	92,738	64.0%	137%	0.01%
Argentina	43,847,277	64.7%	144%	3.51%
Australia	24,309,330	84.6%	133%	1.95%
Bahamas	392,718	76.9%	80%	0.03%
Barbados	285,006	76.7%	116%	0.02%
Bosnia and Herzegovina	3,802,134	60.8%	90%	0.30%
Brazil	209,567,920	57.6%	127%	16.78%
Brunei Darussalam	428,874	68.8%	108%	0.03%
Canada	36,286,378	87.1%	82%	2.90%
Chile	18,131,850	72.3%	129%	1.45%
Colombia	48,654,392	52.6%	116%	3.89%
Costa Rica	4,857,218	49.4%	151%	0.39%
Dominica	73,016	62.9%	106%	0.01%
EastTimor	1,211,245	1.1%	117%	0.10%
FY Republic of Macedonia	2,081,012	68.1%	105%	0.17%
Grenada	107,327	37.4%	112%	0.01%
Guatemala	16,672,956	23.4%	111%	1.33%
Honduras	8,189,501	19.1%	96%	0.66%
Hong Kong	7,346,248	74.6%	229%	0.59%
Israel	8,192,463	71.5%	133%	0.66%
Japan	126,323,715	90.6%	125%	10.11%
Kiribati	114,405	12.3%	39%	0.01%
Macao	597,126	69.8%	324%	0.05%
Malaysia	30,751,602	67.5%	144%	2.46%
Marshall Islands	53,069	16.8%	29%	0.00%
Mauritius	1,277,459	41.4%	141%	0.10%
Mexico	128,632,004	44.4%	85%	10.30%
Micronesia	104,966	29.6%	n.a	0.01%
Monaco	37,863	92.4%	89%	0.00%
Montenegro	626,101	61.0%	162%	0.05%
Nauru	10,263	54.0%	n.a	0.00%
New Zealand	4,565,185	85.5%	122%	0.37%
Nicaragua	6,150,035	17.6%	116%	0.49%
Palau	21,501	39.2%	112%	0.00%
Panama	3,990,406	44.9%	174%	0.32%

VE country	Population	Internet users	Mobile cellular subscriptions	Weighted on population
Paraguay	6,725,430	43.0%	105%	0.54%
Peru	31,774,225	40.2%	110%	2.54%
Republic of Moldova	4,062,862	49.2%	108%	0.33%
Saint Kitts and Nevis	56,183	65.4%	132%	0.00%
Saint Lucia	186,383	51.0%	102%	0.01%
Saint Vincent & the Grenadines	109,644	56.5%	104%	0.01%
Salvador	6,146,419	29.7%	145%	0.49%
Samoa	194,523	21.2%	59%	0.02%
San Marino	31,950	50.8%	115%	0.00%
Serbia	8,812,705	66.2%	121%	0.71%
Seychelles	97,026	54.3%	158%	0.01%
Singapore	5,696,506	82.0%	146%	0.46%
Solomon Islands	594,934	9.0%	73%	0.05%
South Korea	50,503,933	92.1%	118%	4.04%
Taiwan	23,395,600	83.8%	n.a	1.87%
The Holy See	801	57.0%	n.a	0.00%
The United Arab Emirates	9,266,971	93.2%	187%	0.74%
The United States of America	324,118,787	87.4%	118%	25.95%
Tonga	106,915	40.0%	66%	0.01%
Trinidad and Tobago	1,364,973	65.1%	158%	0.11%
Tuvalu	9,943	39.6%	40%	0.00%
Uruguay	3,444,071	61.5%	160%	0.28%
Vanuatu	270,470	18.8%	66%	0.02%
Venezuela	31,518,855	57.0%	93%	2.52%

<b>Total population</b>	<b>1,249,248,277</b>		
<b>Average internet users rate</b>		<b>56%</b>	
<b>Weighted internet users rate</b>		<b>70%</b>	
<b>Average mobile users rate</b>			<b>119%</b>
<b>Weighted mobile users rate</b>			<b>116%</b>

<b>European Union</b>	<b>508,000,000</b>	<b>78.1%</b>	<b>123%</b>
-----------------------	--------------------	--------------	-------------

(PwC elaboration, source for the data: The World Bank, 2014/2015<sup>233</sup>)

<sup>233</sup> International Telecommunication Union, World Telecommunication/ICT Development Report and database and World Bank estimates. See: <http://data.worldbank.org/indicator/IT.NET.USER.P2> and <http://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2015&start=2015&view=map> (consulted 09/2016).

The following graphic shows the evolution of the global Internet penetration rate per region for the period 2009 – 2016<sup>234</sup>.

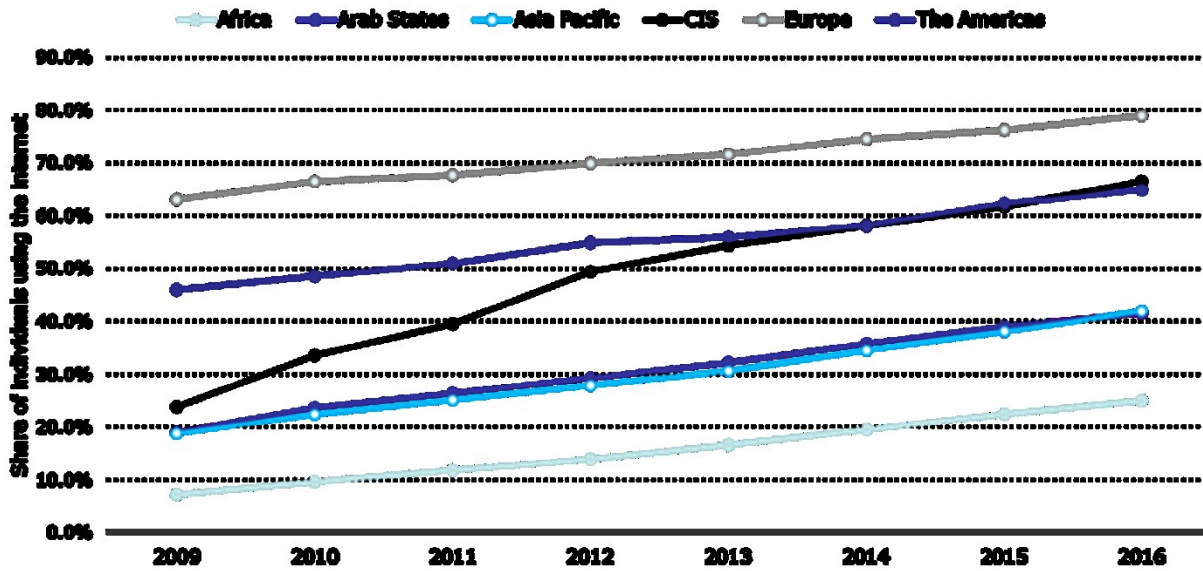


Figure 33: Evolution of the Internet penetration rate per region through time

The above table and figure show that both Internet penetration and mobile phone subscriptions rates are fairly high and are increasing in all visa-exempt countries. As mobile phone subscriptions rates are higher than Internet penetration rates, an ETIAS mobile application could counter the issue of access to technology.

### Data collection method

The following table shows a possible formulation of the data fields collected by the proposed ETIAS website/mobile application:

Table 62: Data collection in the website/app

Data	Format	Option
<b>Biographical data</b>		
First name*	Write-in field	
Surname*	Write-in field	
Name at birth*	Write-in field	
Other name	Write-in field	"Are you known by any other name (e.g. alias, artistic or preferred name)"
Parents' first names	Write-in field	Only the first name of the father and the mother. Write "UNKOWN" if the information is non-applicable"
Date of birth*	Calendar	DD/MM/YYYY
Place of birth*	Write-in field	City of birth
Nationality*	Drop-down menu	61 VE countries
Additional nationalities	Drop-down menu	All countries
Gender	Drop-down menu	Male, female
<b>Passport data</b>		
Passport number*	Write-in field	

<sup>234</sup> Source: Statista (July 2016): <http://www.statista.com/statistics/265149/internet-penetration-rate-by-region> (accessed 08/2016).

Data	Format	Option
Country of issue*	Drop-down menu	61 VE countries
Expiry date*	Calendar	DD/MM/YYYY
<b>Contact details</b>		
Email address	Write-in field	System's feedback: confirmation email
Address (residence)	Write-in-field + drop-down menu for country	3 boxes of writing fields + all countries in the drop-down menu
Telephone number	Drop-down menu + write-in field	282 country codes + write-in field
<b>Background questions</b>		
Education and occupation information	Drop-down menu	<p>"What is your field of employment/occupation?"</p> <ul style="list-style-type: none"> <li>- Unemployed,</li> <li>- Student</li> <li>- Self-employed,</li> <li>- Handicraft,</li> <li>- Public servant,</li> <li>- ...</li> </ul> <p>What is your position?</p> <ul style="list-style-type: none"> <li>- Assistant,</li> <li>- Support,</li> <li>- Management,</li> <li>- ..."</li> </ul>
Convicted of a serious crime	Yes/No tick boxes + drop-down menu if "yes" + additional information or documentation requested by CMPE	<p>"Have you ever been arrested or convicted of any of the following offences:</p> <ul style="list-style-type: none"> <li>- ..."</li> </ul> <p>The list of offences would derive from either the ones contained in Europol's mandate, which are aligned with the criminal acts that would enable a European Arrest Warrant, or the ones listed in Annex II of the PNR Directive.</p>
Been recently present in a war zone	Yes/No tick boxes + drop-down menu if "yes" + additional information or documentation requested by CMPE	<p>"Have you been present in any of the following countries in the last five years?</p> <ul style="list-style-type: none"> <li>- Syria,</li> <li>- Libya,</li> <li>- Yemen,</li> <li>- Iraq,</li> <li>- Sudan,</li> <li>- Somalia.</li> </ul> <p>If yes, why:</p> <ul style="list-style-type: none"> <li>- Tourism/family visit,</li> <li>- Business,</li> <li>- Governmental duties,</li> <li>- Military service,</li> <li>- Journalism,</li> <li>- Humanitarian mission or NGO,</li> <li>- Academia or conference".</li> </ul>
Threat to public health: infectious disease	Yes/No tick boxes + drop-down menu if "yes" + additional information or documentation requested by CMPE	<p>"Do you currently have any of the following diseases:</p> <ul style="list-style-type: none"> <li>- Cholera</li> <li>- Diphtheria</li> <li>- Tuberculosis</li> <li>- Plague</li> <li>- Smallpox</li> <li>- Yellow fever</li> <li>- Viral haemorrhagic fever."</li> </ul>
<b>Disclaimers</b>		
Confirmation of the data	Yes/No tick-boxes	<p>Screenshot of the data inserted by the applicant.</p> <p>"Do you confirm this data is correct?"</p> <p>If "no": "would you like to update your data?" If "yes": back to the main page.</p>
Confirmation of the fulfilment of the entry conditions to the Schengen Area	Yes/No tick-boxes	<p>"Do you confirm you fulfil the requirements of entry in the Schengen Area?</p> <ul style="list-style-type: none"> <li>- I possess a valid passport;</li> <li>- I can justify the purpose of my intended stay</li> </ul>

Data	Format	Option
		and have sufficient means of subsistence; - I am not be subject to an alert for refusal of entry; - I am not considered as a threat to public policy, internal security, public health or the international relations of any Member State.

The fields marked with a "\*" are data available in the passport and would be marked with a sign "as written in the passport". Additional help would be provided for the write-in fields, detailing the data expected, the place to find the information in the passport (if applicable) and the guidance to insert special characters (see table below).

The data collection method and the way questions are asked have a direct impact on the applicant experience, data protection and on data accuracy/quality. They can also trigger more applications to be manually processed, depending on their level of detail. Indeed, if the criminal background questions were asked in general terms like in the eTA ("have you ever committed, been arrested for, been charged with or convicted of any criminal offence in any country/territory"), some applicants would tend to communicate any offences, criminal or administrative (e.g. driving-related ones), that are not relevant for the risk assessment. A list of offences in a drop-down menu would counter this problem.

Data collection for the write-in fields can bring many data quality issues, most of all if travellers use a different alphabet. ICAO offers a complete and detailed set of tables of recommended transliterations<sup>235</sup>. They show the most commonly used characters of the Latin, Cyrillic and Arabic languages and their corresponding transliterations. As ETIAS data collection would be in Latin characters, the inclusion of such tables in the website/app can be very useful to travellers using different alphabets.

The following picture shows which data could be collected automatically with a drop-down menu or any other automated option and which would need to be collected as write-in field. It illustrates that the system aims at being as automated as possible in terms of data collection. The more automated the data is collected, the more data quality the system will offer.

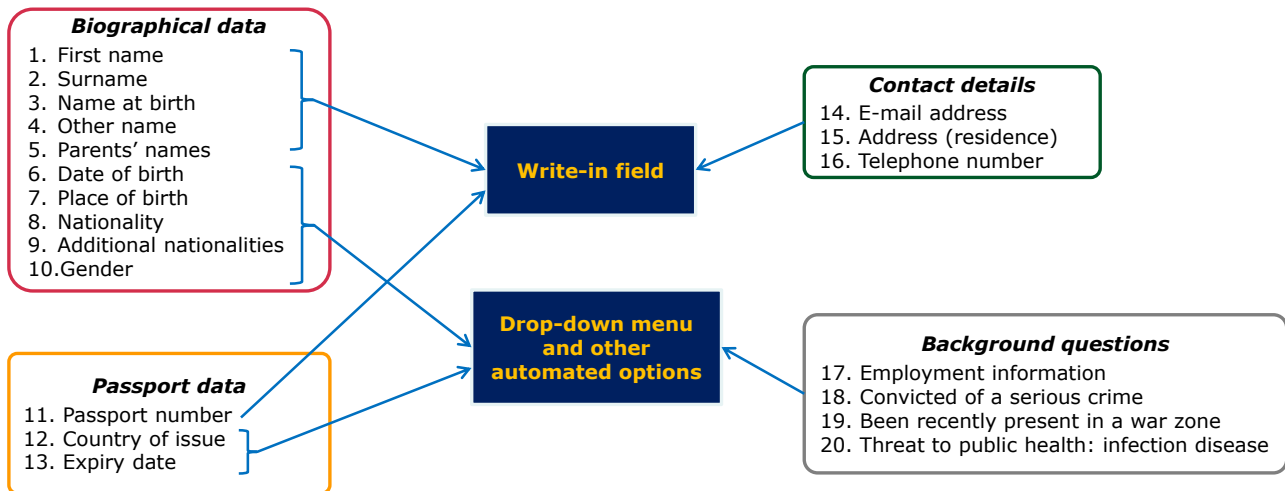


Figure 34: Data set and collection model of the website/app

<sup>235</sup> Available at: [http://www.icao.int/publications/Documents/9303\\_p3\\_cons\\_en.pdf](http://www.icao.int/publications/Documents/9303_p3_cons_en.pdf), p. 30 (accessed 10/2016).

## Interacting with carriers

The table below summarises the main legal requirements, current and future, carriers have to apply as regards verification of entry conditions and advance transmission of passenger information:

Legislation	Carrier	Responsibility
<b>Schengen Convention 1990</b>	Any type of carrier	<p>According to <i>Article 1</i>, a "carrier" means "any natural or legal person whose occupation it is to provide passenger transport by air, sea or land".</p> <p><i>Article 26:</i></p> <p>"1. (a) If aliens are refused entry into the territory of one of the contracting parties, the carrier, which brought them to the external border by air, sea or land, shall be obliged immediately to <b>assume responsibility</b> for them again. At the request of the border surveillance authorities the carrier shall be <b>obliged to return the aliens</b> to the third State from which they were transported or to the third State which issued the travel document on which they travelled or to any other third State to which they are certain to be admitted.</p> <p>(b) The carrier shall be obliged to take all the <b>necessary measures</b> to ensure that an alien carried by air or sea is in <b>possession of the travel documents</b> required for entry into the territories of the contracting parties.</p> <p>2. The contracting parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967, and in accordance with their constitutional law, to impose penalties on carriers which transport aliens who do not possess the necessary travel documents by air or sea from a third State to their territories.</p> <p>3. Paragraphs 1(b) and 2 shall also apply to international carriers transporting groups overland by coach, with the exception of local border traffic."</p>
<b>Directive supplementing the Schengen Convention (2001/51)</b>	Any type of carrier	<p><i>Article 2:</i></p> <p>"Member States shall take the necessary steps to ensure that the obligation of carriers to return third country nationals provided for in the provisions of Article 26(1)(a) of the Schengen Convention shall also apply when entry is refused to a third country national in transit if:</p> <p>(a) the carrier which was to take him to his country of destination refuses to take him on board;</p> <p>(b) or the authorities of the State of destination have refused him entry and have sent him back to the Member State through which he transited."</p> <p><i>Article 3:</i></p> <p>"Member States shall take the necessary measures to oblige carriers which are unable to effect the return of a third country national whose entry is refused to find means of onward transportation immediately and to bear the cost thereof, or, if immediate onward transportation is not possible, to assume responsibility for the costs of the stay and return of the third country national in question."</p> <p><i>Article 4:</i></p> <p>"1. Member States shall take the necessary measures to ensure that the penalties applicable to carriers under the provisions of Article 26(2) and (3) of the Schengen Convention are dissuasive, effective and proportionate and that:</p> <p>(a) either the maximum amount of the applicable financial penalties is not less than EUR 5,000 or equivalent national currency at the rate of exchange published in the Official Journal on 10 August 2001, for each person carried,</p>



Legislation	Carrier	Responsibility
		<p>or            (b) the minimum amount of these penalties is not less than EUR 3,000 or equivalent national currency at the rate of exchange published in the Official Journal on 10 August 2001, for each person carried, or            (c) the maximum amount of the penalty imposed as a lump sum for each infringement is not less than EUR 500,000 or equivalent national currency at the rate of exchange published in the Official Journal on 10 August 2001, irrespective of the number of persons carried.</p> <p>2. Paragraph 1 is without prejudice to Member States' obligations in cases where a third country national seeks international protection."</p> <p><i>Article 5:</i></p> <p>"This Directive shall not prevent Member States from adopting or retaining, for carriers which do not comply with the obligations arising from the provisions of Article 26(2) and (3) of the Schengen Convention and of Article 2 of this Directive, other measures involving penalties of another kind, such as immobilisation, seizure and confiscation of the means of transport, or temporary suspension or withdrawal of the operating licence".</p> <p><i>Article 6:</i></p> <p>"Member States shall ensure that their laws, regulations and administrative provisions stipulate that carriers against which proceedings are brought with a view to imposing penalties have effective rights of defence and appeal."</p>
<b>API Directive (2004/82)</b>	Air carriers	<p><i>Article 4:</i></p> <p>"1. Member States shall take the necessary measures to impose sanctions on carriers which, as a result of fault, have not transmitted data or have transmitted incomplete or false data. Member States shall take the necessary measures to ensure that sanctions are dissuasive, effective and proportionate and that either:</p> <p>(a) the maximum amount of such sanctions is not less than EUR 5,000, or than the equivalent national currency at the rate of exchange published in the <i>Official Journal of the European Union</i> on the day on which this Directive enters into force for each journey for which passenger data were not communicated or were communicated incorrectly; or</p> <p>(b) the minimum amount of such sanctions is not less than EUR 3,000, or than the equivalent national currency at the rate of exchange published in the <i>Official Journal of the European Union</i> on the day on which this Directive enters into force for each journey for which passenger data were not communicated or were communicated incorrectly.</p> <p>2. This Directive shall not prevent Member States from adopting or retaining, for carriers which infringe very seriously the obligations arising from the provisions of this Directive, other sanctions, such as immobilisation, seizure and confiscation of the means of transport, or temporary suspension or withdrawal of the operating licence."</p>
<b>PNR Directive (2016/681)</b>	Air carriers	<p><i>Article 8:</i></p> <p>"1. Member States shall adopt the necessary measures to ensure that air carriers transfer, by the 'push method', the PNR data listed in Annex I, to the extent that they have already collected such data in the normal course of their business, to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where an extra-EU flight has one or</p>

Legislation	Carrier	Responsibility
		<p>more stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to the PIUs of all the Member States concerned. This also applies where an intra-EU flight has one or more stopovers at the airports of different Member States, but only in relation to Member States which are collecting PNR data from intra-EU flights.</p> <p>2. In the event that the air carriers have collected any advance passenger information (API) data listed under item 18 of Annex I but do not retain those data by the same technical means as for other PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer, by the 'push method', those data to the PIU of the Member States referred to in paragraph 1. In the event of such a transfer, all the provisions of this Directive shall apply in relation to those API data.</p> <p>3. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the examination procedure referred to in Article 17(2) or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:</p> <p>(a) 24 to 48 hours before the scheduled flight departure time; and  (b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.</p> <p>4. Member States shall permit air carriers to limit the transfer referred to in point (b) of paragraph 3 to updates of the transfers referred to in point (a) of that paragraph.</p> <p>5. Where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, air carriers shall, on a case by case basis, transfer PNR data at other points in time than those mentioned in paragraph 3, upon request from a PIU in accordance with national law."</p> <p><i>Article 14:</i></p> <p>"Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. In particular, Member States shall lay down rules on penalties, including financial penalties, against air carriers which do not transmit data as provided for in Article 8 or do not do so in the required format."</p>
<b>EES Proposal (under discussion)</b>	Any type of carrier	<p><i>Article 12:</i></p> <p>"2. Carriers may use the secure internet access to the web service referred to in paragraph 1 to verify whether or not third country nationals holding a single or double entry visa have already used the visa. The carrier shall provide the data listed in Article 14(1)(d). The web service shall on that basis provide the carriers with an OK/NOT OK answer. Carriers may store the information sent and the answer received."</p> <p>As stamping would be abolished, the web service would be the only channel available to verify whether a single entry visa was consumed or not.</p>

## Annex 8. – System security

This annex introduces the risk management standard (ISO 31000) used for the risk assessment. Then it describes the different threats, actors and elaborates on the ETIAS risk scenarios along with the mapped safeguards.

