COUNCIL OF THE EUROPEAN UNION

Brussels, 25 March 2013

7840/13

LIMITE

JAI 236
DAPIX 60
CRIMORG 47
ENFOPOL 86
ENFOCUSTOM 49

NOTE

from:	Europol
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	17749/11 JAI 889 DAPIX 165 CRIMORG 230 ENFOPOL 437 ENFOCUSTOM 157
Subject:	Business concept for an Information Exchange Platform for Law Enforcement Agencies (IMS Action 4) - High level solution definition for the IXP / **Draft 4**[1]

1. Introduction

In 2010 the business concept for the Information Exchange Platform (IXP) was elaborated and submitted to DAPIX as the first deliverable of action point 4 of the Information Management Strategy. DAPIX endorsed the concept in December 2010 after which the design of the technical solution could commence. This document aims to provide this design for the IXP. Previous versions were discussed within the WG on Action Point 4 and presented to DAPIX. Meanwhile further work has been done on the security architecture and the preparation for implementation. The results have been integrated in this document. After discussion and acceptance within the WG on Action Point 4 it will be presented to DAPIX.

[1] Changes with regard to the previous version are set out in bold.

In this document the overall approach will be explained, including the general description of the envisaged technical solution. Subsequently, the implementation of this solution will be divided over three consecutive phases. Then, a number of assumptions and preconditions will be described, in particular with regard to the security architecture. Based on these assumptions and preconditions an outline is provided for timelines and costs for the first development phase for the realisation of the IXP. **Considerations on governance and funding have been added since the previous presentation of this subject.** Finally, a specification of the next steps will be provided.

Essential elements for the viability and acceptance of the IXP are data protection, security and access to information. For the solution in general, as well as for the individual phases each of these elements will be addressed.

2. General approach

The IXP is intended as the portal for EU law enforcement to access relevant information related to cross-border cooperation. This can be general information on legal frameworks, national procedures and events, but it also includes access to operational, crime related data. The envisaged solution will enable users from their local environment to find and obtain relevant information in accordance with their access rights and the applicable procedures, in compliance with data protection and security requirements.

In order to meet all essential business requirements the IXP, once fully developed, will have to enable concurrent processing in environments that are currently isolated. This is, for instance, necessary to provide an integrated search function across the SIS, Europol systems and Interpol databases, provided that the user in question is authorised to query these sources.

The concurrent processing in different environments will only be possible if in each environment the necessary controls are embedded that restrict the processing capabilities to those authorised to the user. The design of a basic model of user profiles has been identified as a viable solution for managing such controls efficiently. The following user profiles have been distinguished:

- The general user: this is a profile with the most limited access rights. Access is limited to general, non-restricted data. This can, for example, be a civil servant in a law enforcement organisation without any operational tasks.
- The investigator/law enforcement official: this user profile equally has access to general, non-restricted data, but may also have access in accordance with his business needs to sources containing operational crime related data. Typically such access to data from other Member States would be limited to hit/no hit access and possibly subjected to additional conditions imposed by the data owner.
- The international coordinator: this profile is intended for those that facilitate cross-border information exchange. For that reason they have more extended access to data than the previous two profiles. This enables them to facilitate the information exchange to ensure that the investigator actually gets the information required and identified through the hit/no hit query. The sources this profile has access to is dependent and limited to those that are necessary for the performance of his/her tasks.

In addition to the roles mentioned above there are several other roles related to the platform management. This includes the management of content at the platform, both at the level of creating and uploading content as well as at the level of supervision of the quality and appropriateness of the content.

Furthermore, there will be roles covering control functions of auditors of data protection and security compliance. These roles are distributed across the various partners – Member States and other entities – that provide and retrieve information. It has to be taken into account that content management and quality control will have an impact on resources of the various partners that participate in the use of the IXP. This impact has to be balanced against the practical benefits and efficiency gains of the platform.

In due course, but only at the final stage of the IXP, the information management tools made available through the IXP will require adjustments to implement this model of user profiles. The same applies for identity and access management solutions used in Member States and at EU level. The management of access rights and authentication of Member States' users should predominantly be organised at national level in accordance with the national regulations and procedures in place.

By means of so-called *trusted third clients* cross-border access can then be managed effectively. This means that the authentication of the user is executed at national level after which the tool that is accessed only receives reference data concerning the identity, combined with the applicable user profile and processing rights.

