High-level expert group on information systems and interoperability

Set up by the European Commission

Interim report
by the chair of the high-level expert group

December 2016

1. INTRODUCTION

The European Union currently faces the 'parallel challenges of migration management and the fight against terrorism and organised crime.' As set out in the Commission's April Communication *Stronger and Smarter Information Systems for Borders and Security,*[1] citizens in the EU rightly expect that migration is effectively managed so that we have confidence in knowing who is entering the EU. They also expect that security for all remains a prime objective, to be achieved in part by ensuring that the EU manages its external borders and shares information effectively.

Information systems, by providing border guards and police officers with relevant information on persons, are essential for both external border management and internal security in the EU. The Communication affirmed that there is room for improvement, whether in existing systems or developing new systems. One major path to this end would be through improving the interoperability of information systems as a long-term objective — an objective endorsed by the European Council and the Council.

The Commission therefore decided to set up a high-level expert group on information systems and interoperability, which I have the honour to chair. It comprises experts from Member States and associated Schengen states, and from the EU agencies eu-LISA, Europol, European Asylum Support Office, European Border and Coast Guard (Frontex) and the Fundamental Rights Agency. The Counter-Terrorism Coordinator and the European Data Protection Supervisor also participate as full members of the expert group. In addition, representatives of the secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and of the General Secretariat of the Council attend as observers (see annex for full list).

The high-level expert group aims to submit its final report by the end of April 2017, following which the Commission has indicated it may present proposals on further steps to be taken. The current situation demands that we advance our work as rapidly as possible. The group has agreed that the chair should report already on the work so far, and set out some interim findings and possible ways forward. This is the purpose of the report, which provides a review of the group's work over the first six months of its operation.

1.1. Meetings

The high-level expert group has met three times since its formation.

At the high-level group's first meeting in June 2016, experts established its working methods and timeline. On substance, they agreed on the need to exploit the existing information-sharing environment — notably for the Schengen and visa information systems (SIS and VIS) and Eurodac — and to build upon it after having identified gaps. The group committed to examine various means to improve the interoperability of systems: single-search interface; a shared biometric matching service; and a common repository of data.

In its June meeting, the group also decided to set up three subgroups, one each to examine existing systems, new systems and the interoperability of systems. The subgroup on existing systems has met twice, on new systems once, and on interoperability three times. These subgroups report back to the high-level group with their conclusions and proposed recommendations.

The high-level group's second meeting took place in September. The group emphasised the importance of ensuring the highest standards of data quality and

[1] COM(2016)205, 6 April 2016.

using systems to their potential. The discussions reflected a sentiment that existing systems and practices should be improved before thinking of developing new ones. One particularly promising path to be considered would be a single-search interface for accessing EU systems. The group also acknowledged the need to address conditions of access for law enforcement purposes, and governance of systems generally. When considering information gaps, the group reacted to the Commission's latest thinking, thereby providing input for the subsequent Commission proposal to establish a European travel information and authorisation system (ETIAS).

In the latest meeting, in November, the group considered a set of preliminary recommendations based on the work so far in the subgroups, primarily on single-search interface, data quality and a shared biometric matching service. It also considered the need to identify the obstacles and solutions for law enforcement access, not only for Eurodac but also for the Entry/Exit System (EES) and VIS, and whether such obstacles could be overcome by technical solutions. At this meeting, it was also restated that the group's work is firmly based on all relevant data protection and fundamental rights considerations.

This interim report builds on the discussions and findings that have taken place during all the meetings so far, and in particular of this latest meeting. I have prepared but not consulted this interim report with the members of the high-level group and further meetings will show whether I have faithfully reflected the state of our discussions.

2. FUNDAMENTAL RIGHTS AND DATA PROTECTION

Respect of fundamental rights and data protection rules is a bedrock of the work of the high-level expert group. This was clearly stated in the April Communication that gave rise to the group and it has continued throughout its meetings. As already indicated, the European Data Protection Supervisor and the Fundamental Rights Agency participate as full expert members of the group.

Effective controls at external borders are necessary for the effective management of migration and to contribute to internal security, as does the exchange of information between Member States. The controls are not solely about identifying irregular migrants or terrorists or criminals. They can also serve to identify and protect persons such as victims of trafficking or abducted children. The fact that the Schengen Information System includes missing persons serves to enhance their protection. If Eurodac shows that a person is an asylum seeker, the person's data will not be shared with third countries, especially not with the country of origin.

These and other examples demonstrate that technology and information systems for border management and law enforcement can help public authorities to protect the fundamental rights of citizens. This positive effect of information systems on the fundamental rights of persons is often ignored, and deserves more attention and emphasis.

