EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

Directorate B: Migration and Mobility
Unit B.3: Information System for Borders and Security

Brussels, 4 October 2016

High-level expert group on information systems and interoperability
Subgroup on new systems – meeting of 14 September

Report

Participants: European Commission (chair), experts from Member States and Schengen associated countries (AT, CZ, DK, EE, ES, FR, HU, LT, PL, RO), General Secretariat of the Council, Europol, eu-LISA, Frontex, EASO, and the office of the Counter-Terrorism Coordinator.

1. Opening comments

The chair of the subgroup recalled the April Communication on information systems and the objectives to improve border security and interoperability of systems. The high-level expert group involving Member States and agencies is to pursue an informed reflection process.

This subgroup on new systems would address information gaps for visa-free travellers, EU citizens, and holders of residence permits and long-stay visas. In addition, today's meeting would focus in particular on a European travel information and authorisation system, for which President Juncker — in his state of the Union address — had announced that a proposal would be presented in November.

Under other business, eu-LISA briefly outlined its ongoing reflection on data architecture to review information already available under various systems with a view to envisaging an overarching data architecture. The intention was to improve the design of future systems. The topic should be addressed in more detail in a future meeting.

Also under other business, the Counter-Terrorism Coordinator referred to ma^{3}tch technology (autonomous anonymous analysis), which had been developed by financial intelligence units with funding from the Commission. This technology should be considered when discussing interoperability issues.

2. European travel information and authorisation system (ETIAS)

<u>Design and purpose</u>

The Commission introduced the discussion emphasising that this should include consideration of what ETIAS should and should not do. Designing a system should learn from systems in the US, Canada and Australia, and from all interested parties (including

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: LX46 7/079 - Tel. direct line +32 229-61631

robertus.rozenburg@ec.europa.eu

carriers). Currently, some 1.4 billion people are entitled to visa-exempt travel into the EU and this number could increase significantly.

Under ETIAS, travel authorisations would be available for travel to a Schengen Area border (not to enter Schengen) for visa-exempt third country nationals who would be required to apply for authorisation before their journey. The travel authorisation is designed to determine their eligibility to travel to the Schengen Area and to check if such travel poses a security or migration risk. Travel by air or sea would imply pre-boarding verification whereas land transport would be checked at the border. The system would be designed to be simple and quick with the travel document as the only necessary document. Fees could be set to cover both running and development costs, and payments made by credit card or bank transfers (especially where online payment systems are limited). The system would look to process 95% of applications automatically and 5% manually, with Member State assessment required for a comparatively very small number of applications. The aim would be to provide a decision (authorisation granted or refused, or further information required) for 95% of applications within minutes, and all applications within 72 hours.

For travel by air or sea, verification of the travel authorisation would take place at check-in or boarding. For travel by rail or bus, consideration could be given to verification when booking. For travel by car, verification would not be possible until arrival at the border. Border guards would verify travel authorisation through passport scanning. If this raised any issue, the border guard would only then have possible access to information in the application file.

The primary purpose of ETIAS would be to facilitate migration and security risk assessment. It would also facilitate border checks and the convenience of travellers.

Discussion

The chair invited experts to comment on whether and why ETIAS was needed, what would be the implications of setting up this system, and whether such a system would really support effectiveness at borders. The chair invited experts to consider ETIAS at the general level for its potential added value.

Experts commented or raised questions as follows.

- Would ETIAS be a border or police tool? Could it be designed as an analytics tool, especially to address irregular migration?
- What is the role of partial database queries?
- What happens if applicants have inadequate internet access?
- Should there be more focus on the reasons for travel rather than just the travel document?
- Is ETIAS adding value if air and potentially sea travellers are covered by API/PNR?
- How is data retained especially for refusals?
- Risks involved in retaining personal data.
- How to ensure identification of cases involving misuse of documents?
- If applications are mostly dealt with automatically, how much real (human) assessment is there?
- Advanced information improves the quality and speed of checks and reduces disputed cases at borders.