### Risk Assessment as per ISO 31000

The traveller risk assessment has been performed following the ISO 31000 standard for risk management. In this standard, risk assessment is composed of three steps (risk identification, risk analysis and risk evaluation), while it is preceded by “establishing the context”, and succeeded by “risk treatment”, as depicted the following figure. The focus has been put on risk assessment, making an implicit use of the context. As the system is not yet designed, build or operated, the risk treatment has not been addressed.

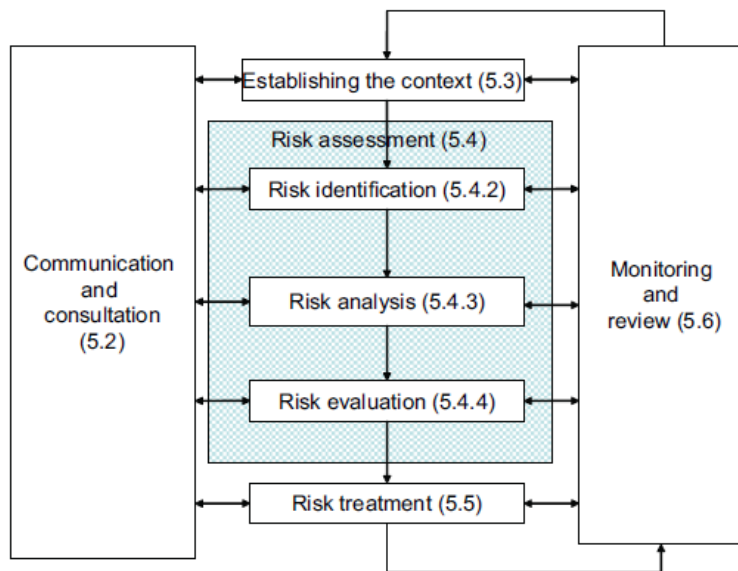


Figure 35: Risk management framework ISO 31000 overview

### Risk identification as per ISO 31000

The standard recommends identifying the sources of risk, the areas of impact, the events (including changes in circumstances), their causes and their potential consequences. The aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of the objectives. It is important to identify the risks associated with not pursuing an opportunity.

Comprehensive identification is critical, as any risks not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under the control of the organisation, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects.

It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider all possible causes and scenarios that show what consequences can occur.

## Risk analysis as per ISO 31000

As per ISO 31000:2009, section 5.4.3:

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.

The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling should be stated and can be highlighted. Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impact. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

## Risk evaluation as per ISO 31000

As per ISO 31000:2009, section 5.4.4:

The purpose of a risk evaluation is to assist in making decisions, based on the outcomes of the risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organisation that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

## ETIAS Risk assessment

The ETIAS risk assessment elaborates on the different risks scenarios and describes the practical impact to the different stakeholders, such as VE-TCN, Member States and border guards. As per ISO 31000, the focus is centred on:

- Identification of sources of risk, areas of impact, events (including changes in circumstances) and their causes and their potential consequences;
- The generation of a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

This risk assessment will follow the following steps:

- Elaboration of a list of risk scenarios based on the risk categories of the preceding step, and taking into account the already available information with regard to specifications (Regulation 36/2010);
- List of the possible safeguards:
  - From the Technical Specifications that have a security contribution;
  - Addition of further security safeguards;
- Evaluation of whether all possible risk scenarios are addressed by at least one safeguard.

### **Process/associations**

The risk assessment takes into consideration the different (business) processes and associations among all the ETIAS stakeholders and components.

### **Assets**

ETIAS represents the combination of ETIAS applications, components and electronically available data that is exchanged and processed along the system components and stored in internal and external databases. These process and exchanges of ETIAS data among the different stakeholders and ETIAS components are illustrated in the secure part in Figure 26: "ETIAS information flow overview".

### **Threats**

Threat agents describe concrete actors that have the capability to perform activities intended to negatively impact ETIAS services and its supporting organisation. The latter are referred to as the assets at stake. Threat agents can belong to one or more threat groups with different motivational goals, impact targets, capabilities and resources. The different threat groups along with the respective description and motivation are summarised in the following table.

Table 63: Threat group overview

Threat Group	Description	Type	Resources
<b>Nation State</b>	Espionage and cyber warfare by foreign States; victims include government agencies, infrastructure, energy, and IP-rich organisations.	Adversarial	High
<b>Organised crime</b>	Theft of financial or personally identifiable information (sometimes with the collusion of insiders). This includes, terrorists (novel) disruption and cyber warfare on government agencies, infrastructure and energy.	Adversarial	High
<b>Hacktivists</b>	Service disruptions or reputational damage; victims include high-profile organisations and government.	Adversarial	Moderate
<b>Insiders</b>	Not only the employees but also trusted partners or suppliers and subcontractors with access to sensitive data who are not directly under the organisation's control.	Adversarial /Accidental	Moderate

The threat strength is thus an association between the threat agent and the threat group, as the differences of capabilities and resources available directly impacts the success of the threat. The table below illustrates the threat strength of different threat agent – group associations.

Table 64: Threat type, threat agent and impact overview

Threat Agent	Threat Group	Threat Strength
Hacker	Nation State	High
Hacker	Organised crime	High
Privileged employee	Nation State	High
Privileged employee	Organised crime	High
Supplier/vendor/partner	Organised crime	High
Privileged employee	Hackivist	High
General employee	Nation State	Moderate
Traveller	Organised crime	Moderate
Supplier/vendor/partner	Hackivist	Moderate
Hacker	Hackivist	Moderate
General employee	Organised crime	Moderate
Privileged employee	Hackivist	Moderate
General employee	Hackivist	Moderate
General employee	Insider	Low
Traveller	Hackivist	Low
Natural disaster	Accidental	Low

## Risk scenarios

Risk scenarios describe the negative activities potentially performed by threat agents. For each risk scenario, probability and impact needs to be evaluated. In the present security risk analysis, impact is classified in two dimensions. The first dimension is the type of negative effect, distinguishing between confidentiality, integrity, availability and privacy (CIAP). The second dimension is the party that undergoes this negative effect, distinguishing between traveller, border guard, and competent authorities<sup>236</sup>.

The present analysis is part of a feasibility study, meaning the system analysed is not in operation, has not been build, and has even not been formally designed. As a consequence the risk assessment focuses on potential impact rather than on probability. As ETIAS is not implemented and estimating probability is a function of how safeguards are implemented and operated, probability is left out of the current risk equation. It is assumed that the safeguards are correctly implemented following the good security practises to create a risk impact hypothesis. Risk scenarios also considered the privacy impact (dimension 1). With regard to the risk categories to the different stakeholders in ETIAS, the four categories of impact (dimension 1) can be considered as depicted in the following table along with the impact per category.

*Table 65: Risk impact dimension 1 - CIAP*

Dimension 1	Description	Impact
<b>Confidentiality</b>	Confidentiality category includes risks of disclosure of any information that is stored, processed and transferred in ETIAS, such as traveller's sensitive information (e.g., personal identifiable information, travel details and payment information) to unauthorised entities or processes.	High
<b>Integrity</b>	Integrity includes risks associated to possible modification or deletion any information that is stored, processed and transferred in ETIAS, such as traveller's sensitive information (e.g., personal identifiable information, travel details and payment information) to in an unauthorised and undetected way.	High
<b>Availability</b>	Availability includes risks of lack or block of the accessibility and use of information within ETIAS by authorised entities (VE-TCN, EU agencies, Member States, and border guard authorities).	Moderate
<b>Privacy</b>	Privacy category embodies the risks to access and disclosure of any personal identifiable information (PII) of travellers during process, storage and transfer in ETIAS by unwanted entities.	Moderate

The risk scenarios elaborated for the different categories consider the ETIAS architecture details and processes, and the impact per stakeholder is summarised in the following table.

<sup>236</sup> The competent authorities denomination considers the stakeholder's group composed by any EU agency and Member State authorities that connect and operate ETIAS.

Table 66: Risk impact dimension 2 – impact on ETIAS stakeholders

Stakeholder	Practical impact	Description
<b>VE-TCN</b>	Extra application workload	VE-TCN required to perform manual processes, extra verifications, and interviews to verify his/her application. This could represent an extra visit to the MS embassy or consulate
	Fundamental rights	Leakage, tampering and deletion of sensitive travel and personal information, such as credit card information, date of birth and other personal identifiable information
	Financial/economic	Stolen/lost payment information leads to economic/financial impact to traveller
	Online fraud	VE-TCN is lead to a fraudulent application
	Duration of border controls	Extra checks, verifications or delays that increase the time during border controls
	Incorrect outcome	VE-TCN incorrect assessment outcome possibly leading to refusal of entry at the border
	Identity theft	Counterfeit/stolen identity may block traveller or mislead traveller with criminal behaviour. This also leads to financial/economic impact
	Inability to perform or access application	VE-TCN is unable to access ETIAS and perform, update and verify the application status
	Legal/criminal	Legal or criminal implications to VE-TCN
<b>Competent authorities</b> (ETIAS, LISA, MS)	Extra workload	Requires a manual verification by the CMPE, additional interviews or verifications within Member States
	Incorrect decision	Granting of invalid or denial of valid application
	Loss of critical data	Disclosure, tamper of VE-TCN sensitive information, ETIAS screening rules, and additional information provided by MS for the application assessment
	Reputation	Reputation damage
<b>Border guards</b>	Extra workload	Requires an additional process of verification, such as interview or document evaluation.
	Incorrect decision	Granting of invalid or denial of valid application
	Inability to access EES and ETIAS	Inability to connect and access VE-TCN information available on EES and ETIAS, leading to extra workload and possible incorrect decision
	Reputation	Reputation damage

The next figure illustrates the threat group and impact summary on the different actors, whereas the full set of risk scenarios is presented in the following table. The aggregated risk impact included in the rightmost column is based on a combination of both risk impact dimensions and worst-case hypothesis.



## Threat Groups



## Adversarial Actions

### VETCN

- Extra application workload
- Fundamental Rights (tamper/leakage of PII)
- Identity theft
- Online fraud (fraudulent application)
- Financial/economic (payment information)
- Inability to perform application

## Impact

### Competent authorities

- Extra workload (interviews, verifications)
- Disclosure/tamper of screening rules
- Leakage of Member States legal data
- Incorrect decision
- Loss of reputation

### Border Control authorities

- Extra workload (interviews, verifications)
- Incorrect decision
- Inability to access EES and ETIAS
- Loss of reputation

Figure 36: Overview of the threat along with possible implications on different actors

Table 67: ETIAS risk scenarios.

Risk ID	Threat Agent	Threat Group	Threat Strength	Risk Scenarios	Risk Scenarios Description	ETIAS Assets	Impact dimensions 1 and 2	Aggregated Risk Impact
RS 01a	Hacker	Nation State	High	Information Disclosure	The threat agent obtains access to sensitive information of travellers in the ETIAS Central System, exploring the access control policies misuse, cryptographic flaws such as key misuse (private or secret key exposed by travellers) or software bugs and vulnerabilities.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage of PII</li> <li>Consequential identity theft</li> </ul> <p><u>Confidentiality: High</u></p> <p><u>Privacy: Moderate</u></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Disclosure of screening rules and Member States additional legal and decisional information</li> <li>Handle formal legal complaints</li> <li>Loss of reputation</li> </ul> <p><u>Confidentiality: High</u></p> <hr/> <p><b>Border guards: Low</b></p> <ul style="list-style-type: none"> <li>Extra workload to handle complaints, and to perform additional verifications</li> </ul>	High
RS 01b	Hacker	Organised crime	High	Information Disclosure	The threat agent obtains access to traveller information by exploring access control misuse, cryptographic flaws such as key and password misuse exposed by the travellers at the ETIAS web service and interface, with the objective to sell data or identity information.	ETIAS Web Server Payment interface	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage of PII</li> <li>Subsequent financial/economic loss by misuse of payment information</li> <li>Consequential identity theft</li> </ul> <p><u>Confidentiality: High</u></p> <p><u>Privacy: Moderate</u></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Disclosure of screening rules and Member States additional legal and decisional information</li> <li>Handle formal legal complaints</li> <li>Loss of reputation</li> </ul> <p><u>Confidentiality: High</u></p>	High

RS 01c	Hacker	Hacktivist	<b>Moderate</b>	Information Disclosure	The threat agent obtains access to traveller information by exploring access control misuse, cryptographic flaws such as key and password misuse exposed by the travellers at the ETIAS Web service and interface.	ETIAS Web Server Payment system	<b>Border guards: Low</b> Extra workload to handle complaints, and to perform additional verifications	<b>Moderate</b>
			<b>VE-TCN: Moderate</b> • Violation of fundamental rights via leakage of PII <i>Confidentiality: Moderate</i> <i>Privacy: Moderate</i>					
			<b>Competent authorities: Moderate</b> • Extra workload to contain information leakage, to handle complaints, and to perform additional verifications <i>Confidentiality: Moderate</i>					
RS 02a	Hacker	Nation State / Organised crime	<b>High</b>	Eavesdrop	A nation state eavesdrops the communication between the different communication channels used by ETIAS to connect to the different components and between the traveller and ETIAS aiming to infer and spy on the VE-TCN applications. The threat agent can retrieve full or partial traveller application information, traveller credentials, and ETIAS screening rules.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<b>Border guards: Low</b> Extra workload to handle complaints, and to perform additional verifications	<b>High</b>
			<b>VE-TCN: High</b> • Violation of fundamental rights via leakage of PII <i>Confidentiality: High</i> <i>Privacy: Moderate</i>					
			<b>Competent authorities: High</b> • Extra workload to contain information leakage, to handle complaints, and to perform additional verifications • Disclosure of screening rules and Member States additional legal and decisional information <i>Confidentiality: High</i>					
RS 02b	Privileged employee	Organised crime	<b>High</b>	Eavesdrop	A privileged employee launches a malicious or network sniffing software to listen the communication between different ETIAS components, in order to retrieve full or partially VE-TCN application information, steal payment information or	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD,	<b>Border guards: Low</b> Extra workload to handle complaints, and to perform additional verifications	<b>High</b>
			<b>VE-TCN: High</b> • Violation of fundamental rights via leakage of PII • Subsequent financial/economic loss by misuse of payment information <i>Confidentiality: High</i> <i>Privacy: Moderate</i>					
			<b>Competent authorities: High</b> • Extra workload to contain information leakage, to handle complaints, and to perform additional verifications					

					credentials.	TDAWN)	<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Disclosure of screening rules and Member States additional legal and decisional information</li> </ul> <p><i>Confidentiality: High</i></p>	
							<p><b>Border guards: Low</b></p> <p>Extra workload to handle complaints, and to perform additional verifications</p>	
RS 02c	Supplier/vendor/partner	Organised Crime	High	Eavesdrop	This threat agent uses installed software or hardware provided to ETIAS containing a malicious process to maliciously listen to the network communication between different ETIAS components. In this way the threat agent is allowed to retrieve full or partially VE-TCN application. This can also be malicious software on the VE-TCN device that listens the communication in order to steal payment information, or the traveller's credentials.	Any communication interface using supplier/vendor/partner products.	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage of PII</li> <li>Subsequent financial/economic loss by misuse of payment information</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Privacy: Moderate</i></p>	High
							<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Disclosure of screening rules and Member States additional legal and decisional information</li> </ul> <p><i>Confidentiality: High</i></p>	
							<p><b>Border guards: Low</b></p> <ul style="list-style-type: none"> <li>Extra workload to handle complaints, and to perform additional verifications</li> </ul>	
RS 03	Hacker	Any	High	Cryptographic Breach	The threat agent performs attacks to the confidentiality and integrity information and data exchanged relying on cryptography protocols: <ul style="list-style-type: none"> <li>Algorithm breach (the algorithm is broken, this applies to one-way functions, symmetrical and asymmetrical encryption algorithms);</li> <li>Key breach (the private or</li> </ul>	All environments of ETIAS that uses cryptography, with main impact on the ETIAS central system.	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage of PII</li> <li>Subsequent financial/economic loss by misuse of leaked or corrupted payment information</li> <li>Consequential identity theft</li> <li>Extra application workload</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>	High

					<p>secret key is exposed or weak);</p> <ul style="list-style-type: none"> <li>Key misuse (an authorised users uses a key for a non-authorised purpose);</li> <li>Protocol or scheme breach (the protocol - e.g. mutual authentication - or scheme - e.g. encryption or signature scheme - is broken).</li> </ul>		<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Incorrect decision due to tampered information</li> </ul> <p><i>Integrity: High</i></p>	
RS 04a	Hacker	Organised Crime	High	Re-routing	The threat agent reroutes the connection of VE-TCN applicants to a fraudulent ETIAS Web Interface or fraudulent payment interface due to lack of authentication. This provides travellers to follow an invalid application process, or the threat agent to perform man-in-the-middle attacks.	VE-TCN data ETIAS Web Server Payment interfaces	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage of PII</li> <li>Subsequent financial/economic loss by misuse of leaked or corrupted payment information</li> <li>Online fraud leading for incorrect travel authorisations with possible criminal consequences</li> <li>Subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>	High
							<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Incorrect decision due to tampered information</li> </ul> <p><i>Integrity: High</i></p>	

RS 04b	Privileged employee	Organised Crime	<b>High</b>	Re-routing	<p>The privileged employee changes configuration files or uses a malware that reroutes the ETIAS component connection to an adversarial component or channels due to the lack of authentication. This forces ETIAS, MS and the competent authorities to process an invalid process. This can also be at connection between EES and ETIAS, leading to a possible wrong outcome of the verification at the border. The privileged employee can also perform man-in-the-middle attacks among the different components.</p>	<p>VE-TCN data</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage of PII</li> <li>• Subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <hr/> <p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• Incorrect decision due to tampered information</li> </ul> <p><i>Integrity: High</i></p>	<b>High</b>
RS 05a	Hacker	Any	<b>High</b>	Third-party communication	<p>The threat agent performs unauthorised monitoring and/or modification of communications to third-party components, while exploring their existing vulnerabilities. This affects any interface with third-party components and web-services, such as:</p> <ul style="list-style-type: none"> <li>• External databases;</li> <li>• External payment providers; and</li> <li>• Travellers communications</li> </ul>	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)</p> <p>Payment services</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage and tamper of PII</li> <li>• Financial/economic loss by abuse and misuse of leaked or corrupted payment information</li> <li>• Online fraud leading for incorrect travel authorisations with possible criminal consequences</li> <li>• Subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Disclosure and tamper of the traveller information, and Member States additional legal and decisional information</li> <li>• Subsequent incorrect VE-TCN assessment and decision</li> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul>	<b>High</b>

							<p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Incorrect decision due to tampered information</li> </ul> <p><i>Integrity: High</i></p>	
RS 06a	Hacker / Privileged employee	Nation State / Organised crime	<b>High</b>	Software Bugs and Vulnerabilities	The threat agent is a high knowledgeable hacker that exploits coding bugs or design flaws (e.g. buffer overflows, improper validation of input) in ETIAS Web Interface in order to gain unauthorised access to the ETIAS Central system and alter the information available databases of ETIAS.	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage and tamper of PII</li> <li>Financial/economic loss by abuse and misuse of leaked or corrupted payment information</li> <li>Consequential identity theft</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>	<b>High</b>
							<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Incorrect decision due to tampered information</li> </ul> <p><i>Integrity: High</i></p>	
RS 06b	Privileged employee	Nation State / Organised crime	<b>High</b>	Software Bugs and Vulnerabilities	The threat agent is a privileged employee with access to the code and introduces coding bugs and flaws to be exploited or exploits existing ones (e.g. buffer overflows, improper validation of input) in ETIAS Web Interface and ETIAS Central system to allow or perform unauthorised alteration of information available databases of ETIAS.	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage and tamper of PII</li> <li>Financial/economic loss by abuse and misuse of leaked or corrupted payment information</li> <li>Consequential identity theft</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>	<b>High</b>

RS 06c	Hacker	Hacktivist		Software Bugs and Vulnerabilities	The threat agent exploits coding bugs or design flaws (e.g. buffer overflows, improper validation of input) in ETIAS Web Interface in order to gain unauthorised access to ETIAS Web Server or alter the traveller information in the masked extraction of the central database.	VE-TCN data ETIAS Web Server Payment services.	<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>• Subsequent incorrect VE-TCN assessment and decision</li> <li>• Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p>	
			<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Incorrect decision due to tampered information</li> </ul> <p><i>Integrity: High</i></p>					
			<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage and tamper of PII</li> <li>• Financial/economic loss by abuse and misuse of leaked or corrupted payment information</li> <li>• Consequential identity theft</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>					
			<p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>• Subsequent incorrect VE-TCN assessment and decision due to invalid data input from</li> <li>• Loss of reputation</li> </ul> <p><i>Confidentiality: Moderate</i></p> <p><i>Integrity: Moderate</i></p>					
							<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> </ul> <p><i>Integrity: Moderate</i></p>	



RS 07a	Hacker	Nation State	<b>High</b>	Authentication	The threat agent performs integrity and access control attacks, exploring authentication and communication vulnerabilities among different ETIAS components, travellers, and third-party services (payment providers, Member State interfaces, EES, SIS, VIS, SLTD, TDAWN). In this attack the threat agent could obtain unauthorised control (hijacks) of a pre-existing and legitimate network session between the ETIAS components, or between ETIAS and the travellers.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage and tamper of PII</li> <li>• Financial/economic loss by abuse and misuse of leaked or corrupted payment information</li> <li>• Consequential identity theft</li> </ul> <p><b>Confidentiality: High</b></p> <p><b>Integrity: High</b></p> <p><b>Privacy: Moderate</b></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>• Subsequent incorrect VE-TCN assessment and decision</li> <li>• Loss of reputation</li> </ul> <p><b>Confidentiality: High</b></p> <p><b>Integrity: High</b></p> <hr/> <p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Incorrect decision due to tampered information</li> </ul> <p><b>Integrity: High</b></p>	<b>High</b>
RS 07b	Hacker	Organised Crime	<b>High</b>	Authentication	The threat agent performs integrity and access control attacks, exploring authentication and communication vulnerabilities between VE-TCN and the ETIAS Web Interface and payment providers. In this attack the threat agent could obtain unauthorised control of a pre-existing VE-TCN session to tamper, learn and steal the application identity.	VE-TCN data ETIAS Web Server Payment system	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage of PII</li> <li>• Subsequent financial/economic loss by misuse of leaked or corrupted payment information</li> <li>• Consequential identity theft</li> </ul> <p><b>Confidentiality: High</b></p> <p><b>Integrity: High</b></p> <p><b>Privacy: Moderate</b></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><b>Integrity: High</b></p>	<b>High</b>

