Moving to the Second Generation of Electronic Passports

Fingerprint biometrics for enhanced security & privacy

July 2007

BANKING & RETAIL

ENTREPRISE

INTERNET CONTENT PROVIDER

PUBLIC SECTOR & TRANSPORT>WHITE PAPER

TELECOMMUNICATIONS

gemalto

security to be free

Summary

The European Commission has requested that all member nations include additional digital biometric information and in particular fingerprint biometric data on ePassports by mid 2009.

This second generation of electronic passports is a major step in biometrics. It creates a very strong link between the document and its owner as fingerprints offer a sure and proven means of personal identification.

The European Union has made it clear that a new security mechanism known as Extended Access Control (EAC) was necessary for access protection.

The implementation of this new security scheme for the second generation of ePassports is a global first and requires a significant amount of coordinated work from all EU members.

Executed properly, EAC offers huge advances in secure travel documents and strong border control, but the deadline is fast approaching. So, in order to enjoy the benefits of this exciting evolution, now is the time to start.

EAC implementation is a complex affair and requires skilled handling and cooperation from all EU members throughout the migration process.

The new system requires to set up a complete Public Key Infrastructure (PKI) and two new security mechanisms and has a significative impact on all major players, including governments, national printers, the ePassport industry and citizens.

As the industry moves forward and interoperability tests proceed at a fast pace, it is clear that countries that have yet to broach EAC migration have a lot of work to do. This has to be done step-by-step, and even with help from experienced and already established Brussels Interoperability Group (BIG) countries, resources must be allocated fast.

ePassport:
a powerful tool for security & privacy

ePassports combining visual and electronic security features

ePassports are biometrics-enhanced machine readable travel documents (MRTDs) based on specifications defined by the International Civil Aviation Organization (ICAO), and introduced with the aim of strengthening international border security by preventing illegal immigration and trans-border crime and reducing the threat of identity theft.

ePassports contain a contactless microprocessor with at least 32 kilobytes of memory, on which they can store the holder's biographic data like their name, date and country of birth, as well as the holder's face image as biometric data. This data can be read from the passport using a contactless reader.

By combining visual and electronic security features while ensuring high privacy standards, the ePassport is a powerful tool for border control authorities.

First generation ePassports

In the aftermath of September 11, 2001, the US changed its entry requirements and obliged all countries participating in the Visa Waiver Program to start deploying electronic passports as of October 26, 2006.

Subsequently, in December 2004, the European Commission (EC) passed the (EC) 2252/2004 regulation, calling for common technical specifications to enable biometric markers on travel documents.

Then, on February 28, 2005, the EC adopted the first phase of the ePassport technical specifications, which set August 28, 2006 as the deadline for all member states to include a facial biometric image on ePassports. Pioneer states such as Sweden and Norway were first to introduce a fully European and ICAO-compliant ePassport using facial biometrics in October 2005. Twenty-three other U.S. Visa Waiver countries met the August 28, 2006 deadline.

Second generation ePassports

The second phase of the technical specifications from (EC) 2252/2004, which called for the use of fingerprints as a second biometric marker in ePassports, was adopted by the European Commission on June 28, 2006. The deadline for compliance is set for June 28, 2009.

Under the specifications, when implementing fingerprint images on second generation ePassports, access rights to read the fingerprints must be further protected by a security measure called Extended Access Control.

First Generation: A contactless chip containing holder's personal information and facial image added to the passport booklets

- Holder's photo in physical and electrical format in the passport booklet
- Additional security

Second Generation: Fingerprint images securely stored on the passport microprocessor

- Tightly linking a document and its holder together (preventing the fraudulent use of passports by a physically similar traveler)

Why Extended Access Control and what is it?

First generation ePassports are meant to be easily read. They have also been carefully designed to be tamper- and forgery-proof.