Nevertheless, the use of personal data envisaged in these systems also raises questions about their impact on the right to privacy and the protection of personal data. Our group has been very sensitive to such potential privacy risks. As a group, we have constantly noted that personal data should only be retained for as long as necessary for the purpose for which they were collected.

Effective controls at external borders and the sharing of information, therefore — and the systems used to apply them — are to be implemented in compliance with data protection principles, including data protection by design and by default, and the requirements of necessity, proportionality, purpose limitation and quality of data.

Improving the systems offers the prospect of making decisions with greater confidence that they are the right decisions based on reliable and up-to-date data.

This is not about administrative convenience but is clearly in the public interest. Information systems that do not perform well or are not properly used may produce false matches, or no matches at all, which may negatively impact on the fundamental rights of persons. Systems that are unsafe and that can be easily hacked will bring personal data into the wrong hands, and could expose people to great risks. Appropriate security measures, adequate safeguards and effective rebuttal mechanisms will therefore be part and parcel of any information system.

The group will continue to take full account of the recommendations of the European Data Protection Supervisor and of the Fundamental Rights Agency. We acknowledge that their early involvement in the design and further evolution of EU information systems is essential to ensure their systems fully comply with all relevant fundamental rights considerations.

3. SUGGESTED ORIENTATIONS FOR THE FINAL REPORT OF THE GROUP

The Communication *Stronger and Smarter Information Systems for Borders and Security* defines 'interoperability' as the ability of information systems to exchange data and to enable the sharing of information. It distinguished four dimensions of interoperability, each raising technical, operational and legal issues, including on data protection:

- a single-search interface to query several information systems simultaneously and to produce combined results on one single screen;
- the interconnectivity of information systems where data registered in one system will automatically be consulted by another system;
- the establishment of a shared biometric matching service in support of various information systems; and
- a common repository of data for different information systems.

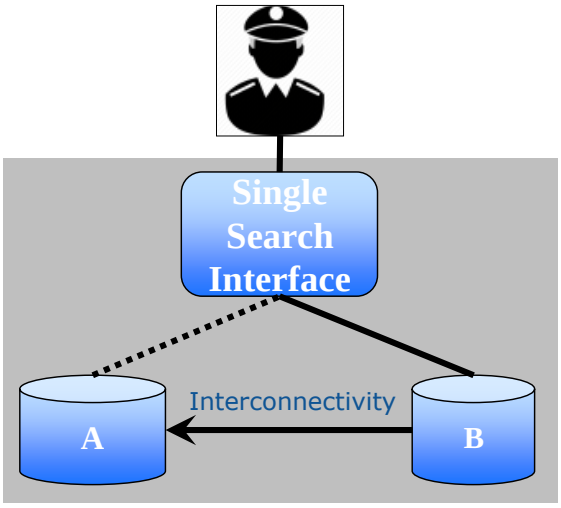

Figure 1: Single-search interface v interconnectivity

The expert group has discussed each of these dimensions of interoperability in considerable detail. An important finding was that the second option (interconnectivity of systems) should only be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system.

Consider the example with two systems, A and B that can be consulted via a single-search interface. The interconnectivity of system B with system A only makes sense if system A systematically and automatically needs to store and process data from system B.

If no data reuse is necessary or if such reuse requires a human (legal) decision, the interconnection is without interest: the single-search interface is a better and sufficient option.

One real example is the interconnection of the Entry/Exit System (EES) and the Visa Information System — as proposed in the draft EES Regulation — where data contained in VIS would be systematically and automatically consulted by the EES in order to store a very small sub-set of VIS data (visa-sticker, number of entries, period of stay). This would enable the EES to process data on visa-holders correctly while at the same time meeting the requirements of data minimisation and data consistency. The group considered that — provided sufficient progress is made on

the other three dimensions of interoperability — there is less need for interconnectivity between systems for the sole reason of improving and facilitating access to and exchange of data.

Our first suggestion would therefore be to focus further discussions and reflections on the three remaining dimensions of interoperability: the single-search interface, the shared biometric matching service and the common repository of data.

The group considered one aspect to be of fundamental importance, and a precondition for any progress towards the better use of systems: the quality of data.

3.1. Cross-cutting issue: data quality

Chair's suggestions

- Explore, together with eu-LISA, options for establishing — for all systems under the agency's operational responsibility — automated data quality control mechanisms and common data quality indicators.
- Explore, together with eu-LISA, the possibility of establishing a data warehouse with anonymised data and the various examples of reporting that it would enable.
- Agree — for each of the relevant systems and within the responsible governance frameworks — updated rules for scrutinising data quality and data quality reporting processes.
- Establish a biannual peer review of data quality.
- Develop relevant training modules on data quality for staff responsible for feeding the systems at national level.