Also the auditing of security and data protection compliance by Member States' users should in principle be organised at national level. To facilitate the auditing the audit logs should be made available in a similar way as the IXP had facilitated the access. This means that if a user made a query in several tools concurrently, the logs should be also be available concurrently, showing the processing of information across tools. This does not only make the auditing easier, but will also present a more realistic picture of the actions of the user.

3. Phased implementation

In this chapter the realisation of the IXP is described on the basis of a gradual development, consisting of three phases.

3.1. Phase 1: A central communication portal

The first concrete step towards the fully fledged IXP is even for a non-technical audience rather straight-forward: the establishment of a common web portal.

The envisaged portal gives access to general, restricted and non-restricted information and communication facilities. This can be national information pages, guidelines, handbooks, but also collaboration platforms for law enforcement practitioners. The portal as well as the sites and platforms it gives access to are not intended for the processing of personal data related to crimes.

The main IXP platform will be hosted in a secure domain, protected up to a confidentiality level of EU restricted/Restreint UE. On this platform general information is available, both at unprotected and at EU restricted level. This domain can only be accessed by authorised law enforcement officials that work in a local environment that is adequately protected and interconnected to the IXP domain via an adequately secured connection after successful logon.

To maximise access for the law enforcement community the web portal will also be made available over the internet. This platform is a copy of the main IXP platform that is hosted in the secured environment. Although the content on this mirroring platform is not supposed to contain any restricted information, still access will be controlled by means of a secure domain (https) with password authentication.

A strategy, most likely consisting of automated controls, will be implemented to avoid inappropriate transfer of classified information from the main platform to the internet-facing mirror. Owners of information will at all times have full control over the information they have provided.

As the IXP in this stage is not used for personal data, the impact from a data protection perspective is limited. Nevertheless, data protection aspects concerning contact details of law enforcement staff using the platform need to be clearly arranged and communicated. Also compliance with the prohibition of using crime related personal data has to be enforced. Equal considerations can be made from a security perspective. Given the content the impact may be deemed limited, but nevertheless the necessary precautions have to be taken.

In terms of access management the intended content does not yet require a differentiation between the user profiles defined in the previous chapter. However, it is recommended already in this phase to organise access management of in particular Member States' users at national level.
Resource requirements to establish this first stage of the IXP depend in particular on the ambition level of the participating partners. The technical realisation will be manageable, but the main effort is expected to be required for the composition, translation and maintenance of the content of the websites and platforms. Details on the realisation of phase 1 are provided in paragraph 5.

3.2. Phase 2: Direct connection to all relevant tools and information

In phase 1 the central portal would link the user through to information sites, platforms and tools available on the same domain. Basically, all areas where the user can go from the portal are hosted in the same environment. The next step, to be implemented in phase 2, would be the technical re-direction of users from the portal to sites, tools and applications hosted on different domains. This would, for instance, allow the user to go from the portal to the Visa Information System.

This has huge advantages from a business perspective. It enables the user to go (in accordance with his access rights) to all relevant sources, tools and platforms. This is also the stage at which the portal can assist the user in finding the relevant tools, cooperation channels and applications on the basis of his/her practical business needs. This assistance will be based on predefined and commonly agreed criteria for the selection of sources, processing tools and cooperation channels.

The technical possibility of re-directing users to different domains does not imply that users would also get access to those domains or to the tools and sources hosted on those domains. That is explicitly not the case. Access authorisation is not affected by this technical change. Still users need to be authorised by the applicable instances responsible for authorising users to access the domains, tools and sources in question. And when accessing such environments the user still has to be authenticated in accordance with the existing access management arrangements in place (user password, etc.).

The way the re-direction to other domains works is fairly simple: it makes use of the already established routing mechanisms that are in place. So, if a user from his computer had access through the national infrastructure to the Schengen Information System, then this existing routing is used for the re-direction from the central portal to the SIS.

For security reasons the redirection is only possible from the main IXP portal to assets that are equally protected and accessible via adequately protected network interconnections. This means that the redirection is limited to those tools and applications that can be securely made available through navigation over trusted networks.

In this second phase the main IXP platform will contain links to tools for the processing of personal data related to crimes, such as SIS, SIENA and Interpol databases. However, this does not mean that the portal itself would be used for the processing of such personal data. That is explicitly not the intention. Only the tools intended for that purpose to which the portal can re-direct the user, will process personal data, in accordance with their already established data protection framework.

