EUROSMART

The Voice of the Smart Security Industry

# Position Paper

# ePassport & Border Control

November 2009

## 1. Towards a standardization and harmonisation of the border control process

Standardization, regulation and roll out of ePassports have now been achieved. Today, more than 60 countries are issuing electronic Passports. However, the Border Control process doesn't really make use of the e-Passport advantages, and projects of automatization for border control are using various techniques.

This EUROSMART document reflects EUROSMART member's analysis of the current situation and their position in favour of an international standardization and harmonization of the workflow and technologies used in the border control process, in order to achieve a right level of interoperability, an equivalent level of security at all borders and a common user interface for travellers.

## 2. Objectives and characteristics of the Border Control process

Border control is in place in the European Union with the following targets:

- Reduction of illegal immigration at border control entry;
- Facilitation of crossing EU borders for bona fide travellers;
- Fight against terrorism and organized crime;
- Better understanding and management of migration flows;
- Identification of overstayers and wanted persons.

The electronic and the biometric passports were designed for a better achievement of these targets and the possibility to introduce an automatization of border control.

Border control is a complex matter that has to take into account:

- The variety of borders: airports, maritime and land borders with car passengers and pedestrians;
- The various types of passengers:
    - The citizens of the controlling country;
    - Foreigners who don't need a visa and foreigners for whom a visa is necessary;
    - Low risk trusted travellers, high risk known people and unknown passengers.

One example for border control process, based on travel document verification and biometrics according to the new ICAO standard (**I**nternational **C**ivil **A**viation **O**rganization) is the US VISIT Program, which has been in place since January 2005. VISIT stands for **V**isitor and **I**mmigration **S**tatus **I**ndicator **T**echnology.

## 3. Status and outlook on ePassports worldwide

ePassport technology has been developed after 9/11 with the target to increase the security of travel documents and border processes. This led to worldwide initiatives for standardisation and deployment of e-Passports:

- An intensive international standardisation work done at ICAO (2003–2005), and in the European Union by Article-6-Committee through its subgroup BIG (2006-2007) for biometric passports;
- The Visa Waiver Program of the US, published in 2004;

- Regulation in the European Union, published in 2004[1];
- The organization of interoperability test sessions (2004–2006 under ICAO 2006 – 2008 under BIG).

The first roll out on new standards started in November 2004 in Belgium. Previous programs introducing ePassports, like in Malaysia (since 1999), were proprietary.

Nowadays more than 60 states are performing e-passport roll outs. Most of them are of the 1st generation and provide Passive Authentication, Active Authentication, Basic Access Control (BAC) security and the biometric face image.
The EU Member States (Schengen Area) are moving to 2nd generation, i.e. biometric passports, with Extended Access Control (EAC) security protecting access to fingerprint images.

The Commission Decision C(2005)409 of 28 February 2005[2] defines two deadlines for all EU Member States: August 2006 for the implementation of ePassport with face images and BAC; And July 2009 for the implementation of face image combined with two fingerprint images and ICAO/BAC and BIG/EAC.

Nowadays, at border control, several kinds of documents can be presented by passengers as travel documents: classic chip-less passports, first generation electronic passports, second generation passports and Identity cards that may be regionally considered as travel documents.

For electronic passports, Basic Access Control, and Active Authentication are optional security mechanisms. The decision to implement them belongs to the national issuing authority.

The life time of traditional Passports is typically 10 years. This means that the first EU Member States that issued electronic passports will still have in use traditional passports in 2014. It will not be until 2016 that all 27 EU Member States have only electronic passports in use.

## 4. Status and outlook on Border Control worldwide

Today there are different procedures for border control:

- Pure manually by officials;
- Manually by police with the support of computers, optical readers and checks against blacklists;
- Manually by police with the support of computers, optical readers, checks against blacklists and infrastructure for reading electronic passports;
- Completely automated gates.

Tomorrow, automated inspection and authentication of an electronic passport must help to optimize in terms of security and speed the police officer's decision.

Automated inspection of an electronic passport is made by reading first the MRZ that opens access to the electronic reading of the data, including biometric facial image. As States move

[1] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States
[2] Decision C(2005) 409 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States

to 2nd Generation biometric passports so will Border Control be able to consider the second phase which requires a live image of fingerprint matching it with an image stored in the electronic component. This second phase starts with a mutual authentication between passport and inspection system (EAC). When electronic passport authentication (EAC) is done successfully, acquisition of fingerprint and/or facial image by border control system will permit the verification of the passenger (owner of the electronic passport) by a one to one matching of biometric data stored in the e-Passport and data acquired.

The effective use of EAC implies that the EU Member States exchange their EAC certificates cross border. Unfortunately there is no legal framework or regulation available yet for this exchange of certificates although the technical specification using to facilitate certificate exchange has been ratified by the Commission.

At the present time, border control processes are placed in more than 150 states. Within some regions like in the Schengen area, EU citizens may be exempted from Border Control procedures.

It seems that the new aircraft types like BOEING Dreamliner and AIRBUS A380 increase the pressure to speed up the passenger clearing process at airports. Speeding up of border control is only possible by better automatization of the passengers flow, and by introducing e-gates.