The following security measures were implemented with first generation ePassports:

- **Passive Authentication (mandatory with ICAO)** – Allows reader to check the authenticity of the data stored in the microprocessor. The data are digitally signed by the issuing country.
- **Basic Access Control (mandatory for phase one EU ePassports)** – Prevents passport reading without the holder's involvement. To protect against skimming and eavesdropping, a key must be used to gain access to the microprocessor and the communication is encrypted. This requires that the passport must be intentionally shown and optically read before access to the chip is granted.
- **Active Authentication (optional with ICAO)** – Prevents the copying of the microprocessor. The readable data in the microprocessor contains a public key and the corresponding private key is stored in the microprocessor but cannot be read.

Second generation ePassports will contain more biometric data than current documents, including images of the passport holder's fingerprints in addition to their facial image. EAC provides a means to protect this data against disclosure to unauthorized parties, including border control authorities of unfriendly countries. In second generation ePassports, fingerprints are considered to be highly sensitive information.

- **Extended Access Control (mandatory for phase two EU ePassports)** - Limits access to additional biometrics to the issuing country and countries that have permission from the issuing country. This capability will be used to protect fingerprints, iris scans as option and other privacy-sensitive data.

The ICAO recommends the use of EAC to protect fingerprints and iris scans, but leaves the definition of the actual mechanism up to the individual country. The technical specifications for the EU were prepared by the BIG (Brussels Interoperability Group) and approved by EU Article 6.

Chip cloning impossible with EAC

Through the chip authentication process in EAC, the microprocessor also contains a private key that can never be read out, and is used to authenticate that the data and the microprocessor fit together.

A brute force attack, in which a computer is used to run continuous attempts at guessing encrypted data, is always theoretically possible but not feasible with EAC, as the number of possible keys is so large that testing them all would take an unfeasibly long time.

When trying to gain access to microprocessor data protected by EAC, the attacker would need to guess a PKI key with a length of 1024-2048 bits (if using RSA). To check the validity of one key, one would need to carry out trial transactions with the ePassport microprocessor which take about half second each or a maximum of 63 million tests in one year. Because there are at the minimum $2^{1,024}$ possible keys using EAC, testing all the possible key combinations would take in theory 2,8 x10^{300} years (2,8 and 300 zeros).

What is Extended Access Control?

Extended Access Control consists of three phases: Basic Access Control (BAC), followed by Chip Authentication and then Terminal Authentication.

- **Basic Access Control** is used to prevent skimming and eavesdropping. This is achieved by encrypting the communications using a symmetric key obtained and created by reading the optical data in the Machine Readable Zone (MRZ).
- **Chip Authentication** performs the same function as Active Authentication in the ICAO standards, i.e., proving the microprocessor is genuine and thus protecting the electronic passport against cloning. It will also enhance the BAC security mechanism by replacing the encryption key with a totally random key.
- **Terminal Authentication** aims to prove to the microprocessor that the terminal is allowed to access the data on the microprocessor. This access is granted through a chain of certificates, the root of which is the passport issuer. In other words, only the issuer of the passport controls who can access the data on the document.

The introduction of EAC will not make the security mechanisms of BAC obsolete, but it will supplement them. In the future, the entire reading process for a biometric ePassport will always be carried out in three consecutive steps: Basic Access Control, Chip Authentication and Terminal Authentication.

How Does EAC Work?

Terminal Authentication

In the Chip Authentication stage when the reader authenticates the microprocessor, a standard PKI challenge-response process between the reader and the microprocessor is used whereas Terminal Authentication process is a somewhat more complex system.

To decode the encrypted data contained on an ePassport microprocessor, the border control authorities of the visited country where the ePassport is being inspected must request authorization to access the passport holder's fingerprint data from the home country where the ePassport was issued.