The Communication *Stronger and Smarter Information Systems for Borders and Security* stated that systems such as the Schengen Information System (SIS), the Visa Information System (VIS) and Eurodac — but also other mechanisms like the Prüm Decision[2] on cross-border cooperation — are up and running, but that Member States could use them better. Our group discussed this challenge on several occasions. We looked in particular into the cross-cutting issue of improving the quality of data submitted into the respective systems.

Each information system used for processing data put in by human operators is prone to have data quality problems. This can have consequences not just for not being able to identify irregular migrants or terrorists, but also by affecting the fundamental rights of innocent people. Various automatic validation rules are thus implemented to prevent operators from making mistakes. Examples include checks on empty fields, checks on unallowed characters, checks on formats, checks on dates, and checks on inconsistencies.

The automated quality, format and completeness checks imposed or suggested by the (central) systems should be improved or completed. To prevent rejections on the central level, these checks then need to be implemented in an identical way at the point of input in the source systems. The group considered that further analysis is required on the possible development of automated data quality control of the various data fields in SIS, VIS and Eurodac, and in any new systems. Common data quality indicators are also required for the purpose of automated data quality control (see Figure 1).

[2] Council Decision 2008/615/JHA of 23.6.2008, OJ L 210 of 6.8.2008.

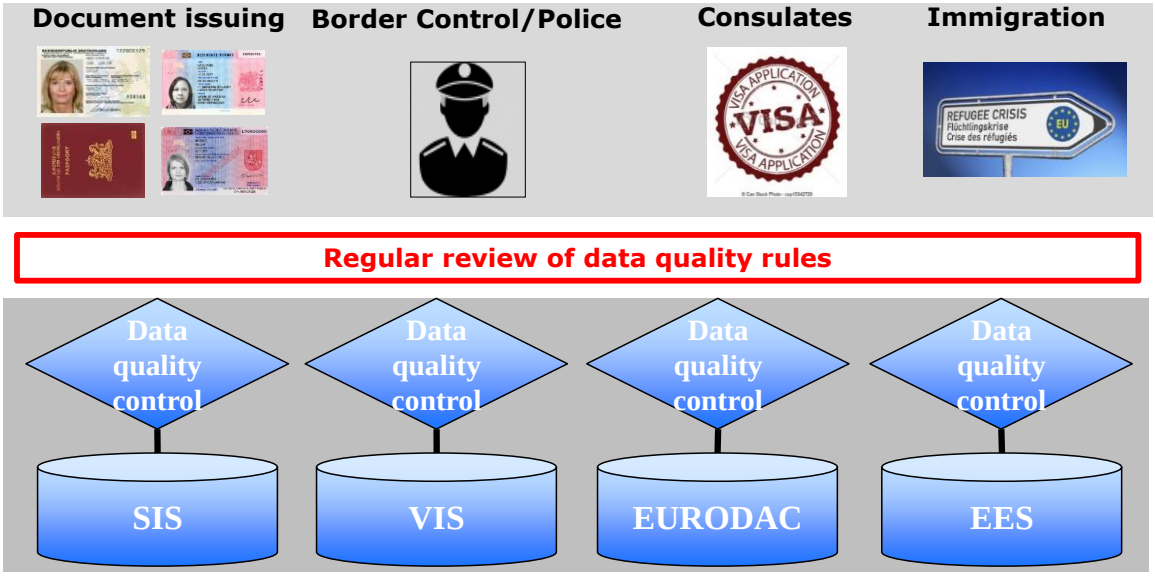

Figure 2: Improving data quality[3]

In this context, a balance must be found between strict rules and end-user flexibility, while recognising the specificities of the information system and its user community. The collection of validation rules should be regularly reviewed to cope with business, organisational, technical and political changes. Member States remain responsible for the quality of their data. Therefore, the goal of such a data quality control mechanism will be for the central systems to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions. It is to be noted that, on 21 December 2016, the Commission's proposal concerning the Schengen Information System already reflected some of the discussions on data quality that took place in the high-level expert group. Similar to the approach taken in the EES proposal of April 2016, this SIS proposal aims to empower eu-LISA to produce data quality reports to Member States at regular intervals. This activity could be facilitated by a data repository for producing statistical and data quality reports.

The group considered that operator training and awareness-raising, peer pressure and end-user feedback should be used to remedy poor data quality. Such a lack of quality can become apparent when performing *ex post* statistical reporting and audits to monitor and improve data quality.

