EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

High-level expert group on information systems and interoperability

Second meeting — 20 September 2016

Report

Matthias Ruete, chair of the high-level expert group, introduced the meeting by referring to recent developments: President Juncker’s State of the EU speech, the Communication *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*, the new Commissioner for the Security Union, Sir Julian King, and the Bratislava roadmap. It was clear that the work of the high-level group would be a top priority.

Existing systems

The chair recalled that the first challenge to be addressed by the group is to improve the implementation and use by Member States (and Europol) of existing systems, looking in particular at the feeding of systems, the consultation of systems, and data quality. He invited eu-LISA to present its assessment.

eu-LISA began by recalling that the Commission had asked the agency to analyse data usage and statistical data. System usage is potentially a major issue, as is the feeding of data into systems. For example, 80 % of SIS is fed by just three Member States. There is also a lack of appropriate access to the system: Eurodac is open for law enforcement access but use is low, or law enforcement agencies do not have the technical access. eu-LISA had also found that only 50 % of Schengen visas are checked at borders: this is not a technical issue but an end-user issue.

eu-LISA argued that data quality has a substantial impact on the efficiency of a system, affecting performance. For text data, this includes improper use of fields, code tables, inconsistency of data, and improper use of free text. For biometric data, there are problems with the quality of biometric data, missing biometric data, and the use of invalid formats.

eu-LISA argued that usage can be increased through a standard architecture and input interface, and standardised devices, including mobile devices. A harmonised end-user interface could result from working with Frontex and EASO officers on the ground. One objective should be centralised data quality monitoring and data quality standards and better statistics on data quality. eu-LISA should be tasked with greater responsibilities to improve data quality.

The Commission reported on the meeting of the subgroup on existing systems, which had been asked to explore the current use of existing systems and how to improve them. At its meeting of 20 July, discussions focused on the actual use of systems, or the lack of it. The Commission commended eu-LISA for raising all the relevant issues. However, discussions in the subgroup also demonstrated that the problem of underuse of systems cannot and will not be solved through technological innovation alone. There are a lot of concrete, straightforward actions to be taken, close to the shop floor.

It had been suggested that more investments are needed for basic equipment and infrastructure, such as hand-held devices and e-gates. Staff shortages and lack of appropriate training could also be a cause. Conflicting interests arose such as trying to speed up passage at borders in the interests of promoting tourism. And some Member State experts reported about organisational and behavioural issues hindering the full use of available systems.

Legal considerations were also in play, such as legal bases unduly limiting possibilities to collect and disseminate statistics. Provisions on law enforcement access and data protection had to be considered. Rules in place seemed to impede access and so merited simplification.

Usage under the Prüm framework decision was rising but still many more connections could be made. Use of vehicle recognition systems and fingerprint analysis was not fully implemented. This could indicate a need for greater governance at EU level but this was not yet under consideration. Europol had presented its latest developments especially in view of its new legal base and the QUEST pilot project. The subgroup had discussed how to ensure information reached the end-user and under which legal provisions, and whether there was a need to strengthen links between SIS and EIS.

The chair invited experts to respond to the question of why there is such low usage of data, both in feeding and consulting systems, and to consider what recommendations the expert group could put forward. In particular, he invited experts to comment on whether the analysis offered by eu-LISA — in terms of usage and quality — was correct. If it is, this indicates a failure of usage. In which case, what should be done at EU or national level? The chair invited comments on the eu-LISA recommendations. He took as an example the figures that indicated that only 50 % of visas were cross-checked against fingerprints, and asked whether this was a teething problem, or a lack of personnel, or inadequate legislation.

Comments from experts

Data quality & usage

- Without quality data, data processing is not valuable.
- Greater analysis of the statistics — and raising the standards of their reliability — is necessary to help accelerate the process in response to requests made by political leaders. EU funds could perhaps support this.
- The reported underuse of systems is a surprise. Reasons could be related to conditions for access, or national legislation compared with EU legislation. Training was absolutely necessary. Technical reasons did not seem to be the cause of underperformance but eu-LISA had outlined technical remedies, including a suggestion to extend its authority to look at data quality.
- The expert group is right to look into any inadequate usage with a view to ensuring full usage of both existing and future systems, especially to check potential terrorists against national databases. Important to have systems that identify people who have been previously identified.

Existing or new systems

- The high number of migrants does not automatically imply a public risk. Identify shortcomings and address them, and define clearly who has access to data.
- Focus on existing systems and practices rather than developing new ones, even if good systems can also present problems. Many systems with their varying purposes can be a challenge to those responsible. Europol offered a practical solution by using its data, subject to data protection provisions.
- The Commission and Member States should simply work together to find solutions. Many of the problems identified are already being addressed in other fora (JAI, CTC) so the expert group should avoid duplication.
- The group should focus on interoperability and the single-search interface. The subgroup on existing systems should present a clear overview of what is needed, including addressing conditions of access for law enforcement purposes.