							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	
RS 07c	Privileged employee	Organised Crime / Nation State	High	Authentication	The privileged employee exploits internal authentication flaws by sniffing the internal network or communication between the components by hijacking an existing session to gain unauthorised access to the ETIAS Central system to alter information.	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)</p> <p>Payment system</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage of PII</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>• Subsequent incorrect VE-TCN assessment and decision</li> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <hr/> <p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• A case of misuse of sniffed credentials of a border guard by a perpetrator could lead to the lock-out of credentials and the inability of the border guard to access EES and/or ETIAS database to verify applications</li> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	High
RS 08a	Hacker	Organised Crime	High	Credentials Forgery	The threat agent forges or uses fraudulent credentials (copy, imitation) to gain unauthorised access to ETIAS. This attack allows the adversary to produce fake applications using stolen or invalid	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>Payment system</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights via leakage and tamper of PII</li> <li>• Consequent identity theft</li> </ul> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>	High

					information.		<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Integrity: High</i></p>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	
RS 08b	Privileged employee	Organised Crime	High	Credentials Forgery	The threat agent produces fraudulent credentials that allows unauthorised users to access to ETIAS or to VE-TCN. The privileged employee with access to the ETIAS central system can forge or create new fraudulent credentials to be used during the application to ETIAS. This affects the systems as well as the VE-TCN credentials (ETIAS login credentials, ETIAS application information, identification documents).	VE-TCN data ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage and tamper of PII</li> <li>Consequent identity theft</li> </ul> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p>	High
							<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Integrity: High</i></p>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	
RS 09a	Privileged employee	Organised Crime	High	Insider	The threat agent performs adversarial or accidental actions to delete, block access to information and tamper with an application at the ETIAS Central system (e.g. altering sensitive information, granting unauthorised travelling, denial of travelling, and steal and sell VE-TCN information). The threat agent is a privileged employee capable to access one or	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage and tamper of PII</li> <li>Financial/economic loss by abuse and misuse of leaked or corrupted payment information</li> <li>Incorrect travel authorisations with possible criminal consequences</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a</li> </ul>	High

					multiple ETIAS components responsible for the screening outcome, such as EU agency, a Member State authority and Border guards agency	<p>new or update an application <i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>• Block communication to external databases affecting screening decision</li> <li>• Subsequent incorrect VE-TCN assessment and decision</li> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <hr/> <p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• Inability to access EES and/or ETIAS database to verify application</li> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	
RS 09b	General employee	Hackivist	Moderate	Insider	The threat agent performs adversarial or accidental actions with limit privileges, such as block access to information and application data.	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Inability to access ETIAS to perform a new or update an application</li> <li>• Extra application workload and subsequent extra interviews and manual processing</li> </ul> <p><i>Availability: Moderate</i></p> <hr/> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>• Block communication to external databases affecting screening decision</li> <li>• Extra workload to handle complaints, and to perform manual verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p> <hr/> <p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>• Inability to access EES and/or ETIAS database to verify application</li> </ul>	Moderate

							<ul style="list-style-type: none"> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: Moderate</i></p>	
RS 10a	Hacker	Organised Crime	High	Network and Interface interactions	The threat agent performs network attacks tackling ETIAS Web Interface and Web Service communications with the payment server to learn, modify and tamper with the VE-TCN information, by using injections, malware, botnets, exploit kits and web application attacks at the VE-TCN side. These attacks deliberately make changes to compromise the integrity of travellers' information during application any of the ETIAS Web servers, by corrupting information.	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDawn)</p> <p>Payment system</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage and tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Integrity: High</i></p> <p><i>Privacy: Moderate</i></p> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>Block communication to external databases affecting screening decision</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	High
RS 10b	Privileged employee	Organised Crime	High	Network and Interface interactions	The threat agent performs attacks tackling ETIAS to learn, modify and tamper with ETIAS and VE-TCN information, such as injections, malware, botnets, exploit kits and web application attacks at the ETIAS Central System. These attacks deliberately make changes to compromise the integrity of ETIAS, by corrupting	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD, TDawn)</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Integrity: High</i></p>	High

					or deleting stored information in the databases or transferred between the different ETIAS components. This also creates risks to the communication between the front- and back-end of the ETIAS and external components, including payment interfaces, external database and any logical communication.	Payment system	<p><i>Availability: Moderate</i></p> <hr/> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>• Tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>• Block communication to external databases affecting screening decision</li> <li>• Subsequent incorrect VE-TCN assessment and decision</li> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <hr/> <p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>• Inability to access EES and/or ETIAS database to verify application</li> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Subsequent incorrect decision outcome</li> </ul> <p><i>Integrity: High</i></p>	
RS 10c	Hacker	Hackivist	Moderate	Network and Interface interactions	The threat agent performs network attacks tackling ETIAS Web Interface to learn, modify and tamper with the VE-TCN, such as injections, malware, botnets, exploit kits and web application attacks ETIAS Web Interface.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD; TDAWN) Payment system	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>• Violation of fundamental rights tamper of PII</li> <li>• Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>• Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <hr/> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>• Overload and block of ETIAS public interface and applications</li> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p>	High

								<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	
RS 11a	Hacker	Organised Crime	High	Denial Service of	The threat agent performs attacks tackling ETIAS availability, by exploring vulnerabilities to the ETIAS Web Service and user interface, through (D)DoS, injection, and network scans attacks. These attacks deliberately impair the availability and performance of the ETIAS Web Service and connections to the ETIAS components, by flooding with fraudulent application requests and exploring vulnerabilities in the ETIAS user interface and Web Service.	VE-TCN data ETIAS Web Server ETIAS Central System	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Privacy: Moderate</i></p> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Block communication to external databases and other ETIAS components, or overload and block of ETIAS public interface and applications</li> <li>Extra workload to hold the system performance, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p> <p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	Moderate	
RS 11b	Hacker	Hackivist	Moderate	Denial Service of	The threat agent performs attacks tackling ETIAS availability, by exploring vulnerabilities to the ETIAS Web Service and user interface, through (D)DoS, injection, and network scans. This attack deliberately impairs the availability and performance of the ETIAS Web Service by exploring vulnerabilities in the ETIAS user interface and Web Service.	VE-TCN data ETIAS Web Server	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Privacy: Moderate</i></p> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Overload and block of ETIAS public interface and applications,</li> <li>Extra workload to hold the system performance, to handle complaints, and</li> </ul>	Moderate	

							<ul style="list-style-type: none"> <li>to perform additional verifications</li> <li>Loss of reputation</li> </ul> <i>Availability: Moderate</i>	
							<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <i>Availability: Moderate</i>	
RS 12a	Hacker	Nation State	<b>High</b>	Malware	The threat agent explores the adversarial or accidental installation of malicious software at ETIAS Central System or on employee's computers through phishing scam or website downloads, such as malware, botnets, virus, Trojan horses and spyware. Such software is designed to deliberately listen and compromise the integrity and confidentiality of data in ETIAS storage or at an employee computer.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <i>Integrity: High</i> <i>Availability: Moderate</i>	<b>High</b>
							<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Disclosure and tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>Block communication to external databases and other ETIAS components, or overload and block of ETIAS public interface and applications</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to hold ETIAS availability and performance, information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <i>Confidentiality: High</i> <i>Integrity: High</i> <i>Availability: Moderate</i>	
							<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul>	



							<p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p>	
RS 12b	Hacker	Hackivist	Moderate	Malware	<p>This threat agent explores the adversarial or accidental installation of malicious software at the VE-TCN computer or at the payment server through phishing scam or website downloads, such as malware, botnets, virus, Trojan horses and spyware. Such software is designed to deliberately compromise the integrity and confidentiality of the application at the ETIAS Web interface and the ETIAS Web service.</p>	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>Payment system</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via leakage and tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Confidentiality: High</i></p> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Overload and block of ETIAS public interface and applications</li> <li>Extra workload to hold ETIAS availability and performance, information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p> <p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	Moderate
RS 13a	Supplier/ vendor/ partner	Organised Crime	High	Hardware malfunction, failure, or fraudulent	<p>The threat agent explores installed and supplied fraudulent hardware, such as document readers, ETIAS application reader and its integrity.</p> <ul style="list-style-type: none"> <li>Hardware counterfeiting (illegal imitations);</li> <li>Hardware forgery (illegal alteration);</li> <li>Hardware malfunction or failure of information system hardware (e.g. hard disk drives, memory, routers, or network switches);</li> </ul>	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD; TDAWN)</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Tamper of the traveller information,</li> </ul>	High

				<ul style="list-style-type: none"> <li>Hardware performance/efficiency.</li> </ul>		<p>screening rules and Member States additional legal and decisional information</p> <ul style="list-style-type: none"> <li>Block communication to external databases affecting screening decision, and other ETIAS components, or overload and block of ETIAS public interface and applications</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><b>Integrity: High</b></p> <p><b>Availability: Moderate</b></p>		
						<p><b>Border guards: High</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><b>Integrity: High</b></p> <p><b>Availability: Moderate</b></p>		
RS 13b	Privileged employee	Organised Crime	<b>High</b>	Hardware malfunction, failure, or fraudulent	This threat agent explores the risks of accidental or adversarial compromise of the used hardware at ETIAS infrastructure.	<p>VE-TCN data</p> <p>ETIAS Web Server</p> <p>ETIAS Central System</p> <p>ETIAS external databases (EES, SIS, VIS, SLTD; TDAWN)</p>	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><b>Integrity: High</b></p> <p><b>Availability: Moderate</b></p>	<b>High</b>
						<p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Tamper of the traveller information, screening rules and Member States additional legal and decisional information</li> <li>Block communication to external databases affecting screening decision, and other ETIAS components, or overload and block of ETIAS public interface and applications</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul>		

							<p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p>	
							<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	
RS 13c	General employee	Hacktivist	Moderate	Hardware malfunction, failure, or fraudulent	This threat agent explores the risks of accidental or adversarial compromise of the used hardware, such as document readers, ETIAS application reader and its integrity.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD; TDAWN)	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Availability: Moderate</i></p>	Moderate
							<p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Deletion and block to VE-TCN information, screening rules and Member States additional legal and decisional information</li> <li>Block communication to external databases affecting screening decision, and other ETIAS components, or overload and block of ETIAS public interface and applications</li> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p>	
							<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	
RS 14a	Hacker	Nation State	High	Traffic analysis	The threat agent performs passive observations (full or partial of two or more dedicated components) by attackers to information exchanges and calls to the ETIAS	VE-TCN data ETIAS Web Server ETIAS Central System	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via travelling information leakage</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications</li> </ul>	Moderate

					system by travellers, to derive inferences regarding sensitive information, such as destination, frequency and number of traveller applicants.	ETIAS external databases (EES, SIS, VIS, SLTD; TDAWN)	<p>with possible incorrect outcome <i>Privacy: Moderate</i></p> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Infer of screening rules and Member States additional legal and decisional information</li> <li>Extra workload to contain information leakage, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Privacy: Moderate</i></p> <p><b>Border guards: Low</b></p>	
RS 14b	General employee	Organised Crime	Moderate	Traffic analysis	The threat agent performs passive observations of the information exchanges and calls to the ETIAS Central system to another component by a general employee, to derive inferences regarding sensitive information, such as destination, frequency and number of traveller applicants.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via travelling information leakage</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> </ul> <p><i>Privacy: Moderate</i></p> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Privacy: Moderate</i></p> <p><b>Border guards: Low</b></p>	Moderate
RS 15a	Hacker	Hackivist	Moderate	Abuse	The threat agent explores and abuses the functionalities at the front-end interface of ETIAS exposing lack of validation issues, so that ETIAS Web Service is overloaded limiting bandwidth and availability of ETIAS and force tampered and invalid information.	VE-TCN data ETIAS Web Server ETIAS Central System ETIAS external databases (EES, SIS, VIS, SLTD, TDAWN)	<p><b>VE-TCN: High</b></p> <ul style="list-style-type: none"> <li>Violation of fundamental rights via tamper of PII</li> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p> <p><b>Competent authorities: High</b></p> <ul style="list-style-type: none"> <li>Overload and block of ETIAS public interface and applications</li> </ul>	High

							<ul style="list-style-type: none"> <li>Subsequent incorrect VE-TCN assessment and decision</li> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Integrity: High</i></p> <p><i>Availability: Moderate</i></p>	
							<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	
RS 15b	Traveller	Hackivist	Low	Abuse	The threat agent explores and abuses the functionalities at the front-end interface of ETIAS exposing lack of validation issues, so that ETIAS Web Service is overloaded limiting bandwidth and availability of ETIAS.	VE-TCN data ETIAS Web Server	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Availability: Moderate</i></p>	Moderate
							<p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p>	
							<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>Inability to access EES and/or ETIAS database to verify application</li> <li>Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	
RS 16a	General employee	Hackivist	Moderate	Stress	This threat agent applies actions and conditions which cause delays, disruptions, or failures lead to deactivation (i.e. unavailability) of the application and verification ETIAS system.	VE-TCN data ETIAS Web Server ETIAS Central System	<p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Availability: Moderate</i></p>	Moderate

						<p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p>	
						<p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>• Inability to access EES and/or ETIAS database to verify application</li> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	
RS 16b	Natural Disaster	Accidental	Low	Stress	Unanticipated interactions associated to environmental stress caused by natural causes and disasters, which may lead to disruption and deactivation (i.e. unavailability) of the application and verification ETIAS system.	<p>VE-TCN data ETIAS Web Server ETIAS Central System</p> <p><b>VE-TCN: Moderate</b></p> <ul style="list-style-type: none"> <li>• Extra application workload, and subsequent increased duration at border crossing, requiring extra verifications with possible incorrect outcome</li> <li>• Inability to access ETIAS to perform a new or update an application</li> </ul> <p><i>Availability: Moderate</i></p> <p><b>Competent authorities: Moderate</b></p> <ul style="list-style-type: none"> <li>• Extra workload to contain information leakage, to handle complaints, and to perform additional verifications</li> <li>• Loss of reputation</li> </ul> <p><i>Availability: Moderate</i></p> <p><b>Border guards: Moderate</b></p> <ul style="list-style-type: none"> <li>• Inability to access EES and/or ETIAS database to verify application</li> <li>• Extra workload to handle incorrect authorisations and complaints, and to perform additional verifications</li> <li>• Subsequent incorrect decision outcome</li> </ul> <p><i>Availability: Moderate</i></p>	Moderate

## Safeguards

This part of the annex elaborates on the safeguards and how they mitigate the security risk scenarios previously described, by following the structure of the **ISO 27002:2013** clauses.

### **Introduction of safeguards**

The following table describes the 14 main safeguards covering all ISO 27002:2013 clauses to mitigate the threats from the different risk scenarios identified, along with the respective security controls to be implemented in order to mitigate the impacts in dimensions 1 and 2 (privacy impact and impacted party).

Table 68: Safeguards and associated controls

Safeguards identification	Safeguards description	Key implementation aspects of the proposed safeguards
<p><b>SG.01 Human Resources</b></p>	<p>Human Resources safeguards address the human factor:</p> <ul style="list-style-type: none"> <li>• Prior to employment;</li> <li>• During employment; and</li> <li>• At time of termination and change of employment.</li> </ul> <p>It includes the recruitment, training and management of all staff involved in ETIAS design, implementation and operation. This includes staff from the relevant competent authorities (CMPE, eu-LISA, MS) and border guards. All involved personnel should be educated about the risks related to information systems, and be trained on how to act, and which security controls to apply, in order to avert relevant threat events.</p>	<p>Human Resources security safeguards include the recruitment, management and training of staff within the competent authorities (CMPE, eu-LISA, MS) and border guard authorities. This includes:</p> <ul style="list-style-type: none"> <li>• Job descriptions and screening;</li> <li>• Continuous training and awareness;</li> <li>• Processes to manage used information;</li> <li>• Access privileges;</li> <li>• Legal confidentiality statements (NDA);</li> <li>• Security awareness training.</li> </ul>
<p><b>SG.02 Access Control</b></p>	<p>Access control safeguards address:</p> <ul style="list-style-type: none"> <li>• Business requirements of access control;</li> <li>• User access management and user responsibilities;</li> <li>• System and application access control.</li> </ul> <p>ETIAS assets should be identified, classified and monitored to then implement different levels of physical and logical access control among different ETIAS stakeholders to the information stored, transferred and processed within ETIAS.</p>	<p>Physical and logical access control should be implemented.</p> <p>Commission Decision of 29 October 2009 defines the access rights for license and certificate data when residing in the registers. ETIAS system should be aligned similarly, and should distinguish the following roles:</p> <ul style="list-style-type: none"> <li>• Competent authorities of all the involved Member States;</li> <li>• The ETIAS Responsible Agency (eu-LISA) ;</li> <li>• The ETIAS applicants themselves for their own information;</li> <li>• Investigation bodies (e.g. Europol).</li> </ul> <p>As such, the ETIAS logical access control should grant access to the applications, files and databases, as per the requirements of these different roles. This always requires asymmetrical authentication. This would be based on role attributes embedded in public key certificates.</p>
<p><b>SG.03 Cryptography</b></p>	<p>Cryptographic controls address the confidentiality and integrity of the ETIAS information assets, in accordance with the classification of that asset. Cryptographic controls should be in place for each component, particularly addressing entity and message authentication, as well as the protection of information in transfer/in storage.</p>	<p>The ETIAS controls should include cryptographic controls and key management mechanisms.</p> <p>Cryptographic means should be employed to protect the confidentiality and/or integrity of the ETIAS system and travellers information assets (PII), in accordance with the assessed classification of the information asset. Cryptography should exist for each technology component, for authentication, storage and transfer of information.</p> <p>Also, all cryptographic keys should be stored in trusted hardware. There should be individual keys or key pairs per actor. Each actor should be responsible for his keys or key pairs. Appropriate root key</p>



Safeguards identification	Safeguards description	Key implementation aspects of the proposed safeguards
		<p>certificates and all intermediate certificates required to validate a certificate should be stored on-card during the card issuance process.</p> <p>Public key certificates should be embedded in the trusted storage of each ETIAS component and external party under responsibility of their owners.</p> <p>The cryptographic algorithms and key sizes should follow the best practises and the ENISA guidelines.</p>
<p><b>SG.04 Communications Security</b></p>	<p>Communications security addresses network security management and the security of information transfers. ETIAS networks should be designed securely, and ETIAS communications and information (travellers' data and screening information) should be processed through secure communication channels. Appropriate mutual authentication protocols should be used to guarantee the authenticity of the different communicating authorities using ETIAS, and to protect the content of the communications. For instance, connections between VE-TCN and the ETIAS Web Server, as well as connections between ETIAS Central System components (e.g., ETIAS Web Server, ETIAS management and screening engine) and other systems (e.g. EES, SIS, VIS, SLTD, TDAWN and MS systems) should be encrypted. Consideration should be given to encrypting communication at the different layers of the networking stack (i.e. application, transport, and network level).</p>	<p>In particular, ETIAS networks should include security controls, network security design and operational practises, including:</p> <ul style="list-style-type: none"> <li>• Implement secure and authenticated connection support between VE-TCN environment (browser) and ETIAS (Web interface), such as TLS;</li> <li>• Separating sensitive/critical internal business systems and traffic from less sensitive and/or externally-accessible systems/networks using firewalls or equivalent;</li> <li>• Securing the perimeter of the network using firewalls or equivalent in such a fashion as to limit the exposure of applications and infrastructure to only those services that are required to be provided externally;</li> <li>• Using secure variants of critical services (i.e. DNSSEC instead of DNS and SFTP instead of FTP);</li> <li>• Implement malicious code and unauthorized software countermeasure processes;</li> <li>• Allow secure and controlled access through IPsec (Internal Protocol Security) or VPN connection among sensitive components (e.g. Interpol and Europol).</li> </ul>
<p><b>SG.05 System acquisition, development and maintenance</b></p>	<p>System acquisition, development and maintenance safeguards address security requirements of information systems, as well as security in development and support processes, and for test data. During acquisition, development and maintenance of ETIAS, a secure SDLC (software development lifecycle) should be followed. ETIAS software modules should be periodically reviewed and updated as required, and information systems periodically checked for compliance.</p>	<p>Security controls that should be included in standard development lifecycle are:</p> <ul style="list-style-type: none"> <li>• Disabling of unnecessary services;</li> <li>• Changing insecure default configurations;</li> <li>• Ensuring the latest system patches/security updates are in place;</li> <li>• Installation of malware protection software, host IPS, and other security software;</li> <li>• Securing the bios/boot loaders;</li> <li>• Secure software development review;</li> <li>• Full documentation and restriction of changes;</li> <li>• Protect applications and transactions.</li> </ul> <p>A formalised system development methodology (SDLC) should be</p>