A second approach to improving data quality is the creation of a data warehouse containing anonymised data extracted from the systems (see Figure 2). This could facilitate the processing and analysis of these raw anonymous data and subsequent statistical reporting. While many reports can be (and are) created using the actual personal data in the parent systems, this is not a best practice for several reasons:

- all data, including personal data, is directly accessed, which is not proportionate;
- such a bulk approach constitutes an extra processing burden on the system:
- it requires dedicated and secured reporting infrastructures for each system; and
- it prevents holistic 'cross-system' analysis by only looking at data from one system.

[3] Currently, Eurodac records fingerprints only but under the current proposal this will be extended to include alphanumeric data.

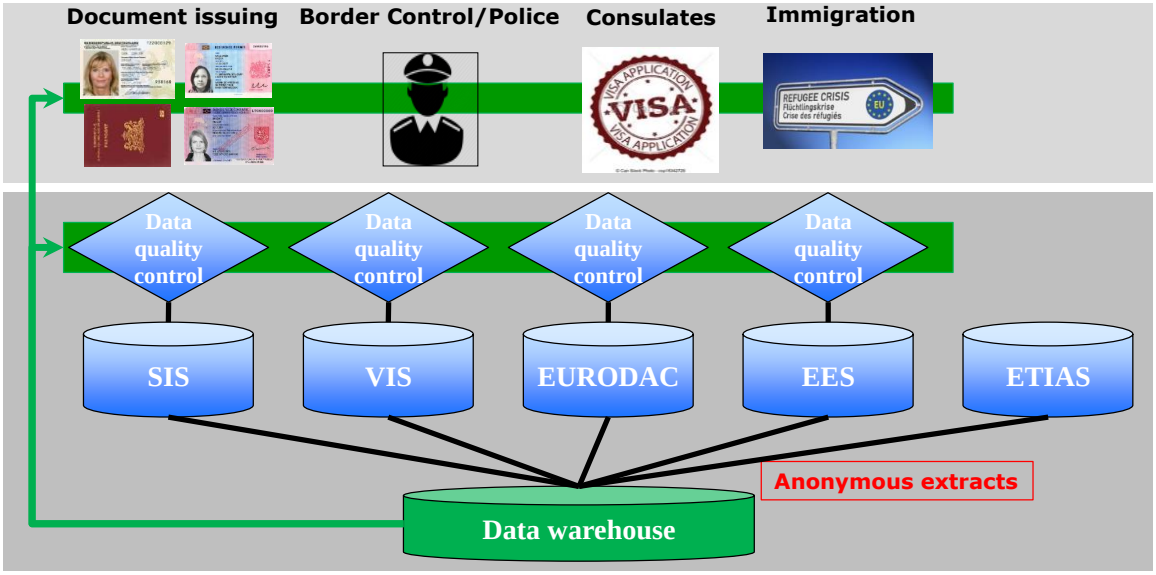

Figure 3: Data warehouse

In addition to avoiding these downsides in current practice, a data warehouse would be able to generate reports that will help Member States to better use the systems, including by taking informed decisions on EU policies in the area of migration and security. Examples include:

- the percentage of empty fields in SIS person & object alerts, in VIS records and in future systems, grouped by Member State authority;
- the percentage of visa overstayers by country of first entry, grouped by third country;
- the percentages of nationalities that enter in a different Member State than the one indicated in the visa application; and
- the distribution of fingerprint quality by Member State, authority and parent system.

3.2. Establishing a single-search functionality

Chair's suggestions

- Explore, together with eu-LISA, a proof of concept on the feasibility of creating a European search portal capable of searching in parallel all relevant EU systems. The proof of concept would consist of a study and a pilot project focusing in particular on SIS and VIS.[4]
- Explore, together with eu-LISA and Europol, whether Europol data could be accessed through a European search portal, and if so, under what conditions.
- Explore, together with eu-LISA and Interpol, whether Interpol databases could be accessed through a European search portal, and if so, under what conditions.

The Commission issued a questionnaire on the use by Member States of single-search interface (SSI) solutions. A main finding was that all Member States use an SSI of some kind. Following discussion in the group, we concluded that the development of a standardised national SSI is unnecessary and impractical.

However, the development of a **centralised** SSI or **European search portal** was considered promising. It would be capable of searching various central systems (SIS,

[4] The proof of concept of a European search portal would by default accept transactions compliant with the interface control documents of the various systems (pass-through) but in addition would implement search transactions under the third phase of the Universal Message Format project. It should therefore be ensured that the proof of concept will accept transactions from SIS and VIS channels using both the SIS/VIS interface control document formats and the third–phase Universal Message Format.

