EUROSMART

The Voice of the Smart Security Industry

Position Paper

Advantages of combining a Central Database and Smart Tokens for an EU Entry-Exit programme

July 2010

1. Summary of content

Digital identity became a reality with electronic passports based on the international ICAO standard, electronic health cards, electronic national ID cards, electronic driving licences, and e-Government services cards.
Up until now, Government focus was national–oriented. Digital identity, however, could also be used at the EU's external borders.

More than 500 million travellers (EU citizen and third country nationals combined) cross the EU's external borders every year. The EU therefore needs to remain accessible to third country nationals fulfilling the entry conditions on the one hand but also to control and protect Schengen territory against illegal immigration.

For immigration purpose, as well as the abolition of border controls between the twenty-five member states (Schengen convention[1]), a system (tools) needs to be implemented to register the Entry-Exit of third country nationals and to control and identify illegal immigration and overstayers. The system should procure interoperability (more than 200 airports concerned) and versatility (possible switch from online checking to offline in case of communication collapse) in respect with passenger flow and security constraints.

This Position Paper gives Eurosmart's analysis of the comparison between two different system implementation approaches dedicated to the management of third country national Entry-Exit in respect with European guidelines.

2. Objective of Entry-Exit project

According to the impact assessment made by the European Commission[2]:

The general objectives are in order of priority:

- to reduce illegal immigration currently estimated between 3 and 8 million (especially overstayers who represent 50% of this total);
- to contribute to the fight against terrorism and serious crime;
- to improve the effective management of economic migration.

The specific objectives are:

- to generate information which could help to apprehend irregular and illegal immigrants;
- to generate information that would prevent terrorism and serious criminal activity;
- to allow border control resources to focus on higher risk groups of travellers.

[1] The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *OJ L 239, 22.9.2000.*
[2] SEC(2008)153 - Commission staff working document - Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union - Impact assessment

The operational objectives are:

- to identify overstayers;
- to facilitate the sanctioning of overstayers;
- to identify cross-border movements and potentially dangerous third country nationals;
- to identify the compliance of seasonal and other categories of third country national migrants to the EU with their conditions of migration.

There are three different key categories of population:

- European citizens who can move within the Schengen area with national identity documents accepted by EU member states;
- third country nationals subject to Visa requirements. These people must provide their biometric data for the Visa Information System (VIS) during their application at a consulate of an EU member state;
- third country nationals not subject to Visa requirements.

The below table summarizes the documents and processes for non-European citizens:

Type	Duration < 90 days	Duration > 90 days & < 5 years
Third-country national with visa	SIS*, VIS**	Resident Permit
Third-country national without visa	/	/
Asylum	EURODAC	/

SIS*, VIS**	- Document based on ID2 format + Fingerprint based on 10 fingers - Only optical security features in the document in the Schengen visa sticker
EURODAC	+ Fingerprint based on 10 fingers - Only optical features in the National printed document
Resident Permit	+ Secure document based on ID1 format + May 2011: face biometry will be added (based on ICAO) + May 2012: 2 fingerprints (regulation based on BIG*** standards)

SIS*: Schengen Information System
VIS**: Visa Information System

⇨ *For more details, please see "Third-country nationals and digital identity management in the EU", Eurosmart Position Paper dated January 2010.*

An Entry-Exit system would focus on all third country nationals travelling into the Schengen area. Entry-Exit means an identity check of all third country nationals, a count and registration, including date and place of the border control. For Visa Waiver Programmes (VWP)-country-nationals the travel document with their MRZ-data would be used. For non-VWP-country-nationals the Schengen-Visa, with their MRZ-data, should be used. The Visa is

an ID2-self adhesive sticker in the travel document of the third country national. The Schengen-Visa is valid for maximum 90 days.
This system would include the recording of information regarding time and place of entry and duration of authorized stay and would be connected to existing databases such as Eurodac.
If the system shows a person has overstayed the authorized stay, the national authorities would be alerted if no exit data has been captured.

The Entry-Exit system could be linked with Automated Border control gates. In this case the traveller's biometric data are automatically compared with the biometric data stored in the travel document (Smart Secure Device) and in the Entry-Exit system database in question.
Automatic border control gates also support EC objectives of facilitating cross-border flows. The database could be counterproductive to the EU target.

Why third country nationals staying shorter than 90 days need a visa with a simple label when a person staying some months needs an electronic residence permit (including biometric information)? There is a huge difference in the security level between a visa level and a polycarbonate Smart Secure Device (including biometrics and internationally accepted security mechanisms). A potential terrorist from a third country trying to enter Europe illegally will counterfeit a Schengen visa and not an electronic Residence Permit.

3. System comparison

This Entry-Exit approach could be based on either central or decentralized systems. These systems could use (i) a Central Database, (ii) a Smart Secure Device or (iii) a combination of the two. Eurosmart makes a comparison of these options for a better use in a European Entry-Exit system context.

