High-level expert group on information systems and interoperability

Fourth meeting — 21 February 2017

Report

1. Introduction

The meeting was opened by Matthias Ruete, chair of the high-level expert group, highlighting the continuing urgency of the group's work in light of ongoing attacks and continuing calls for action from political leaders.

He also referred to the interim report, for which the main focus of the meeting would be to receive comments from experts specifically on the suggestions. This report had been well received at the informal meeting of justice and home affairs ministers in January as part of the overall discussion on IT systems for borders and security.

The draft agenda was agreed as presented.

2. Chair's interim report

The chair recalled that the interim report was his summary of the group's discussions and areas of agreement. He invited feedback on the suggestions set out in the report. This would in due course provide a basis for the group's final report, to be agreed by consensus.

a. Data quality

The chair recalled the suggestions set out in the interim report, noting that responsibility would in part lie with Member States. Some improvements could be made without recourse to designing new structures. Funding under the Internal Security Fund could be made available. eu-LISA reported that it had updated — partly in light of discussions in the group and with stakeholders — the previously circulated draft roadmap on a single-search interface. Work would progress soon on SIS and in due course on VIS and Eurodac.

---

1 See Chair's interim report: 
Comments from experts

There was general support for the suggestions as presented, and additional comments were made.

- Care is needed to limit the risk of data entered at national-level being rejected, perhaps by flagging poor data rather than rejecting it. Fuzzy data can also play a role but can also hamper investigations, so careful judgement is needed.
- Common data formats and data quality controls would offer real benefits.
- Ensure peer reviews are not burdensome.
- Pseudonymised data should also be considered in addition to anonymised data; the latter can present legal obstacles because it is not always truly anonymised.

The chair concluded the group recognised the importance of good data quality and of continually improving data quality standards. Peer reviews should be light at least in the first stages. While the goal is to ensure good data quality, the group accepts that there remains a place for fuzzy data. Existing frameworks should be used to the utmost.

b. Single-search interface / European search portal

The chair reported that the January Security Union Progress Report had announced the launch of a study on a European search portal, which was expected to lead to a feasibility study being ready by mid-May, to be followed by a proof of concept before the end of the year. He also distinguished National Uniform Interface (NUI) from single-search interface (SSI) while noting that both would be expected to work together.

The Commission also advised that it was commissioning a study already based on the interim report. This would examine possibilities to consult not only the central systems managed by eu-LISA but also Europol data and Interpol systems. As for the data quality, the initial study (including UMF/ICD\textsuperscript{2} aspects) would be followed by a proof of concept (in 2017) and in due course examination of legal and financial aspects.

Comments from experts

Experts expressed general support for the approach.

- Be careful to ensure than an extra query level does not lead to delays, and that combining security and migration objectives does not create legal obstacles. An SSI should not lead to extensive system requirements at national level.

\textsuperscript{2} Universal Message Format / Interface Control Document.
• Doubts were expressed whether ECRIS should be included in an SSI, but there was general support for including Europol (in line with the QUEST project) and Interpol.

• A flagging system for biometric searches should be considered, which would require agreed standards for biometric identifiers.

• Clarity was also needed on what would be the expected follow-up of a hit following a query, especially for systems other than SIS.

• It was argued that the EBCG in particular could benefit from such an approach

• Potential implications for fundamental rights and for data privacy were raised. Also, any attempt to simplify (or combine) systems requires a proper risk assessment. The point was also made that data privacy by design is to be part and parcel of systems. It was also argued that a European search portal, including a flagging system, could be designed in a way that provides the desired results while also safeguarding data privacy.

• A first step towards a European search portal should be to ensure that all existing systems are being used to their fullest potential.