VIS, possibly the Europol data, Interpol's Stolen and Lost Travel Documents database, the future European Criminal Records Information System (ECRIS) insofar as third-country nationals are concerned[5] and the future EES, ETIAS and the new Eurodac) (see Figure 3). An assessment of such a European search portal would be undertaken, but it would be expected to require relatively minor technical changes on the national side.

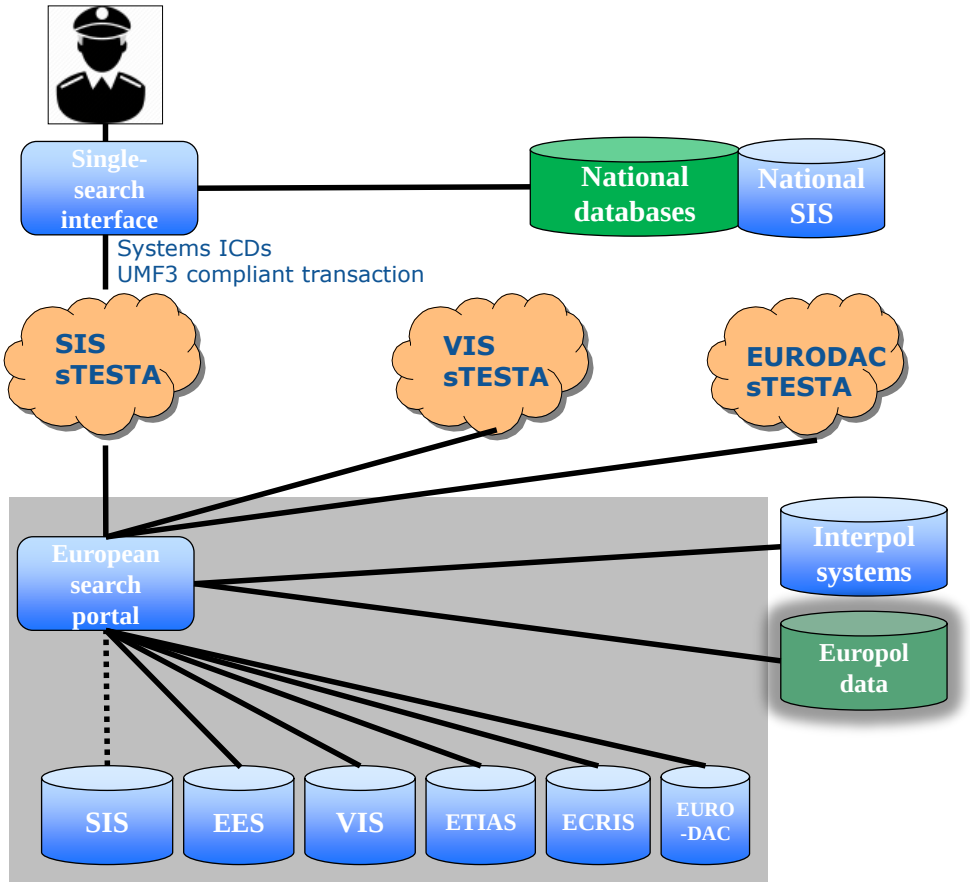

Figure 4: Conceptual view of a European search portal[6]

A European search portal would not connect to national databases. Existing national SSI solutions would remain necessary for that purpose. These national SSIs would, however, be connected to the European portal for the querying of relevant EU systems in line with existing rules on access and use of the data.

The potential practical and operational challenges for Member States to fully exploit the benefits of such a centralised SSI would need to be further explored. Europol efforts to incorporate queries to its information systems via its web service QUEST (Querying Europol Systems) in national SSIs (including through a pilot project) is promising and should be supported: it is expected to go live in the first half of 2017. Looking to the future, the introduction of QUEST also anticipates the eventual linkage of the Europol data to a European search portal.

---

[5] At the current time, the European Criminal Records Information System for the exchange of criminal records information is a decentralised system. As such, it does not lend itself well to being included in a number of the initiatives discussed by the expert group. However, a proposal to provide for a new solution for third-country nationals and stateless persons was put forward by the Commission in January 2016. Discussions at Council level have now demonstrated a clear preference for a centralised system. A revised legislative proposal is needed and in the preparations for such a proposal, the work of the high-level expert group will be fully considered. For that purpose, a specific expert meeting has been organised for January 2017 to discuss how the work of the group can best be reflected in this respect.

[6] sTESTA (Secure Trans-European Services for Telematics between Administrations) is the EU's secured dedicated communication infrastructure. It is soon to be replaced by a new generation version TESTA-NG.