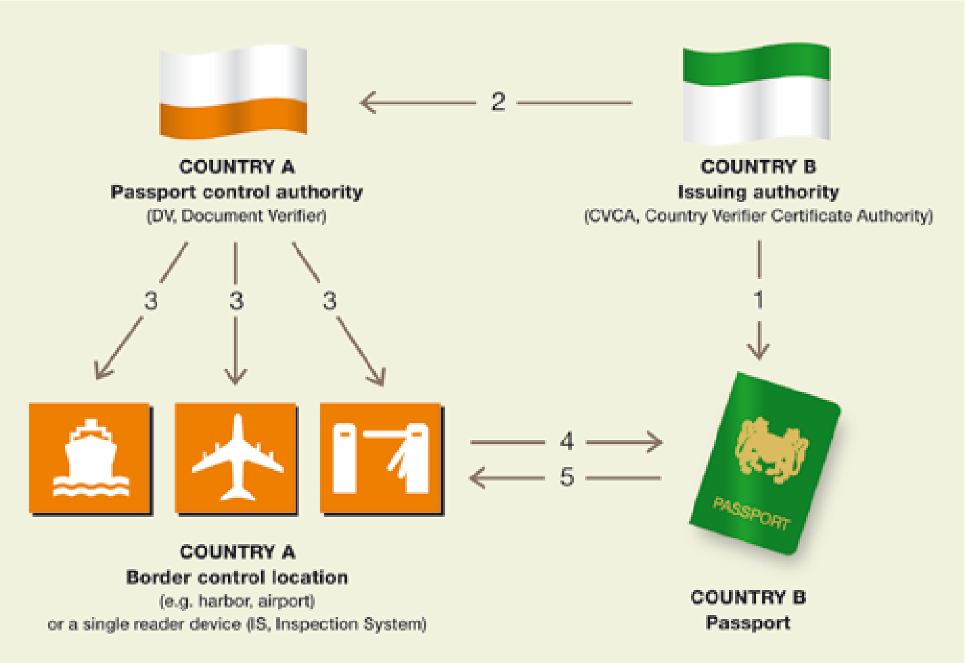
Friendly countries will have mutual agreements in place that enable their border control authorities to share information. Subsequently, a specially adapted key agreement protocol will allow both the issuing and inspecting countries to generate the same secret and unique key, which is contained within every second generation passport, to access the information needed.

Every second generation ePassport can use the secret key to establish a secure communication channel with an inspection system at a border control post and to prove that it is the original passport and not a counterfeit. The trustworthy public key allows the ePassport mechanism to verify the credentials presented by the inspecting party and then permit or deny access to biometric data.

The fact that with EAC the ePassport challenges the inspection system before providing sensitive data ensures that the passport issuer retains control over who is allowed to view the secure data stored on an ePassport's microprocessor, since each government controls the issuing of credentials to the border control posts of other states. Second generation ePassports are thus armored against counterfeiting and can protect their biometric data more securely.

Terminal Authentication calls for a Public Key Infrastructure that supplies the relevant certificates to the reader terminals.

EAC Terminal Authentication



1. CVCA certificate from the issuing country is stored on the passport chip during passport personalization. This certificate will be used to verify the inspection systems certificates (access rights to fingerprint data) in the passport reading step

2. Country B certifies i.e. gives permission to Country A's passport control authority to authorize their access to read the fingerprint data from Country B's passport

3. Country A's border controlling authority certifies i.e. gives permission to its border control locations or individual devices (Inspection Systems) to have an access to read the fingerprint data from Country B's passport

4. Country A's border control reader (Inspection System) shows Country B's passport its authorization to access the fingerprint data on the chip

5. Country B's passport allows reading of fingerprints once the inspection system has proven its authorization from the Country B

The implications for key players

In fact, all players involved in the enrolment, passport manufacturing, personalization, border control processes must consider that many complex competencies will be involved in second generation ePassport deployments, some of which are completely new.

These include the following:

- Cryptography and advanced authentication techniques
- Implementing new EAC-compliant operating systems on the microprocessors in use
- Management of a PKI certificate authority, responsible for the registration of public keys, revocation of certificates etc.
- Biometric data capture, storage and matching of configurations in accordance with both high security standards and strict privacy policies
- Capture of enrolment data material, preparation and formatting
- Authenticating individuals' identities with the appropriate government entities and verifying that the applicant provides valid ID credentials
- Establishing a chain or network of trust, especially internationally

The impact on enrolment

The most visible element to implementing second generation ePassports are reader stations that will be installed for fingerprint collection at passport application agencies. The least visible element – to citizens – is how to protect fingerprint privacy all the way from enrolment to personalization. As the purpose of EAC is privacy protection of fingerprints, the privacy must be protected not only when the fingerprints are on the microprocessor but also throughout the whole application and issuing process. Even the staff operating the passport enrolment system must not have access to fingerprints.

