Council of the European Union
General Secretariat

Brussels, 21 June 2024

WK 5835/2024 REV 1 DCL 1

LIMITE

VISA
FRONT
COMIX

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

DECLASSIFICATION

From:	German delegation
To:	Delegations
Subject:	Handbook on visa fraud

Delegations will find attached the declassified version of the above document. The content of this document is identical to the previous version.

Handbook Visa Fraud

Preventive measures and repressive control approaches

EMPACT

BUNDESPOLIZEI
FEDERAL POLICE

Proof of amendment

Responsibility:
Federal Police Headquaters
Section 34
Heinrich-Mann-Allee 103
14473 Potsdam

Version	Amendments	Entry into force
1.0	Initial creation	December 2023

Key findings

- Visa fraud facilitates bogus legal entry, accompanied by an uncontrolled influx of migrants into the Schengen area, associated in part with significant threats to public security.

- Combined with high financial profits, criminal networks actively, indirectly or directly influence the visa issuing process.

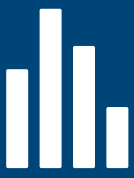
- Through the common Schengen area, all Schengen states are affected (to varying degrees) by transit/secondary migration caused by this phenomenon.

- A uniform legal offence in all EU member states is indispensable for a targeted and effective fight against visa evasion. First of all, a common (working) definition of visa fraud in the EU must be established.

- Valid phenomenon-related and EU-wide statistics as well as a standardised active exchange of information between the national and European agencies involved in the visa process are prerequisites for the analysis and development of control approaches. Here, a cooperation triangle of diplomatic missions abroad responsible for issuing visas, national asylum agencies and EU Agency for Asylum as well as national border and police authorities, supported by Frontex and Europol, must be formed.

- Detecting visa fraud requires expertise and sensitivity in the application process, in (border) police checks and in the context of migration law application examination.

- A central office (within the EU) should be appointed or commissioned to collect and evaluate all indications of visa fraud and modi operandi, to issue appropriate warnings to visa offices, police and asylum authorities and to initiate appropriate awareness, training and countermeasures. Another task of this unit would be the creation of typical risk profiles of visa applicants.



- Handouts with process, check and interview recommendations for visa offices (including appropriately commissioned external service providers), border and police authorities and asylum agencies should be regularly prepared, updated and used accordingly.

- A unified future digital application process must meet security interests.

Contents

Table of figures

List of Annexes

1 Introduction

1.1 State of play

„Most irregular migrants originally enter the EU legally on a short-term visa, but stay in the EU after their visa expires for economic reasons.[1]“

The EU Commission is of the opinion that a considerable number of migrants already have permanent intentions to stay when they apply for a visa, as a result of which they enter the country illegally with a previously obtained Schengen visa for a short stay. This allows for self-determined primary, secondary and transit migration within the Schengen area, which is largely beyond the control of one country. The full extent and effects of visa fraud remain to be determined.

Visa fraud, as a form of illegal migration, is a means to an end for asylum applications and subsequent crimes, such as unauthorised employment, labour exploitation or human trafficking.

As a rule, migrants do not have the necessary knowledge and logistics to successfully obtain a visa by fraud on their own. The financial profits of traffickers amount to up to 20,000 € per visa obtained by fraud.[2] Consequently, this is a criminal business field of considerable proportions.

At present, the phenomenon is not adequately represented at the European level and EU member states follow different and sometimes divergent approaches in their preventive and repressive measures to combat the phenomenon.

1.2 Objective

The handbook serves as an aid for European law enforcement, border and asylum authorities as well as visa offices at diplomatic missions abroad. It is intended to contribute to the prevention of future crimes, to initiate investigations and to initiate recommendations for action for criminal law reforms in the Schengen states.

1.3 Background

The German Federal Police, through an exchange with the German Federal Office for Migration and Refugees, noted an increase in visa fraud cases related to illegal migration since 2017.[3] Due to the fact that the majority of the foreign representations of the Schengen states are affected[4] to varying degrees the need arose to draw up a police situation report at the European level.

Within the framework of the EMPACT[5] priority on smuggling of migrants, Germany initiated the Operational Action „(OA) Visa Fraud“ in 2020. In this context, EU Agency for Law Enforcement Cooperation (Europol) published a first report on visa fraud in the EU in April 2021.[6]

In essence, it was documented that:

- every year about 25,000 to 35,000 migrants enter the Schengen area with a fraudulently obtained Schengen visa,
- the majority of cases of visa fraud are detected domestically by administrative authorities after entry into the Schengen area (e.g. in the context of asylum applications),
- In some cases, employees of visa offices are actively involved in criminal acts of support,
- The scale and complexity of the application process to obtain a visa suggests the involvement of organised criminal networks,

[1] *https://ec.europa.eu/home-affairs/what-we-do/policies/irregular-migration-return-policy_en [online] accessed: 17.2.2021; “Most irregular migrants originally enter the EU legally on short-stay visas, but remain in the EU for economic reasons once their visa expired.”*

[2] *Annex I: Europol, Visa Fraud in the EU, page 19, number 4.1*

[3] *04_02_Border_police_tasks_ (5) \0600_Secondary_migration\Volume2_Reports\Visa_abuse\180402-20171011 Asylum seekers in possession of valid Schengen visas*

[4] *Visa statistics 2022 of the Federal Office for Migration and Refugees; transmitted to Federal Police Department 13 Visa Office; correspondence dated 11.10.2022*

[5] *European Multidisciplinary Platform Against Criminal Threats*

[6] *Annex I: Europol, “Visa Fraud in the EU”*

- Iranian, Turkish and Syrian nationals are most frequently detected as fraudsters with fraudulent visas,
- Criminal networks exploit existing loopholes, e.g. in legal provisions, in the increasing digitalisation of the application process or weaknesses in the visa issuing procedures,
- There is a lack of solid data for a reliable EU-wide intelligence picture of the situation,
- It is a control related offence with a focus on the air borders.

So far, the phenomenon has only been mapped in the context of a situation report (see Annex I: Europol, Visa Fraud in the EU). Moreover, conclusions concerning the dark field are currently not possible.

As a result, the participants of the OA „Visa Fraud“[7] agreed on a three-part strategic plan[8]. This includes the analysis of the phenomenon, the adoption of appropriate preventive measures and the repressive fight against visa fraud“.

1.4 Addressees

Visa fraud concerns the performance of tasks by various authorities within all Schengen states in the context of the visa application process, (border) police checks, asylum applications and further legitimisation of residence.

The following information is intended to support national and international partners (police and border control authorities, embassies and consulates, European agencies such as the EU Agency for Asylum (EUAA)[9], European Border and Coast Guard Agency (Frontex), Europol as well as national asylum authorities in clarifying and identifying potential visa fraud.

[7] *participants of the Operational Action Plan 2022: AT, BG, CY, CZ, EE, ES, FI, HR, LU, LT, PL, PT, SE, EUROJUST, NO, UK, USDSS,*

[8] *Annex II: Visa Fraud – Strategic Working Paper*

[9] *Since January 19, 2022 the EU Agency for Asylum (EUAA) replaces the EU Asylum Support Office (EASO)*

2 Legal framework

Legal bases such as definitions, an overview of the most relevant legal texts and the visa application procedure can be found in Annex III Legal Basis.

3 Verification process

In principle, visa fraud can only be prevented by means of a targeted and active check at the time of application or by detecting it at the border or within the country. The core of this examination is the fulfilment of the requirements for the issuance of a visa pursuant to Article 21 of the Visa Code (VC) or the determination of the purpose of the journey pursuant to Article 6 of the Schengen Borders Code (SBC). This is done by means of targeted interviews, using all available sources and a final evaluation of the findings. The purpose of these comprehensive checks is to prevent unauthorised migration, threats to public security and order or burdens on the social systems of EU member states and Schengen-associated states.