3.3. Phase 3: Seamless access control mechanisms

As the third and, for the time being, final stage of the IXP it is envisaged to implement an integrated identity and access management mechanism. This would imply that a user, when accessing a domain, application or data source, would no longer require logging in separately.

This so-called *single sign-on* is in particular required for services that run concurrently over various tools and sources. A good example is an investigator that wants to launch a query in all relevant data repositories, such as SIS, the Europol Information System, Interpol databases and potentially in the future also certain national systems.

The response would most likely be based on a hit/no hit mechanism to enforce control and coordination. Nevertheless, running such a search in various environments and getting results in one integrated overview, is an essential and important step towards the realisation of the Principle of Availability.

Although perhaps not strictly necessary from the beginning, it would be recommended at some point to consider the implementation of a simplified and standardised model of user profiles, as described in chapter 2. Scalability and efficiency will require a simplification of identity management and authentication mechanisms, especially if in due course also national data repositories would be made available under certain conditions. This, of course, does not imply reducing the security and data protection controls.

Having the model of user profiles implemented in this third stage of development would also be beneficial from a business perspective. It would enable the single sign-on necessary for the referred services across various domains and tools.

Not only the investigator would benefit from this, but also the staff tasked with the coordination of cross-border information exchange (SIRENE, NCB, ENU). An important key to the success is the swift follow-up to successful queries. Therefore, also for the international coordination function immediate access to relevant domains, tools and data sources is of essential.

The way the single sign-on would work as follows: Based on the concrete business needs of staff their access rights for accessing and data processing in cross-border domains, applications and data sources, are managed by the authorities within the state or international organisation they work for.

The access authorisation provides the user with the credentials necessary to access the domains, tools and sources they are allowed to access. However, when accessing foreign services the access credentials do not have to be checked again, because the authentication is already executed in the local environment.

This local authentication is trusted by the target system and, based on the forwarded user reference and credentials, the user will be allowed to access and use the functions he is authorised for. Although the user reference transmitted in this process does not have to reveal the identity of the user, it remains available to trace back the identity through the access authoriser in case of any breach of confidentiality, security or data protection.

As described in chapter 2, the concurrent processing across various domains comes with specific requirements for the effective auditing of actions from a data protection and security perspective. It must be possible for auditors to trace the activities of users and the results this has triggered with the same simplicity as offered to the user. To this purpose integrated audit logging must be foreseen, where the activities of individual users across the various systems can be traced in the order of execution.

Also in this third stage of the IXP, the central portal itself is not intended for the processing of personal data related to crimes. It only re-directs the users to the tools intended and suited for that purpose. The search function discussed previously as example should be considered as an integrated service that falls under and has to comply with the security and data protection provisions of the individual data processing tools it provides access to. It goes without saying that such a service is hosted and operated in an adequately protected environment.

Also in phase 3 the strict separation between networks with different classification levels is consistently maintained. In this phase, however, there is the business requirement to enable a single search across various data repositories that may be hosted on domains with a different confidentiality level.

To accommodate this requirement the query is transported from the network on which the main IXP platform runs, to networks with a higher classification level by means of a one-way diode. This ensures that only one-way traffic is possible. The results of the queries are not communicated back to the user directly. Instead, the notifications go to the SPOC through adequately protected channels. The SPOC then has the responsibility to follow-up on the result, most likely through exchange of information with the SPOC of the Member State that holds the information and to deliver the result to the user that launched the query through appropriate procedures and means that respect the confidentiality of the exchanged information.

4. Preconditions for the platform evolution

The evolution over time through the three phases mentioned above to reach the envisaged end stage will come with a number of challenges. In particular, for reaching phases 2 and 3 some assumptions are made that deserve clarification in order to understand what needs to be done. These assumptions are related to the interoperability of existing identity and access management mechanisms, the interconnection of networks and the alignment of general services like search in business applications to allow for data processing across multiple applications.

In general, it is assumed that all law enforcement authorities in the Member States have a robust framework for unified identity and access management in place (which is not always the case). It is also assumed that national solutions can be made interoperable with identity and access management mechanisms of EU-wide systems. To a certain extent in phase 1, but certainly after that, it is imperative to have common standards and a compatible infrastructure in place that facilitate the authorisation, authentication, access control and auditing of users across networks and systems.