The upcoming European Entryt/Exit program will increase the pressure to work with eGates, in order to enhance the passenger clearing rate within the European Union. Seven EU Member States (Portugal, Spain, Netherlands, France, UK, Germany and Finland) already have eGate programs at airports running or in progress with Poland having the first registered traveller program running at a land port. Other Member States are expected to follow.

A new upcoming programme from the European Commission called Passenger Information Unit (PIU) starting in December 2010 should have an impact on border process at the European Economic Area.

## 5. Status and outlook on eGate programs worldwide

eGate programs are running in 20 countries. Only four of them combine eGate equipment with ePassport documents according to the international ICAO standard and technology. These are Thailand, Australia, Malaysia,and Portugal. So it seems that ePassport and eGate programs take divergent directions: the EU is creating an Entry/Exit system for the Schengen area while the eGates standard is only deployed in the USA.

eGate programs use biometric identification/authentication without or in association with a document that can either be a national identity one or a secure token issued by another authority.

### 5.1. Biometric technologies:

At present 3 major biometric technologies are widely used:

- Fingerprint (template/image), e.g. in the USA, France, UK, Japan, Bahrain and UAE;
- Face (image), e.g. in Australia, Malaysia, Portugal and Thailand;
- Iris (template), e.g. in The Netherlands, Germany and UK.

A new one might be introduced: Vein pattern (or network).In Israel, hand geometry is in study. But it should be noted that vein pattern is not recognised by ICAO as an interoperable biometric.

Selection of a biometry technique needs to take into account accuracy, performances, ease of use, traveller's acceptance. Some technologies can be used "on the fly" mode without requesting the traveller to stop and interact with a border control equipment.
Additionally, using a combination of biometric technologies can increase accuracy.
When using biometry, a key question is, are we using 1:1 or 1:n matching?

1:n control means identification of 1 person in a database of black listed or white listed people. One example is the program in Germany, Fraport, called ABG (**A**utomatische **B**iometrische **G**renzkontrolle).

1:1 control means authentication of the document holder with the biometric data stored in his document. Then, the matching can be made in the document chip (MOC) or in the border control equipment. Examples are running programs in Japan (iPass), the USA (CLEAR), The Netherlands (PRIVIUM), France (PEGASE), UAE (eGate) and UK (e.g. miSense).

MOC supposes that the chip contains both matching algorithm and already processed biometric information that has to remain secret.

Except for face, normally everyone owns several similar biometric: 2 Iris and 10 fingers. It is in general recommended to work with the 2 iris and 8 to 10 fingers biometric data.

### 5.2. Secure Tokens for eGates

Basically two ways are possible to realize eGate Programs

i) with secure token
ii) without secure token

On i) there are three ways in use, with

i1) ePassport, e.g. in Australia, Thailand and Portugal
i2) Registered Traveller Program with token, e.g. in the US, UK, Japan, France, UAE, The Netherlands, Canada
i3) Citizen eID card, e.g. in Hong Kong/Macao

Token-less solutions might be considered as more user friendly, but in the case of an automated border control system, a token can give eligibility to access the gate, avoiding others to be mistaken. In the UK, there is an Iris recognition e-gate programme in use for pre-registered and frequent UK citizens with no token.

Token can be the electronic passport. Thus, no specific enrolment is required. Background checks and security controls at enrolment are made by the issuing country. Therefore there is the need to trust other nation issuance including a complex key distribution between countries.

National ID documents that have a travel document statute can bring in future other constraints, for example in terms of interoperability.

Specific tokens can be issued to frequent and preregistered travellers. They allow 1:1 matching that leads to limited search times and better performances. They may also avoid creating specific biometric databases and restricting biometric control to face + 2 fingerprints as defined by ICAO specification.

Tokens may be part of a global solution provided by private public/private operators that want to provide a more convenient entry/exit service to their customers.

In case the secure token is not the ePassport, the security concept could be different to the ICAO standard, e.g. the access condition to the data on the token could be done without MRZ-scanning and calculation of the hash value. A token process without MRZ-scanner reduces work process time and equipment cost.
When using a biometric template, the total cycle time of the eGate can be enhanced significantly, because the data set is more than 10 times smaller, because a template only contains the biometric features and not the image. One example:

- Fingerprint, image, ePassport need 12k – 16k Byte data
- Fingerprint, template, secure token need 0,5k – 0,7 k Byte data.

However using a template solution does lock an issuer to a particular supplier which can reduce the flexibility and expansion of the scheme.

As discussed in this paper there are various technologies available and in use based on different secure token and different biometric technologies. Future evolutions enhancing accuracy, performance, security and ease of use can be expected.

## 6. EUROSMART Position for Europe

**Based on the statements above, Eurosmart recommends the following actions:**

(1) A Regulation for electronic travel documents, based on standardized biometric technologies and contactless crypto-controller was published by the European Commission in 2004 (Council Regulation (**EC**) No **2252**/2004). However, a regulation about the border control use case and the related roadmap is still missing.