The verification process must be adapted to the respective performance of tasks.

3.1 Plausibility assessment

The plausibility check compares the information provided by the applicant/visa user with the available information. The information contained in the Visa Information System (VIS) is compared with the statements made by the visa holder/applicant and the contents of personal, travel and accompanying documents or similar documents submitted.

It is questioned whether all requirements for the issuance of a visa pursuant to Article 21 of the VC are fulfilled, were fulfilled at the time of the application or whether requirements are no longer fulfilled.

It is advisable to ask open-ended questions during interviews.[10] It makes sense to repeat and modify these if the statements are not plausible or inaccurate. Documenting the survey makes it easier to compare the statements.

Purpose of travel:

- What is the purpose of the journey?
- Can the person independently provide information about the purpose of travel?
- Are the aim and purpose of the journey proportionate to the cost and length of stay?
- What preparations have been made for the trip?
- Is the journey related to the circumstances of the person's life or professional activity?
- Is there false or omitted information?
- Can the purpose be provided with supporting documents (bookings, flight tickets, itinerary)?

The stated purpose of travel should be in a meaningful relationship to the expense, costs and benefits. If the cost and duration of the trip are disproportionate to the declared income or occupation, the purpose is generally implausible. The assessment of proportionality is ultimately the responsibility of the decision-maker and can rarely be determined upon single individual statements.

Willingness to return:

- Are there any circumstances that would prevent a return?
- Has the applicant already arrived and left within the time limit given in prior trips?
- Does the applicant have regular living conditions in their home country? (Family, residential property, work)
- Is there a valid return ticket?

The action of a person must indicate a willingness to return. This would be particularly questionable if, for example, the applicant would have no or little ties (anymore) in their home country, but possibly in one of the EU Member States. A willingness to return is also doubtful if property is sold in the home country, bank accounts are dissolved or there are

[10] *See Annex IV: Catalogue of questions*

further indications that all connections have been terminated.

Financial resources:

- Are there any financial resources for living in the destination country (-ies) for the duration of the planned stay?
- What are the origins of these and are they transparent, comprehensible?
- Is the person insured in case of sickness?
- Is there a declaration of commitment[11] by a third person?
- Has the credit rating already been checked by another body?

Usually, the applicant's bank statements serve as proof of existing financial resources. In addition, income from non-self-employed and self-employed activities, as well as employment contracts and pay slips may serve as proof. The cost of the stay includes accommodation, meals and means of transport for the round trip. These also depend on the nature of the planned stay and the duration.

If the financial means are too low or not available, importers may, by document, undertake in writing to pay for the costs of the stay. An overview of the various commitments can be found in Annex 15 to the Visa Code Manual. This obligation covers all costs incurred by the foreigner. This also includes repatriation costs and medical expenses. When issuing a declaration of commitment, the obliged person must provide evidence of financial resources. In order to avoid abuse, these should be reviewed and questioned. The relationship must be taken into account.

The reference amounts for crossing the external borders, which are published in the EU Official Journal in accordance with Article 39 I c of the SBC and are different for each Member State, serve as the basis for calculating the costs for the duration of stay[12].

Cash, on-site cash withdrawals or bank statements, as well as information from the Visa application documents, on commitments, scholarships, and the profession indicating, allow conclusions to be drawn on the financial means.

When examining the asylum application, the Visa application documents can provide necessary information on the financial resources.

In addition to the objective assessment of the facts, conclusions about the truthfulness of the statement can be drawn in parallel from a person's behavior and reactions, through targeted observation.

3.2 Travel and identity documents

Travel, residence and identity documents submitted shall be checked for authenticity, integrity and validity

Interview during the visa examination

- Ask open questions
- Alteration, repetition and variation of questions
- Intensification of questions in case of ambiguities or contradictions
- Conscientious documentation of the survey

Observation during a survey

- Observation of reactions and behavior to asked questions. Avoid questions, nervousness, long pauses of thinking before answers
- Appearance and appearance in accordance with living conditions, travel purpose or weather conditions

Figure 1: Interview and Observation during visa verification

[11] *Declarations of commitments and money on blocked accounts are intended to support the willingness to return or, if necessary, to cover parts of costs by means of end-of-stay measures*

[12] *Indicative amounts for the crossing of the external borders referred to in Article 5(3) of Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)*

in accordance with the six pillars of the document verification.[13] [14]

Ensure that the identity of persons between the applicant and the photograph is present in the personal document.[15]

A query in the inventory excludes the use of stolen/lost documents.

In parallel, the entry and exit stamps must be checked accordingly.[16] Stolen or counterfeit entry/exit stamps are generally listed in the Schengen Information System (SIS).[17]

3.3 Risk profiles

Following the plausibility check and the assessment of the travel documents submitted, it is appropriate to check the applicant for conformity with known risk profiles.

A risk profile[18] summarises information on applicants with visas by gender, age, groups of persons, origin, itinerary and means of travel, importer, issuing authority of the visa, specified destination, purpose and, where applicable, other abnormalities.

The development of a risk profile should ideally be developed as part of a cooperation between the border police, migration/asylum authorities and with the involvement of international authorities such as Interpol, Europol and Frontex. The resulting findings should be shared with all Member States in order to prevent possible displacement effects in advance. The collection, evaluation and creation of such risk profiles should be centralised by one authority, ideally on national and European level.

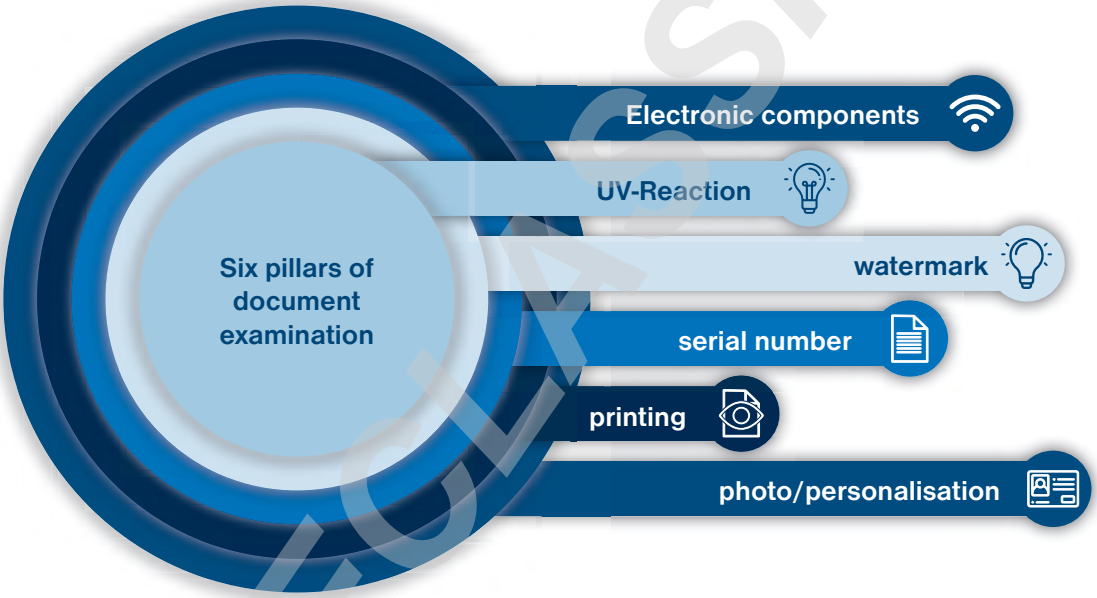


Figure 2: Document examination

[13] *See Annex V: Basics of document verfcation*

[14] *Regulation (EU) 2016/399 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of March 9, 2016 establishing a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), Section II External Borders, Chapter II Control of external borders and refusal of entry, Article 8 Border controls of persons No 3(a) i*

[15] *Schengen Borders Code Section II External Borders, Chapter II Control of external borders and refusal of entry, Article 8 Border controls for persons No 3(a)(ii)*

[16] *Schengen Borders Code Section II External Borders, Chapter II Control of external borders and refusal of entry, Article 8 Border controls for persons No 3(a)(iii)*

[17] *In addition, the Member States and Schengen associated countries have a national register of the check digits and whether the border stamps have been used for an incorrect date or check digit.*

[18] *Annex VI: Examples for Modi Operandi*

3.4 Databases

In order to check the prerequisites, a database query is explicitly mentioned for the Schengen Information System and Visa Information System.[19] In addition, a full assessment can only be made using all sources such as:

- the Interpol-database for stolen, lost and found travel documents (SLTD)
- the national police information systems and databases
- the national and international asylum/foreign databases
- the internal message processing systems or communication from VIS-Mail.