Safeguards identification	Safeguards description	Key implementation aspects of the proposed safeguards
		implemented, and should incorporate information security throughout the process (e.g. requirements, design, testing, implementation, and privacy by design).
<b>SG.06 Information Security Incident Management</b>	Information security incident management addresses the management of information security incidents and improvements. A formalised incident management process should be established to identify, respond to, recover from, and follow-up security incidents. Intrusion detection or prevention system should be implemented in ETIAS key network points and at key information systems.	ETIAS should designate a security team responsible to implement the following controls: <ul style="list-style-type: none"> <li>• Monitor and report security weaknesses and events;</li> <li>• Assess and respond to security events;</li> <li>• Collect evidence and learn from the security event to reduce impact and likelihood of a future event.</li> </ul>
<b>SG.07 Operations Security</b>	Operations security addresses: <ul style="list-style-type: none"> <li>• Operational procedures and responsibilities;</li> <li>• Backup, as well as logging and monitoring;</li> <li>• Control of operational software;</li> <li>• Technical vulnerability management including protection from malware;</li> <li>• Information systems audit considerations.</li> </ul>	Security controls for operations security include: <ul style="list-style-type: none"> <li>• Document procedures of ETIAS architecture and processes;</li> <li>• Implement technical malware protection, vulnerability management and imply software installation restrictions in ETIAS;</li> <li>• Backup, log and monitor ETIAS data exchanges.</li> </ul>
<b>SG.08 Asset Management</b>	Asset management ensures the identification and classification of the ETIAS information assets. The ETIAS information assets should be identified, classified and tracked, so that they can be used and disposed of in accordance with their level of sensitivity/classification. This allows identifying/mapping the level of protection that each data processed, stored and transferred in ETIAS should have.	Controls should enforce that ETIAS data should not be exposed externally without a defined and approved requirement, and should be used in accordance with their classification and sensitivity. Data should be securely destroyed when no longer required. This includes: <ul style="list-style-type: none"> <li>• Hardware tamper resistance and hardware protection safeguards (sensors and alarms, memory content protection, bus protection);</li> <li>• Application (web and mobile) security safeguards to protect the integrity and the process of information;</li> <li>• Database security connections;</li> <li>• Data protection safeguards;</li> <li>• Access control rules and policies.</li> </ul>
<b>SG.09 Physical and Environmental Security</b>	Physical security encompasses the physical measures to protect the building, facilities and physical infrastructure, whereas environmental security ensures protection against environmental and natural hazards.  For physical security, procedures to grant, limit and revoke access to all relevant premises should be defined and implemented. ETIAS premises, buildings and areas should be secured and monitored against unauthorised access and physical attacks.	Security controls include: <ul style="list-style-type: none"> <li>• Implementation of secure areas of the ETIAS database;</li> <li>• Secure and resilient equipment;</li> <li>• Decentralisation of the ETIAS Central Server and Web Server implementations.</li> </ul>

Safeguards identification	Safeguards description	Key implementation aspects of the proposed safeguards
	For environmental security, measures should be established to protect against environmental hazards (e.g. fire, water, smoke, humidity, power outages, natural disasters such as floods, earthquakes). Consideration should be given to installing specialised equipment and devices to monitor and control the environment.	
<b>SG.10 Supplier Relationships</b>	Supplier relationships ensure a strategic plan related to the risks of the supplied components and software provided by external parties. These risks should be identified and managed throughout all stages of the relationship with external suppliers (including organisations in the supply chain), in order to mitigate fraudulent and tampered equipment and interactions with unwanted suppliers, vendors and partners.	
<b>SG.11 Information Security Aspects of Business Continuity Management</b>	Business continuity management ensures the resilience and continuous operation of ETIAS services upon any disruptive incidents. A formalised plan, such as a Disaster Recovery Plan should be in place to enable the ETIAS systems, assets and IT to respond to incidents and disruptions in order to continue operation of the ETIAS system and required IT services, while maintaining the availability of information at an acceptable level. This plan should be periodically tested, and updated as required.	<p>ETIAS should include the following controls in order to proceed business in case of a security event.</p> <ul style="list-style-type: none"> <li>• Implement a Disaster Recovery Plan (technical plan, focus on ICT systems) as well as a Business Continuity Plan (oriented towards business functions, including both ICT and non-ICT aspects);</li> <li>• Test and update both plans timely and after a major security event.</li> </ul>
<b>SG.12 Information Security Policies</b>	Information security polices addresses security regulation among the different ETIAS assets and components. Security policies englobe a set of rules that regulate the ETIAS system assets, components and organisations.	<p>ETIAS should include the following policies:</p> <ul style="list-style-type: none"> <li>• A highest level Enterprise Risk Management policy, that serves to anchor the lower policies, and addresses all Enterprise risks, including information and ICT but also e.g. safety and legal compliance;</li> <li>• An Information Security High Level policy (typically a short, 1-page document outlining key principles); and</li> <li>• 'Information Security Detailed policies', that defined how to apply the key principles of the High Level Policy to the various domains such as Human Resources, Software Development, Communication and Operations, Business Continuity, etc.</li> </ul> <p>These policies should be reviewed and planned timely and whenever significant ETIAS changes occur.</p>
<b>SG.13 Organisation of</b>	Organisation of information security ensures the definition and management of information security on the full scope	The security controls that should be implemented in ETIAS

Safeguards identification	Safeguards description	Key implementation aspects of the proposed safeguards
<b>Information Security</b>	organisations. ETIAS should have a structure management framework that directs, monitors and controls the implementation of information security as a whole within the full architecture and organisation of ETIAS. This includes a development of an Information Security strategy within ETIAS system, entities and assets that adopts, incorporates, reviews and implements the regulations and security controls.	organisation are as follows: <ul style="list-style-type: none"> <li>• Internal controls: division of responsibilities and segregation of duties, and project management security;</li> <li>• Mobile device and teleworking controls, such as VPN setting when ETIAS are outside ETIAS premises.</li> </ul>
<b>SG.14 Compliance</b>	Compliance with information security regulations is necessary for ETIAS. Access control and authorisation, as well as logging, are key requirements of most compliance industry standards. ETIAS should verify which regulations apply to their assets, and what each regulation requires.	ETIAS should be compliant with information security standards and best practises guidelines, such as ISO 27000, the German Federal Office for Information Security's and ENISA security guidelines.

### **Safeguards mitigating risk scenarios**

Risk scenarios are matched to safeguards, to ensure that every possible risk scenario is at least countered by one safeguard. This is marked by "X" table below, whereas the next one describes the mapping rational between the safeguards per threat scenario. Safeguards such as Organisation security (SG13) are important for ensuring coordination of accountability, budgets and resources to implement security within the full organisational scope, hence are important to help mitigate all the risk scenarios.

Table 69: Risk scenarios - safeguards matrix

	SG01 - Human Resources	SG02 - Access Control	SG03 - Cryptography	SG04 - Communications Security	SG05 - System acquisition, dev. and maintenance	SG06 - Incident management	SG07 - Operations security	SG08 - Asset Management	SG09 - Physical Security	SG10 - Supplier Relationships	SG11 - Business Continuity / Disaster Recovery	SG12 - Security Policies	SG13 - Organisation Security	SG14 - Compliance
RS01 - Information Disclosure		x	x	x	x	x	x	x					x	
RS02 - Eavesdrop			x	x				x		x			x	
RS03 - Cryptographic breach			x										x	x
RS04 - Rerouting		x	x	x	x	x				x			x	x
RS05 - Third-party communication		x	x	x	x	x				x			x	x
RS06 - Software bugs/vulnerabilities					x	x					x		x	
RS07 - Authentication		x	x	x			x	x				x	x	
RS08 - Credentials Forgery			x			x		x					x	
RS09 - Insider	x	x					x					x	x	
RS10 - Network and Interface interactions				x	x	x	x						x	
RS12 - Denial of Service				x		x	x				x		x	
RS13 - Malware/Spyware	x	x	x	x		x	x	x		x		x	x	
RS14 - Hardware malfunction, failure, or fraudulent					x					x	x		x	
RS16 - Traffic Analysis				x									x	
RS17 - Stress	x								x		x		x	
RS18 - Abuse	x								x		x		x	

## Annex 9. – Implementation approach

This annex gives additional information on the methodology and the assessment of the implementation options which lead to the highlight of a preferred option. The following tables show the result of the assessment, the assessment criteria, and the scoring reasoning for the analysis of the different implementation options:

Table 70: Assessment of ETIAS implementation options

Option / Criteria	Cost	Technical complexity and risks	Flexibility and adaptability	Preparatory measures	Convenience for travellers	Convenience for border guards	Convenience for carriers
A. "Big bang"	€€	-	--	-	-	-	--
B. Gradual per border type	€	+	++	+	-	+	0
C. Gradual per region	€	-	++	--	--	-	-
D. From voluntary to mandatory	€	+	++	+	+	-	+

Table 71: Legend and scoring system

Legend	Technical complexity and risk	Flexibility and adaptability	Preparatory measures	Convenience for travellers	Convenience for border guards	Convenience for carriers
++	The option can be easily implemented from a technical point of view. It bears no major risks.	The option is flexible and leaves room for adaptation in case of need.	The option does not require much preparatory effort.	The option positively impacts travellers and is convenient for this end-user.	The option positively impacts border guards and is convenient for this end-user.	The option positively impacts carriers and is convenient for this end-user.
+	The option can be implemented fairly easily from a technical point of view. It bears no major risks.	The option is fairly flexible and leaves some room for adaptation in case of need.	The option does not require too much preparatory effort.	The option positively impacts travellers and is fairly convenient for this end-user.	The option positively impacts border guards and is fairly convenient for this end-user.	The option positively impacts carriers and is fairly convenient for this end-user.
-	The option cannot be easily implemented from a technical point of view. The option can also be risky.	The option is not flexible and leaves no/some room for adaptation in case of need.	The option requires preparatory effort.	The option negatively impacts travellers and is fairly inconvenient for this end-user.	The option negatively impacts border guards and is fairly inconvenient for this end-user.	The option negatively impacts carriers and is fairly inconvenient for this end-user.
	The option's implementation	The option is not	The option requires a	The option negatively	The option negatively	The option negatively

Legend	Technical complexity and risk	Flexibility and adaptability	Preparatory measures	Convenience for travellers	Convenience for border guards	Convenience for carriers
	leads to important technical complexity. It is also risky.	flexible and leaves no room for adaptation in case of need.	significant amount of preparatory measures.	impacts travellers and is inconvenient for this end-user.	impacts border guards and is inconvenient for this end-user.	impacts carriers and is inconvenient for this end-user.
<b>0</b>	Impact is null or the criteria is not applicable.	Impact is null or the criteria is not applicable.	Impact is null or the criteria is not applicable.	Impact is null or the criteria is not applicable.	Impact is null or the criteria is not applicable.	Impact is null or the criteria is not applicable.

For the cost criterion, the study understands the “big-bang” option as a baseline. Indeed, the cost-benefit analysis analysed in details how much this option would cost (779 million euros). The gradual option “from voluntary to mandatory” has also been analysed and the result is cheaper (734 million euros). Taking this baseline into account and the assumption that all the gradual options would be cheaper than the “big-bang” (and thus comparable to “from voluntary to mandatory”), the assessment on this criterion is based on the following:

*Table 72: Legend and scoring system for the cost criterion*

Legend	Cost
<b>€</b>	The option is cheaper than the baseline
<b>€€</b>	Baseline: cost of the big-bang implementation
<b>€€€</b>	The option is more expensive than the baseline



Table 73: Explanation of the scoring per option

<b>Option A: "Big bang"</b>	
This option would mean that ETIAS is operational in all the regions of the world and at all border types in one go. This option entails that all end-users, basic IT components, communication channels and procedures are targeted and ready at the same time.	
<b>Cost</b>	As all resources (connections and devices) must be all ready at once, all costs are incurred at once (after the go-live, there would only be maintenance costs). However, the costs would not be accumulated through time and there is less probability for budget expansion. Big bang implies a high set-up cost but also immediate and full benefit realisation. It is the simplest option from a cost point of view.
<b>Level of technical complexity and risk</b>	Rolling-out ETIAS for all VE-TCN at all border-crossing points would necessarily require important resources to be put in place, and the back-up system would need to be already in place. All the possible connections of ETIAS with end-users (travellers, border guards and carriers) should also be ready from go-live date. This option, although straightforward, would bring consequent preparation and could lead to delays in case the IT system is not ready. A testing phase could help spotting potential issues.
<b>Flexibility and adaptability</b>	No flexibility and adaptability can be foreseen with this option. In case of failure the system would have to provide a full back-up and would not allow much change of implementation as it would be running. In addition, this option can expect significant delays in case one or several of the 26 MS or stakeholders are not ready. Indeed, ETIAS should as well be rolled-out in all MS at once.
<b>Preparatory measures</b>	Intense preparation measures should be put in place prior to the roll-out as all resources must be ready at once. In addition, in case of failure, all end-users would be more impacted than with other options. The negative impact of this factor (workload, tight schedule, mobilisation of all resources, possible delays, etc.) can be mitigated by the overall level of preparedness reached and the ability to quickly solve a potential issue.
<b>Convenience for travellers</b>	Visa-exempt travellers would all have to comply with the same rules at the same time. The impact can be mitigated by a large and comprehensive communication campaign. The measure has the advantage of being unambiguous.
<b>Convenience for border guards</b>	All Schengen border guards from all border crossing types would have to be ready at once. The impact can be mitigated by extensive trainings, workshops and overall communication and awareness-raising for all border control authorities (border guards, border police, agents, etc.). A testing phase could help spotting potential issues. It would need to be included in the legal proposal. Another option could consist in establishing a period in which ETIAS would be live but having a travel authorisation would not be mandatory.
<b>Convenience for carriers</b>	Intense preparation and workload prior to the roll-out day are to be foreseen. In case of technical issues with either the system or the communication channel, carriers would have to bear important legal responsibilities, leading to significant fines. The impact can be mitigated by a large and comprehensive public consultation of carriers' representatives, alongside with workshops and possible training sessions. A testing phase could help spotting potential issues.

<b>Option B: Gradual per border type</b>	
With this option, ETIAS would be implemented at one border type at a time. It would also be gradually implemented by carriers in their own systems. Given that the highest number of VE-TCN arrive by air to the Schengen Area, ETIAS could be implemented first at air, then at sea borders and lastly at land borders.	
<b>Cost</b>	As for all the gradual options, this option could seem less costly as technical issues can be adapted from one step of the implementation to another. However, the dilution of the cost throughout time can cause additional budget not foreseen

<b>Option B: Gradual per border type</b>	
	in the first assessment of the costs. In other terms, the gradual roll-out probably gives lower set-up costs but it spreads it over time, increasing recurrent costs and also ramping up benefit realisation.
<b>Level of technical complexity and risk</b>	The level of technical complexity and risk remains high as this remains a very significant effort, but focused on less cases and less stakeholders at once. This option allows for more room for manoeuvre in case any issue happens, as the negative impact would be limited to certain border-crossing points. Any technical difficulty can be a good practice for the roll-out of the following borders in order to avoid falling into the same pitfalls.
<b>Flexibility and adaptability</b>	All the gradual options are very flexible and possible to adapt to new requirements and changes if necessary. This option also takes into account more specificities of the border type. For instance, rolling-out at air borders also means that the carriers' connection must be ready.
<b>Preparatory measures</b>	For air (and possibly sea) borders, this option would allow carriers to run their own communication campaign to travellers in order to familiarise them with the new requirement. However, for land borders (and individual travel in general – no carriers involved) the situation might get more complicated as travellers might not be all aware of the new requirement. A grace period could help solve this issue.
<b>Convenience for travellers</b>	Although this option could be confusing in the beginning, it could give more time for travellers to adapt to ETIAS. However, and as previously seen, border types often match with regions, which could lead to the same undesirable effects as the regional approach.
<b>Convenience for border guards</b>	After assessments of the needs and preparatory measures, this option could be beneficial for border guards as it could allow them to focus their resources gradually at the border types of the roll-out. It could also allow them to spot and rectify any issue from border roll-out 1 to 2.
<b>Convenience for carriers</b>	<p>Given the current EU context, advance passenger information is a requirement only for air carriers. Although ETIAS would also be a requirement for all types of carriers as it would legally be a similar requirement as a visa, technical feasibility (communication channels) makes it more complicated to be implemented for sea and land carriers. Whilst the latter would most probably have more time to adapt, as there is currently little to no automatic communication channels in place, and the opportunity to learn from the experience of others, the former would have to be ready to connect to ETIAS on the day of the air border roll-out.</p> <p>As a result, an implementation at air border would logically require the carriers to be able to receive ETIAS status notifications. In that sense, from a carrier's point of view, a border type roll-out would be similar to a big-bang approach.</p> <p>This option can have positive and negative impact depending on the type of carrier.</p> <p>Lastly, it is relevant to note that carriers themselves play an important role in the awareness campaigns for travellers as they would also publicise the system.</p>

<b>Option C: Gradual per region</b>	
With this option, the travel authorisation would be first required for travellers with a nationality from a specific region x of the world, then from region y and finally from region z.	
<b>Cost</b>	As for all the gradual options, this option could seem less costly as technical issues can be adapted from one step of the implementation to another. However, the dilution of the cost throughout time can cause additional budget not foreseen in the first assessment of the costs.
<b>Level of technical complexity and risk</b>	Travel flows are complex and heterogeneous and all TCN from different nationalities can use the same transport carrier from the same country of origin. Although this option might seem more progressive than a big-bang, all communication channels and border facilities would need to be fully equipped at once. From a technical and security point of view, this option would have the same impact as the big-bang option.

<b>Option C: Gradual per region</b>	
<b>Flexibility and adaptability</b>	All the gradual options are very flexible and possible to adapt to new requirements and changes if necessary. In addition, the approach per region allows defining the regions, as done for the VIS roll-out (19 regions).
<b>Preparatory measures</b>	Although mostly arriving by air, VE-TCN can cross any type of border. As a result, all border-crossing points should be ready at the same time of the roll-out of the first region. Concerning this criteria, this option would have the same impact as a big-bang roll-out.
<b>Convenience for travellers</b>	This option might bring a negative impact on travel if some regions are spotted as a priority for the ETIAS roll-out. It is possible that travellers and businesses from the first regions would feel targeted and would have a sensation of mistrust from the EU. Therefore there could be a transient impact on tourism from travellers originating from a new region submitted to ETIAS.
<b>Convenience for border guards</b>	<p>This option would allow border guards at air (and possibly sea) borders to anticipate flows of travellers by their origin. For instance, if several flights arrive from North and Central America at the same time, the force would be able to allocate more resources and staff to the relevant terminal. This option could also be an opportunity to adapt to the new requirement from a smaller sample of the VE-TCN crossing the borders.</p> <p>However, for border guards at land borders, this roll-out would more or less have the same impact as a big-bang. An important mitigation measure would be the establishment of a grace period.</p>
<b>Convenience for carriers</b>	<p>As previously observed, the regions tend to be aligned with the type of border crossing. Consequently, a similar reasoning applies for options two and three: this option can have positive and negative impact depending on the type of carrier.</p> <p>Lastly, it is relevant to note that carriers themselves play an important role in the awareness campaigns for travellers as they would also publicise the system.</p>

<b>Option D: From voluntary to mandatory</b>	
With this option, holding a travel authorisation is voluntary in all regions and at all border types at first and then it becomes mandatory requirement after a pre-defined period of time.	
<b>Cost</b>	As for all the gradual options, this option could seem less costly as technical issues can be adapted from one step of the implementation to another. However, the dilution of the cost throughout time can cause additional budget not foreseen in the first assessment of the costs. In addition, the voluntary option should be free in order to incentive travellers to apply for a travel authorisation. As a result, the longer the voluntary period is, the longer it will take for ETIAS to bear its costs.
<b>Level of technical complexity and risk</b>	This option would give time to solve any last technical issue or adjust the system before it becomes mandatory, whilst allowing its end-users to get used to it. Any anomaly would have less effect with this option as the requirement would not be mandatory.
<b>Flexibility and adaptability</b>	All the gradual options are very flexible and possible to adapt to new requirements and changes if necessary. Additionally, ETIAS would not be mandatory at boarding.
<b>Preparatory measures</b>	The legal basis should be clearly defined prior to the implementation in order not to create confusion for end-users, particularly for travellers (what does a denied authorisation legally mean in a non-mandatory system?).
<b>Convenience for travellers</b>	If the preparation measures are well established and communicated, this option would allow travellers to get used to this requirement and prepare for the full mandatory roll-out.
<b>Convenience for border guards</b>	If the preparation measures are well established and communicated, this option would allow border guards to get used to the system and prepare for the full mandatory roll-out.
<b>Convenience for carriers</b>	The liability for carriers should be clearly defined as well.

#### **Conclusion of the assessment of options A, B, C and D:**

A gradual roll-out from voluntary to mandatory is the option with the highest score of the assessment, especially in terms of flexibility and adaptability. Contrary to the other types of gradual implementations, this approach has a positive impact on carriers and travellers, making it the most convenient option for the end-users.

## Annex 10. – Data protection impact

### Legal framework

Five pieces of EU law may apply to the set-up of ETIAS.

#### **The Charter of Fundamental Rights**

Article 7 of the Charter establishes a general right to respect for “private and family life, home and communications”. Article 8 provides for the protection of personal data, their fair processing for specified purposes on a legitimate basis. Finally, Article 52 provides that any limitation to these rights must:

- Respect their essence;
- Be proportional;
- Be necessary;
- Genuinely meet the objectives of general interest or the need to protect the rights of others.

The necessity of ETIAS would be analysed<sup>237</sup> in light of the EU context of large-scale IT systems (existing and future). It is thus necessary to identify these systems, their purposes and the data they collect, to ensure as limited overlap as possible.

#### **Regulation on the processing of personal data by the Community institutions and bodies**

The Regulation applies to EU agencies. As such, it would be applicable to eu-LISA should the agency be chosen to operate any component of ETIAS, and to the CMPE.

Components and processing done by Member States would be regulated by the current Data Protection Directive<sup>238</sup> or, most likely, the package succeeding to it.

#### **Data Protection Directive**

The Data Protection Directive is the current act regulating data protection for the EU. However, it will be replaced in 2018 by the EU Data Protection Reform package, which will then become applicable.

The package contains two legal acts:

1. The General Data Protection Regulation;
2. A directive on the processing of personal data for the prevention, investigation, detection or prosecution of criminal offences.

#### **General Data Protection Regulation**

The Regulation<sup>239</sup> would apply to any processing that is not covered by the Regulation on the processing of personal data by the Community institutions and bodies or the Directive on personal data processing for the prevention of criminal offences.

#### **Directive on personal data processing for the prevention, investigation, detection or prosecution of criminal offences**

The Directive does not apply to EU agencies<sup>240</sup>. It would thus not apply to the processing of personal data by eu-LISA. It may however apply to Member States processing applications (Schengen states) as one of the system’s objectives is the safeguarding against and the prevention of threats to public security<sup>241</sup>.

All these pieces of legislation coherently provide for principles to be respected in the course of data processing.

---

<sup>237</sup> Notably by the European Data Protection Supervisor (EDPS).

<sup>238</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>239</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>240</sup> Article 2(b).

<sup>241</sup> Article 1, paragraph 1.