The EU roadmap for biometric passports should define the border control use cases at Schengen borders, in terms of process, user interface and architecture recommendations. Such a roadmap would provide benefits to all actors:

- Travellers will have to follow the same process at each border control. This will avoid confusion, provide more comfort and speed in the process.
- Such recommendations would provide more confidence to solution providers that would be able to provide similar solutions in a more competitive environment. The market would be organized with cost effective solutions.
- Demonstrate to the passport holder that the additional cost and stated security in the passport was a worthwhile investment.

(2) The EU legislation shall integrate the fact that eTravel documents may have some evolutions, such as new access control mechanism (e.g. replacing BAC by a more advanced mechanism), more biometric and/or other biometric data information. Upward compatibility shall be provided by the systems.

- Security is a moving world. Integration of new security mechanisms will increase the respect of privacy and increase the global security against forgery.
- Introduction of more biometrics will enhance the False Reject Rates, whilst reducing a False Acceptance Rate that is already very low.

- It is vital that issuers stay at least one-step ahead of fraudsters and endeavour to take advantage of the ever evolving improvement in technology.

(3) A recommendation for a standardized e-Gate process in Europe at airports should be helpful for various stakeholders, such as frequent travellers, airlines, ground handlers and border police. This implies interoperability in the work flow and in the technical aspects. A similar technology should be used for land border process. Such recommendation should be proposed by the European Commission.
e-Gate process' aim is to provide a maximal automatization, by making full use of the new eTravel documents. Significant advantages will be provided to:
   - Users that will get a faster border control clearance;
   - Airports and airlines that will obtain a better satisfaction from their customers;
   - Authorities that will not need to increase significantly their headcounts.

(4) A secure token solution might be a new service offered to frequent travellers. A business case for various actors could be established that would re-finance the e-Gate equipment and maintenance. Secure token solutions might feed proposals for new features to be integrated in future ePassport specifications.

   A secure token solution is a way to organize and test better services on identified population, and that could then be generalized to all.

EUROSMART can support the European Commission along the way for international standardization and pan-European interoperability of eGate procedures at all ports (air, land and sea), if this is requested.

EUROSMART members have made a lot of contributions in setting up standards, specifications, definition of test suites and homologation scheme. Their support could bring a useful vision from the industry.

Note:

(1) ICAO is thinking to extended use cases of the electronic passport. The services offered by secure token could be integrated in the ePassport new specifications.
(2) EU Commission has initiated and sponsored three studies on Registered Traveller, with BIOPASS [1] and EPAIC [2] (FRONTEX, 2008) and Registered Passenger [3] (DG TREN, 2007).
(3) USA TSA has initiated and sponsored a working group in 2005, called Registered Traveller Interoperability Consortium [4], which has worked out the specification for the national Registered Traveller program, called CLEAR, which was expanded in 2007 with Canada to NEXUS.

Glossary

| | |
|---|---|
| A380 | New generation aircrafts; minimum 500 seats/aircraft |
| ABG | **A**utomatische **B**iometrische **G**renzkontrolle |
| BIG | **B**russels **I**nteroperability **G**roup |
| BAC | **B**asic **A**ccess **C**ontrol; a security concept for travel documents of ICAO |
| CLEAR | Registered Traveller Program in US, since 2005 |
| DG | **D**irectorate **G**eneral |
| DG TREN | **D**irectorate **G**eneral **Tr**ansport and **En**ergy |
| EAC | **E**xtended **A**ccess **C**ontrol; a security concept for travel documents of ICAO |
| EC | **E**uropean **C**ommission |
| EPAIC | **E**uropean **P**ort **A**ccess **I**dentity **C**ard |
| EU | **E**uropean **U**nion |
| EUROSMART | EUROSMART is an international non-profit association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications |
| FRONTEX | European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union |
| iPass | Registered Traveller Program in Japan, since 2006 |
| ICAO | **I**nternational **C**ivil **A**viation **O**rganisation |
| MOC | Match on Card |
| miSense | Registered Traveller Program in UK, since 2006 |
| NEXUS | Registered Traveller Program in US, since 2005 |
| PEGASE | Registered Traveller Program in France, since 2006 |
| PRIVIUM | Registered Traveller Program in The Netherlands, since 2003 |
| UAE | **U**nited **A**rabian **E**mirates |
| UK | **U**nited **K**ingdom |
| US | **U**nited **S**tates |
| VISIT | **V**isitor and **I**mmigration **S**tatus **I**ndicator **T**echnology; an US border program, since 2005 for biometric registration of all foreigners entering the US. |

Source:


[1] Study on Automatic Biometric Border Crossing Systems of Registered Traveller on Four European Airports
http://www.frontex.europa.eu/gfx/frontex/files/biopass_study.pdf

[2] EPAIC = European Port Access Identity Card
http://ec.europa.eu/dgs/energy_transport/tenders/doc/2006/s157_168865_specifications_en.pdf

[3] Facilitation on Aviation Security; DG TREN/J2/114 - 2006

[4] Registered Traveller Interoperability Consortium Specification V1.0-F, July, 2006

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