Findings from international and national (fact) search databases play an important role in assessing a person's threat to public security and order.

The purpose of the journey, the inviting persons, companies and the history of the Schengen visas applied for, issued or refused can be viewed in the VIS. An initial applicant needs to be examined in more detail if no information on the applicant is already available. If the entry control at the external Schengen border determines that an entry in the VIS is missing, this must be critically questioned. In rare cases, this can be caused by a data conflict or data transmission problems with the issuing authority. If such sources of error can be excluded, the visa must be re-examined as set out in number 3.2.

National and international asylum and foreign databases may provide information about the applicant's residence status or applications submitted.

Internal databases allow conclusions about links to other applications already submitted and their processing status. VIS-Mail allows the direct exchange of information between messages on current applications.

If links can be made to other EU Member States, e.g. through statements made or previous visa applications and stays, presented documents or specified entry points, contact with other neighbouring authorities with security tasks should be used. Liaison officers, document and visa advisors and existing bilateral networks assist for the exchange of information.

3.5 Open Sources

Open sources for research, refer mostly to content from the Internet. For example, addresses, hotel reservations, data on events, companies and other information could be used to check and verify the stated travel purpose. Through deposited contact on file options, contact persons can then be asked about the validity of reservations or travel bookings, bank accounts, participants, content and duration of seminars or similar. In addition, it is possible to find background information on a topic (e.g. the destination) in order to ask the applicant specific questions.

Social media and networks are becoming increasingly important. In some cases, they are openly accessible and provide useful information. It may be possible to check whether the traveller is active in them and which content is displayed, which groups they belong to, or which places were last visited. Job profiles can allow conclusions about the actual profession and thus income. Comparable information can be obtained from the importer or the declaration of commitment.

[19] *Schengen Borders Code Section II External Borders, Chapter II Control of External Borders and Refusal of Entry, Article 8 Border Controls on Persons No. 3(b), as well as Title III, Chapter III, Article 21 of the VC; see Annex III*

3.6 Auditing institutions

3.6.1 Embassies/Consulates' visa application procedures

As described in number 3, in the context of a visa application, the aim of the examination procedure is to identify and avert threats to the Schengen area already in the country of origin. Fraud attempts, the submission of falsified documents, false statements or a probable threat to public security, order or health lead to a rejection of the application.

Findings from prior application rejections make it possible to establish regional trends or patterns, with particular emphasis on modi operandi and regional specificities or resources (documents) being used. The collection and management of information should reveal correlations, enable investigations and, as a whole, serve the creation of risk profiles.

Since smuggling organisations often submit applications for several persons to the consulate abroad, at different times, these findings are of great importance for the visa decision-maker for the identification of fraud attempts and possibly related memberships of group travellers.

3.6.2 (Border) Police

Border guards are guided by number 3 of the survey content, but there are other framework conditions. The consideration of specially created risk profiles and warning notifications (up-to-date operational information) increases the detection rate of visa fraudsters.

Local knowledge of the specified destination as well as the survey of inviting person can help to quickly uncover contradictions. Group travellers are often on site at the same time and can be asked separately about the journey. The survey of a local pick-up provider provides information about their personal background or motivation, residence status and, if necessary, existing listings in databases.

Furthermore, personal and carried items or documents may indicate a different purpose of travel. This may be the case if:

- the nature and extent of personal objects carried along suggest a permanent stay instead of the specified short stay
- wearing clothes inappropriate and atypical for the specified purpose or the season
- school certificates, graduation certificates, birth and marriage certificates, family book and similar documents that would not normally be necessary for a planned short stay
- work equipment and clothing are in the luggage of an alleged tourist
- high amounts of cash, proof of bank transfers to European nationals, certificates for the dissolution of accounts abroad
- notes, addresses or contact information indicating another travel intention

3.6.3 Asylum authorities

The aim of the asylum authorities is to investigate the grounds for persecution. To do this, they clarify the facts and collect the necessary evidence.

A VIS comparison allows identification of the person, clarification of nationality.

If a previously issued visa is related to the entry of the asylum seeker, an initial suspicion of visa fraud[20] can be obtained, as it may have already existed in the visa application[21]. During the asylum survey, information on the travel route, information on the use of the support of smugglers can also be obtained.

If findings of individual applications are linked and evaluated, this can give rise to valuable foundations for the initiation or enrichment of investigation procedures and preparation of risk profiles (see number 6.1.3, number 7).

Only some EU Member States use the VIS intensively in the framework of the asylum application examination[22]. The result of an examination of the VIS may lead to a change in the competence of the conduct of proceedings under the Dublin III Regulation.[23]

---

[20] *See Annex VII: Joint Handout Excerpt, annex 4, paragraph 2.1*

[21] *Judgment of the CJEU of March 7, 2017 in Case C-638/16 PPU (X, X v. Belgium); The Visa Code only regulates the granting of short stays of up to 90 days, an asylum application is contrary to this*

[22] *Europol Operational Action 5.6 Visa Fraud Meeting, October 13, 2021, EASO presentation on VIS- checks*

[23] *Regulation (EU) No 604/2013 of the European Parliament and of the Council of June 26, 2013 establishing the criteria and mechanisms for determining the Member State respon-sible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)*

If there is cooperation to exchange information with police authorities, a basis for repressive as well as preventive measures can be established on the basis of defined parameters that justify the suspicion of visa smuggling during the asylum procedure.

This presupposes a fundamental interest and the possibility for the authorities involved to combat the phenomenon together. A possible cooperation model is presented as an example under number 7.1.

3.7 Risk assessment

The risk assessment compares all the findings of the verification process (plausibility check, verification of travel and accompanying documents, comparison with known risk profiles and warning notifications, results of searches in databases and open sources) with the requirements of Article 21 VC.

For example, if a falsified document is submitted or an existing refusal of entry is identified, the risk assessment leads to the conclusion that the above-mentioned conditions are not met. On the other hand, the comparison of intention and previously provided information may be more complex and thus require a balanced and appropriate assessment of the information presented in individual cases.

If the findings suggest that incorrect information has been provided, it is likely that there is a deliberate intention to deceive.

Serious doubts, concrete indications of abuse or potential danger, in principle lead to administrative measures as described in number 4 below. Criminal procedural measures and investigative proceedings may be initiated provided that there is a concrete initial suspicion. The following overview should clearly summarise the risk assessment.