Governance aspects

- Support for greater governance, especially to enable associated countries to be fully part of the Schengen Area. Prüm and Eurodac are not part of Schengen and the PNR system, and Europol, and a possible ETIAS, is not open to non-EU states.
- Proper governance is required to consider which eu-LISA suggestions should be taken forward. Similar concerns apply to the FADO system, and investigation into improving Prüm governance could be pursued.
- ECRIS requires more discussion about the legal base.

Other aspects

- Europol seeks to help end-users get the right information, taking account of costs and benefits. A fresh view is worthwhile on how to better use Eurodac, VIS and SIS to ensure they are easier to use and so that better information comes out.

Responding to the discussion, eu-LISA said that it cannot devise answers for each and every Member State but it can develop common standards to be applied by each Member State. It was suggested that eu-LISA prepare for the subgroup a practical roadmap on what it had set out, focusing on two priorities: harmonisation of the human interface; and data quality.

The chair noted that the expert group has a remit to look at future systems, interoperability and existing systems. The subgroups should draw up recommendations to be discussed by the high-level group.

Single-search interface (SSI)

The Commission introduced the discussion of the single-search interface as a tool to query several information systems simultaneously, and to produce combined results on one single screen for border guards or police officers, with full respect of their access rights, in line with the respective purposes.

Responses by Member States to a questionnaire showed that they all generally used some kind of SSI for a variety of end-users. Use of mobile and hand-held devices is increasing.

Systems most frequently consulted were SIS, VIS and SLTD; EIS is not consulted. Biometric searches are exceptional. Searches are generally a simple hit/no-hit. It was difficult to discern to what extent intelligence services used the systems. No data protection issues were cited.

The Commission offered some conclusions: a major challenge would be to include decentralised EU systems (e.g. Prüm, ECRIS) in a standard SSI; work on UMF should be accelerated to open the possibility of accessing the EIS through SSI; another challenge is to create platforms that can be accessed by using biometric data; involvement of national and European data protection supervisors at the earliest possible stage is essential; and consideration should be given to whether a single feeding interface could be developed.

The chair invited the group to consider whether it could make any recommendation about SSI.

<u>Comments from experts</u>

National systems

- In the absence of an EU solution, Member States have developed their own SSIs and they were working well, though greater use of eu-LISA could be considered.
- Current systems should not be removed since national police needed them. Deeper analysis is required before deciding how to proceed.
- A national uniform interface (NUI) could work at the instigation of the EU, being easier and cheaper.
- Estonia's X-Road system is a good model, paying attention to securing the desired data but not prescribing the channel — it is vendor and ISP-independent. A goal should be to make connectivity cheaper than under sTESTA.

SSI outlook

- SSI was becoming more important so ambition was right but the extent should be considered. SSI should facilitate feeding of systems, not just consulting them and SSI can only be as good as the systems to which the SSI gives access.
- SSI based on a common interface is vital for officers at borders. Separate national SSI systems for border guards and the police already exist but a common approach for an EU SSI should be pursued, especially in the interests of accessing biometric data.
- Member States have done much good work already. SSI would not replace national systems but provide a common standard. Technical solutions are already available.
- Decisions need to be made on what data it is desired to exchange, especially from the national level. What are the information needs of the stakeholder groups involved in SSI? For example, there are differences in the interests of a police officer and a border guard. How to develop a UMF project on technical standards? Currently this is addressed under law enforcement.
- In short, SSIs are technically and practically feasible and will gradually be developed.

Practical challenges

- Not only technical but also legal aspects should be addressed. Did eu-LISA have sufficient resources to pursue this? Priorities should be set and adequate funding and time made available.
- Do Member States have rights to access other systems? Even if technically possible, there can be legal challenges for access to other systems.
- SSI shows its value by providing a strictly hit/no-hit response. There are difficulties in combining existing systems in a common interface. A common SSI for all Member States would mean a broadening of the central system beyond the national interface. This raises not just technical questions.
- Practical issues include whether the end-user will know which databases are actually being consulted. Is there a risk of violating purpose limitation? Should the person concerned be informed? How can data quality be assessed without knowing which databases are being consulted? Will there be a possibility to annul bad decisions because of poor quality data? Use of hand-held and mobile devices will require safeguards. The legal base sets limits on biometric searches in SSI.

The chair concluded that there was a desire to continue the discussion on whether there should be a common single-search interface at EU level. This should address access rights (who can use it and for which data?). The subgroup on existing systems will be invited to make recommendations.

European travel information and authorisation system

The chair introduced the discussion by recalling that the EU offered more visa-free travel than any other country, with the prospect of more to come. An information gap exists from a security and migration perspective. The Entry-Exit System will be in place but this is only applicable at borders. VIS provides information where visas are required. In this vein, the Bratislava roadmap has supported a proposed ETIAS.

The Commission presented the main characteristics of a possible ETIAS and the constraints and challenges it may incur. Designing an EU system should learn from similar systems in the US, Canada and Australia. ETIAS would be a travel authorisation for visa-exempt third-country nationals to travel to a Schengen country (by air and sea) or border (by land). Its purpose is to assess security and migration risks, to enable border control that is more effective, and to facilitate journeys for travellers. It would be connected with SIS, EES, VIS, Eurodac, EIS and possible other systems. Critical success factors in the design of ETIAS would be added value, security, user-friendliness, costs, universal applicability and interoperability.