The possibility to search the Interpol systems (Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated With Notices (TDAWN)) via a European search portal, greatly facilitates access to this international data (not all available in European systems) in particular for Consular affairs and Asylum/migration entities.

The fact that these Interpol systems are (also) being fed by non-European countries will require a specific focus on data protection issues.

3.3. Building a shared biometric matching service

Chair's suggestions

- Request eu-LISA to analyse the technical and operational aspects of the possible implementation of a shared biometric matching service on the basis of the required new EES infrastructure. Such a new biometric matching service for EES should include scenarios for integrating other relevant systems. Once established, this EES-based biometric matching service could be used to progressively match biometric data from SIS, VIS, Eurodac and potentially other systems.
- Invite Europol, together with eu-LISA, to analyse how such a shared biometric matching service could also match biometric data from the Europol data.
- Explore, together with eu-LISA and the Prüm stakeholders, options for supporting the Prüm exchange and hosting national data from automated fingerprint identification systems in a shared biometric matching service.
- Explore, together with eu-LISA, the technical and legal aspects of utilising the future shared biometric matching service for the purpose of flagging the existence of biometric data from other systems.

The legal instruments of SIS, VIS, Eurodac and the Entry/Exit System do not prescribe the technical implementation details of the infrastructure that performs the fingerprint identification functions. Instead of a dedicated automated fingerprint identification system per individual system, a shared biometric matching service (BMS) could be implemented (see Figure 4). Whereas the former is only capable of matching fingerprints, the biometric matching service would be able to process both fingerprints and facial images. And rather than serving just one system, the shared biometric matching service would perform identifications and verifications for all the centralised systems (SIS, VIS, Eurodac, the future Entry/Exit System and the European Criminal Records Information System for third-country nationals, and possibly the Europol data). This would not necessarily require any changes to the legal instruments as each parent system will by default only search within its own data, in line with existing rules on access and use of the data. Personal data protection rules enshrined in the legal bases of the systems will be respected by compartmentalising the data, with separate access control rules for each category of data.

A shared biometric matching service has a number of potential advantages:

- easier, better, more secure and cheaper operations and maintenance of one single biometric system (which are generally very complex systems) from one provider;
- cheaper to procure/implement one system instead of six separate systems; and
- the prospects of better data protection.

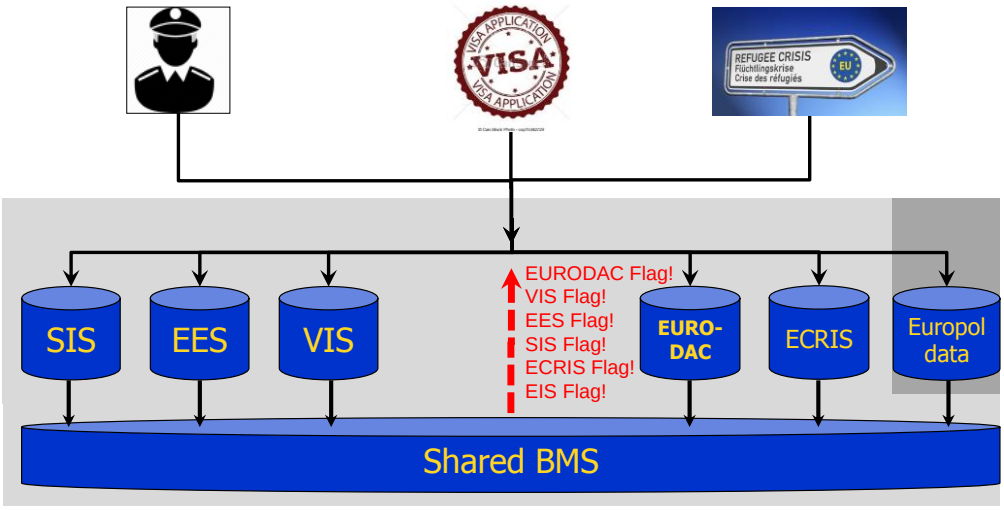

Figure 5: Shared biometric matching service (BMS) with 'hit flags'

In addition to these economies of scale, a shared biometric matching service would also open the possibility for a very important innovation: it would enable single searches with biometric data. A person who is the subject of a check can be registered in several systems simultaneously — potentially under different identities — given the specific purpose of each system. Public authorities should be able to obtain reliable and up-to-date information about the status of such persons on the basis of possible matches from all relevant EU systems. While various scenarios can be envisaged, the group considered that the most solid in terms of data protection safeguards is based on anonymous hit/no-hit 'flags'. The shared biometric matching service would match biometric data from various 'parent systems' such as the Entry/Exit System, SIS, VIS and Eurodac. At the same time, it would respect the original data access control of the parent system and the need to comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data. These aspects could be further explored with the European Data Protection Supervisor and the Fundamental Rights Agency. The shared biometric matching service could be designed in such a way that the specific search transaction from a parent system (a fingerprint search from Eurodac for example) would not only contain the specific data of that system (the asylum seeker's identity in the case of Eurodac) but in addition a flag indicating possible data from other systems.