## ETIAS necessity and proportionality

### Data collected for the migration risk assessment

The study proposes the collection of the following data for assessing the risk of overstay. The data set comply with necessity and proportionality as each data is necessary for carrying out a meaningful assessment; no more data than what is required would be collected (other data would be collected for the security risk assessment):

- Biographical and passport data, necessary to check EES, VIS and SIS:
  - **EES** would provide information on whether a person has overstayed or has been refused entry;
  - **VIS** would be used to check whether the person has been denied a visa and for what reason<sup>242</sup>;
  - **SIS** would be used to check whether the person is subject to an entry ban as these can be issued for migration reasons.
- Within the address, the country of residence as it is an indicator of the likeliness of return;
- Education and occupation information, which would support the assessment of the means of subsistence of the traveller and of his/her ties to the country of residence. The study proposes to ask the two following questions, which would be answered using drop-down menus:
  - What is your field of employment/occupation?
  - What is your position?

### Access for law enforcement purposes

Organised crime (notably trafficking in human beings, drug trafficking and firearms trafficking) can be linked to international travel – including visa-exempt travel. Information about travellers can thus be helpful in criminal investigations<sup>243</sup>. This has been demonstrated by the use of the VIS for law enforcement purposes, which has allowed law enforcement authorities to make substantial progress in cases related to trafficking in human beings, drug trafficking and terrorism<sup>244</sup>.

Necessity and proportionality of the access for law enforcement purposes would also come from two main safeguards:

- **Law enforcement authorities would not have access to all ETIAS data;**
- A number of **conditions should be met** for a law enforcement authority to access ETIAS data.

## Breakdown of safeguards by data protection principle

The following part of the annex lists possible safeguards for ETIAS, drawing on the following sources:

- a) Existing legislation in the area of EU large-scale IT systems and data sets (VIS and SIS Regulations and Decisions, PNR Directive<sup>245</sup>);
- b) Upcoming legislation (the EES proposal).

The examples provided by these systems are relevant to different extents:

- **PNR** is a decentralised data processing: there is no central PNR system but each Member State is required to analyse PNR data. ETIAS would, on the contrary, be based on a centralised system even if the decision-making is shared with Member States. PNR's safeguards however retain relevance for the following reasons:
  - PNR data are used to conduct a risk assessment on incoming travellers in a similar manner to what ETIAS would do. Both would collect advance information on travellers;

---

<sup>242</sup> For those coming from a country which has just changed visa regime.

<sup>243</sup> Contrary to EES, ETIAS data cannot be used for identification purposes, as the system would not contain biometrics.

<sup>244</sup> See Explanatory Memorandum of the EES proposal, p. 6.

<sup>245</sup> The API Directive is older and much less precise than the PNR, VIS, SIS and EES legal bases. It thus contains a limited number of data protection safeguards, which is the reason why it is not part of the table and analysis below.

- Existing teams involved in API/PNR data processing within Member States may be the authorities contributing to the processing of applications where Member State involvement is necessary. PNR safeguards are thus relevant for cases in which **Member State processing** would be required.
- As **VIS** and **SIS** are centralised/semi-centralised systems, their Regulations and Decisions are more likely to provide examples of safeguards for ETIAS in relation to **processing by the CMPE**.
  - VIS is a repository of third-country nationals' data as ETIAS would be, and collect data through an application form as ETIAS would;
  - SIS is less relevant; however the system processes sensitive information (regarding criminal offences) as ETIAS would.
- The **EES proposal** still have to be approved by the European Parliament and the Council and is likely to change before the end of the legislative cycle. However, if ETIAS is implemented as a module of EES, both systems should have similar safeguards in order to be **coherent** in the approach chosen and reinforce the **consistency** of the EU legal framework.

Taking into account these similarities allow this study to assess the safeguards that would be **relevant for ETIAS**. Safeguards that do not fit with the purposes and design of ETIAS have been excluded.

### **Lawfulness, fairness and transparency**

ETIAS would meet the first criteria for lawfulness, fairness and transparency (processing should be based on consent or be necessary for legitimate purposes) as processing would be necessary for the legitimate purposes defined. ETIAS processing could not be based on consent since, where the person is required to comply with a legal obligation, there is no free choice and thus no genuine consent<sup>246</sup>.

The second criteria for lawfulness, fairness and transparency (processing should be based on EU or Member States' law) would be met by the Commission's legislative proposal for ETIAS and its approval by the European Parliament and the Council. ETIAS data processing would not take place before such a proposal is approved and becomes EU law.

### **Purpose limitation**

The compliance of ETIAS with the principle of purpose limitation is demonstrated, as each data would be collected for a specified, explicit and legitimate purpose. However, other EU systems and data sets use additional safeguards to ensure that data is not further processed in a manner that would be incompatible with the purposes.

---

<sup>246</sup> See perambulatory provision (35) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The table below presents these safeguards<sup>247</sup>:

Table 74: Purpose limitation safeguards

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS<sup>248</sup></b>	<b>SIS</b>	<b>PNR<sup>249</sup></b>
<b>Access reserved exclusively:</b> – <b>to duly authorised staff</b>	Art.8(1)	Art.6(2)	Art.31(4)	Art.(4)
– <b>of the authorities of each MS which are competent for the purposes</b>	Art.8(1)	Art.6(2)	Art.31(4)	
<b>Access limited:</b> – <b>to the extent needed for the performance of the tasks</b>	Art.8(1)	Art.6(2)	Art.28	
– <b>in accordance with the purposes and proportionate to the objectives pursued</b>	Art.8(1)	Art.6(2)		
<b>MS to designate competent national authorities and duly authorised staff.</b> <b>List to be communicated, specifying purpose of access.</b>	Art.8(2) Art.26 (same for law enforcement authorities)	Art.6(3)	Art.31(8) (including which data they may search)	Art.7(1) and (3)
<b>List to be published. If amendments, new list published once a year.</b>	Art.8(2)	Art.6(3)	Art.31(8)	
<b>Competent authority to ensure that the use of the system is necessary, appropriate and proportionate</b>	Art.9(1)	Art.7		
<b>Access for law enforcement purposes is subject to conditions</b>	Art.28 and 29 Art.52			

The safeguards presented above would all be appropriate for ETIAS. All these safeguards are currently in the EES proposal; should ETIAS be implemented as one module of EES, using them for ETIAS would provide coherence of the EU legal framework.

## Data minimisation

As illustrated below, only the SIS has a dedicated provision specifying that data entered shall be adequate, relevant and important enough because Member States are not supposed to transform each and every need for finding a person or an object into a European alert by including it in SIS.

Table 75: Data minimisation safeguards

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>Data entered shall be adequate and relevant</b>			Art.21 (MS to enter alerts for cases "adequate, relevant and important)	

<sup>247</sup> The API Directive is older and much less precise than the PNR, VIS, SIS and EES legal bases. It thus contains a limited number of data protection safeguards, which is the reason why it is not part of the tables and analysis below.

<sup>248</sup> For all articles related to VIS and SIS, the article numbers mentioned in the tables refer to the article numbers in the Regulations (by opposition to the article numbers in the Decisions).

<sup>249</sup> PNR data processing is implemented through a directive, which are usually less precise than regulations. This explains the lower number of safeguards for this data set.



enough”)

This safeguard is not relevant as such for ETIAS, which purpose, scope and design differ from the SIS’s ones. ETIAS would not require applicants or the CMPE to assess the relevance of the data entered in it. However, a similar provision could be useful for ensuring that the investigation triggers entered by Member States in the screening rules are adequate and relevant.

## Accuracy

It should be kept in mind that the data collected through the ETIAS form would only be declarative: accuracy in the sense that the data is true cannot be entirely ensured. However, the responsibility and accountability of the data controller concerning accuracy is limited to:

- Take reasonable steps to ensure the accuracy of the personal data obtained;
- Keep data up-to-date;
- Ensure deletion or rectification of inaccurate data.

Table 76: Accuracy safeguards

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>MS responsible for data accuracy, up-to-date</b>	Art.36	Art.29	Art.34	

In the case of ETIAS, responsibility and accountability for data accuracy would have to be shared between Member States and the CMPE<sup>250</sup>. Member States’ responsibility and accountability would be limited to the data they enter in the system (investigation triggers). The CMPE would be responsible for all other ETIAS data, including data entered by travellers. Indeed, most of the ETIAS data would be entered by applicants themselves instead of Member States. Having Member States responsible for travellers’ data accuracy would require determining which Member State is responsible which data, which would be particularly complicated in the case of ETIAS, and is thus not the preferred solution.

In case of inaccurate data (e.g. change of name), individuals have a **right of correction**. EU systems and data sets generally hand over the responsibility and accountability for correction to the Member State that entered the data, as illustrated below:

Table 77: Right of correction safeguards

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>MS responsible for correction of inaccurate data</b>	Art.46	Art.38	Art.41(5) (right of persons)	Art.13(1) (MS to ensure that passengers have these rights)
<b>Right to bring an action/complaint before the competent authorities or courts of that MS which refused the right of correction</b>	Art.48	Art.40(1)	Art.43	

<sup>250</sup> In cases of disambiguation or typing error, the CMPE and Member States would not update ETIAS data as such; instead, they would add corrected data to the application file. This would allow keeping trace of the original data and of the correction made. Changes would be logged. The CMPE and Member States would not be able to change all fields, but only data collected on the application and, within the data entered by travellers, write-in fields. Drop-down menus, calendar and tick-boxes could not be changed as they would be less prone to typing errors (the traveller would have to submit a new application).

This approach is not directly appropriate for ETIAS. Indeed, as mentioned above, the CMPE should be responsible and accountable for travellers' data accuracy<sup>251</sup>. This includes the correction of inaccurate data.

The following procedure would allow ETIAS to guarantee the right of correction:

*Table 78: Ensuring the right of correction for ETIAS*

Remedy	Responsibility
<ul style="list-style-type: none"> <li>• Set-up of a function responsible for correction and deletion of inaccurate and unlawfully recorded data.</li> <li>• Procedure in place for appealing to a mandated body or court.</li> </ul>	<ul style="list-style-type: none"> <li>• The <b>DPO of the CMPE</b> handles requests for access, correction or deletion.</li> <li>• <b>EDPS and/or the Court of Justice of the European Union</b> handle complaints.</li> </ul>

Applicants would have to communicate these cases to the CMPE as a first step, before bringing a complaint before a mandated body or court. This would allow increasing convenience for applicants, as a solution could be found within a shorter timeframe and at limited to no cost. In case of disagreement between the CMPE and the applicant, he/she would have the right to bring a complaint before the mandated body or court in charge of reviewing the decisions related to correction and deletion made by the CMPE.

Within the CMPE, requests for correction or deletion should be handled by a dedicated data protection officer. The mandated body role would be given to the European Data Protection Supervisor (EDPS) and the Court of Justice of the European Union (CJEU)<sup>252</sup>.

### Storage limitation

The table below presents the safeguards that exist for other systems and data sets:

*Table 79: Storage limitation safeguards*

Safeguard	EES proposal	VIS	SIS	PNR
<b>Anonymisation</b>	Art.57			Art.12(2) (after six months)
<b>Access after anonymisation</b>				Art.12(3) (permitted for law enforcement if approved by a competent authority)
<b>Exceptions to deletion</b>				Art.12(4) (data permanently deleted except in cases where specific data are used in the context of specific cases for combatting terrorism or serious crime)

The relevance of storage limitation safeguards for ETIAS is discussed below:

#### a) Dormant database

This technique is used by the US travel authorisation system: ESTA data is retained for three years in the active database (the two years validity of the travel authorisation and an additional one year after it expires). After that period, it is placed in a dormant database for 12 years, to allow retrieval for law enforcement purposes<sup>253</sup>.

<sup>251</sup> In practice, complaints related to inaccuracy would be solved by the application being deleted and the applicant being requested to submit a new application. This would allow checks to be carried out on the basis of the new, accurate information.

<sup>252</sup> Article 32 of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

<sup>253</sup> See: <https://www.cbp.gov/travel/international-visitors/frequently-asked-questions-about-visa-waiver-program-vwp-and-electronic-system-travel> (accessed 06/2016).

Transferring **data which is not needed for applications processing** anymore into a dormant database could be provided for ETIAS as a data protection safeguard. Such data would be moved from the active database **at the latest at end of the two-year validity period of the travel authorisation. Only access for reporting purposes and law enforcement access**, under specific conditions<sup>254</sup>, would be allowed. The following table proposes which data could be placed in the dormant database and for how long.

Table 80: Data stored in a dormant database

Data	Storage location <sup>255</sup>	Justification
<b>Biographical data</b>		
First name	Active database	Data necessary for applications processing = remains in active database
Surname		
Name at birth		
Other name		
Date of birth		
Place of birth		
Parents' first names		
Nationality		
Additional nationalities		
Gender		
<b>Passport data</b>		
Passport number	Active database	Data necessary for applications processing = remains in active database
Passport expiry date		
Country of issue		
<b>Contact details</b>		
Email address	Active database	Data necessary for applications processing = remains in active database
Address (residence)		
Phone number		
<b>Background questions</b>		
Education and occupation information	Active database during the authorisation validity period (or less if deemed necessary) then in the dormant one	Data not necessary for applications processing beyond the validity of a granted travel authorisation = moves to dormant database
Convicted of serious crime		
Been recently present in a war zone		
Threat to public health: infectious disease (e.g. tuberculosis)	Active database during the authorisation validity period (or less if deemed necessary - aligned with the topic it covers) then in the dormant one	Data not necessary for applications processing beyond the validity of a granted travel authorisation = moves to dormant database
Additional information sent by the applicant at the request of the CMPE and/or a MS for the purpose of the risk assessment <sup>256</sup>		

Using a dormant database for ETIAS has the following advantages and disadvantages:

<sup>254</sup> The safeguards described in section 2.2.9 "Access management and data ownership" would apply to law enforcement access to the dormant database as well.

<sup>255</sup> From the moment the application is granted, denied or revoked. This table refers to the analysis provided in the section 2.2.8 "Data retention".

<sup>256</sup> This information is treated as Background questions data.

Table 81: Advantages and disadvantages of using a dormant database

Advantages	Disadvantages
<p><b>Data protection</b> - Higher level of protection compared to the situation without a dormant database as access to data, in particular special categories of data such as health-data, is limited</p>	<p><b>Complexity</b> – Increased overall (technical) complexity of the system</p>
	<p><b>Usefulness</b> – Only a limited data set would be placed in the dormant database</p>

While the technical complexity and limited usefulness suggest a dormant database would not be needed for ETIAS, this technique **ought to be foreseen** to ensure adequate treatment and protection of some data, especially sensitive data, contained in the background questions<sup>257</sup>.

#### b) Anonymisation

Data anonymisation is used for the processing of EES data for statistical reporting purposes. Retaining part of ETIAS data in an anonymised form could, similarly, be envisaged following the principle of storage limitation, and would facilitate:

- **Applications processing** (identifying risk profiles and patterns as part of risk assessment); and
- **Reporting** (gathering of statistics).

Access to anonymised data, or to the personally identifiable data set, adequately secured and monitored, would be restricted to specific stakeholders for specific needs, for example law enforcement authorities in the context of an ongoing investigation.

A possible set of data to be anonymised is proposed below<sup>258</sup>:

Table 82: Anonymised data

Data	Anonymised data
<b>Biographical data</b>	
First name	✓
Surname	✓
Name at birth	✓
Other name	✓
Date of birth	
Place of birth	✓
Parents' first names	✓
Nationality	
Additional nationalities	
Gender	
<b>Passport data</b>	
Passport number	✓
Passport expiry date	
Country of issue	
<b>Contact details</b>	
Email address	✓
Address (residence) <sup>259</sup>	✓

<sup>257</sup> This result could be achieved by using different technical means (e.g. access control or masking out background questions, which could be "de-masked" in case of necessary – appeal or law enforcement purposes).

<sup>258</sup> Place of birth, parents' first names, passport number, email address and phone number are not considered useful for reporting and statistical purposes.

<sup>259</sup>

Country of residence	
Phone number	√
<b>Background questions</b>	
Education and occupation information	
Convicted of serious crime	
Been recently present in a war zone	
Threat to public health: infectious disease (e.g. tuberculosis)	
Additional information sent by the applicant at the request of the CMPE and/or a MS for the purpose of the risk assessment	

The following table presents the advantages and disadvantages of anonymising a part of the ETIAS data set:

*Table 83: Advantages and disadvantages of using anonymisation*

<b>Advantages</b>	<b>Disadvantages</b>
<b>Data protection</b> – Higher level of protection as it would prevent the identification of individuals	<b>Complexity</b> – Increased overall (technical) complexity of the system
<b>Coherence</b> of the EU legal framework – Approach similar to the one used in the EES proposal	<b>Limited utility</b> – Data may need to be de-anonymised nonetheless (frequently and at short notice), e.g. for use for disambiguation

Based on the above, the **use of anonymisation for ETIAS should be assessed further** to confirm its relevance and added value before embedding in the design of the system.

### **Integrity and confidentiality**

The table below presents some examples of safeguards used by other EU systems.

*Table 84: Integrity and confidentiality safeguards*

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>MS to adopt security measures, including a security plan</b>	Art.39	Art.32	Art.10	
<b>Data processing to be carried out within secure location(s)</b>				Art.6(8)
<b>eu-LISA to adopt a security plan</b>	Art.39	Art.32	Article 16	
<b>eu-LISA to take the necessary measures for security and only duly authorised staff has access</b>	Art.36(2)	Art.29		
<b>MS to apply national rules on confidentiality to the staff</b>			Art.11 (and professional secrecy)	Art.13(2) (and national rules on data security)
<b>eu-LISA to apply rules of professional secrecy (and confidentiality)</b>		Art.26(9)	Art.17	
<b>Common protocols and secure transmission</b>				Art.16(1)(2)
<b>Staff shall receive appropriate training</b>	Art.35(4)	Art.28(5)	Art.14 (on data protection, security, related offences and penalties, before	Art.13(3)

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
			staff is authorised to process data)	
<b>Transfer</b>	Art.38 (permitted for identification purposes)	Art.3(3) (permitted for specific purposes)	Art.39 (not permitted)	Art.11 (permitted if certain conditions are met)
<b>MS responsible for ensuring the security of the data</b>	Art.39			Art.13(7)
<b>Communication in case of breach:</b> – <b>To the person;</b> – <b>To national DPO</b>				Art.13(8) (where high risk for the data or affect privacy)

The following safeguards would be appropriate for ETIAS, as ETIAS data would be processed centrally (safeguards aiming at eu-LISA apply) as well as by Member States (safeguards aiming at Member States apply):

- Member States to adopt security measures, including a security plan; eu-LISA to adopt a security plan;
- Data processing to be carried out within secure location(s);
- eu-LISA to take the necessary measures for security and only duly authorised staff has access;
- MS to apply national rules on confidentiality to the staff; eu-LISA to apply rules of professional secrecy (and confidentiality);
- Common protocols and secure transmission;
- Staff shall receive appropriate training.

**Transfer** of data to a third country, an international organisation or any private party is not allowed in the EES proposal, with one exception: transfer is authorised if necessary to prove the identity of third-country nationals for the purpose of returning them to a third country. As ETIAS, contrary to EES, would not collect biometric data, ETIAS data set cannot be used for identification. Transfer to a third country, international organisation or private party would thus not be justified.

MS responsibility and accountability for **ensuring the security** of the data would be limited to the data they receive from the CMPE for manual processing. eu-LISA would be responsible and accountable for the security of the rest of ETIAS data.

**Communication in case of breach** (i.e. if data has been accidentally or unlawfully lost, destroyed, accessed etc. and if there is a risk for the rights of the person, the data controller informs the DPO and the person concerned) could be envisaged for ETIAS.

## Accountability

The table below presents some examples of accountability safeguards used by other EU systems.

*Table 85: Accountability safeguards*

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>MS are liable</b>	Art.40	Art.33	Art.48	
<b>MS to cooperate with national DPOs</b>	Art.42	Art.35	Art.13	
<b>MS to designate a controller</b>	Art.49(4)	Art.41(4) (and to communicate its details to the Commission)		
<b>MS to keep records</b>	Art.41 (of the staff duly authorised)	Art.34	Art.12 (of access and exchanges of data)	Art.13(5)(6) (of personnel and processing)
<b>eu-LISA to keep records</b>	Art.41	Art.34	Art.18	Art.13(5)(6)
<b>LEA access logged and monitored</b>	Art.53			
<b>Appointment of a data protection officer</b>				Art.5

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>National DPOs responsible for monitoring compliance</b>		Art.41(1)		Art.15(1)(2) Art.3
<b>Audit of MS processing by national DPOs</b>	Art.49	Art.41(2)	Art.44	
<b>Audit of eu-LISA processing by the EDPS</b>	Art.50	Art.42	Art.45	
<b>Cooperation between national DPOs and EDPS</b>	Art.51	Art.43	Art.46	

As in other EU systems, accountability should be ensured for ETIAS through:

- Recording of the staff having access and of processing activities;
- Logging functionalities;
- Auditability;
- Responsibility allocation;
- Cooperation between authorities.

All the safeguards would thus apply to ETIAS but two of them would need to be adapted to the system's specificities:

1. Liability for damage suffered as a result of unlawful processing would have to be allocated between the entities processing data: the CMPE, Member States and eu-LISA;
2. The audit of eu-LISA processing by the EDPS would have to be completed by an audit of the CMPE processing.

### Other safeguards: right of information

*Table 86: Right of information safeguards*

<b>Safeguard</b>	<b>EES proposal</b>	<b>VIS</b>	<b>SIS</b>	<b>PNR</b>
<b>Responsibility for informing persons</b>	Art.44 (MS to inform TCN in writing; common leaflet and website to be set-up by COM, available in a linguistic version that the person (is reasonably supposed to) understand and completed by MS)	Art.37 (MS to inform applicants)	Art.42 (in as much as possible, persons on which an alert is issued should be informed)	
<b>Information campaign</b>	Art.45 (by COM in cooperation with the EDPS)		Art.19 (about the objectives, data stored, the authorities having access and the rights of persons)	

The right of information would be ensured for ETIAS through the following measures:

- An information campaign would be carried out (for more details on the information campaign, see section 2.5 "User interaction");
- The ETIAS website or possibly mobile application would provide, in accordance with EU law<sup>260</sup>:
  - The identity and contact details of the data controller;
  - The contact details of the data protection officer of the CMPE;
  - The purpose of the processing;
  - The recipients or categories of recipients of the data;
  - The period for which the data will be stored;
  - The rights of the person (rights of correction and deletion etc.);
  - The consequences of not providing the data;
  - The existence of automated decision-making and information about the logic involved, the significance and consequences of such processing.