To avoid heavy and expensive security mechanisms for enrolment stations for example, systems based on PKI technology have been developed and can conveniently be used to answer these privacy requirements. The system securing privacy for the whole issuing chain from enrolment to personalization is called end-to-end-privacy.

The impact on passport manufacturing

When implementing second generation ePassports, the biggest change for passport booklet manufacturers and security printers is using a passport cover or datapage containing the microprocessor that meets all the interoperability and security requirements set by EAC.

Compared to first generation ePassports, there is a vast set of requirements that needs to be fulfilled. First of all, a fully EAC-compliant operating system must be used. In addition, 32 KB microprocessors are not big enough. A minimum 64 KB memory capacity is needed as MRZ and passport holder data take up some 5 KB, facial images 20 KB, and fingerprints some 10 KB each.

There is also a requirement from EU which stipulates that the operating system on the microprocessor must be security certified.

The security certification must be done following the international Common Criteria process designed for evaluating secure IT

systems. The context of the second generation ePassport evaluation - a document called Protection Profile – has been developed by European national standard bodies and security organizations like BSI (Bundesamt für Sicherheit in der Informationstechnik) and DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) with support from the industry and was finally endorsed by the EU Article 6.

The purpose of the certification is to provide an independent 3rd party evaluation that guarantees that security mechanisms in ePassports contactless microprocessor are robust even for the most sophisticated intrusion attacks.

However, operating system, electronic datapage (paper, polycarbonate…) suppliers will take care of the operating system development and CC security evaluation, ensuring a smooth and convenient changeover for passport manufacturers.

The impact on personalization

There are several new challenges facing personalizers, mostly around security and productivity.
New data and keys must be prepared, requiring updates of numerous systems at the personalization site. Implementing EAC will require changes for the key management system as unique asymmetric Diffie-Hellman keys are to be generated for each passport and more certificates need to be incorporated on the microprocessor. It is also important during the personalization stage to protect fingerprint privacy before the data are securely stored on the passport microprocessor. This is achieved through end-to-end-privacy between enrolment and personalization.

Moreover, it is important to remember that after personalization, readers used for passport quality insurance must perform both Chip Authentication and Terminal Authentication, to verify the certificate confidence chain from the issuing authority (CVCA, Country Verifier Certificate Authority), to get access rights to read the data from the microprocessor and finally to confirm their accuracy. As in normal Terminal Authentication during border inspection, these certificates must also be renewed periodically.

Also while some 25 KB of data were loaded on the microprocessor with first generation of ePassports, some 45 KB must be loaded on the microprocessor for EAC passports. This has effect on productivity, unless latest personalization technologies are put in place to offset the personalization time increase.

The impact on border control

Just like during enrolment, the most visible part for users during border control is that new reader stations for fingerprint reading will be installed.

Not only will fingerprint scanners be installed, but the entire border control reader must be compatible and equipped with the document authentication software with link to the passport controlling authority (DV, Document Verifier). In practice, this means that the whole reader system needs to be updated.

This in turn means that the whole PKI scheme required by EAC must be extended to the inspection system on borders, to be able to propagate, verify, and revoke numerous certificates.
In addition, the inspection system in border control stations must be compatible with several algorithms such as RSA and elliptic curves in different passports.

The size of data read from the microprocessor will be twice as much compared to the first generation passports. The EAC mechanisms and the enhanced security calculations on the microprocessor are to be performed as well. As a result, the inspection times during the border inspection will increase and therefore it is essential to use the latest microprocessors and state of the art operating systems. With top-quality operating systems, the impact on reading times will still be less than 3 seconds compared to first generation ePassports.

The impact on governments and citizens

EAC stands a good chance of success as long as governments support this evolution with an adequate framework of laws, manpower and infrastructure. In almost all EU countries, the introduction of biometric passports has legislative implications and regulations must be adapted or revised.