- For security risk assessment, search engines can identify targeted lists of sensitive people.
- For migration risk assessment, information is needed on the location of accommodation.
- Providing feedback to travellers under ETIAS would be an advantage, as would providing a complaint mechanism for them.
- For those who provide false information, an ETIAS check at the border will not necessarily provide the required information.
- Inadmissible persons are not all entered in to the Schengen Information System because some Member States only enter information in national systems. This could lead to travellers being refused entry even though they assume they have authorisation.
- Declaration of visit purpose cannot be used for more than one visit.
- Much of the current system is guesswork. There is a need to identify what is missing and what is already duplicated.
- ETIAS could offer advantages but could also be unnecessary given existing systems, such as VIS.
- Existing travel authorisation systems in US/Canada/Australia fall under common law jurisdictions. Would such a system be feasible in the EU?
- Any system must respond to necessity and proportionality, and respond to civil society concerns. Will ETIAS do so, or are existing systems sufficient?
- In the case of refusal of a travel authorisation, an application for a visa provides a fallback.

Challenges - technical

The Commission presented a review of technical, operational and financial challenges.

Technical challenges included dealing with payments (directly or by an intermediary), defining information retention periods, designing automated risk assessment and incorporating manual risk assessment. A positive travel authorisation is only part of the border checks procedure and carriers are the ones who ultimately decide — using API/PNR — if a traveller can board. Entry information should be added to the future Entry/Exit System (EES).

Accessing data would require that ETIAS would consult other systems (e.g. SIS, VIS, EIS, Interpol and a possible screening engine to address verification that cannot be done by other systems). What data should be collected? Systems in US/Canada/Australia can include information on education, employment details, available financial resources, purpose of visit, convictions, illnesses, health insurance… Is such information of interest and, if so, is it legally accessible? Data privacy and fundamental rights issue have to be considered. How would ETIAS interact with the EES?

Technical challenges include ensuring access to systems for travellers and carriers, for authorities as end-users, and for manual processing. ETIAS would be connected to EU and non-EU systems and could have access to screening engines. A system should seek to minimise impacts upon carriers, especially where they have other obligations under the EES. ETIAS could be expected to deal with over 30 million applications each year, substantially more than the combined total of 17 million for US/Canada/Australia.

Discussion

Experts commented as follows.

- Making the public interface with authorities (in submitting applications) presents challenges on information security, and complexity and costs, but these are unavoidable.
- In an area of multiple languages, what will be the language regime of ETIAS?
- Misspelling (e.g. of names) can raise problems.
- Is there a risk that criminals can self-check?
- In terms of data quality, what if there are false positives?
- When using a screening engine where information is only in national databases, care is needed in working with algorithms.
- Integration of systems should take account of the varying rates of use, especially where a country has a minimal number of applications.
- Which databases would be cross-checked? What would be the criteria to refuse travel authorisation before deciding to consult databases.
- Why should there be any reluctance to use payment/credit card data as such data is usually very secure.
- What role is there for the European Criminal Records Information System?
- Currently, responsibility for any one application rests with one Member State. ETIAS raises the prospect that this will no longer be the case. Which Member State will ultimately be responsible for the travel authorisation, whether automatic or manual?
- ETIAS could be so expensive that it would not provide value for money.
- What will be required of carriers, especially small ones?
- Will security services have access to ETIAS?
- Consideration should be given to enabling border guards to see if the information provided at the crossing point is the same as provided in the application for travel authorisation.
- How long will data be retained, since data history can be useful.
- Will ETIAS be linked to EES, where biometric information can guard against multiple identities?
- If a travel authorisation is denied, but the carrier allows the travel, can the third country stop exit?

The Commission commented on some of the issues raised.

- To achieve greater certainty on names, information could be asked on city of birth or names of parents.
- Those inputting the data are responsible for the information but tick-box systems will facilitate accuracy.
- Multiple language systems already exist and language issues can be dealt with through limiting free-field input and by using drop-down lists.
- Banks play an upstream role in checking credit card payments before the travel application is submitted.
- Without an EU database, it is not possible to know if residence permits are annulled.
- ETIAS would be guided by data minimisation.

<u>Challenges – operational and financial</u>

Operational challenges include ensuring timely handling of applications whether through automatic or manual processing, including directly at borders.

Development costs might have to cover interactivity with other systems; the impact of ETIAS queries on other systems capacity; interaction with API or carriers; security; and a possible information campaign. Canada's annual running costs of €14 million is an indicator for ETIAS.

Critical success factors include security, universal applicability, user-friendliness, interoperability and added value for internal security and immigration authorities.

Discussion

Experts commented as follows.