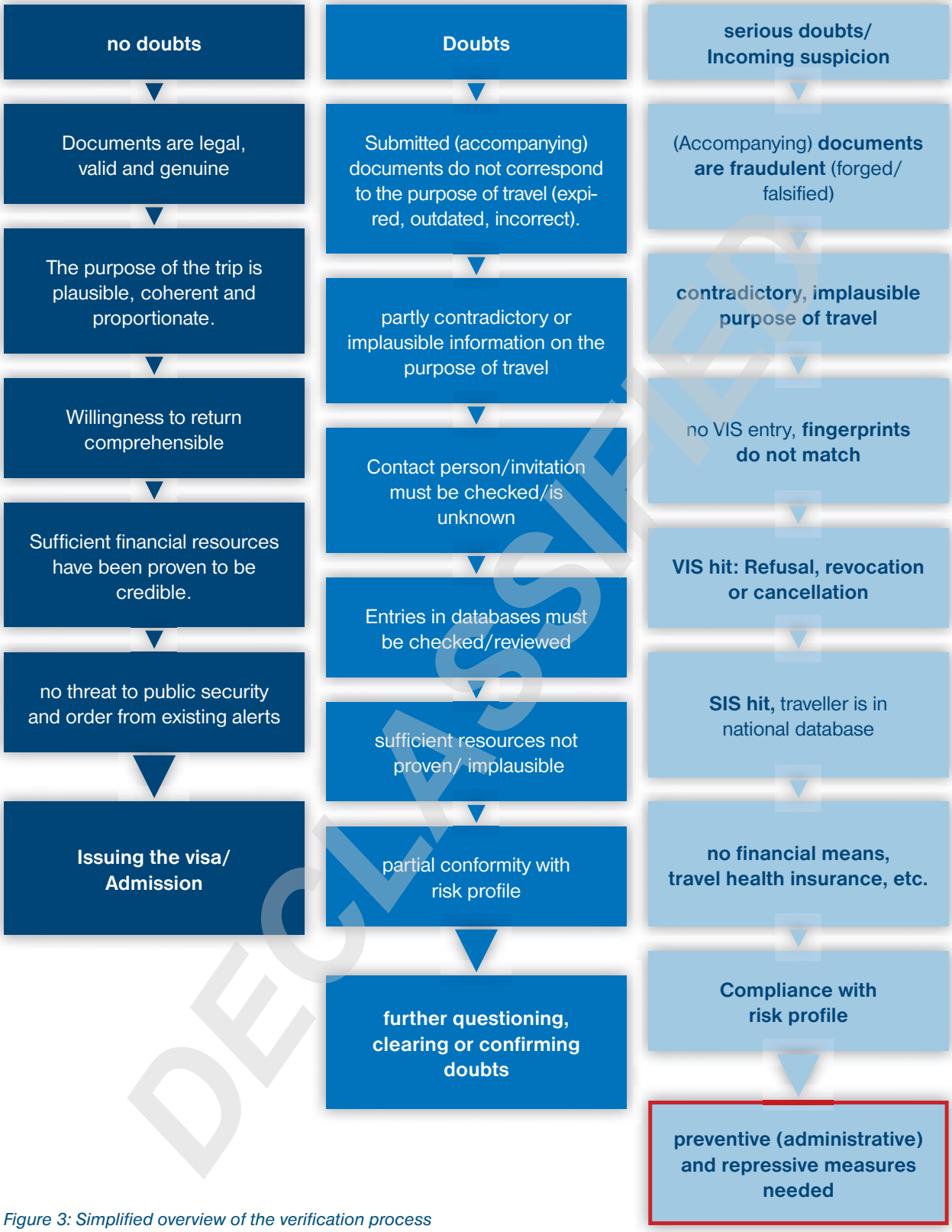


Figure 3: Simplified overview of the verification process

4 Administrative measures

If the verification process and the subsequent risk assessment lead to the conclusion that the conditions are not fulfilled or have never been met at the time of issue, the Schengen visa must be refused, revoked or cancelled.[24] Those measures either have the effect of preventing the exit by means of a visa refusal or lead to a refusal of entry at the border by failing to fulfil the entry requirements laid down in Article 6 of the SBC. In addition, depending on the situation of access, these administrative measures may lead to the termination of residence.

The administrative measures are in principle taken by the competent issuing authority. If this is not possible, the visa will be cancelled or revoked by another Member State. The issuing EU Member State must be informed of this[25] and make the registration in the VIS.

4.1 Visa refusal

Once a visa application for a Schengen visa has been lodged and was not withdrawn, a decision has to be taken.[26] If the condition laid down in Article 21 of the VC (See Annex III and number 3) is not met, the visa is refused in accordance with Article 32 VC.

The recognition of an attempt to deceive in the context of the application and, consequently, the refusal of the visa prevents the subsequent unlawful use.

The registrations in the VIS shall be made accordingly and accompanied by a statement of reasons.[27] The registration and justification of a visa refusal does not have any legal or banning effect with regard to future visa applications for the applicant, but should be taken into account for subsequent applications.

4.2 Annulment

A visa shall be annulled in accordance with Article 34 VC if it turns out to have been obtained by declaring false facts[28]. The authority then retrospectively establishes that it would never have issued the visa given prior knowledge of these facts.[29]

The annulment shall take place retroactively on the date of issue of the visa. The third-country national is therefore treated as if he had never had a visa. This circumstance leads to refusal of entry at the external border in accordance with Article 14(1) of the SBC.

The user of the issued visa may have committed a criminal offence under national law.[30] The person constitutes a threat to public security and order in accordance with Article 6(1) e SBC. The cancellation of a visa is for law enforcement, prevention and security.

However, if the visa application or use of a fraudulently obtained visa is not a criminal offence under national legislation, the annulment is mandatory. Nevertheless, it could be an attempt to enter illegally without a valid visa.

The visa sticker is marked as annulled after the opening of the administrative procedure[31]. The cancellation must be shown in the VIS and must be accompanied by a reason. It has no immediate legal effect or refusal of issuance for the future. This should be taken into account within the review process of future visa applications.

Risk profiling should include all annulments related to fraudulently obtained visas.

---

[24] *Titel III, Kapitel V, Artikel 34 (1), (2) VC*

[25] *Title III, Chapter V, Articles 34 (1), (2) and 34 (6) VC*

[26] *Title III, Chapter III, Article 23(4) VC*

[27] *Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 on the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) Article 13; Annex to the Commission Implementing Decision amending Commission Decision C(2010) 1620 final as regards to replacement of the Handbook for the processing of visa applications and the modification of issued visas (Visa Code Handbook I), Part II 11.3 Information to be added to the VIS when a visa is refused*

[28] *"Failing deception", see Title II, Chapter V, Article 34(1) VC*

[29] *Annex to the Commission Implementing Decision amending Commission Decision C(2010) 1620 final as regards to replacement of the Handbook for the processing of visa applications and the modification of issued visas (Visa Code Handbook I) Part V Modification of issued visas, 2. Annulment of an issued visa*

[30] *Provided that the use of a flawed visa does not constitute a criminal offence, the attempt to enter illegally may be considered, previous entries and stays with this visa are prohibited.*

[31] *Title III, Chapter V, Article 34 (5) VC*

4.3 Revocation

A visa must be revoked in accordance with Article 34 VC if the conditions laid down are no longer met. This shall be done at the time when the Authority becomes aware of the cancellation of at least one application requirement.

The revocation prevents future use of the visa, previous travels are not affected. Where this is ascertained during the external border control, this shall result in the refusal of entry in accordance with Article 14(1) of the SBC in conjunction with Article 6(1) (b) of the SBC. If the person is identified within the Schengen area (on national territory), this may lead to an end of residence under national law.

The visa sticker shall be marked as repealed after the opening of the administrative procedure and the registration in the VIS shall be adjusted.[32] The revocation does not have any legal effect in relation to future visa applications.

[32] *Title III, Chapter V, Article 34 (8) VC*

5 Repressive measures

The use of a fraudulently obtained Schengen visa is not uniformly regulated. It is considered by majority of EU countries as a criminal offence or administrative offence[33]. In the case of visas, it is likely that the applicant or document user is not punishable alone. In most cases the support by third parties (criminal networks) may be assumed. These findings must be passed on to law enforcement agencies by migration authorities.

The aim is to determine to what extent third parties have influenced the application process. Such active support would exceed the legitimate services of external service providers (see annex III). These can for example consist of the provision of fraudulent accompanying documents, demonstrative money/ money transfers or travel documents and the targeted preparation for interviews at the visa offices of the consulates abroad.