In addition, ETIAS website/app should provide:

<sup>260</sup> See Article 13 of the General Data Protection Regulation.

- The rules for short stay in the Schengen Area;
- In which languages help can be received through the helpdesk;
- Details on the procedure to appeal the decision;
- Details on the procedure to obtain remedy for a breach of a data protection right;
- Details on the procedure to seek asylum.
- The emails sent to travellers to communicate denial would contain information on how to appeal the decision and how to obtain remedy for a breach of a data protection right.

## Other safeguards: remedies

Table 87: Remedies safeguards

Safeguard	EES proposal	VIS	SIS	PNR
<b>DPOs to deal with complaints</b>				Art.3
<b>Courts or other competent authority under national law to deal with complaints</b>	Art.48	Art.40	Art.43	
<b>National DPOs to cooperate and advise people</b>	Art.47			Art.15(4)
<b>Assistance of the national DPOs throughout the proceedings</b>	Art.48(2)	Art.40(2)		

As highlighted by the table, the systems/data sets deal with complaints in different ways:

- For some, complaints are handled by national Data Protection Officers (DPOs) (decentralised system: PNR);
- For others, complaints are handled by national courts or other competent authorities designed by national law (systems with a central component: EES, VIS, SIS).

These safeguards are not directly appropriate for ETIAS. Indeed, the CMPE would, as well as Member States, be responsible for some data processing (e.g. disambiguation).

Complaints would be dealt with in the following way:

Table 88: Overview of data protection procedures and responsibilities for remedies

Remedy	Responsibility
<ul style="list-style-type: none"> <li>• Procedure in place for appealing to a mandated body or court against the treatment of personal data<sup>261</sup>.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>EDPS and/or the Court of Justice of the European Union</b> handle complaints related to processing by the CMP; <b>national competent authorities</b> handle complaints related to processing by MS.</li> </ul>

## Other safeguards: fundamental rights

Table 89: Fundamental rights safeguards

Safeguard	EES proposal	VIS	SIS	PNR
<b>Competent authorities to ensure that it does not discriminate</b>	Art.9(2)	Art.7(2)		Art.6(4)
<b>Pre-determined criteria must be targeted, proportionate and specific</b>				Art.6(4)
<b>Set criteria are regularly</b>				Art.6(4)

<sup>261</sup> Applicants would be informed about this procedure in the email received on the outcome of the decision-making process. For a list of the information that would be provided to applicants, see Annex 10. – “Data protection impact”.



These safeguards are relevant to ETIAS screening rules for two main reasons:

- Flexibility and adaptability of the rules are essential to achieve the security objectives of the system;
- Safeguards must also be applied to ensure that the rules are continuously necessary, proportionate and do not violate fundamental rights.

For these reasons, ETIAS screening rules could be reviewed periodically.

Part of the assessment would need to be “operational”, i.e. related to the relevance of the rules in light of the threats that may have evolved. The EDPS and possibly national DPOs would as well need to be involved to ensure fundamental rights are respected; discrimination during the risk assessment should always be avoided. These two review types (operational relevance and fundamental rights) could be separated or merged.

## Overview of data protection safeguards for ETIAS

The table below summarises the safeguards used by other systems/data set legal bases, and the ones that should be used for ETIAS’s. Each safeguard is related to the data protection principles it satisfies<sup>262</sup>.

---

<sup>262</sup> Safeguards that are not satisfying a data protection principle (relating to the right of information, remedies or fundamental rights) are not present in the table for brevity reasons.

Table 90: Overview of data protection safeguards provided for by a specific article in the legal basis.  
Data protection principles not explicitly covered in the legal basis remain applicable by virtue of the legislation on data protection

	Safeguard in the legal bases of <sup>263</sup>				Appropriate for ETIAS	Data protection principles						
	EES	VIS	SIS	PNR		Lawfulness, fairness and transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Integrity and confidentiality	Accountability
<b>Safeguard</b>												
<i>Access reserved exclusively: - to duly authorised staff</i>	✓	✓	✓	✓	✓		✓					
<i>- of the authorities of each MS which are competent for the purposes</i>	✓	✓	✓		✓		✓					
<i>Access limited: - to the extent needed for the performance of the tasks</i>	✓	✓	✓		✓		✓					
<i>- in accordance with the purposes and proportionate to the objectives pursued</i>	✓	✓			✓		✓					
<i>MS to designate competent national authorities and duly authorised staff. List to be communicated, specifying purpose of access.</i>	✓	✓	✓	✓	✓		✓					
<i>List to be published. If amendments, new list published once a year.</i>	✓	✓	✓		✓		✓					
<i>Competent authority to ensure that the use of the system is necessary, appropriate and proportionate</i>	✓	✓			✓		✓					
<i>Access for law enforcement purposes</i>	✓				✓		✓					

<sup>263</sup> While not all safeguards are present in all legal bases, many of them are implemented in practice. This is the case, e.g., of the secure transmission that is *de facto* existing for EES, VIS and SIS. As another example, access to PNR data is *de facto* reserved to the authorities of each Member State that are competent for the purpose.

	Safeguard in the legal bases of <sup>263</sup>				Appropriate for ETIAS	Data protection principles						
	EES	VIS	SIS	PNR		Lawfulness, fairness and transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Integrity and confidentiality	Accountability
<i>is subject to conditions</i>												
<i>Data entered to be adequate and relevant</i>			✓		✓			✓				
<i>MS responsible for data accuracy, up-to-date</i>	✓	✓	✓		✓				✓			
<i>Anonymisation</i>				✓						✓		
<i>Access after anonymisation</i>				✓						✓		
<i>Exceptions to deletion</i>				✓	✓					✓		
<i>MS to adopt security measures, including a security plan</i>	✓	✓	✓		✓						✓	
<i>Data processing to be carried out within secure location(s)</i>				✓	✓						✓	
<i>eu-LISA to adopt a security plan</i>	✓	✓	✓		✓						✓	
<i>eu-LISA to ensure only duly authorised staff has access</i>	✓	✓			✓						✓	
<i>MS to apply national rules on confidentiality to the staff</i>			✓	✓	✓						✓	
<i>eu-LISA to apply rules on confidentiality</i>		✓	✓		✓						✓	
<i>Common protocols and secure transmission</i>				✓	✓						✓	
<i>Staff shall receive appropriate training</i>	✓	✓	✓	✓	✓						✓	
<i>Transfer</i>	✓	✓	✓	✓	✓						✓	
<i>MS responsible for ensuring the security of the data</i>	✓			✓	✓						✓	

	Safeguard in the legal bases of <sup>263</sup>				Appropriate for ETIAS	Data protection principles						
	EES	VIS	SIS	PNR		Lawfulness, fairness and transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Integrity and confidentiality	Accountability
<i>Communication in case of breach to the person, to national DPO</i>				✓	✓						✓	
<i>MS are liable</i>	✓	✓	✓									✓
<i>MS to cooperate with national DPOs</i>	✓	✓	✓		✓							✓
<i>MS to designate a controller</i>	✓	✓			✓							✓
<i>MS to keep records</i>	✓	✓	✓	✓	✓							✓
<i>eu-LISA to keep records</i>	✓	✓	✓	✓	✓							✓
<i>LEA access logged and monitored</i>	✓				✓							✓
<i>Appointment of a data protection officer</i>				✓	✓							✓
<i>National DPOs responsible for monitoring compliance</i>		✓		✓	✓							✓
<i>Audit of MS's processing by national DPOs</i>		✓	✓	✓	✓							✓
<i>Audit of eu-LISA's processing by the EDPS</i>		✓	✓	✓	✓							✓
<i>Cooperation between national DPOs and EDPS</i>		✓	✓	✓	✓							✓

# Annex 11. – Detailed cost-benefit analysis

## Methodology

The approach applied for the ETIAS CBA draws from the general guidance to the Commission services and can be therefore considered as a standard methodology<sup>264</sup>. The section below highlights the main principles of the method. Afterwards detailed parameters, assumptions and the approach for each cost and benefit item are provided.

### Main principles

#### Incremental approach

The CBA compares a scenario with-the-project with a baseline scenario without-the-project, i.e. the starting point for a CBA is the current 'business as usual'. This means that the financial and economic cash flows, as well as the financial and economic performance indicators are calculated on an incremental basis only.

#### Discounted Cash Flow (DCF) method

The DCF method is used for the CBA in compliance with section III (Method for calculating the discounted net revenue of operations generating net revenue) of Commission Delegated Regulation (EU) No 480/2014. This means that a discount rate is applied to calculate the present value of the future cash flows, so that the comparison could be done of the cash flows occurring at different times. In the analysis **4 % discount rate** in real terms is applied as the reference parameter for the real opportunity cost of capital in the long term, as recommended in the Commission CBA guide<sup>265</sup>.

#### Approaches for costs and benefits estimation

At this stage of the project there are no detailed functional and technical specifications, therefore both top-down and bottom-up estimation methodologies are applied. The top-down approach is used when the technical specifications remain at a high-level and detailed cost items cannot be identified. When the cost or benefit elements are more detailed, the bottom-up approach is used. The table below presents the method used per main cost and benefit item.

Table 91: The approaches used for different cost and benefit items

Top-down estimates	Bottom-up estimates
<ul style="list-style-type: none"> <li>Contractor development (development of the central system, NUI and integration of the NUI)</li> </ul>	<ul style="list-style-type: none"> <li>Administration costs (e.g. project management, grants management, monitoring of the systems)</li> <li>Hardware costs</li> <li>Software costs</li> <li>Network costs</li> <li>Cost of the meetings and training</li> <li>Office space and datacentre space costs</li> <li>Fee revenues</li> <li>Time savings</li> </ul>

#### Top-down

In the top-down approach the current cost estimates of ETIAS are compared with **real data** from **existing systems** that were developed and are currently in operation, such as similar large-scale trans-European systems (e.g. VIS, systems developed by DG TAXUD). The method, primarily developed by DG TAXUD, is used for systems where only high-level design is available without detailed functional and technical specifications, which is the case for ETIAS.

The top-down is based on three main components:

- Historical data from large-scale trans-European IT systems:** real data provides the

<sup>264</sup>See: [http://ec.europa.eu/regional\\_policy/sources/docgener/studies/pdf/cba\\_guide.pdf](http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/cba_guide.pdf) (accessed 07/2016).  
<sup>265</sup>[http://ec.europa.eu/regional\\_policy/sources/docgener/studies/pdf/cba\\_guide.pdf](http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/cba_guide.pdf), p. 42 (accessed 07/2016).

- benchmark for comparison.
- **Assumptions:** the assumptions are documented and detailed in order to ensure the estimates are in line.
- **System parameters:** common characteristics of a large-scale system such as:
  - Number of processes;
  - Number of tasks per process;
  - Number of information exchanges/messages in those processes;
  - Number of interfaces with other existing systems or process areas.

### Bottom-up

The bottom-up approach means detailed analysis of the specific cost and benefit components, as

- These components are used by existing systems; or
- The study has enough information to make relatively reliable estimates.

The method encompasses detailed compilation of cost and benefit items for the selected components for which a bottom-up approach can be used at this stage of the design of the systems.

### **Performance indicators**

The determination of investment and operational costs, as well as benefits, enables the estimation of key performance indicators, namely the Net Present Value (NPV), Internal Rate of Return (IRR) and the benefit-cost ratio (B/C). The estimation of the indicators and their interpretation are described in more detail below.

The **Net Present Value** (NPV) of a project is the sum of the discounted total benefits and costs of a project. The NPV is a very concise performance indicator: it represents the present amount of the net benefits (i.e. benefits less costs) flow generated by the project expressed in one single value.

The aggregation of costs and benefits occurring in different years (B - C) can be carried out by weighting them through the discount rate (d) to obtain their present value.

$$NPV = \sum_{i=1}^n \frac{(B - C)_n}{(1 + d)^n}$$

A positive NPV means that the project generates a net benefit (because the sum of the weighted flows of costs and benefits is positive) and it is desirable. When different options are considered, as in our case, the ranking of the NPVs of the alternatives indicates which one is the best from a financial point of view.

The **Internal Rate of Return** (IRR) is defined as the discount rate that zeroes out the net present value of flows of costs and benefits of a project, that is to say the discount rate of the equation below:

$$NPV = \sum_{i=1}^n \frac{(B - C)_n}{(1 + IRR)^n} = 0$$

The Internal Rate of Return is an indicator of the relative efficiency of a project that should be used with caution as there may be multiple IRRs for a single project. On the other hand, it has the advantage of being a pure number and this allows for a simple comparison of projects regardless of their size.

The **benefit-cost ratio** (B/C) is the present value of project benefits divided by the present value of project costs:

$$B/C = \frac{PV(B)}{PV(C)}$$

When this ratio is bigger than the present value, the benefits are greater than the costs and the project is desirable.

## General parameters and assumptions

This section details general parameters and assumptions of the CBA model, i.e. they are applicable for all or several cost and benefit items. Specific parameters and assumptions are detailed in the sections below with the description of each cost and benefit component.

- The CBA is conducted from the point of view of the infrastructure owner, i.e. it takes into account costs and benefits for the Member States, but excludes costs and benefits for VE-TCNs and carriers. It is acknowledged that:
  - VE-TCNs will bear the costs of the additional time needed to fill-in ETIAS applications and will also have to pay the fee, however at the same time they will benefit from avoided trips to and back from the border in case of prior refusal via ETIAS;
  - Carriers will also benefit from less costs for taking back travellers refused at the border ("inadmissible arrivals") and less penalties as ETIAS allows also to check whether the traveller is correctly documented (for VE, a valid passport), however at the same time carriers will bear the costs of ETIAS connection.
- The CBA is done on the basis of cautious assumptions throughout the sizing: the estimates avoid accumulating "reserve buckets" at all levels but at the same time make assumptions that are always on the "safe side". As an example the current costs of technological components are applied over the whole time span while the trend is having a reduced cost for equivalent capacity or performance. This benefit was found too risky to quantify and the safe approach of keeping costs constant for equivalent performance was adopted.
- The current list of Visa Exempt countries (VE) contains 61 countries. The model does not cover countries that might become visa exempt in the future, however it is estimated that countries that are currently in the visa liberalisation process might increase the number of ETIAS applications by approximately 2.3 million<sup>266</sup>.
- The assumption on the timeline are :
  - By the end of 2016, the Commission issues the ETIAS legal proposal;
  - By the end of 2017, the co-legislators will adopt the Commission proposal;
  - Development starts after this adoption, which means from 2018 onwards;
  - The development can be performed over a 3-year period,
- Schengen acquis and its future development will apply to 30 countries, i.e.:
  - Schengen EU countries (Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain and Sweden);
  - Schengen non-EU countries (Iceland, Liechtenstein, Norway and Switzerland);
  - Accession countries working to implement the Schengen rules (Bulgaria, Croatia, Cyprus and Romania).
- The analysis evaluates the costs and benefits over a ten-year period following the assumption that the legislative proposal for ETIAS will be adopted by the end of 2017 and that ETIAS implementation will start in 2018. Thus, the CBA reference period is 2018 to 2027 which fits into the next EU Multi-annual Financial Framework.
- The assumption is made that ETIAS will follow a "big-bang" or uniform implementation approach: the system starts being operational in all the regions of the world in one go, be it from voluntary to mandatory or not. In case of gradual approach per region or border type, the maintenance costs during the first years of operations would be lower depending on how progressively the system would be rolled-out and the fee revenue would only be collected for travellers who are in the scope of application of ETIAS.
- Both the baseline and regulatory scenarios account for the historical based natural growth trend in foreign national arrivals. It is not anticipated that ETIAS fee will reduce demand for travel to Schengen Area.
- The assumption is made that ETIAS authorisation will be valid for two years, which is the most conservative approach out of the most favourable options proposed by Member States<sup>267</sup>. If the validity period of ETIAS authorisation was longer, the number of applications would be lower, as frequent travellers would have to re-apply for authorisation

---

<sup>266</sup> Estimation is based on number of uniform visa applications.

<sup>267</sup> During consultations Member States were mostly in favour of two to four years ETIAS validity period.

to enter less often. Lower number of ETIAS applications would result in lower revenues from ETIAS fee and lower operational costs because of e.g. smaller number of applications to be processed manually.

- The assumption is made that each ETIAS application will require the payment of a non-refundable amount of 5 euros. The amount is sufficiently small to avoid a lasting impact on tourism even coming from less affluent regions. Any change of this fee amount impacts benefits significantly.
- In order to ensure coherence and consistency of the EU legal framework it is envisaged that data entered in ETIAS would be retained for five years, as is the case for EES and VIS. In case of shorter data retention period, less storage would be required, but this would mean very marginal impact on hardware and software costs, because of overall low storage requirements (please see hardware costs estimation for further reference).
- It is assumed that some of the EES infrastructure components will be re-used, like TEST-ng network and National Uniform Interface (NUI), however the sizing of the database was performed as if it was built as a standalone database. This was considered as the most conservative approach as there is still a high uncertainty about how EES will be implemented.

## Cost model

This section provides a detailed description of the cost components and of the methodology for their estimation, including main assumptions and sizing parameters, as well as the outcome of the estimation. The following costs items are included in the model:

- Contractor development costs;
- Network costs;
- Hardware costs;
- Software costs;
- Administration costs;
- Costs of the meetings and training;
- Costs of the premises.

### Contractor development costs

#### Costs components

During the development phase, contractor development costs cover the costs for specifying, developing, testing till entry into operations, and the management of that project for the following software components which are described in section 2.4 "Architecture":

- ETIAS IT application;
- Traveller's application processor;
- The software that provides the "Internet services", composed of the website, mobile app, field validation logic, masked extraction of the central database, notification and mail server and carrier gateway(s);
- Search interface to other systems (EES, VIS, SIS);
- Customisation for ETIAS of the National Uniform Interface (NUI) assumed to have been developed for EES;
- The changes to software of other systems (VIS, SIS, EES, SLTD, TDAWN) as ETIAS will both access them for consultation and receive notifications of changes on existing data;
- Development of the safeguards to address security requirements.

During the operations phase, Contractor Development Costs cover the costs for software maintenance and evolutions of the system: again from drafting specifications till entry into operations.

The detailed descriptions of the components are provided in section 2.4.5 "ETIAS key IT architectural blocks" and section 2.6.6 "Safeguards" of the study.

The contractor development efforts include preparation of functional and technical system specifications, design, build, test activities, deployment and rollout as well as project management and quality assurance contracting.



## Methodology

The **development costs of the ETIAS IT application** are estimated through a top-down approach. The development cost estimation is built on the following assumptions:

- Applying a categorisation of processes defined by DG TAXUD, all processes are defined at a level of detail where a process solves a particular issue by transforming a defined business input into a defined and measurable business output via the execution of one or more process steps (i.e. tasks). This allows assigning the right estimate of development work per process.
- Updates to tasks and to messages lead to the same implementation effort.
- All tasks are assumed to be automated tasks, i.e. to be implemented by an IT system.

The development **costs of the traveller application processor, search interface to other systems** (EES, VIS and SIS) and **ETIAS Internet services** are estimated based on consultation with experienced developers.

The **costs of NUI** are determined based on the assumption that EES (NUI) will be re-used for the purpose of ETIAS, therefore only customisation costs of the EES NUI are included in the model. The customisation efforts are estimated as 50% of initial development and integration efforts. Customisation percentage was defined based on consultation with experienced developers. The NUI customisation costs cover:

- Customisation effort of the NUI to adapt it for the purpose of ETIAS;
- Integration effort necessary to enable the link between the NUI and the national border management systems already existing within the Member States, as well as all necessary infrastructure. The Member States' systems will have to be put in condition to comply with the standard created by the NUI and to pass communication and compliance tests. These costs are accounted as national expenses to be funded via ISF.

The costs of **the impact on the other systems (VIS, SIS, EES, SLTD, TDAWN)** are estimated based on the increased number of queries to those systems. Those costs cover development efforts needed to address new requirements, because of ETIAS implementation.

Development of the **safeguards to address security requirements** is estimated as a percentage out of all development efforts. The percentage is defined based on industry practice and amounts to 4%. This covers safeguards such as *SG.02 Access Control* and *SG.05 System acquisition, development and maintenance*, that are described in detailed in section 2.6.6 of the report.

## Sizing

Based on the methodology explained in the previous section, only the ETIAS IT application can be sized based on the development of other large-scale IT systems. The estimation of the costs of ETIAS IT application is based on the following sizing parameters:

- *Number of processes* is assumed to determine the effort for **Functional System Specifications** (FSS) activities.
- *Number of processes* where a change occurs is assumed to determine the effort for the **Technical System Specifications** (TSS) activities. Since ETIAS will be newly developed systems, as opposed to upgraded ones, a change will occur in all of the processes, therefore the number of processes and the number of processes where a change occurs is the same.
- *Number of tasks* in those processes: the number of tasks is assumed to determine the effort for the **Design-Build-Test** (DBT) activities.
- *Number of information exchanges* (messages/services): The number of new or updated information exchanges (messages) is assumed to also determine the effort for the **Design-Build- Test** (DBT) activities.
- *The number of interfaces adds an effort percentage to the DBT activities.* The DBT effort is increased by an additional 3% per changed interface to another existing system (e.g. if the project needs to change 3 interfaces to other systems for instance, the effort is increased by 9%).

The percentages for FSS, TSS and DBT efforts estimations are based on the method used by DG TAXUD to estimate development costs and are provided in the table below on the basis of.