New technologies such as smart cards, biometrics and contactless technology have gained attention and their usefulness is becoming better understood, but questions of privacy and security continue to hold the prevailing political focus. Countries that have successfully tested eID schemes recognize the importance of safeguarding citizens' privacy and communicating the potential benefits of these new solutions, and public opinion and the activities of pressure groups can potentially influence how second generation ePassport mechanisms are designed and accepted during this development stage.

Uniquely, the EAC protocol requires authorization from the ePassport issuer to allow certain specific data groups to be read by specified groups of readers. Without this protection, anyone with the necessary technical skills could read all the data on a passport. When implemented, EAC will have the effect of strengthening all the other security measures because the protocol will not operate as a stand-alone. EAC-equipped readers will link back to national Public Key Directories (PKD) so Passive Authentication need no longer blindly trust the document signer certificate held within the ePassport. Instead, this certificate can be validated against the country signer certificate in the PKD.

In such a scenario, governments will provide a second and more significant block of security infrastructure for the benefit of the citizens of the issuing countries:

- Enhanced security of digital identities eliminates the threat of identity theft, thus addressing privacy concerns
- Increased service levels via automated gates and fast track lines can slash queuing times by a third

New Key Challenges for Governments and Border Control Authorities:

- At the enrolment stage, to create the infrastructure to capture fingerprints
- At the production stage, to ensure privacy and secure storage of personal data
- At the border control stage, to adapt the infrastructure to biometric verification

The current status of second generation ePassport implementations

In August 2006, Singapore implemented a biometric passport including fingerprints and a related security scheme.
The implementation of BioPass – as the Singapore ePassport is called – had gone smoothly according to the authorities. Some privacy concerns have been voiced over the introduction of biometrics in travel documents. The authorities have clearly stated that biometrics technology will not restrict civil liberties, that it will make it more difficult for terrorists to assume false identities and will also facilitate legitimate travel, as accurate verification of the identity of the bona fide traveler will be made easier. This is a national initiative.

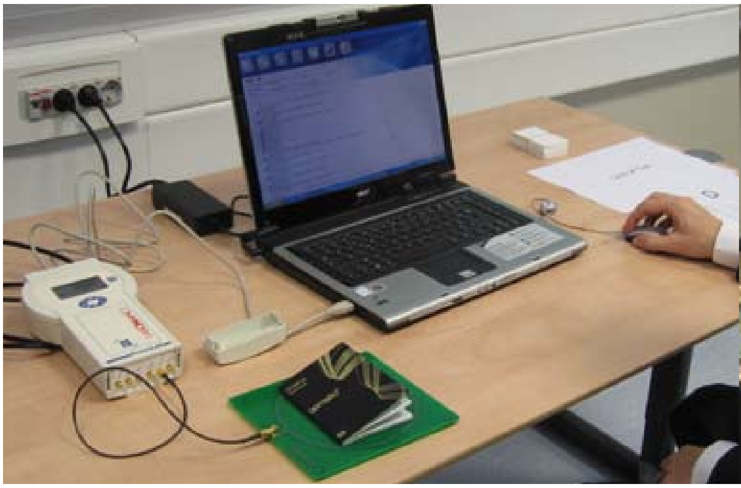
In the EU, the Brussels Interoperability Group (BIG) was formed in 2006 to resolve the technical issues related to the development, implementation and application of EAC in the member states. The group's tasks include finalizing the certificate policy for EAC, setting up a pilot implementation, and providing guidelines to EU member states on the implementation of technical specifications.

Preliminary EAC interoperability sessions were held in December 2006 in Italy to get the level of common understanding of the EAC specifications. After this session, comments and clarifications were asked by countries and manufacturers to improve the previous specifications.

Considering the complexity of such secure protocol and in the continuity of ICAO tests specifications, it was decided to develop the EAC tests specification for EU ePassports implementations.

In mid-March 2007 an official interoperability session was held in Prague, where all the EAC passports inspected with an official inspection system successfully passed the test. This proved that EAC interoperability is guaranteed on a local scale and ePassport manufacturers have the same reading of the documents. Nevertheless BIG members considered that more complete cross tests are necessary to enhance the interoperability of the global system.