As set out in number 3.6.3, cross-agency cooperation between the asylum authorities and (border) police is necessary, as so far the majority of visa checks carried out are only identified in the context of the application for asylum[34]. Asylum authorities have the opportunity to contribute to raising awareness of the phenomenon and to generate investigative approaches. Such a cooperation variant is exemplified in number 7.1.

Annex IV contains, a questionnaire as guidance for with interviews or interrogations Moreover, Annex VII contains a handout with indicators to detect potential visa fraud cases, for asylum authorities.

Three key points need to be taken into account for the purpose of obtaining the suspected crime and subsequently dismantling cross-border criminal networks:

- the intensive use of databases and open sources in the examination of accompanying documents to support an initial suspicion
- control at the Schengen external borders is the last option to prevent illegal/unauthorized migration
- several Member States may be affected by the phenomenon and only international cooperation enables investigative success

5.1 Investigative approaches

If indications of a fraudulent visa application are already identified during the examination process, the rejection of the application or the administrative measures listed above are not the only necessary measures.
As a result of the finding that only in few cases persons acquire visas without third-party assistance[35], the support of investigative approaches depends on:

- How was the authority attempted to be deceived?
- Are there already similar cases or similar modi operandi?
- Who were the third-party supporters (facilitators)?
- Is there any evidence of (systematic fraudulent activities and hence) the involvement of a criminal network?

These questions should not only be raised by investigative authorities, but also by authorities with migration tasks, as they contribute to the investigation of criminal offences and the identification of smugglers within their competence. For example, asylum authorities can ask specific questions in the context of a travel survey[36] to determine the circumstances of entry or visa offices in the context of the application procedure for suspected fraud.

If possible, document and visa advisors can be consulted abroad or (border) police experts in Germany.

The comprehensive information collection ultimately forms the basis for further investigation and the possible identification of perpetrators and helpers.
If the visa has already been used for travel and the applicant is located in the Schengen area, further investigative approaches can be generated in the case of detected offences in addition to the sources of information already accessible abroad:

[33] *Annex VIII: Visa Fraud in the Member States or Annex III: Legal Basis*
[34] *Annex I: Europol, Visa Fraud in the EU*
[35] *Annex I: Europol, Visa Fraud in the EU, see key findings*
[36] *The so-called travel survey serves as a priority to clarify the competence.*

- Interviews of the applicants
- Interviews with identified contact persons (e.g. inviting party) or fellow travellers
- Evaluation of data from secured electronic devices (mobile phone, laptop…) and accompanying papers, as well as for example details as the stamping position in passports
- Checking the connections within social media, relevant forums or chat groups
- Requesting visa application documents

In domestically initiated investigative measures the supporting documents and other findings available at the consular offices abroad shall be included in the criminal proceedings.

Where an investigation has been initiated, the whole of the accumulated intelligence shall be assessed. In particular, indications of possible impact on other EU Member States or Schengen-associated Countries should be obtained. This may be the case if the visa has been issued by another country, if information indicates a contact person residing in another EU Member State, if circumstances of the visa holder's entry into or residence in an EU or Schengen country point towards a known modus operandi or on-going criminal proceedings.

For inquiries in the context of criminal investigations, the established channels via SIENA[37] and Interpol must be used.

5.2 Investigative proceedings with embassies and consulates

Investigations at embassies and consulates determine the possible participation of local employees or officials posted at a consular mission abroad in visa appraisals. This determines the extent to which an official may have influenced the visa granting process. These can act as individual offenders, be part of a criminal network, or are corrupted by perpetrators outside the diplomatic mission. Internal offenders in foreign representations can provide extensive services:

- Granting illegal access to representation
- Declaring fraudulent documents genuine and place them into the regular proceedings of a visa application
- Documentation of fictitious interviews to deceive the application decision-maker
- Documentation of fraudulent prior consents by migration authorities for family reunifications of non-relatives
- Lower verification or assessment thresholds by providing so-called "bona fide declarations"[38] for first-time applicants
- Acceptance and processing of applications despite legal or regional competence (applicants domiciled outside the jurisdiction)
- Issuing visas without prior consultation with law enforcement authorities (constructed emergency cases)
- Issuing visas without visa applications only on the basis of a bona-fide statement by the embassy official

[37] *Secure Information Exchange Network Application: SIENA is a secure intelligence exchange system developed by Europol for Member States, third countries/entities (as defined by Europol) and Europol itself. SIENA is used for the fast, secure and user-friendly exchange of operational and strategic crime-related intelligence." (Source: Federal Criminal Police Office, Extrapol: SIENA, Introduction and Brief Overview)*

[38] *In good faith, this term is used if a traveller has already proven to be trustworthy; Annex to the Commission Implementing Decision amending Commission Decision C(2010) 1620 final as regards to replacement of the Handbook for the processing of visa applications and the modification of issued visas (Visa Code Handbook I) Part II Operational instructions on the processing of visa applications, 5.2.3 Treatment of "bona fide" applicants*

6 Preventive measures

The aim is to recognise the attempt to fraudulently obtain a visa and to prevent it already in the application process by rejecting it. Consequently, when applying for visas before entry, potential dangers should be prevented and displacement effects should be avoided.

In conjunction with the increasing digitalisation, databases and automated testing programs are playing an increasingly important role. The use and maintenance of data as well as the provision of concise information for the visa decision-maker are therefore essential for the final evaluation. Implementation and necessary amendments to the Regulations are already planned (see Annex III).

The introduction of standards as well as additional automated tools for document review and integration of other sources of information for background information are considered useful. However, all this requires sufficient education and training. The role of a visa decision-maker should not correspond to that of a service provider, but rather should be understood as part of the EU security architecture. The verification process shall reflect this.

6.1 Preventive approaches

6.1.1 Embassies and Consulates

Visa departments in embassies and consulates have to cope with the ever-increasing number of visa applications while maintaining a high level of quality during the inspection.

Up-to-date information on fraudulently obtained visas and related modi operandi should be included in the evaluation process of future visa applications.

Consequently, the assessment of existing entries in the VIS is of particular importance.[39] Where an application has already been rejected or cancelled by another authority, findings which led to this measure should be obtained.

Direct communication via VIS-Mail already enables a rapid exchange of information between the individual visa departments of the Schengen countries and should be actively used. Nevertheless, deviations in compliance with the common Schengen acquis are continuously identified, so that the conditions for granting may differ.[40]

A common platform for exchanging findings and mutual agreements, such as border and police authorities or asylum authorities, is usually not available. The need for harmonisation of visa issuance, and the formation of a network to exchange trends and other insights has already been recognised and implemented partially implemented with a so-called "Regional Schengen Coordination Officer" in 2020.[41]

6.1.2 EU and Schengen external borders

If border authorities detect a misuse of visas, entry may be refused. In order to prevent future misuse or displacement effects, the visa must be cancelled as described in number 4.2. If a visa is applied for at the border and there are reasonable doubts about an attempted visa fraud, the visa shall be refused (number 4.1). As a result, future applications of this applicant will receive a different assessment in the context of the audit process. Furthermore, these findings may be entered in SIS, linked to alerts or alerts on border searches. This will allow other EU Member States to draw attention to possible smugglers and facilitators.

In addition to these measures, the Visa Alert File was introduced in Germany with the introduction of the VIS.[42] This data platform is primarily used to support decision-making in the visa application process and is enriched by the German Federal Police and other German authorities with insights into related suspicious visa applicants, contact persons or inviting parties. The VIS does not provide an opportunity to share findings directly with other EU Member States.