After hearing the Commission's presentation on the state of play in view of presenting a formal proposal in November, the chair invited experts to offer their guidance, focusing on four areas:

1. The purpose and legal base of a proposal (e.g. Article 77)
2. How to organise ETIAS? Where to hold data centrally? How to involve Member States? Whether to implement centralised or decentralised coordination?
3. What would be the implications for land borders?
4. How to implement a screening engine?

Comments from experts

Purpose of ETIAS

- ETIAS is necessary for security reasons. The system should be kept simple and become operational soon. An early ETIAS proposal to be considered alongside the EES proposal is desirable. Clarity is needed on the purpose and legal basis of ETIAS. Either eu-LISA or Europol could be called upon to be the central agency to implement ETIAS.
- ETIAS must add value and security. The quality of data and access to it is of utmost importance. Would more sophisticated data be input under a screening engine to facilitate better profiling?
- The climate seems to be changing from one concerned with migration to one where security is the dominant interest. A decentralised approach based on a Ma^{3}tch approach offers a promising path.
- ETIAS deserves full support for migration and border control reasons. It would complement API/PNR procedures. Border guards should implement ETIAS effectively. Even if the system is substantially automated, the final decision on allowing entry rests with the Member State.

Procedures (especially at land borders)

- Securing external borders is a must. Implementation at land borders (especially long ones) is a challenge. A feasibility study would be advisable.
- Is ETIAS still worthwhile at land crossings if a border check is to take place immediately after any on-the-spot authorisation? Practically, would authorisation be given to travel to the EU, or to the Schengen area, or to one or more specific Member States?
- If ETIAS is not an authorisation to enter Schengen, might there be a temptation for travellers to request a visa rather than conform to ETIAS. Would ETIAS apply to visa-exempt third-country nationals if they already had a residence permit? How would ETIAS deal with Schengen states that do not fully apply Schengen?
- Many travellers (especially the local population at land borders) lack the credit cards and adequate access to the internet to be able to request prior authorisation to travel.
- Arrangements are required for last-minute travel and for pedestrians to be able to submit on-the-spot applications. Deeper analysis required on how to implement ETIAS for land borders. How would a kiosk deal with one passenger in a car or bus? What would be the duration of an authorisation?
- The idea of a central EU unit to review even a small number of crossings would impinge on Member State competence. Would information be inserted by Member States, Europol or centrally?
- Submitting applications by internet still risks that they are based on travel documents that are not authentic. What will be the carrier's liability under the provisions of Article 26 of the Convention implementing the Schengen Agreement?
- Who is responsible for the decision in the case where a third-country national goes to one Member State but is wanted in another? There is value in involving national Passenger Information Units.

Appealing refusals and data protection aspects

- Is ETIAS about advanced information or advanced authorisation? What remedies would be available in the event of a refusal? What are the consequences for data protection? Would an envisaged automated process comply with data protection?
- Fundamental rights aspects are at issue. How necessary is ETIAS given that API/PNR already caters for travellers by air. The data to be held in ETIAS (identity, contact, purpose, sex, race…) could be grounds for discrimination claims. How can travellers rebut false assumptions based on answers to background questions? Will individuals have a right of access to their own data? Would ETIAS be offering too much law enforcement access?
- What happens if there is a revocation after passage? Do the US/Canada offer an example to follow in requiring lorries crossing the border to declare ahead of time?

Linking to other systems

- ETIAS should limit the data to a minimum and rely upon checking with other systems.
- Who would perform checks on a central data repository — a central or the national authority? What would be the interaction with SIS & VIS? Is ETIAS complementary to API/PNR, or duplication? It is necessary to demonstrate that there is added value in consulting all databases for all travellers.
- Would ETIAS be consistent with VIS, for example where — under Article 21(9) of the Visa Code — new applications cannot be automatically denied.
- Need for increasing efficiency and avoiding duplication in an environment where so many checks are being made. A data repository — to be used consistently — must be available and Europol could play a role in storing and making available data on third-country nationals.

The chair commented that kiosks could be established to deal with on-the-spot applications but travellers who did not pre-register risked delays from further checks or even refusal of authorisation. At this stage, it is for the relevant Member State to act upon any SIS alert. Authorisations could be for a long period but ongoing checks could lead to a revocation of the authorisation. Refusal of entry would remain to be implemented under the Schengen Borders Code through a decision of the border guard. An ETIAS refusal is not an automatic refusal of entry, but implies that a check is necessary. Carrier liability will continue to be in force; entry is not guaranteed by a travel authorisation, and authenticity of documents will be checked at borders.

The chair concluded the discussion by recalling the need for efficient systems, clearly identifying where manual checks are to take place, and identifying which systems are to be consulted. Europol, eu-LISA and Frontex all offered possibilities while many questions remained unanswered. The high-level expert group could return to this topic in its November meeting.

Conclusion

The chair informed the expert group that its next meeting was scheduled for 29 November, by which time the new Commissioner for the Security Union will have taken up office.