*Table 92: Cost elements computation methods used by the methodology of DG TAXUD*

<b>Cost elements</b>	<b>Computation method</b>
1. Deploy-rollout	<b>20%</b> of the Design-Build-Test (DBT)
2. Conformance Test activities	<b>20%</b> of the Technical System Specifications (TSS)
3. Project Management	<b>15%</b> of all above costs (DBT, TSS, deploy-rollout and conformance test activities)
4. Quality Assurance	<b>20%</b> of all above costs (DBT, TSS, deploy-rollout, conformance test activities and project management)

The sizing parameters in terms of number of processes, tasks, messages are summarised in the table below. The whole list of processes, tasks and messages for ETIAS is provided in the Annex 12. – "ETIAS sizing parameters".

*Table 93: Sizing parameters for ETIAS development costs estimation*

<b>Sizing parameter</b>	
Number of processes	7
Number of tasks	43
Number of messages	68
Interfaces to systems	5

As mentioned above, the development effort for the traveller application processor, search interface to other systems (EES, VIS and SIS) and ETIAS internet services were determined based on consultation with developers. During consultations the number of man-days needed to develop the component were determined based on high-level description of their functionalities.

The costs related to the maintenance of the Central System and NUI (i.e. costs of contractor operations) are estimated as a percentage (12.5%) from the initial development. The percentage is higher than average yearly development effort for large scale systems, because of the continued testing with carriers.

The model also takes into account the costs of ETIAS evolutions. Development work to address new requirements are estimated at 10% of the initial development efforts. The estimation should be revised once the requirements for the evolutions will be specified.

The tables below provide the results of the contractor development costs estimations.

Table 94: Results of the contractor development cost estimations

Investment phase			Operational phase							TOTAL
2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	

#### eu-LISA expenses

Central system												
Contractor development (Central System, interfaces, impact on other systems '000)	5,940	5,940	5,940	4,010	4,010	4,010	4,010	4,010	4,010	4,010	4,010	<b>45,887</b>

#### National expenses to be funded via ISF

National systems												
Contractor development (integration and operations of NUI, '000)	20,000	20,000	20,000	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500	<b>112,500</b>

<b>TOTAL</b>	<b>25,940</b>	<b>25,940</b>	<b>25,940</b>	<b>11,510</b>	<b>11,510</b>	<b>11,510</b>	<b>11,510</b>	<b>11,510</b>	<b>11,510</b>	<b>11,510</b>	<b>11,510</b>	<b>158,387</b>
--------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	----------------

### Network costs

#### Costs components

With regards secure network (TESTA-ng) costs, two types of costs have been identified based on existing network data for the VIS:

- One-time costs to create the communication link;
- Monthly costs to operate and maintain the communication link.

Four types of communication link have been identified:

- Member States' communication links (uniform interface) for conveying the messages for border control checks (so one verification of the existence of an ETIAS at each entry) and the exchange between the CMPE and Member States and back (so one Member State consultation and answer per case where one or more Member State(s) are consulted);
- Central Unit / Backup Central Unit (CU/BCU) communication links;
- Support Operation Centre / Central Services Domain (SOC/CSD) communication links;
- Communication links to the Central Manual Processing Entity (CMPE), because it is foreseen that CMPE will be able to connect directly to ETIAS central database.

Additional other costs (e.g. setup, security) were also taken into account.

As regards internet connection, the costs of its integration and monthly usage are included.

#### Methodology

The estimation of the internal secure network cost of ETIAS is based on figures and tariffs of TESTA-ng network, which is currently used for VIS. The structure of TESTA-ng network can serve

as a blueprint for the network of ETIAS, because both VIS and ETIAS exchange information through a network and consist in similar data emission/reception centres. At Member State level information is transmitted through border-management administrations, BCP and NUI, whereas at EC level the information is transmitted/received by Central Unit and Backup Central Unit. The estimation of internal secure network costs is further based on the following assumptions:

- The cost estimation of internal secure network is based on figures and tariffs of TESTA-ng network, which is currently used for VIS.
- Even though existing communication links of TESTA-ng network are not fully utilised and possibly could be used for the purpose of ETIAS, the costs for new communication links creation are added, because the consumption of the network is hardly predictable once not only ETIAS, but also EES will become operational.
- The costs of the communication links creation are added from the first year of development, because of network usage needs during the development phase for testing purposes. The network is not scaled-up on a yearly basis, as it is assumed that initial bandwidth capacity will be sufficient for the operational years under review.
- Other services (for set-up, enhanced security) will comprise 25% of network lines creation and maintenance costs, as is the case for VIS.
- Since contractual prices of TESTA-ng network are 50% lower than the average bidding price, a correction factor is applied for the estimation by increasing TESTA-ng prices by 50%.

The Internet costs are estimated based on consultation with Internet providers. The estimation is based on the following assumptions:

- The Internet connection will require the services of a Network Cloud Provider, which will supply load balancing over globally distributed points of presence (POPs), along with advanced threat/attack protection, but with no caching or visibility of the traffic. The Network Cloud Provider will route the traffic to and from BU and BCU sites hosting the application, as well as the third possible location e.g. datacentre in Luxembourg.
- The system will have interconnections with other sensitive/classified external systems (Europol, Interpol) as well, using VPN technologies and/or specialized Turnkey Access Points (TAPs).

## Sizing

The first estimation for the number of ETIAS applications is 40 to 51 million per year, which the system and the network must be able to service. There is currently no estimation of the actual data traffic requirements, but it is in the order of 20 – 1000 TB p.a.

The same number of communication links is foreseen for the ETIAS, as for VIS, except additional 2 more communication links for the Central Manual Processing Entity (CMPE).

## Results

The tables below provide the results of the network cost estimations.

*Table 95: Results of the network cost estimations*

	Investment phase			Operational phase							TOTAL
	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	
<b>eu-LISA expenses</b>											
Network development ('000)	3,968	-	-	-	-	-	-	-	-	-	<b>3,968</b>
Network operations ('000)	2,472	2,472	2,472	2,472	2,472	2,472	2,472	2,472	2,472	2,472	<b>24,725</b>
<b>TOTAL</b>	<b>6,441</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>2,472</b>	<b>28,693</b>

## Hardware costs

### Costs components

Two types of costs have been identified:

- One-time costs to acquire the hardware during the investment phase;
- Costs to operate and maintain the hardware during the operational phase.

The cost calculation takes into account the following environments:

- Production environment (applicable to CU and BCU);
- Pre-production environment (applicable to CU and BCU);
- Active-active set-up (applicable to CU), as defined in section 2.2.4 "General architecture" of the report;
- Playgrounds and testing environments (only applicable to CU).

The following types of hardware have been identified:

1. Database servers;
2. Application servers;
3. Other servers:
  - a. Search engine servers;
  - b. Virtualisation Servers (ESX);
  - c. Management Servers (MGT).
4. Enclosures and racks;
5. Network hardware:
  - a. Core Switches;
  - b. Front-End Switches;
  - c. Load Balancers;
  - d. Firewalls management station (MGT);
  - e. Firewalls Front-End etc.
6. Miscellaneous (e.g. UPS).

### Methodology

The estimation of the hardware costs of ETIAS has been done using existing VIS data to estimate the sizing of the two new systems. The comparison with the VIS is supported by similarities of the two systems. They both intervene in border-management processes at BCPs and have strong similarities in their respective service catalogues.

The costing of hardware is based on several assumptions:

- **Testing requirements:** ETIAS will require some IT infrastructure for testing purposes starting from the beginning of the development phase (2019). This hardware and software will be used for the purpose of operations starting from 2022, at which date playground and testing environments will be added.
- **SLA:** the SLA required will vary depending on the type of environment, so as to save on the overall cost. Production and pre-production servers, being business-critical environments, should require a high SLA, while playground and testing environments should require a low SLA. Also, playground and testing environments will not be redundant as opposed to production and pre-production environments.
- **Ratio between pre-production and production needs:** the pre-production environment should be similar to the production environment in terms of size and SLA, so as to allow testing and deploying of new releases under conditions virtually identical to the production environment itself.
- **Ratio between production and playground environment needs:** two playgrounds will be considered for this calculation. Playground 1 will be used for load/stress/performance tests, while Playground 2 will be used for functional testing. Playground 1 is assumed to represent 20% of the cost of the production environment, and Playground 2 is assumed to represent 15% of the cost of the production environment.
- **Testing environment needs:** learning from the experience of SIS and VIS, 16 testing environments will be considered for this calculation to allow for timely execution of tests by Member States. These environments will be provided by virtualisation technology.
- **Maintenance and evolutions:** routine maintenance costs of hardware components are estimated as 20% of the initial investment costs, whereas evolution costs are estimated as

10% of the initial investment costs. The latter ones should be revised, once requirements for the upgrade of the system will be defined.

- **Costs distribution over the development period:** the hardware was first sized for the 1<sup>st</sup> year of operational phase. For the development phase, the assumption is that the 1<sup>st</sup> year of development requires 20% of that estimated hardware cost as only the equipment necessary for development and testing is necessary and the remaining 80% are added the 3<sup>rd</sup> year as then the system needs to be made ready for operations and tests mimicking real conditions are also conducted in a pre-production environment.
- **Enhanced security measures:** hardware for the safeguards to address security requirements is estimated as a percentage out of all hardware costs. The percentage is defined based on industry practice and amounts to 4%. This covers safeguards such as SG.03 Cryptography, as described in detailed in section 2.6.6 "Safeguards".

## Sizing

VIS system was used as reference for the estimation of the main modules of ETIAS (IT application and search interface to other systems (EES, VIS, SIS). The number of required cores and the required amount of storage space have been adjusted to account for the differences in scope of the systems. The measurement is mainly based on three metrics that are given in the table below.

*Table 96: Main sizing parameters for the costs estimations of ETIAS IT application, traveller application processor, ETIAS internet services other hardware*

Parameter	Value
Max number of applications to be stored in the system, in millions (in case of 5 years data retention)	200
Queries in scope of the system per day in millions	7
Size of application file (in kb)	10

The number of cores per each module of the system are provided in the table below together with more detailed approach/ assumptions for estimation.

*Table 97: Number of cores and nodes for ETIAS hardware estimations*

Management Authority – production environment			
	Cores required for ETIAS <sup>268</sup>	Computing capacity nodes for ETIAS	Explanations/ comments
<b>[1] ETIAS IT application</b>			
Application servers	26	3	Benchmark with VIS; Δ in queries is applied for VIS data to get the number of cores for ETIAS IT application.
Search engine servers	154	13	Benchmark with VIS; Δ in queries, multiplied by number of applications, is applied for VIS data to get the number of cores for ETIAS IT application.
Database servers	31	3	
<b>[2] Traveller application processor</b>			
Application servers	26	3	Assumption that the number of tasks for ETIAS IT application will be similar to traveller application processor.

<sup>268</sup> By "core" we refer to the unit that is capable of reading and executing instructions. We realise that cores are usually made available in pairs or quadruples. However, since it is assumed the environment will be wholly or partially virtualized, we do not round-off the numbers here to even numbers, because core provisioning in a virtualized environment is quite flexible.

Database servers	12	1	Very small database will be needed for screening rules, therefore the costs of only one node with 12 cores are included.
<b>[3] Search interface to other systems (EES, VIS, SIS)</b>			
Servers for search interface	20	2	Benchmark with EES NUI.
<b>[4] ETIAS internet services</b>			
Database servers (for status of applications)	18	3	40% less cores foreseen than for ETIAS IT application, because only carriers' and travellers' connection through internet services.
Webservers	36	3	Number of cores defined based on consultation with vendor, based on potential number of connections.
<b>[5] National Uniform Interface</b>			
Application servers	72	6	Estimation is based on the assumption that EES NUI will be re-used for the purpose of ETIAS, therefore only 20% of the initial NUI costs are added.
Database servers	72	6	
<b>Other hardware for ETIAS</b>			
Virtualisation Servers (ESX)	12	3	Benchmark with VIS; median $\Delta$ of sizing parameters is applied for VIS data to get the number of cores for ETIAS.
Management Servers (MGT)	15	3	Benchmark with VIS; median $\Delta$ of sizing parameters is applied for VIS data to get the number of cores for ETIAS.

	<b>Number of items for other hardware for ETIAS</b>	<b>Explanations/ comments</b>
Enclosures	14	One enclosure holds 4 or 16 servers, depending on type + 2 enclosures are added for redundancy purpose.
Racks	5	Estimation is based on number of enclosures; each rack can include 3 enclosures.
Core Switches	4	Double higher number of nodes as for VIS foreseen, because of additional modules like traveller application processor, internet services etc.
Front-End Switches	4	Double higher number of nodes as for VIS foreseen, because of additional modules like traveller application processor, internet services etc.
Load Balancers	4	Double higher number of nodes as for VIS foreseen, because of additional modules like traveller application processor, internet services etc.
Firewalls management stations	8	Double higher number of nodes as for VIS foreseen, because of additional modules like traveller application processor, internet services etc.
Firewalls Front-End	4	Double higher number of nodes as for VIS foreseen, because of additional modules like traveller application processor, internet services etc.
Miscellaneous		10% of total HW costs added.

Hardware for other systems			
	Cores required for ETIAS	Nodes for ETIAS	Explanations/ comments
Servers for EES	5	1	Estimation is based on the assumption that the number of cores required for EES will be amount to 20% of the cores for ETIAS IT application.
Servers for SIS	5	1	Estimation is based on the assumption that the number of cores required for SIS will amount to 20% of the cores for ETIAS IT application.
Servers for VIS	3	1	Estimation is based on the assumption that the number of cores required for VIS will amount to 10% of the cores for ETIAS IT application.
Servers for Interpol systems	5	1	Estimation is based on the assumption that the number of cores required for Interpol systems will amount to 20% of the cores for ETIAS IT application.

## Results

The table below provides the results of the hardware cost estimations to be covered by eu-LISA.

*Table 98: Results of the hardware cost estimations*

Investment phase			Operational phase							TOTAL
2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	

### eu-LISA expenses

<i>Central system</i>											
Hardware ('000)	1,932	343	8,743	1,829	1,829	1,829	1,829	1,829	1,829	1,829	23,822

## Software costs

### Costs component

Two types of costs have been identified:

- One-time costs to acquire software licences during the investment phase;
- Costs to operate and maintain software during the operational phase.

The same as in hardware costs estimation, software cost calculation takes into account different environments, namely production and pre-production environment with active-active set-up in the CU, as well as playgrounds and testing environments.

The software was first sized for the 1<sup>st</sup> year of operational phase. For the development phase, the assumption is that the 1<sup>st</sup> year of development requires 20% of that estimated software cost, and the remaining 80% are added the 3<sup>rd</sup> year.

The table below lists the categories of software licences necessary for the functioning of the IT infrastructure.



Table 99: Overview of the categories of software licences and of their impact on the overall cost of the IT system

	Category of software licences	Impact on the overall software cost
1.	Search Engine	Very high
2.	Database software	High
3.	Application and Messaging software	High
4.	Virtualisation server	Medium/low
5.	Storage	Medium/low
6.	Helpdesk and support	Medium/low
7.	Operating System	Low
8.	Security	Low
9.	Directory Server software	Low
10.	Monitoring and administration software	Low
11.	Other licences	Low

## Methodology

The estimation of the software costs of ETIAS has been carried out following a bottom up approach by using existing VIS data to estimate the sizing of the new systems.

The cost of the Search Engine licence, the biggest cost items of the software, has been estimated through consultations with vendors and by looking at the VIS experience. The cost of the database and application software licences has been estimated by applying the prices of the DIGIT's software framework contract to the number of cores estimated with the hardware sizing.

The total SW cost is driven by the fact that it needs to be implemented in five environments (a production CU (with redundancy counts as two) and BCU, a pre-production CU (without redundancy) and BCU,). Most software costs are therefore multiplied by five and this both during development and operations. During the operations phase maintenance requires the continuous availability of these five environments. On top of these environments there are two so-called "playground" environments and a testing environment but requiring less software licences than the other environments.

Software for safeguards to address security requirements is estimated as a percentage out of all software efforts. The percentage is defined based on industry practice and amounts to 4%. This covers safeguards such as *SG.02 Access Control* and *SG.05 Cryptography*, that are described in detailed in section 2.6.6 "Safeguards".

## Sizing

The same sizing estimation applies for the software costs estimation as for the hardware, which are outlined in the section above.

## Results

The tables below provide the results of the software cost estimations to be covered by eu-LISA.

Table 100. Results of the software cost estimations

Investment phase			Operational phase							TOTAL
2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	

**eu-LISA expenses**

Central system												
Software licenses ('000)	8,862	1,974	38,352	10,075	10,075	10,075	10,075	10,075	10,075	10,075	10,075	109,638

**Administration costs**

**Costs components**

The term "Administration costs" is somewhat misleading as in fact it mainly covers the costs of technical staff required to build and operate the system. It is to be understood as the cost for the administration to deliver the services. Administration costs consist of the components listed below.

- **Central system related costs:**
  - Expenditure on the staff that would be responsible for budget grants management and fee distribution, as well as staff for the program/ project, contract management, contract;
  - Costs of additional staff needed with specific technical expertise (solution architect, system architect, SOA architect, database designer, application administrator, system administrator, network administrator, test engineer, security officer);
  - Costs of additional staff needed to monitor central system and provide helpdesk support for Member States and carriers (24/7);
  - Staff costs of the Central Manual Processing Entity (CMPE);
  - Legal expenses for CMPE;
  - Administrative ICT expenses for CMPE and teams in Member States, involved in PNR/ API processing (e.g. telecommunication costs, infrastructure for work stations etc.);
  - Information campaigns to inform the general public about the implementation of ETIAS, including translation costs.
- **National systems related costs:**
  - Expenditure on the staff that would be responsible project/system management, grants administration, integration, testing etc. at national level;
  - Costs of the additional staff for teams in Member States, involved in PNR/ API processing, including staff that will handle applications manually, as well as managerial staff;
  - Costs of liaison officers (seconded national experts);
  - Administrative ICT expenses for the additional staff for teams in Member States, involved in PNR/ API processing (e.g. telecommunication costs, infrastructure for work stations etc.).

**Methodology**

The bottom-up approach is used for estimating administration costs. First of all, the sizing parameters are determined and then multiplied with pricing parameters.

**Sizing**

The main sizing parameter for administration costs is a full-time equivalent (FTE). The estimated need of FTEs per profile is provided in the table below.

**Central system related costs**

The need for FTEs for **eu-LISA** and **DG Home** has been defined based on eu-LISA and DG Home experience with large-scale trans-European systems (VIS and SIS). A higher number of technical experts and testers is proposed for eu-LISA than e.g. for EES, because of the high complexity of ETIAS architectural blocks, the high number of interfaces to other systems, as well as the continuous need for testing with carriers.

The number of FTEs for **the Central Manual Processing Entity (CMPE)** is defined based on the assumption that 5% of all applications will be processed manually and that it will take on average 10 minutes to process one application. Helpdesk support team for VE-TCNs at CMPE is defined based on the assumption that 0.5% of all applications will raise requests/ questions to the helpdesk team and that it will take 5 minutes for them to answer to the request. 10% more FTEs are foreseen for managerial positions and on top of that 15% for DPO, legal advice, audit, monitoring, HR, procurement, finance, IT support, appeals officers and other positions.

Managerial and support staff are assumed as temporary agents and other staff as contract agents. More information about the functions and structure of the CMPE is provided in section 2.3.4 *Four main processes* of the study.

The managerial and support staff at the CMPE will start working half a year before ETIAS becomes operational, whereas remaining staff will start working 4 months before ETIAS becomes operational.

Administrative ICT costs for CMPE and teams in Member States, involved in PNR/ API processing, would cover telecommunication, administrative hardware and software among other costs. The assumption is made that these costs would amount to EUR 10.000 per staff member per year.

In addition, legal expenses for the CMPE are included to cover expenses of potential appeals. It is assumed that there would be around 10 court cases per year and the costs of one case would amount to EUR 12.000 on average.

It is assumed that the costs of information campaign and translations will be 50% higher than the costs of eTA information campaign, given higher number of travellers in scope of the system, i.e. larger target audience to reach. The information campaign will start during the last year of development and will continue for the first years of ETIAS operations.

### **National systems related costs**

The need for FTEs for project management, grants administration and other functions at Member State level has been determined on the basis of consultation with experts who are experienced in developing and operating national systems in such a scale.

The size of additional staff for teams in Member States involved in PNR/ API processing is defined on the assumption that they will have to process 3% of all ETIAS applications and that it will take 30 minutes<sup>269</sup> for them to process 1 application. 10% more FTEs are added for managerial positions. Since it is assumed that applications will be processed manually at Member State level in existing organisation, no additional support functions are foreseen.

The additional staff for teams in Member States involved in PNR/ API processing will be hired 4 months before ETIAS becomes operational, whereas managerial staff will be hired half a year in advance.

The FTEs expected to be required to support operations of systems take into account the need to provide a 24/7 service, i.e. an uninterrupted service at all times. A 24/7 helpdesk support factor amounting to five is calculated based on the assumption that there are 220 working days per year and eight working hours per day.

The main pricing parameter is the average salary for permanent staff, including basic salary, employer fees, benefits, and average contractual fee per day for contractual staff. In addition to average employment costs, shift allowances are included for staff who will provide 24/7 service.

---

<sup>269</sup> Member States indicated that it takes from 1 to 4 hours to resolve complicated cases for Passenger Information Units (PIUs). The shorter duration is selected for ETIAS, because automation of certain process steps e.g. automated checks done.