In the absence of EU-wide analysis products, the exchange of experience and intelligence between (border) police, liaison officers and document and visa advisors is of great importance. Essential and

[39] *Chapter I, Article 6 of the Regulation; here authorities and staff responsible for visa tasks*

[40] *Launch of the call for expression of interest under the Specific Action "Visa policy — digitalisation, consular cooperation and other" under the Instrument for Financial Support for Border Management and Visa Policy (BMVI) — Reference BMVI/2022/SA/2.3.1*

[41] *He serves as a mediator between the visa departments and aimed at achieving greater uniformity in issuing visas by different Member States; Conclusions meeting on Activity 1.ii Assisting consular authorities on document fraud related to visa applications by Giovanni Cioffi EC, DG Home, Unit C1 Irregular Migration and Return Unit, December 9,.2020*

[42] *https://www.bva.bund.de/DE/Das-BVA/Aufgaben/V/Visa_Warndatei/vwd_node.html [online] queried at: June 27, 2022*

timely findings can be transmitted quickly and, if necessary, directly to the concerned border crossing points. The entry with a fixed visa can thus already be prevented at the external border.

The absence of EU and Schengen-wide aligned criminal laws targeting visa fraud reduces the possibilities for engagement of border police to administrative measures. This makes it difficult to identify facilitators and criminal networks. A consistent prosecution is the cornerstone for future investigative actions and enables the analysis of modi operandi as well as the detection of involved officials as offenders. The dismantling of facilitators and criminal networks, both inside and outside the EU and the Schengen area, plays an important role in preventing future abuses in the long term.

6.1.3 Application for asylum

As part of the European security architecture, asylum authorities can contribute not only to law enforcement but also to the creation of intelligence pictures, risk profiles and warning notifications. In addition, they can submit their own findings to the issuing visa authority so that it can carry out an independent assessment of the facts. This is partly already done at national level[43] (see number 7). A bundled analysis and sharing of such findings at international level for preventive use is not known yet.

Furthermore, links with fraudulently obtained visas can only be established if the applicants are automatically checked in the VIS. The main focus here is on the aspect of security.

According to a consultation by the EU Council Working Group on Asylum in 2020, an automated search of asylum applicants in the VIS is not carried out in four EU Member States.[44] However, the VIS is widely used by only three EU Member States. Germany, Sweden and the Netherlands carry out 89 % of the border checks or the examination of asylum applications.[45]

The EU Agency for the Operational Management of Large-Scale IT Systems in the area of Freedom, Security and Justice (eu-LISA) informed during the meeting of the Council Working Group on Frontiers on December 19, 2022 that in 2022, from January to the end of July, out of 3.4 million visas issued, only 44,65% were checked in VIS. Fingerprints were checked in less than 25% of all visas, contrary to existing obligations. EU-LISA assumes that either the processes or the technical conditions were not adapted.[46]

Analysis and sharing of asylum data requires respective legal conditions. It also requires an exchange of intelligence and experience with (border) police authorities and the identification of recommendations for action to identify indicators. This cooperation already exist in different forms at national level in some Member States. There is no EU-wide and uniform approach to cooperation, exchange and, where appropriate, training between the authorities concerned.

6.2 Analysis and evaluation

Criminal intelligence analysis products are necessary to highlight the extent of the crime phenomenon in the national and international context. Intelligence analysis at the same time to create risk profiles and warning notifications to be used to prevent future crimes and prevent displacement effects. In addition, these products provide the opportunity to identify weaknesses, to justify training needs and to identify the need for adaptation and implementation of legal bases and laws.

A solid data base is required for a sound intelligence analysis. This usually results from the criminal proceedings initiated (criminal statistics). As mentioned above, fraudulent obtaining of visas is not a criminal offence in every Member State or Schengen-associated Country. In addition, an analysis of criminal proceedings would have to be in place already at national level, to allow sharing with national or international partners. A holistic picture of the situation is not yet possible, due to the lack of and incomplete data.

Another way to explore the scale is the VIS. As set out in number 4, all administrative measures must be

[43] *Annex X: Report of the EASO Advisory Group on Visa and Asylum, December 21, 2021, Contribution of the Netherlands*

[44] *Annex X: Report of the EASO Advisory Group on Visa and Asylum, December 21, 2021: Result of consultation to the EU - Council Working Group on Asylum of 26.10.2020*

[45] *Annex X:: Report of the EASO Advisory Group on Visa and Asylum, December 21, 2021: 2 million queries carried out between October 2017 and the end of September 2019*

[46] *Meeting oft he Council Working Group on Frontiers on December 19, 2022, presentaion eu-LISA „Checks against the Visa Information System at the external borders" (WK 17914/2022 INT)*

registered in the VIS. A filter function according to administrative measures in connection with visa fraud or its attempt is conceivable. A refusal, cancellation or revocation of visas related to visa fraud should therefore be implemented in the VIS in a concrete and researchable manner. The prerequisite for this is the provision of information from VIS users and a consistent registration in the VIS with uniform registration requirements. Despite a uniform database structure of the VIS and support through the eu-LISA, the data can only be obtained after the consent of the respective data owner (e.g. EU Member State). A central evaluation cannot be carried out in the framework of EMPACT at the moment.[47]

Highlighted cases and modi operandi of visa fraud are reported to Frontex as part of the European Document Fraud — Risk Analysis Network.[48] However, these reports only include criminal offences related to findings at the EU's external border. Internal border findings are not reported in the absence of a mandate. The lack of a uniformly binding definition of visa fraud also results in differing outcomes and results in a partial picture.

An analysis of the refusals[49] to enter at the Schengen external border in connection with visa fraud is also conceivable. Such statistics could contribute to the creation of an intelligence picture. Considering the Dublin Regulation as another way of identifying a potential link between visa and asylum, this source does not give a clear picture either. Cases where the visa applicant travels directly to the issuing EU Member State will not be reported. Furthermore, there is no Dublin request when exercising the right of self-entry or if other reasons prevent a Dublin procedure.

The survey carried out by EUAA found that EU Member States/Schengen-associated countries have some information on visa clearance. These are usually only used for internal use. Nevertheless, asylum authorities seem interested in improving the quality and quantity of data in order to identify trends.

[47] *Annex I: Europol, Visa Fraud in the EU*

[48] *See footnote 47*

[49] *https://ec.europa.eu/eurostat/databrowser/view/migr_eirfs/default/table?lang=en [online] retrieved June 26, 2022*

6.3 Exchange of information

The continuous intelligence analysis and creation of risk profiles and warning notifications, as well as other analysis products, could provide an intelligence picture for all affected or involved entities. Ideally, an exchange takes place between (border) police and migration authorities as well as the relevant visa offices of embassies/consulates. Findings from criminal proceedings and asylum procedures should be made available to visa offices and used in the decision-making process. Equally important is a constant exchange between visa offices abroad in order to identify local specificities and regional displacement effects at an early stage.

In addition to preparedness, national legislation of all Member States is needed to enable such data collection and exchange. This is not currently the case as a result of the quality and quantity of the information submitted in the context of the analysis report by Europol.[50] A comprehensive cooperation between police, border guards and other authorities within the Member States should be sought.

Finally, it should be noted that regular exchange of information at national and international level is essential for the production of analysis products. A common collection of data should be centralised by an EU agency. Frontex would be primarily considered in a preventive cross-border context. Alternatively, Europol could create an intelligence picture of the offences detected. An analysis of the asylum data related to visa fraud could be carried out by the EUAA.

Only a holistic approach and the collection and integration of all the above mentioned authorities and agencies can in the future make it possible to adequately assess this phenomenon, identify gaps and initiate countermeasures.

6.4 Education and training

As mentioned in number 5.1 above, education and training, along with awareness-raising in this area of crime, is important. For this reason, the EU-funded (BMVI/ISF) Visa Code Training Project is developing an EU-wide training concept for visas for the first time. The project is led by Sweden in partnership with the Czech Republic, Germany, Poland and Spain, and is expected to deliver the training in December 2023. The training will focus on the common visa regulations and cover the entire visa process, from application to exit of the Schengen area. The main target group are staff at visa issuing authorities and border control authorities, but the training can also be relevant for example to asylum officers and third parties working with visas. Most of the training is expected to be available online, with eventual face-to-face sessions.[51]

Prior to this, training is provided at national level by the EU member states. However, discrepancies in the implementation of the Visa Code show that a uniform training concept is necessary. In addition, this concept is intended to facilitate an easier transition towards digitalisation and to drive the implementation of supporting applications for the detection of counterfeit accompanying documents.[52]

This makes it possible for targeted training of consular and visa departments to increase sensitivity in this regard. Accordingly, training should be offered and carried out at regular intervals. In terms of content, regional specificities must be taken into account.