The transition from phase 1 to phase 2 requires that users can access various restricted networks, depending on their specific needs. This implies that these networks are to some extent interconnected and accessible by end users, and that mechanisms are in place to manage compliance with the applicable security regimes. Not all users will be authorised and not all actions will be permitted.

The transition from phase 2 to phase 3 offers the possibility to unify services of various applications, such as launching a query in various databases. Implicitly this requires from those applications that they offer comparable services and that they respond similarly to the actions of the user. Equally as for the identity and access management, this requires the development and implementation of common standards. It is expected that the establishment and evolution of the Universal Message Format (UMF2) can provide for such standards.

Also in terms of security common standards are required. The principle that navigation can only be made possible between networks with a similar confidentiality level is essential to ensure adequate protection and trust.

It speaks for itself that the work on security risk management and risk mitigation will continue throughout the evolution of the platform and in particular in preparation for the next phases of the IXP development.

5. Outline for the realisation of phase 1 of the IXP

An assessment of the expected work required for developing and implementing phase 1 of the IXP has resulted in a cost estimate of around € 1,365,000. This includes the annual maintenance and operating costs of around € 250,000. These figures do not include the resources required for content management, business product management and the roll-out to the user community. These costs depend on the availability of identity and access management mechanisms, national infrastructure and the ambition level as to the content and outreach of the platform.

High-level estimates for the timelines indicate that the first phase could be realised in a timeframe of **18-24** months. An important factor in this timeframe is the elaboration of the detailed user requirements, which will require engagement and involvement of the business representation of Member States and other stakeholders.

6. Options for governance

The development and implementation of the IXP can only be successfully realised if there is a sound and sustainable perspective for governance and funding. Several options have been identified and compared. The following three options were considered most realistic:

1. **Europol. Within Europol a product management framework is established for the IXP with representation of relevant stakeholders (Member States, EU Agencies, Interpol, Non-EU States, Commission). The design, development, implementation, operation, maintenance and further evolution are executed by Europol under the guidance of the stakeholders represented in the product governance framework. The costs for IXP would be funded by an increase of the Europol budget, including an adequate increase of the number of staff.**
2. **EU Agency for large IT systems. A similar arrangement is made as described above under option 1, but then the referred tasks related to the IXP would be executed by the EU Agency for large IT systems. Also for the funding a similar arrangement would be made as under option 1.**

3. **<u>Action Grant</u>. Phase 1 is initiated as a Commission funded pilot project by a consortium of stakeholders. These stakeholders take a joint responsibility for the governance and implementation of phase 1 of the IXP. If the pilot turns out to be successful, then a structural governance and funding framework, such as the ones mentioned under options 1 and 2, takes over the governance, management and further evolution of the IXP.**

For option 1 it was identified that the wide scope of the IXP exceeds the boundaries of the Europol mandate and mission. Moreover, in the current economic climate chances for an increase of the Europol budget and staff are limited. The IT capability is already overstretched and would have severe difficulties absorbing the tasks related to the IXP without an increase of resources.

The EU Agency for large IT systems has just been established. Although there is room in its legal framework to support new developments, the actual possibility for the Agency to support such developments will only come in a couple of years, when it is fully settled and incorporated its current tasks.

Option 3 has been identified as the most viable solution to start in a reasonably short timeframe. The project based funding does, however, require that a future embedment in a standing organisation takes place to ensure the sustainability of the product governance and funding. This clearly requires and is dependent on the initiative of at least a number of Member States to turn the IXP into a success; in terms of technical development as well as in providing and maintaining sufficient content at an adequate level of relevance and quality. Based on the comparison of the options, the EU Agency for large IT systems would be the most likely environment for such a future embedment. Therefore, active participation of the EU Agency for large IT systems in the pilot project is advised to ensure a smooth transition in due course and with that, the availability of resources from the side of the agency to follow the development is an important factor for future evolution.

7. Next steps

This high-level solution definition for the IXP has been amended and extended in several rounds of consultation. Still, also in this latest version it is to be submitted for consultation and adoption in several gremia, including **(…)** DAPIX on data protection.

In regard to the preconditions referred to in paragraph 4 it is advised to create an Action Point on the 4th IMS Action List (July 2014-December 2015) to assess the extent to which the preconditions are met for the phases 2 and 3 of the IXP evolution and to identify the concrete work that needs to be done to prepare for the interoperability between the various identity and access management systems in place.

(…)

DAPIX delegations are invited to discuss this document at their meeting of **27 March 2013**.