In May 2007, the Portuguese Aliens and Borders Service (SEF) in Lisbon hosted the interoperability tests performed by various European Countries set up by BIG of the European Commission.



The goal was to check the first proposal of EAC tests suite specifications developed by the ad hoc group (participants from France, Germany, Joint Research Centre, The Netherlands, UK) with verification of certificate update in the ePassport.

This was a new release for the majority of suppliers. Preliminary results of tests suite illustrated firstly that the AFNOR-BSI specifications have been well defined and well understood by developers, secondly that the four tools are well advanced and most of the ePassports have been tested successfully.
Two methods for certificates verification were used. Results must be considered as indicators of advancement of work and quality of the two specifications (passport and test tools) taking into account that developers have had only two weeks for preparation.

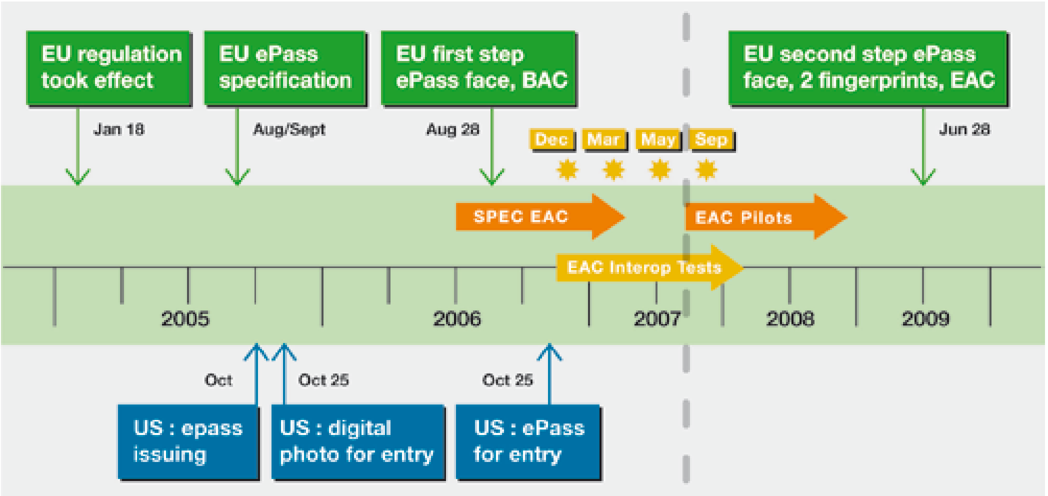
For countries and members of the industry, this also means good news as a choice in test platforms will mean competitive tools. However developing test tools with the complete specifications does take time and commitment for September 2007 is crucial.

Specifications should be frozen before summer 2007 and the next interoperability tests end September 2007 should be more complete. Test of large panel of readers should be organized in same time to fulfill the objectives of end-to-end interoperability.

Pilots are set to begin in several countries by September 2007. Full-scale interoperability testing of EAC readers and passports between countries will take place in 2008.

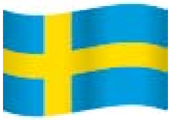
Timeline

EAC pilots in Europe are scheduled for 2007. Within the Brussels Interoperability Group, all major European countries are planning to study the impact of EAC migration in terms of functionality and interoperability.



What they're saying about EAC...

Sweden



As one of the first countries to roll out a national ePassport scheme, Sweden is once again demonstrating its quick uptake with a series of EAC pilot schemes due to roll out in the very near future. The plan for the pilots, which will start well before the necessary legislation amendments come into play, will be done on a voluntary basis and with real passports. The Swedish National Police Board has already begun the country's eBorder project and the EAC pilots will be part of this.

Supplier tests have so far been carried out with prototypes and not final passports as yet, and the results will be more meaningful when this takes place, but the Swedish National Police Board believes it is essential to have good dialogue between governments and industry.

Certification process management is still being debated and the final decision on how the Swedish authorities plan to distribute certificates and deliver them to other countries partially depends on how the ICAO Public Key Directory (PKD) will develop. It is also unclear where certificates will be stored and circulated, and an automated distribution system is currently under consideration.