These hit/no-hit flags would not contain any specific data. They merely indicate the possibility of finding specific data, on the person in question, in another system.

Reporting this flag to indicate the presence of data in other systems would require changes to the legal instruments of all systems for which such a flag is requested.

In addition to matching biometric data from EU systems, the shared biometric matching service could also host purely national data, thus potentially relieving Member States of having to operate and maintain complex and expensive biometric systems. This centralised hosting of national data could be interesting for the Prüm exchange by providing a centralisation of searches and an improvement in performance; it would need to be explored in detail.

3.4. Towards a common repository of data

Chair's suggestions

- Explore further whether it is necessary, technically feasible and proportionate to extend to other systems the common identity repository envisaged for the Entry/Exit and European Travel Information and Authorisation systems.
- Request eu-LISA to analyse the technical aspects of the establishment of a common repository of identity data, including the requirements for eventually relocating data from existing systems (SIS, VIS, Eurodac) into such a common repository.
- Request eu-LISA and Europol to analyse the same for Europol data.
- Explore, together with the European Data Protection Supervisor and the Fundamental Rights Agency, the data-protection implications of the establishment of a common repository of data.

The establishment of the shared biometric matching service would bring immediate advantages on its own. In due course, it could also be complemented by the development of a common repository of alphanumerical identity data. Starting with the biometric attributes of an identity, a further step could be to migrate the common biographical attributes (such as name, date of birth, gender) from the various existing systems to a centralised common repository (see Figure 5). Establishing such a common repository would overcome the current fragmentation in the EU's architecture of data management for border control and security and the related risk of blind spots. This fragmentation is linked to the way purpose limitation of each system is currently being implemented, and it results in the same data being stored several times. A common identity repository for all systems would also help to avoid duplication and overlaps of data.

The identity records in the common repository would be linked to specific data that remain in the system that actually 'owns' this identity record. All established and future rules and limitations on access control are obviously also applicable to the records in the common identity repository.

The common repository of identity data and the shared biometric matching service would enable single identifications using biographical and/or biometric data, based on a hit/no-hit concept, in line with existing rules on access and use of the data. This could drastically facilitate the work of law enforcement entities while limiting pointless access to sensitive data.

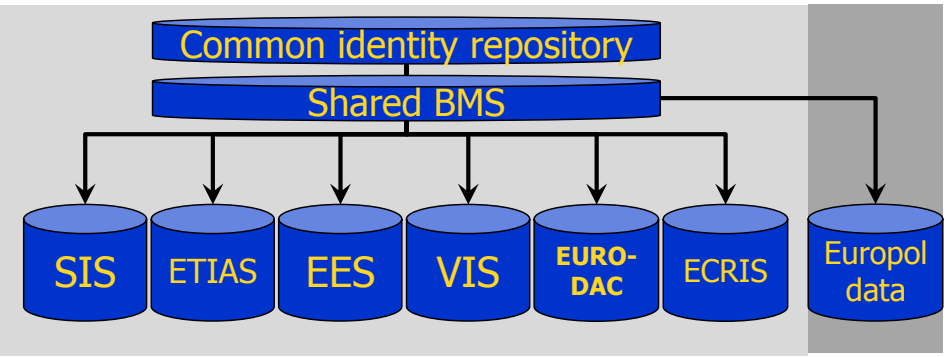

Figure 6: Conceptual view of a common identity repository

The Commission's legislative proposal for the establishment of the European Travel Information and Authorisation System (ETIAS) envisages already to put this concept into practice: *'ETIAS and EES would share a common repository of personal data of third-country nationals, with additional data from the ETIAS application (e.g. residence information, answers to background questions, IP address) and the EES*

entry-exit records separately stored, but linked to this shared and single identification file.' (COM(2016), 731 final, page 15).

Building on the envisaged common EES/ETIAS repository, and assuming that a shared biometric matching service will be established, it would be an additional step to also transfer biographical data of other central systems (SIS, VIS, Eurodac, possibly the European Criminal Records Information System for third-country nationals) into such a repository. To avoid duplication of data and to facilitate further efficiency in use of the systems, a data architecture for the justice and home affairs domain will also be required.