Table 101. Components and sizing parameters of staff costs

Cost component	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027
----------------	------	------	------	------	------	------	------	------	------	------

**Parameters for DG Home expenses**

<i>Central system</i>										
Management of ISF funds (FTE)	3	3	3	3	3					
ETIAS fee distribution (FTE)				1	1	1	1	1	1	1
<b>TOTAL</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>4</b>	<b>4</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>

**Parameters for eu-LISA expenses**

<i>Central system</i>										
Program/ project management (FTE)	4	4	4	4	4	4	4	4	4	4
Contract management (FTE)	2	2	2	2	2	2	2	2	2	2
Quality assurance (FTE)	1	1	1	1	1	1	1	1	1	1
Technical experts (FTE): <ul style="list-style-type: none"> <li>• Solution Architect</li> <li>• System Architect</li> <li>• SOA Architect</li> <li>• Database designer</li> <li>• Application Administrator (x2)</li> <li>• System Administrator</li> <li>• Network administrator (x2)</li> <li>• Security Officer</li> </ul>	10	10	10	10	10	10	10	10	10	10
Testing (FTE)		2.5	5	5	5	5	5	5	5	5
Helpdesk support (1st line, <u>24/7 factor taken into account</u> ) (FTE)			5	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)
Operators monitoring the Central System ( <u>24/7 factor taken into account</u> ) (FTE)			5	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)	10 (2x5)
<b>TOTAL</b>	<b>17</b>	<b>19.5</b>	<b>32</b>	<b>42</b>	<b>42</b>	<b>42</b>	<b>42</b>	<b>42</b>	<b>42</b>	<b>42</b>

**Parameters for national expenses to be funded via ISF**

<i>National systems</i>										
Technical system management (FTE)	15 (30x0.5)	15 (30x0.5)	15 (30x0.5)	2.5						
Project/ grants administration (FTE)	15 (30x0.5)	15 (30x0.5)	15 (30x0.5)	2.5						
Technical expertise (FTE)	30 (30x1)	30 (30x1)	30 (30x1)	5						
Testing (FTE)			30 (30x1)	5						
<b>TOTAL</b>	<b>60</b>	<b>60</b>	<b>90</b>	<b>15</b>						

2020 <sup>270</sup>	2021	2022	2023	2024	2025	2026	2027
---------------------	------	------	------	------	------	------	------

**Parameters for expenses of the EU body to be in charge of Central Manual Processing Entity**

<i>Central system</i>								
Number of new applications if the validity period of the application is 2 years ('000)	0	40600	35870	37230	38590	39950	41412	42908
Number of ETIAS applications to be processed manually ('000)	0	2030	1794	1862	1930	1998	2071	2145
Number of requests for helpdesk support from the Central Manual Processing Entity ('000)	0	203	179	186	193	200	207	215
Staff of the Central Manual Processing Entity that will process ETIAS applications manually (FTEs)	64	192	192	192	192	192	196	203
Helpdesk support staff for VE-TCNs at Central Manual Processing Entity (FTEs)	3	10	10	10	10	10	10	10
Managerial staff of the Central Manual Processing Entity (FTEs)	10	20	20	20	20	20	21	21
Support staff (DPO, legal advice, audit, monitoring, HR, procurement, finance, IT support etc.) at the Central Manual Processing Entity (FTEs)	17	33	33	33	33	33	34	35
<b>TOTAL number of staff for CMPE (FTEs)</b>	<b>94</b>	<b>255</b>	<b>255</b>	<b>255</b>	<b>255</b>	<b>255</b>	<b>260</b>	<b>270</b>

**Parameter for national expenses to be funded either by national budgets or national programmes in the ISF funds**

<i>National systems</i>								
Number of ETIAS applications that will raise requests to teams in Member States, involved in PNR/API processing ('000)	0	1218	1076	1117	1158	1199	1242	1287
Additional staff for teams in Member States, involved in PNR/API processing (FTEs)	87	346	346	346	346	346	353	366
Managerial staff for teams in Member States, involved in PNR/API processing (FTEs)	17	35	35	35	35	35	35	37

<sup>270</sup> The number of FTEs is equivalent to the number of staff in 2021 hired few months in advance before the launch of the system. It is assumed that staff that will process ETIAS applications manually and helpdesk support staff will be hired 4 months in advance, whereas managerial and support staff will be hired half a year in advance.

<b>TOTAL number of staff for teams in Member States, involved in PNR/API processing (FTEs)</b>	<b>104</b>	<b>381</b>	<b>381</b>	<b>381</b>	<b>381</b>	<b>381</b>	<b>381</b>	<b>388</b>	<b>402</b>
--	------------	------------	------------	------------	------------	------------	------------	------------	------------

## Results

The tables below provide the results of the estimations under the heading "administration costs" for DG Home, eu-LISA, the EU body to be in charge of Central Manual Processing Entity and the teams in Member States, involved in PNR/ API processing.

DG Home expenses are estimated to decrease in 2023, because there will be no need to manage ISF funds further. eu-LISA administrative expenses will increase significantly with the start of operations, because of the need for 24/7 support to Member States and carriers, as well as operators to monitor the system. There are costs for CMPE in the last year of the development phase, because it is assumed that the staff will be hired a few months in advance before the start of operations.

*Table 102: Results of the administration cost estimations)*

	Investment phase			Operational phase							TOTAL
	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	
<b>DG Home expenses</b>											
<i>Central system</i>											
Administration ('000)	402	402	402	536	536	134	134	134	134	134	<b>2,948</b>
<b>eu-LISA expenses</b>											
<i>Central system</i>											
Administration ('000)	2,278	2,453	3,325	4,207	4,207	4,207	4,207	4,207	4,207	4,207	<b>37,507</b>
<b>Expenses of the EU body to be in charge of Central Manual Processing Entity</b>											
<i>Central system</i>											
Administration ('000)	-	-	12,294	26,897	26,897	25,877	25,877	25,877	26,392	27,341	<b>197,453</b>
<b>National expenses to be funded via ISF</b>											
<i>National systems</i>											
Administration ('000)	9,240	9,240	18,047	22,103	19,793	19,793	19,793	19,793	20,188	20,918	<b>178,905</b>
<b>TOTAL</b>	<b>11,920</b>	<b>12,095</b>	<b>34,068</b>	<b>53,743</b>	<b>51,433</b>	<b>50,011</b>	<b>50,011</b>	<b>50,011</b>	<b>50,922</b>	<b>52,600</b>	<b>416,813</b>

## Meetings costs

### Costs components

Meeting costs include:

- Comitology meetings;
- Committee/sub-group meetings with national experts to discuss issues specific to Member States;
- Management Authority (eu-LISA) monthly progress meetings during the development phase of the system and quarterly when the system is operational;
- COM meetings for grant management and missions for auditing grants at Member

- States;
- Advisory groups.

## Methodology

The meeting costs are estimated based on a bottom-up approach, i.e. the need for the meetings is determined based on DG Home and eu-LISA experience. Once the number of meetings was determined, it was multiplied by the number of participants and costs for one participant.

## Sizing

The main sizing parameter for meeting costs is the number of meetings per year. It is also assumed that there will be one expert per Member State in the meetings (i.e. 30 participants). The cost per meeting when participants from Member States are reimbursed for expenses is 20 k€.

The sizing parameters are presented in the table below.

*Table 103: Sizing parameters of meeting costs estimation*

Cost component	Unit	Parameter	Source
<b>DG Home expenses</b>			
<i>Central System</i>			
Comitology meetings	# per year	10	DG HOME
Committees/sub-group meetings with national experts per year during development	# per year	25	DG HOME
MA Monthly Progress meetings during development	# per year	10	DG HOME
<b>eu-LISA expenses</b>			
<i>Central System</i>			
Committees/sub-group meetings with national experts per year during development	# per year	25	DG HOME
MA Monthly Progress meetings during development	# per year	10	DG HOME
MA Quarterly Meetings during operations	# per year	4	DG HOME
Advisory groups	# per year	4	DG HOME

## Results

The table below provide the results of the meetings costs estimations.

*Table 104: Results of the meetings costs estimations*

	Investment phase			Operational phase						TOTAL	
	2018	2019	2020	2021	2022	2023	2024	2025	2026		2027
<b>DG Home expenses</b>											
<i>Central system</i>											
Meeting costs ('000)	323	323	323	323	323	200	200	200	200	200	<b>2,615</b>
<b>eu-LISA expenses</b>											

Central system												
Meeting costs ('000)	819	819	819	168	168	168	168	168	168	168	168	<b>3,633</b>

TOTAL	<b>1,142</b>	<b>1,142</b>	<b>1,142</b>	<b>491</b>	<b>491</b>	<b>368</b>	<b>368</b>	<b>368</b>	<b>368</b>	<b>368</b>	<b>368</b>	<b>6,248</b>
-------	--------------	--------------	--------------	------------	------------	------------	------------	------------	------------	------------	------------	--------------

## Training costs

### Costs components

Training costs cover training for border guards on the new process steps and new functionalities of the system.

Handover of ETIAS to eu-LISA during which the functionalities of the system should be introduced as well as business training are included in the salary costs estimation. Training for the staff of the Central Manual Processing Entity and teams in Member States involved in PNR/ API processing are also included in the salary costs estimation, therefore not calculated separately under this section.

### Methodology

Expenditure on training for border guards are estimated based on a bottom-up approach, i.e. expected number of staff to be trained is calculated and then it is multiplied by average costs per training.

### Sizing

Based on a survey to border-management authorities done in another project, it was determined that around 50.000 border guards would be trained just before the launch of ETIAS. The average cost per training is determined by the market price for large-scale IT projects training. The average cost per training and per person has been estimated at 200 euros.

### Results

The table below provides the results of the training cost estimations that would be funded either by national budgets or national programmes in the ISF.

*Table 105: Results of the training cost estimations*

Investment phase			Operational phase							TOTAL
2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	

#### National expenses to be funded either by national budgets or national programmes in the ISF funds

National systems												
Training costs ('000)	-	-	10,000	-	-	-	-	-	-	-	-	<b>10,000</b>

## Costs of the premises

### Costs components

This cost category covers the following components:

- Setup and operational costs of the central and backup central site (in Strasbourg, France and Sankt Johann im Pongau, Austria);
- Office space to host external contractor development team, as well as additional staff for eu-LISA;



- Office space for the Central Manual Processing Entity.

The Cost Model excludes datacentre space costs for hosting national systems as well as costs for renting or acquiring office space for national authorities, based on the assumption that existing spaces will be used. Office space costs for the teams in Member States involved in PNR/ API processing PIUs are included in the annual staff costs estimation (please see the section on administrative costs above).

## Methodology

The assumption cannot be made that existing datacentre and office space would be available for hosting the additional staff required centrally to deliver ETIAS.

Therefore the setup and operational costs of the datacentre space are estimated in the paragraphs below by multiplying the need for datacentre space in square metres with the setup and operational costs per square metre. Accordingly the office space costs for the external contractor development team and Central Manual Processing Entity are estimated by multiplying the need for office space in square metres with average operational costs per square metre.

## Sizing

The need for datacentre space is defined based on eu-LISA experience with other large scale trans-European systems and amounts to 52.5 sq. meters.

Office space requirement for 1 person is defined as per Statement of Minimum Future Requirements developed by Deloitte and amounts to 12 sq. meters. This requirement is multiplied by number of additional staff indicated in *Table 99. Components and sizing parameters of staff costs.*

## Results

The tables below provides the results of office and datacentre space cost estimations.

*Table 106: Results of the premises costs estimations*

Investment phase				Operational phase							TOTAL
2018	2019	2020	2021	2022	2023	2024	2025	2026	2027		
<b>eu-LISA expenses</b>											
<i>Central System</i>											
Costs of the premises ('000)	1,061	798	798	644	644	644	644	644	644	644	<b>7,168</b>
<b>Expenses of the EU body to be in charge of Central Manual Processing Entity</b>											
<i>Central System</i>											
Costs of the premises ('000)	-	-	1,129	1,129	1,129	1,129	1,129	1,129	1,151	1,193	<b>9,115</b>
TOTAL	1,061	798	1,927	1,773	1,773	1,773	1,773	1,773	1,796	1,837	<b>16,283</b>

## Benefits valuation

ETIAS implementation would offer more **individualised risk assessment of VE-TCNs, better data tracking and intelligence**, therefore resulting in **increased levels of safety and security** in the Schengen Area. Even though these are considered as the main benefits of the

implementation of ETIAS, they could be hardly expressed in monetary terms. Therefore the following sections only detail the quantifiable benefits of ETIAS which are only a part of the benefits.

## Time savings

### Description

Border guards would benefit from the implementation of ETIAS in terms of time savings, because they will not have to interact with the travellers who will avoid trips to and back from the border due to prior refusal of entry via ETIAS.

### Methodology

Benefit from time savings is calculated based on a bottom-up approach, i.e. assumptions on time savings have been done and then they were multiplied by the average wage to get a monetised expression of the benefit.

### Sizing

The main sizing parameter for the time savings estimation is the number of avoided trips. This parameter is afterwards multiplied by an assumption on the duration of the trip and the average wage in VE countries, as well as the average wage paid to border guards.

*Table 107: Sizing parameters for time savings estimation*

Parameter	Unit	Value	Source
Time savings to the border guard for handling a refusal of entry case	Hour	2	MSs Border Management Authorities
Average hourly wage paid to the border guard in the Schengen Area	EUR	17	MSs Border management authorities (provided 2.720 EUR as monthly wage)
Monetary benefit from time savings for border guards to handle one refusal of entry	EUR	34	Estimation based on the assumptions provided above
% of VE-TCNs out of all TCNs crossing the air border	%	57	Technical Study of Smart Borders, data collected by MS during week 20 of 2014
% of VE-TCNs out of all TCNs crossing the land border	%	10	Technical Study of Smart Borders, data collected by MS during week 20 of 2014
% of VE-TCNs out of all TCNs crossing the sea border	%	62	Technical Study of Smart Borders, data collected by MS during week 20 of 2014

	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027
Number of refusals of entry for TCNs	130	135	139	144	149	154	159	165	171	177

at external borders ('000) <sup>271</sup>										
Number of refusals of entry for TCNs at external air borders ('000)	48	48	49	49	50	50	51	51	52	52
Number of refusals of entry for TCNs at external land borders ('000)	76	79	82	86	90	94	98	102	107	111
Number of refusals of entry for TCNs at external sea borders ('000)	7	7	8	8	9	10	10	11	12	13
% of VE-TCNs who will avoid trips to BCPs due to prior denial through ETIAS <sup>272</sup>	-	-	-	-	70%	75%	80%	85%	90%	95%

## Results

The table below summarises the estimation of the time saving benefit for border guards.

*Table 108: Results of time savings estimation*

	Investment phase			Operational phase							TOTAL
	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	
Benefit from time savings for border guards ('000)	-	-	-	989	1,014	1,114	1,219	1,329	1,446	1,568	<b>8,679</b>

## ETIAS fee

### Description

As described in section 2.5.2 "Interacting with travellers", VE-TCNs will be required to pay a fee for processing their application via ETIAS. The fee will be collected in order:

- To limit fraudulent applications;
- To cover annual operational costs of ETIAS.

### Methodology

<sup>271</sup> Projection based on number of refusals of entry provided in Frontex Risk Assessment, 2016.

<sup>272</sup> Assumption confirmed by Member States.

The fee of **EUR 5** was assumed, so that the annual operational costs of ETIAS would be fully covered by the fee revenues. The fee is competitive with fees collected by Travel Authorisation Systems in other countries such as the US and Canada and is much lower than the Schengen visa fee. Therefore it is assumed that it will not have any impact on tourism.

## Sizing

The main sizing parameter used for the ETIAS fee revenues estimation is the expected number of ETIAS applications during the operational period under review. The VE-TCN travellers flow is forecasted by applying a moving average method taking the estimations provided in the Technical Study on Smart Borders as basis. The number of ETIAS applications is expected to be lower than the projected number of travellers from the second year of the system operations, due to the assumption that ETIAS authorisations would be valid for two years.

It is important to note that the forecast does not take into account possible changes in relation to visa liberalisation. These changes would increase the number of travellers and the number of applications.

*Table 109: Sizing parameters for ETIAS fee revenues estimation*

	Investment phase			Operational phase					
	2019	2020	2021	2022	2023	2024	2025	2026	2027
Number of VE travellers (in millions) <sup>273</sup>	37.5	39	40.6	42.2	43.8	45.4	47	48.7	50.5
Number of ETIAS applications with 2 years data validity (in millions)	-	-	-	42.2	37.23	38.59	39.95	41.41	42.9

## Results

The tables below summarise the results of fee revenues estimations.

*Table 110: Results of ETIAS fee revenues estimation*

	Investment phase			Operational phase							TOTAL
	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	
ETIAS fee revenues ('000)	-	-	-	203,000	179,350	186,150	192,950	199,750	207,060	214,540	<b>1,382,800</b>

## Sensitivity analysis

This section of the study provides the results of the sensitivity analysis, which identifies the critical variables of the project. Such variables are those whose variations, be they positive or negative, have the largest impact on the costs and benefits of the project. In ETIAS case, the most critical variables are the following:

<sup>273</sup> Technical Study on Smart Borders (2014).

- **The number of VE travellers:** if the number of travellers was 10% lower than assumed in the estimations, the overall costs would be 5% lower and the benefits would be 10% lower. The investment rate of return (IRR) would amount to 29%, i.e. it would lower by 4 percentage points and cost-benefit ratio (B/C) would amount to approximately 1.5, i.e. it would be lower by 10 percentage points.
- **Percentage of the applications to be processed manually:** if 10% of all applications were processed manually, instead of 5% that are foreseen in the model, this would almost double the costs of the CMPE. This would also increase the total costs significantly – by 23%, as CMPE costs comprise very large share in the total costs. IRR would decrease to 23%, whereas B/C ratio would decline to 1.3.
- **Time needed to process 1 application manually at CMPE:** if it took 12 minutes, instead of anticipated 10 minutes, to process 1 application manually, the administrative and premises costs of CMPE would be 18% higher and total costs of ETIAS would be 5% higher. The total cost calculation is very sensitive for this parameter. The average 10 minutes per case is a conservative estimate compared to other benchmarks.
- **ETIAS fee:** 1 EUR decrease in fee would result in 25% reduction of ETIAS fee revenues. If ETIAS was made available for free for children under 12 years old and if they comprise 15% share of all travellers, this potentially would lower the fee revenues by around 18%. IRR would decrease to 31%, whereas B/C ratio would decline to 1.53.
- **Maintenance costs of hardware and software:** if the percentage for the maintenance costs of hardware and software was increased to 25%, instead of 20%, this would result in 10% increase of overall software costs and 8% increase in hardware costs, however the impact on total costs of ETIAS would be negligible. It would amount to only 2% increase.
- **Costs for ETIAS evolution:** if 15% margin for ETIAS evolution was foreseen, instead of 10%, this would result in IRR decrease by 1 percentage point and B/C ratio decrease by 5 percentage points.
- **Validity period of ETIAS application:** if the validity period for the ETIAS application was extended to 5 years (rather than 2 years in the current computation), the workload for CMPE and teams in Member States, involved in PNR/ API processing would decline gradually for the first 4 years of ETIAS operations, due to the declining number of new applications. Therefore administrative costs of CMPE would decrease by 13% and administrative costs of teams in Member States, involved in PNR/ API processing would decrease by 11%. The maximum storage requirements and processing power requirements could be lower in case of the longer validity period for ETIAS. This could result in an approximately 9% decrease of hardware costs, 2% decrease of software costs and 7% decrease of overall costs. Since a lower proportion of travellers would require ETIAS, the revenues would be also lower by 11 percentage points. At the end the revenue decrease (about EUR 154 million over 10 years) would be more important than the cost decrease (about EUR 52 million). At the end the IRR would decline to 33%, whereas B/C ratio would decrease to 1.6.
- **Transition period for ETIAS application:** in case of a 1-year transition from voluntary to mandatory, it is assumed that only 20% of travellers will use the application. This would have a significant impact (of around 13% decrease), on administrative costs, because less staff will be needed for CMPE and teams in Member States, involved in PNR/ API processing, technical managers and other staff at the first years of operations. Total cost would thus amount to approximately 735 million euros. The collected revenues from the ETIAS fee would be also by approximately 7 percentage points lower, because of lower number of applications.

## Annex 12. – ETIAS sizing parameters

Table 111: ETIAS sizing parameters in terms of processes, tasks and messages

Process	Task	Request	Response
<b>Application</b>	Create application	v	v
	Check application	v	v
	<i>Variant: confirm application, return application</i>		
	Masked extraction of the central database	v	v
	Update of the masked extraction database	v	v
	Payment of application request	v	v
	<i>Variant: confirm payment, reject payment</i>		
<b>Decision</b>	Query SIS	v	v
	Query EES	v	v
	Query VIS	v	v
	Query SLTD	v	v
	Query TDAWN	v	v
	Query risk engine watchlist	v	v
	Create risk assessment rules	v	v
	<i>Variant: delete the rules, update the rules</i>		
	Perform risk assessment	v	v
	Create application decision	v	v
	<i>Variant: discontinue assessment, grant authorisation, flag authorisation, refuse authorisation</i>		
<b>Modification of application decision</b>	Correct application decision	v	v
	<i>Variant: close application, grant authorisation, flag authorisation, refuse authorisation</i>		
	Delete decision	v	v
<b>Notification</b>	Notify Central Manual Processing Entity	v	v
	Notify teams in Member States, involved in PNR/ API processing	v	v
	Notify applicant	v	v
<b>Usage of data</b>	Check status	v	v
	<i>Variant: by traveller, by carrier</i>		
	Search application examination	v	v
	Counter terrorism search	v	v
	MS administration search	v	v
	Retrieval	v	v
	<i>Variant: application examination</i>		
Retrieve application with full decision history	v	v	
<b>Reporting</b>	Define report	v	v
	<i>Variant: read, delete, update report definition</i>		
	Execute report	v	v
	<i>Variant: schedule report execution, delete report execution, read report execution</i>		
	Execute ad-hoc report	v	v

Process	Task	Request	Response
	Search report by authorized user	v	v
	Automated deletion report	v	v
	Automated log entry deletion report	v	v
<b>Support to end-users</b>	Open support ticket	v	v
	Close support ticket	v	v
	Transmit to MS	v	v
<b>Total number of processes</b>	<b>Total number of tasks</b>	<b>Total number of messages</b>	
<b>7</b>	<b>43</b>	<b>68</b>	

## HOW TO OBTAIN EU PUBLICATIONS

### Free publications:

- one copy:  
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:  
from the European Union's representations ([http://ec.europa.eu/represent\\_en.htm](http://ec.europa.eu/represent_en.htm));  
from the delegations in non-EU countries  
([http://eeas.europa.eu/delegations/index\\_en.htm](http://eeas.europa.eu/delegations/index_en.htm));  
by contacting the Europe Direct service ([http://europa.eu/eurodirect/index\\_en.htm](http://europa.eu/eurodirect/index_en.htm))  
or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (\*).

(\*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

### Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

### Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union  
([http://publications.europa.eu/others/agents/index\\_en.htm](http://publications.europa.eu/others/agents/index_en.htm)).