The chair concluded that the group's final report should set out clearly the purpose of a single-search interface / European search portal, which is essentially to facilitate the work of those who have rights to access the systems concerned (especially SIS, VIS, Eurodac). The development of a single-search interface / European search portal should include a proper risk assessment, including aspects related to logging and finance. Other aspects to be considered are centralised identity management, data protection, and devising a flagging system in the context also of those who do not have access rights to the flagged system. A more detailed proof of concept outline should be prepared.

c. Shared biometric matching service

The chair again referred to the January Security Union Progress Report, in which the Commission stated that work towards a shared biometric matching service was a top priority. Questions to be considered included whether it was feasible to construct such a system, how it could work with Europol and Prüm and how flagging could be implemented.

eu-LISA reported that it had started work on a study, which was looking at construction feasibility and Europol. Issues related to Prüm and flagging would be for a later stage. At the very least, such a system would require common standards for biometric data.

Comments from experts

Again, there was general support, and interest in the eu-LISA study.

• Discussion on flagging provisions should consider whether notifications are sent not only to those with authorised access to the information but also to others for whom a procedure would then be needed to make the information available as appropriate.
• Sharing data is not the same as mixing datasets.
• Interpol and NIST standards could provide some guidance for determining standard formats for data exchange.
• With a view to limiting any risks in dissemination of data, consideration should be given to logging those who access the system.

The chair concluded that the group generally welcomed the move towards a shared biometric matching service, acknowledging that technical and operational questions are to be considered. Formats currently in use should be considered by examining how they would have to change to be part of a shared system. Financial aspects and data protection elements of flagging should also be considered.

Scenarios to be considered:

• A person can submit a query to the shared BMS and will receive a response if they have access rights.
• A response can flag the presence of data in a system to which a person does not have access rights. Consideration could be given to informing those responsible for that system that another ongoing search has led to data in this system being flagged.
• A response can flag the presence of data in a system to which a person does not have access rights, but in this case the national entity coordinating the use of that system could be informed as to who exactly has been querying the shared biometric matching service with a view to making contact.

d. Common repository of data / common identity repository

The chair reported that the subgroup on interoperability had held a substantial discussion especially to consider data protection aspects. The discussions had reflected the view that those resorting to identity fraud cannot rely upon data protection.

A common repository of data — or rather common identity repository — would enable linking, potentially fraudulent, biographical data together, regardless of the 'owning' system. Using this with a shared biometric matching service would enable linking biographical data together, based on biometric matches. A common identity repository would provide a view. The view would differ according to access rights, a bit like seeing the view through different spectacles.

The Commission presented how a common identity repository could fit in to an overall architecture. A shared biometric matching service would enable linking biometric data of the same person together, regardless of the 'owning' system, authority or legal basis. A common identity repository would enable linking, potentially fraudulent, biographical data together, regardless of the 'owning' system. By using both, it would be possible to link biographical data together, based on biometric matches, to combat identity fraud.
In response to those who questioned whether a European search portal and a common identity repository both had a role to play, it was noted that Europol and Interpol systems would continue to be searched via the European search portal. Moreover, the common identity repository would not necessarily be a database as such; data would remain held in the basic systems.

**Comments from experts**

Experts generally saw the benefits of the common identity repository but made the point that other priorities existed before fully committing to this one, as set out in the chair’s interim report.

- Issues related to data protection and fundamental rights were again raised, in particular by ensuring that proper consideration is given to what is specifically provided for under the legislation, for example in terms of access rights and purpose limitation.
- Questions were raised about whether views would be stored, and what would be the potential risk from hacking.
- While acknowledging the potential benefits of such a system, some considered that it would be a challenging project, but that it could nevertheless be justified if the purpose and consequences were clarified in detail. Do not try to advance too quickly, especially given the activities already ongoing (EES, ETIAS, Eurodac, SIS…)
- Others saw benefits and distinguished the roles of national single-search interfaces, a European search portal accessing Europol and Interpol, and a common identity repository for EU centralised databases.
- A business case would be helpful to justify its role in combating crime and fraud, especially as ultimately a common identity repository could play a key role in countering attacks.
- The FRA reported its intention to publish a paper addressing fundamental rights aspects of interoperability generally, to be shared with the group before the final meeting.

The chair concluded that the group acknowledged the different conceptual framework of a common identity repository. The group would recommend further study to have a better understanding of the potential design, operation and benefit of such a repository.