- If a traveller is referred to a consulate but no consulate is available, where can they go?
- Which country is responsible if a traveller is referred to a consulate — this country of first or final point of entry?
- What are the implications for freedom of movement for EU citizens?
- Would ETIAS apply to any EU citizens or holders of residence permits?
- Success of ETIAS will depend on how land borders and crossings are managed.
- For residents living near borders, can they apply for authorisation on the spot?
- Facilities must be available at borders for impromptu travel.
- Why is travel authorisation necessary if somebody simply turns up at the border crossing?
- Should Council Directive 2001/51/EC be amended to address carriers that allow travel by those who do not have a travel authorisation?
- Will cash payments at borders be possible?

The Commission commented that ETIAS would take account of specific situations, such as residents near borders, those without access to internet or payment facilities.

Application screening

The Commission set out how applications could be screened. Identity can currently be screened against all the major systems whereas travel documents cannot be screened against Eurodac or EIS. Screening rules — for both automatic and manual processing — would need to be drawn up and reviewed periodically to ensure respect for data privacy and protection considerations. Such rules could be based on EES statistics for overstayers and refusals, patterns, risk assessment and specific values (e.g. phone number or email). Currently, the national system at the point of entry is consulted but, under ETIAS, this could be extended to all national systems. This could lead to building a common repository of data.

Discussion

Experts commented as follows.

- Checking national databases is not foolproof.
- Will visa-exempt travellers be subject to greater checks than visa-holders?
- How to exploit API/PNR information in relation to common risk profiles?
- Important to cross-check with EIS and take account of data protection.
- Cross-checking data sets through an anonymising filter can reveal a hit without immediately divulging data – this could be supported.
- Important to define clear rules on screening, especially when profiles present risks.

- If authorisation is denied, an individual can appeal but will information be shared if a foreign fighter is denied authorisation?
- In building a common repository, will this be done manually or by automation?
- Fewer links between data sets will facilitate data protection.
- Risks of overloading systems with data (e.g. emails).
- How will PNR and PIU contribute to ETIAS?
- Is SIS sufficient already as a common repository?
- Will Member States retain data ownership in any screening system? If so, what rules will apply to such data?
- Europol could provide a simple solution to implement ETIAS and access Member State data.
- Some authorities are reluctant to share information with Europol.
- Devise a screening system that indicates that data is available without immediately indicating what the data is.
- How to reprocess data? Is it kept under continuous review or only when a person travels again?
- The major challenge currently is handling refugees rather than travellers from visa-exempt countries.

The Commission commented that it is Member States that upload data and so decide what is uploaded. Other authorities finding a hit will know that information is available but accessing this would require a second step. The aim of a common repository is to enable consultation of all systems across Member States instead of just the national system at the point of entry.

The chair advised that ETIAS would be discussed in the forthcoming meeting of the high-level expert group (20 September) and work would continue in the preparation of a legal proposal scheduled for November.

3. Information gaps: EU nationals; holders of EU residence permits/cards & long-term visas

The chair referred to the two other perceived information gaps identified in the scoping paper. Should the travel movements of EU nationals be recorded when passing the external Schengen border, or is it sufficient to conduct systematic checks of EU nationals against the SIS, as provided for by the revised Schengen Borders Code? The other question was whether information held by one Member State regarding residence permits and long-term visas should be shared with others.

Experts raised various points.

- Is there a real prospect of an EES for EU citizens, or are existing systems — if implemented properly — sufficient?
- Smart borders can provide added value if data is retained to enable, for example, regular travel to risky countries.
- Differing parameters across systems weaken interoperability.
- Identifiers can be subject to misspelling or false identity but this can be addressed through biometric identifiers (as in EES)
- Systems serve varying purposes — some for immigration, some for border control.
- Some difficulty in justifying a new system for EU citizens, and especially for biometrics since not all Member States have biometric identity at national level.

- Checking for criminals in Eurodac presents difficulties and leads to information gaps, so Eurodac could be improved.
- Avoid silo approaches across systems: these can make checking of refugees difficult.
- There is a need to use systems to check and protect migrants but also to protect EU citizens. Border guards and police authorities require the power to make checks using biometrics.
- Consideration to be given to ensuring that records are kept of where a Schengen border is crossed.
- It would be beneficial to share greater information on travel authorisations and refused asylums, especially if in a common repository.
- How to use systems to their full potential while respecting data privacy?

The chair announced that these items would again be discussed at the next meeting of the subgroup.

4. Conclusion

The next subgroup meeting is scheduled for 16 November.