Smart Secure Device benefits

In terms of technical considerations, biometric matching against information in a Smart Secure Device is at least as fast and good as matching against a biometric database. In addition, a Smart Secure Device offers some offline capability which is simply not possible with a Database. This is key (i) in case of Host collapse leading to a total system blackout and (ii) to check the status of any overstayed people within EU countries at any time.
Besides, if a Smart Secure Device is used it can also take over the biometric matching. There are a number of European industry solutions for this technology which have the clear advantage of performance (matching in micro seconds!) and the highest possible privacy (personal biometric data does not have to leave the Smart Secure Device).

The result is a better regulation of crowd flows during rush hour disembarkment.
In addition, based on existing eID deployment, a Smart Secure Device programme could be linked to a national eID programme to leverage interoperability and the use of existing infrastructure as readers.
Data privacy and integrity is a major topic that has been addressed within the Schengen area by the emission of Smart Secure Devices (opposite to US model). This scheme clearly complies with human rights and data privacy respect and is considered less intrusive than the database model. The same model should be fairly duplicated to non-Schengen residents in respect of the same privacy reasons.
Last but not least, Smart Secure Devices are excellent to perform strong authentication confidentiality, authorization and integrity and to control the storage information taking benefits of rational certification process delivered by international laboratories. In terms of

attack or fraud, the risk is less with the use of Smart Secure Devices, first of all because there are more system / IT hackers compared to chip hackers but also because holding large amounts of data is always risky; the more data are collected and stored, the bigger the problem when the data are lost, traded or stolen.

Central Database Key benefits

Key benefits of a central database model definitely rely on the global implementation and maintenance cost of the system which could be shared by all the member states. The possible interactions between different databases (EURODAC, VIS, SIS) offer more flexibility to local administrations.

The connection to existing database (for data sharing purposes) would bring more value to the Entry/Exit programme by crossing relevant information.

Combination of the 2 solutions

The combination of two technologies will benefit from key strengths by assuring:

- **privacy** / **integrity / security** of data thanks to a Smart Secure Device;
- **flexible** infrastructure with online / offline capabilities;
- **leverage** of existing structures (existing database, e-gates, readers…);
- **interoperability** thanks to database sharing and reuse of e-ID programmes.

Table 1 : Pros and Cons comparison database and Smart Secure Device

		Legal/Privacy	Security	Cost	Technical	Interoperability
Central Database	PRO			Cost sharing between members and other Databases		Interaction between different Databases offers more flexibility to administrations
	CONS	Risk to share Database with different countries with a different privacy approach	More hacker attacks. No certification process to evaluate database security level	Maintenance costs	Large impact in case system fails. Less performance while 1 to n comparison	
Smart Secure Device	PRO	Personal data remains holder property Selective Data sharing Already accepted by European community, citizens and largely deployed	Leverage security of printing industry Well known certification process Less risk in terms of attack Limited and controlled lifetime	Existing infrastructure reuse	Offline capability High performances as 1 to 1 comparison Possible Biometry evolution towards multi-checking or Match on Card	National e.ID programmes re-use
	CONS				Backup process in case of absence of data (stolen/lost)	

4. Eurosmart position for the EU

The dismantling of the EU's internal border control on the one hand and migratory pressure on the other hand offer a challenge to European members to implement a border management system to identify overstayers and thus control illegal immigration within Schengen territory.
Referring to existing projects that have been deployed in mass production within Europe such as electronic Passports, National ID cards and Driving licences and the above technical analysis of comparison between a database and a Smart Secure Device, Eurosmart recommends the use of a Smart Secure Device as well as a central database in order to benefit from its portability, high security and performances.
The Smart Secure Device represents an ideal storage support of personal data in accordance with and respect of EU recommendations and privacy protection.

EUROSMART´s recommendations on these programmes are as follows.

- to invite the EU to adopt a proposal for an Entry-Exit system regulation;
- to connect the Entry-Exit system to the existing infrastructure deployed for ePassport and resident permits;
- in order to enable offline Identity checks (border control, mobile control…), Eurosmart recommends issuing a Smart Secure Device to third country nationals entering the Schengen area;
- the data included in the Smart Secure Device should be redundant to the data available in the Entry/Exit database. This strengthens the personal rights of every third country traveller in case of non-consistent biometry database content;
- access to the Database must be restricted and limited to authorized people in a secure way;
- to deploy the Entry-Exit system based on the combination of database and Smart Secure Device, including Biometry.

Definitions

European Central database

Databases consist of software-based "containers" that are structured to collect and store information to enable users to retrieve, add, update or remove such information automatically. Database programmes are designed for users so that they can add or delete any information needed.
Example of Eurodac, SIS, VIS database as use cases.

Smart Secure Device

An object which contains a secure microcontroller and embedded software for authentication, integrity, confidentiality and non-repudiation purposes. It also has a rigorous product life cycle management, including personalization by the issuer. It can come in multiple forms, but for travelling the form factors are restricted to smart ID cards and passports.

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work into dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospect emerging markets).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry" and is largely involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Bruxelles
Tel: (+32) 2 506 88 38/ Fax: (+32) 2 506 88 25
Email: eurosmart@eurosmart.com