The inclusion of identity data from the Europol Information System would also be possible, even if this could be more complex given the differences in end-users and different access-control and sensitivity markers.

3.5. Cross-cutting issue: promoting the use of the Universal Message Format

Chair's suggestions

- Increase and promote the use of Universal Message Format (UMF) as the preferred message format. In this context, create 'translators' between UMF and SIS/VIS interface control documents, focusing first on persons and documents.
- Consider the potential need for a UMF committee, involving all stakeholders including eu-LISA and Europol, to pave the way for a wider and better use of UMF, especially considering the developments of the Entry/Exit and European Travel Information and Authorisation systems and other future systems.

Each information system uses a specific data model to organise and store the various properties of data processed. The specific interface or message format — often described in an interface control document — used to interact with the information system is closely linked to this data model and each interface may thus be different.

The UMF is one step towards creating a universal standard at EU level that can be used to orchestrate interactions between multiple systems in an interoperable way.

UMF facilitates the use of single-search interfaces but for existing information systems some form of 'translation' or reformatting will always be necessary.

4. CONCLUSION

There is a growing consensus among the members of the expert group on what issues should be addressed as a priority, in particular to respond to the real needs of the end-user, be it a border guard or a police or customs officer. These are presented briefly in this report.

Raising the standards of data quality and data usage across all systems is a cross-cutting issue. Improvements in this area will ensure that information can be effectively used and compared. Similarly, promoting the use of Universal Message Format will enable systems to benefit from the steps towards interoperability that we envisage.

At this stage, the group considers that the priority options to be considered in promoting interoperability come under three strands: developing a single-search functionality that could become a European search portal for centralised systems; building a shared biometric matching service as a means to raise the level of reliability in identifying persons and to retrieve an alert when data on the same individual is stored in other systems; and considering further whether a common repository of identity data should be an ultimate goal as a means to simplify and accelerate searches, and further minimise the risk of false hits.

In the coming months, the group will attempt to address the issues that are outlined in my orientations. In addition it will look into the following issues that fall under its purview.

- We will schedule for discussion whether it is legally possible, necessary and proportionate for the Entry/Exit System, once it comes into force, to be extended to cover EU citizens, or whether other, more effective, technological solutions can be introduced to meet the objectives of such an extension.
- We shall discuss the need and value of a possible European repository with data on third country nationals holding long-stay visas, residence permits and residence cards.
- Insofar as customs cooperation is concerned, there is a common interest in considering whether the benefits — not only in terms of security but also in terms of costs — that we are identifying for border management and security can apply for these systems too, and whether interconnections and synergies between customs systems and border management and security systems can be established.
- Another subject that merits further reflection by the group is the European Criminal Records Information System, where solutions for a centralised exchange of criminal records on third-country nationals are currently being considered, and which also raises questions of interoperability with other systems.
- Finally, the group should still take a closer look into the challenge of strengthening and improving the functioning of the Prüm cooperation, including at the level of both system architecture and governance.

The high-level expert group has had an intensive period of activity since it was constituted in June. As chair, I appreciate greatly the commitment shown by all those involved. This very much reflects the scale of the challenges that the group has been asked to consider and the urgent nature of the work in responding to justifiable demands of both political leaders and European citizens. These demands concern border management and security, but also data protection and fundamental rights.

The group is on schedule to present its formal report by the end of April 2017. It will then be for the Commission to react. In the April Communication, the Commission said it would present further concrete ideas to the European Parliament and the Council as a basis for a joint discussion on the way forward for policy on information systems in the area of freedom, justice and security.

Annex

Members of the high-level expert group on information systems and interoperability

The group is chaired by the Director-General of the European Commission's Directorate-General for Migration and Home Affairs. The Director-General is Matthias Ruete. It includes high-level representatives of the following entities:

Member State authority

Austria	Germany	Poland
Belgium	Greece	Portugal
Bulgaria	Hungary	Romania
Croatia	Ireland	Slovakia
Cyprus	Italy	Slovenia
Czech Republic	Latvia	Spain
Denmark	Lithuania	Sweden
Estonia	Luxembourg	United Kingdom
Finland	Malta	
France	Netherlands	

Other public entities

EU agencies

European Agency for Fundamental Rights (FRA)
European Border and Coast Guard (Frontex)
European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)
European Asylum Support Office (EASO)
Europol

EU institutions/bodies

Counter-Terrorism Coordinator
European Data Protection Supervisor

Third countries

Liechtenstein
Norway
Switzerland

Observers

Secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs
General Secretariat of the Council