### e. Universal Message Format

The chair recalled that Universal Message Format is an important enabler for the exchange of data across systems. It is in use with the Europol Information Systems, via the QUEST interface, and could be considered for the European search portal as the primary input and output format, to be reflected in a proof of concept.

The UMF 3 project currently led by Germany requires that consideration be given to the governance of its further roll-out, perhaps through a Brussels-based regular
Committee, bringing together all relevant stakeholders, including at the technical and user level.

There was limited discussion on this item, taken as support to advance the work and project. One comment was that rules on purpose limitation can be too strict.

The chair concluded that the group advocated greater use of the Universal Message Format across systems, to be examined initially on a case-by-case basis. For the future governance of UMF, consideration should be given to assigning this to an eu-LISA working/advisory group.

3. Follow-up to subgroup meetings

a. SIS — recording of checks

The chair reported that the subgroup 'new systems' had discussed 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 appropriate, solutions can be introduced to meet the objectives of such an extension. As a result of these discussions a working hypothesis had been developed, containing two elements:

a. the establishment of a common repository for storing and sharing of information on hits obtained in SIS (as recorded in the SIRENE forms);

b. provisions for the recording and searching of SIS checks carried out on persons (by allowing queries of SIS-logs for law enforcement purposes);

The technical, legal and political implications of these options are still under consideration. The Commission presented more detail on a possible technical way forward. The chair invited comments both on the need for such checks on EU citizens, and the suggested way forward using SIS.

Comments from experts

- Generally experts agreed that registration of external border crossings of EU nationals may be justifiable but the way to do this gave rise to differing views.
- Storing of achieved hits on SIS alerts, and making this information available to all Member States was considered a promising way forward. This would make it possible to better monitor travel movements of those EU citizens for which Member States have created an alert in the SIS.
- Building a system that would give law enforcement authorities access to information on border crossings of all EU citizens would go much further. The necessity of such a system needs to be demonstrated.
- A comment was made that including EU citizens in the Entry/Exit System would be a better approach, because the SIS approach would be based on criminal investigation (after the crime) rather than the prevention of terrorism. Another reason was that a SIS-based approach would not work for those Member States that do not fully apply SIS.
The chair concluded that the group considered it important that the travel movements of (certain categories of) EU citizens be registered, and that there is more than one method to do this. Further consideration is required, including an analysis of legal and data protection aspects.

b. Eurodac — security checks on irregular migrants and refugees

The chair recalled that Eurodac is an asylum system for refugees. In the current environment, it is possible that refugees are not always innocent refugees — some can use refugee procedures to pursue criminal intent. So there are security aspects to consider within the framework of Eurodac.

The Counter-Terrorism Coordinator recalled discussions in the informal JHA Council in January where ministers had supported a harmonised approach towards security checks of irregular migrants and asylum seekers. Arguments were put forward to make Eurodac a security and migration tool, not just one for migration. Eurodac was not fit for purpose for law enforcement access, which would also involve alphanumeric searches. Other systems could play a role (ECRIS, SIS, Prüm, Europol, Interpol) but there was a strong case to review Eurodac. This was necessary not just to deal with security but also to ensure that Eurodac does not give rise to a reluctance to accept asylum seekers.

The Counter-Terrorism Coordinator provided some leads as to what could be done:

1. Widen the purpose (dual migration and security purpose);
2. No cascade for law enforcement access;
3. Explore more privacy by design;
4. Pre-consultation of a Member State;
5. Running of SIS and Europol data against Eurodac data every night (comparisons by batches).

Comments from experts

- It was noted that Eurodac was currently subject to a recast proposal.
- Support was expressed for the suggestions put forward to broaden Eurodac so that it also covered security purposes. Connecting to Interpol was not necessarily advisable.
- Some saw the benefits for victims of exploitation that could be gained from the proposed changes, and recalled the interest in gaining all relevant information quickly.
- It was legitimate to provide law enforcement access to Eurodac.