In principle, the entire audit process, as described in number 3, should be mapped in training programmes.

The training courses must be centrally coordinated and carried out according to addressees and tasks. For coordination and organisation, with topic-specific speakers, the EU Agency for Law Enforcement Training (CEPOL) is considered for police authorities. In conjunction with OA 5.4 (Training activities on document and identity fraud - visa section/consular staff) within the EMPACT's Operational Action Plan

[50] *Annex I: Europol, Visa Fraud in the EU*

[51] *EU-Common Visa Training Project, Meeting Presentation and Minutes, March 28, 2022*

[52] *Launch of the call for expression of interest under the Specific Action "Visa policy – digitalisation, consular cooperation and other" under the Instrument for Financial Support for Border Management and Visa Policy (BMVI) – Reference BMVI/2022/SA/2.3.1*

2023 Migrant Smuggling, Frontex already has the opportunity to address the issue to the staff of the visa departments. The scope and content of these trainings relate primarily to document fraud. Synergy effects can arise from the involvement of document experts in the field of general police and border police. This would enable, among other things, an exchange of experience on current trends and new modi Operandi, which affect specific EU representations or regions in third countries. Information and experience for interviews should be included in these training courses.

In the border police sector, training should be offered at regular intervals. The focus here is mainly to train border guard officers in the first line of inspection. Due to the increasing digitalisation, travellers increasingly carry no or few application documents and accompanying documents and/or possess them only in electronic form. In addition, it is not always possible to trace or reconstruct which documents were submitted for the visa application. Training content, in particular, interview techniques and the provision of risk profiles (number 3.3) must be included. Consequently, it makes it easier to identify where a more intensive interview is carried out in the context of border control, in particular of persons matching the risk profile. The organisation and implementation of training can be carried out by trained experts in this field.

Asylum authorities do not focus on law enforcement measures or preventing unauthorised entry. Accordingly, training content should also identify aspects of identifying indicators suggesting fraudulent visa applications in order to be able to effectively contribute to border and domestic security. In this respect, it is advisable to agree in advance certain parameters where migrant smuggling or human trafficking is related to a visa fraud. This can only be done in the context of cooperation with the relevant law enforcement authorities and should include, in the same step, a training needs survey for topics to be addressed. If such a concept exists, these findings can be included.

7 Police and Asylum Authorities cooperation

Visa fraud is a phenomenon that usually concerns the competence of different authorities. Existing cooperation models for the exchange of information are presented below.

7.1 Germany

For several years, the German Federal Office for Migration and Refugees (BAMF) has registered a high number of asylum seekers who enter Germany with the help of a smuggler or a smuggler organisation and/or using fraudulently obtained visas.[53] The German Federal Police found an increase in fraudulently obtained Schengen visas in its area of competence.

In order to counteract visa fraud in connection with asylum applications, the BAMF and the Federal Police have agreed to exchange data on asylum applicants with Schengen visas. The aim of this cooperation is to obtain a better and more comprehensive intelligence picture and to initiate legal proceedings where legally required. The BAMF performs a VIS comparison and a comparison with the national migration authorities for all asylum seekers based on the fingerprint data. These comparisons are absolutely necessary for the further processing of the asylum procedure. From the hits in the VIS, the BAMF generates a list of asylum applicants who previously entered with visas and sends them to the Federal Police. This collection contained an average of 2500 records per month in 2022. This includes, among other things, the issuing country of the visa and the visa category.

The Federal Police creates from this an intelligence picture and risk profiles in order to be able to identify priorities. This includes, among other things, identified suspects, suspicious inviting parties and regional patterns (messages/consulates and itineraries) which indicate high migratory pressure. Alerts are also generated from the collected information.[54] The findings are shared with the German foreign representations, with federal police liaison officers and document and visa advisors deployed abroad, as well as with the subordinate departments of the Federal Police and other partners.

In addition, the Federal Police has prepared together with the German Federal Criminal Police Office a guideline[55] for the BAMF, explaining the phenomenon of visa fraud and possible Modi operandi of migrant smuggling. Furthermore, it is presented in the handout which information the Federal Police need from the asylum procedure hearings in order to be able to conduct successful investigations in this regard. The handout serves as an orientation for the interview by the decision-makers of the BAMF. Through the definition of indicators and reporting criteria, the BAMF additionally submits several suspected criminal cases on a daily basis (individual case reporting on visa fraud and possibly even migrant smuggling). These cases include more detailed information on a single applicant with a Schengen visa and reference to smuggling. The framework of the required or fundamentally needed information is written in the above mentioned guideline. This includes also case studies, shows possible investigative approaches, and describes indicators and the required reporting. This concise guide therefore allows the BAMF to identify potential crimes during the asylum procedure. After the asylum application has been submitted and the applicant has been identified, the initial reception/examination (screening), different hearings and an interview with an interpreter for the formal application for asylum will take place. During this hearing, the asylum seeker must set out his/her circumstances, the itinerary and the reasons for his application, taking into account signs of aid and assistance from facilitators and visa fraud.

If indicators have been identified, all available information and documents are compiled and forwarded to the Federal Police. The Federal Police assesses possible criminal relevance. If this is the case, appropriate investigations will be initiated.

The advantage of this dual reporting is that new trends are identified at an early stage and criminal proceedings can be initiated in a targeted manner.

In order to combat this area of crime holistically, the Federal Police exchanged the results with the Federal Foreign Office. Cases in which charges have been brought are forwarded to the issuing visa office, the federal liaison officers abroad and the local document

[53] *Annex I: Europol, Visa Fraud in the EU*
[54] *Annex XI: Warning notification*
[55] *Annex VII: Joint Handout Excerpt of the Federal Criminal Police and the Federal Police*