The chair concluded that the group did not wish to take a position that might be seen as interfering with co-legislator negotiations on the current Eurodac recast proposal. However, there was a strong feeling that Eurodac should be part of an overall system environment that provides necessary information to law enforcement authorities. The group identified issues that should be considered (cascading, batch comparisons…) whether by a new legal proposal or other means.
c. Prüm — improving performance

The chair reported on subgroup discussions to explore the possibility to strengthen and improve the functioning of the Prüm cooperation, including at the level of both system architecture and governance. The Commission had held a workshop in January where the requirement for Member States to fully implement Prüm had been emphasised. A variety of possible approaches were put forward for discussion in the subgroup. The one concept that was deemed worthy of further exploration and study was, in respect of fingerprints, to replace the mesh connectivity (every Member State connected to every other Member State) by a hub-and-spoke design, a kind of centralised biometric single-search interface.

The Commission presented this concept in more detail and the chair invited comments.

Comments from experts

- It was underlined that the essential priority was to ensure that all Member States are connected under Prüm as soon as possible.
- Technical solutions for facilitating (and hence ‘centralising’) the exchange of Prüm data should be considered
- Prüm is part of the overall picture, but more study would be required before a concrete interoperability initiative could be proposed.

The chair concluded that the group noted that the Prüm system was designed at a time when the systems and methods now available were not yet in place. The group considered that further study is desirable to facilitate information exchange between the users of the Prüm framework and to examine possibilities for making the Prüm system interoperable with other systems.

d. Passenger Name Record (PNR) — next steps

The chair recalled that the April 2016 Communication had pointed to the combined use of PNR and API data as a means to further enhance the effectiveness of PNR data to identify high risk travellers in the context of combating terrorism, drugs trafficking, trafficking in human beings, child sexual exploitation and other serious crimes. Subgroup discussions had shown that Member States were keen to find a pragmatic way to better organise the transfer of PNR data from carriers to Member States, and that the way such data exchange is organised must be compatible with what will eventually be developed for EES and ETIAS.

A presentation was made describing the complexity of collecting and transferring PNR data and offering a solution — through eu-LISA — based on a single point of contact. Carriers would transmit data to the single point of contact, and authorities would access it through the same point of contact. Benefits could include better data quality, better and more secure data flows, and cost effectiveness.

The chair invited comments.
Comments from experts

- Some reservations were expressed about the suggested way forward, because some considered that current systems were working effectively.
- It was recalled that this is about transmission of data from carriers to Member States, and that the suggestion was for a router that simplifies, not to build a new database.
- It was underlined that as carriers will not only communicate information under the PNR and API frameworks, but will in future also need to consult EES and ETIAS it is crucial to establish a coherent and coordinated single approach for all systems.

The chair noted that Member States are required to ensure implementation of the PNR directive by May 2018. He concluded that the group acknowledged that the imminent development of the Entry/Exit and ETIAS systems will need to be brought into this equation. He also mentioned that Member States could opt to pool their approaches on a voluntary basis — to use a router method to transfer information — with legal implications necessarily to be considered.

e. ECRIS for third-country nationals — next steps

The chair observed that the upcoming revised ECRIS/TCN proposal should be consistent with the ongoing work on interoperability. A workshop in in January had explored the outline of the future ECRIS/TCN as well as the interoperability challenges in further detail.

The Commission highlighted that the ECRIS community — in relation to the interoperability discussions — was interested in a common biometric matching service and facilitating access to criminal records information via the ECRIS/TCN system for the purpose of SIS entry bans when deciding on travel authorisations. It saw less value in being associated with a European search portal or with the ETIAS system.

In the absence of comments from experts, the chair concluded that further discussions are necessary to consider whether ECRIS can contribute to improving the interoperability environment, including by establishing links to border management operations and by including it under a shared biometric matching service.

4. Planned calendar of initiatives

The chair informed that the subgroups were scheduled to continue discussions in March/April. A draft final report would be circulated before the scheduled final meeting of the high-level group (25 April). The final report is to be agreed by consensus of the group.

The chair informed that, following agreement on the final report, the Commission will react with new legislative proposals envisaged for late June (ECRIS, eu-LISA).
Ongoing proposals (EES, ETIAS, Eurodac) will be advanced with co-legislators in the coming months.