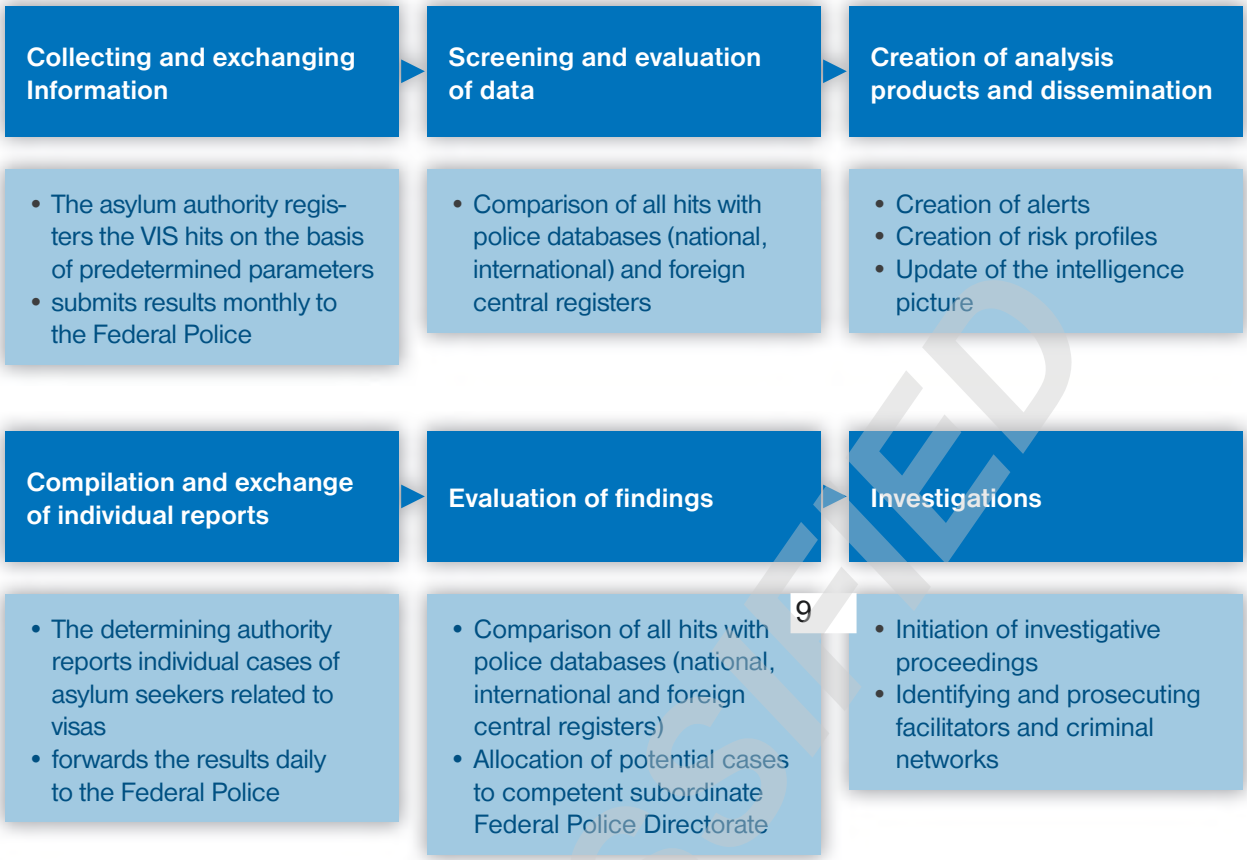


Figure 4: Data flow

and visa advisors in connection with the reference number of the visa application.[56] The evaluation of the results shows focal points, risk profiles and possible vulnerabilities.

7.2 Netherlands

Information-supported decision-making for short-stay visas (KVVs):

The Netherlands has a centralized model for visa decisions. The application examination is carried out by decision-makers in the Netherlands. This decision-making process is supported by two additional applications with information: One, the so-called Country Wizzard, provides relevant information about the country of origin (country of the applicant and regional specificities). The other application, the application assessment database (BAO), contains an extensive collection of data from the Netherlands migration chain: Royal Military and Border Police, Immigration and Naturalisation Service (IND), Repatriation and Departure Service, Social Affairs and Employment Inspectorate. In addition, data of the EU and UN sanction list are included in the BAO. These data allow for the categorization of applications in rapid procedures, regular and intensive examination (profiling). Therefore, "historical" data leads to a characterization and the creation of risk and chance models with which future trends can also be predicted. As a result, all national migration-relevant information on groups of persons is included in the decision-making process. Where an applicant belongs to a group of persons where the risk assessment has shown that there is a high likelihood of illegal migration, that application shall be submitted to the decision-maker for an intensive examination. If all information is available and the applicant is not part

[56] *Due to the quantity, not every case leads to feedback.*

of a risk group, the application will be assigned to the rapid procedure, with no further deeper examination by the visa decision-maker is required.

Information-supported decision-making only assists with decisions on applications. An extra interview may be recommended on the basis of the results. It is never a reason for refusing a visa in itself. The information that the ministry uses ensures that a decision can be taken more quickly and more objectively. Ultimately, it is the consular officer who will decide whether or not to issue a visa. It is not a form of automated decision-making.

A rule-based algorithm forms the basis of the profiles. These are established through a decision tree. This decision tree/algorithm is predetermined using carefully crafted guidelines used by the NL- MFA. When existing applications match based on a number of characteristics, a group is created. If this group of applications complies with the guidelines, a profile is created. Thus, the starting point for profiles is not the outcome of a learning algorithm, but the decision tree that is predetermined based on the guidelines and legally tested.[57]

7.3 Sweden

Sweden has developed a similar approach to counter the effects of fraudulently obtained visas. Through an analysis and evaluation of asylum data, it was found that visas are being used to enter the country and later apply for asylum. This can only be prevented through targeted feedback to the affected visa offices abroad. Therefore, the Swedish Migration Agency conducts automated VIS searches during the asylum application process. It was found that about 20% of the registered asylum seekers already had a visa before their arrival.[58] The VIS hits are evaluated on a monthly basis, anomalies and trends are highlighted and forwarded to the diplomatic missions abroad. Subsequently, the respective Swedish consulates assess the situation on the ground based on the information provided. If another EU member state/Schengen state has issued the Schengen visa, contact and information forwarding is ensured via the Ministry of Foreign Affairs.

[57] *White paper on information-supported decision-making using the Application Decision Database of the Ministry of Foreign Affairs, May 2020*
[58] *Annex X: Report of the EASO Advisory Group on Visa and Asylum, December 21, 2021, page 18*

8 Review

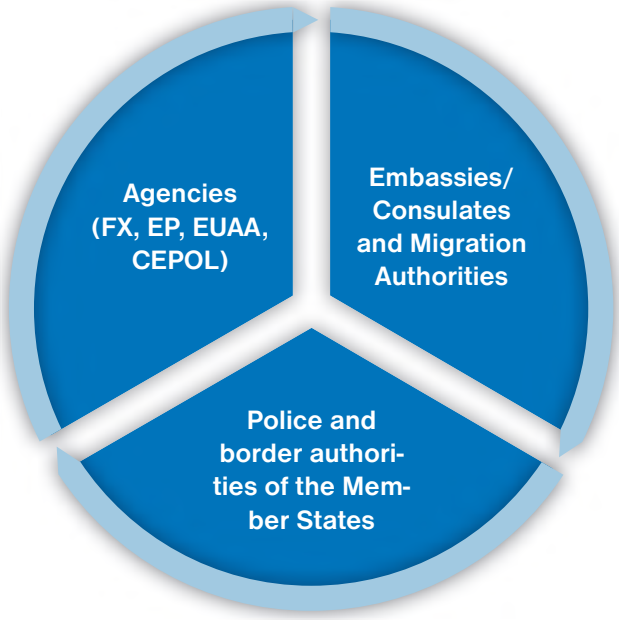


Figure 5: Cooperation and exchange

Visa fraud is a profitable business segment for smuggler networks. In many cases, the (apparent) legal entry follows a permanent residence and an asylum application. As a result of the common Schengen area, all Member States are affected in varying degrees. However, the evaluation of this modus operandi differs significantly, also depending on the criminality of this offence, which is not regulated uniformly across the EU. This directly depends on the will to pursue and the initiation of preventive measures. Visa fraud can only be detected by active checks, resulting in the assumption of a high number of unreported cases. There is some lack of focus and sensitivity to this field of crime.

There is no reliable statistical data available across the EU that would enable reliable analysis. Overall, the quality and quantity of information exchange, such as concerning current trends and modi operandi, is insufficient. Research in VIS and other databases is only used to a limited extent. This makes it more difficult to detect fraud attempts or abuse cases.

A good level of training and the application of the described audit process, as well as the cooperation and exchange of information between all authorities involved in the application and verification process, are essential for a consistent fight against visa fraud. These include the diplomatic missions abroad, asylum and migration authorities or the (border) police authorities. Coordination at EU level should be ensured by Europol, Frontex, CEPOL and EUAA.

A stringent plausibility check and consequently the rejection of suspicious visa applications prevents illegal migration and also serves to prevent threats to public security. The visa application assessment is not a mere service but part of the European security architecture.

With the increasing digitalisation of the application process, existing high security standards should continue to be ensured and new methods of digital auditing should be supplemented. The influence of criminal networks on the issuance of visas must be prevented with all available possibilities. In cases where it does not succeed, consistent prosecution must be ensured.