In addition, we interviewed 3 other European countries.

Because its organization was still being put in place and its ressources defined, the **first country** we interviewed in April 2007 was not ready to comment on its EAC-related activities.

The **second country** we interviewed in May 2007 provided interesting feedbacks.
The Ministry of the Interior of this mid-size European country in turn will be running series of pilot schemes for EAC integration in Q3 2008, in line with the EU deadline of June 2009 for migration.This country will be running two pilots, a first internal, virtual country pilot, and a second external pilot with interoperability.

The country's administrative set-up means that border guards, police, state registries and personalization all fall under the remit of the Ministry of Interior, which will coordinate the process, simplifying administration and avoiding bureaucratic hold-ups and removing the need for large-scale inter-Ministry coordination.

Undecided as to whether to outsource certificate issuance or build an internal structure, the Ministry is keen to learn from other European countries' experiences and recommendations. However, they will be pushing for general EU rules concerning this issue rather than initiatives from individual countries or groups of countries.

The Ministry has a good relationship with the state printer but feels there is not enough cooperation with the private sector due to legal problems with PPPs.

The Ministry has expressed some concerns over the willingness from border guards to carry out the necessary checks with travelers and interoperability between different countries' systems.

If the system works, then the country will enjoy the extra benefits of security and authentication, but without strong EU cooperation, the Ministry is concerned the system will not be effective.

There are some concerns in this country that there is not enough time to ensure good interoperability levels and strong cooperation with EU border guards to ensure a secure external EU border.

The deadline will be challenging to meet, but the interviewed country is determined to fulfill its obligations.

The **third country** we interviewed in June 2007 is one of the largest country in the EU. The country set up a solid new organization in February 2007 to coordinate new biometrics-related eID initiatives including the new EAC passports. The country is presently selecting its providers to start large EAC tests this summer. The country is also actively taking part in the BIG works.

KEY PRIORITY ACTIONS AS SEEN BY OUR CONTACTS

Passport booklet manufacturers

- Select new, higher performance microprocessors together with EAC compliant operating systems in inlays, in passport cover, in polycarbonate datapage

Enrolment system

- Implement biometric data capture, storage and matching of configurations (in accordance with both high security standards and strict privacy policies)
- Install fingerprint scanners at passport application premises

Personalization site

- Update key management system for massive key generation and management of fingerprint end-to-end privacy
- Update quality control stations with Inspection System and Document Verifier functionality so that they can simulate border control terminal authentication
- Use state-of-the-art personalization technologies to offset personalization time increase and avoid throughput deterioration

Governments

- Set up and manage a Public Key Infrastructure (PKI) certificate authority (registration of public keys, revocation of certificates, …)
- Create a chain or network of trust, especially internationally

Border Control

- Install fingerprint scanners
- Update / renew the border control reading systems to be compatible to and equipped with the document authentication software with link to passport controlling authority (DV, Document Verifier)

Conclusions

In a world where international terrorists and criminals are becoming ever more sophisticated in their use of cutting-edge technology, it is imperative that national agencies charged with securing borders stay one step ahead by employing systems and processes that can foil any attempt to gain illegal entrance through border checkpoints.

The second generation of ePassports with fingerprint biometrics is one more tool that agencies can use in order to ensure that the person presenting a passport to a border guard is, in fact, the person represented on the travel document. Extended Access Control through the use of strong encryption and PKI-based public/private key pairs to ensure impenetrable data transmission – a necessity, given the potential for abuse should fingerprint or iris biometric data become compromised – will provide enhanced border security for years to come.

EU countries are expected to introduce second generation ePassports by mid 2009. To succeed in such a challenging but achievable goal, government agencies and state printers should liaise with global technology partners able to integrate the new document production processes.
With strong references and a global footprint, Gemalto has the most complete products, solution and service offering on the emerging identification market.

In 2006, Gemalto actively developed its EAC-compliant operating system, Sealys eTravel EAC Certified, and obtained excellent results (100% success on Chip Authentication and Terminal Authentication tests with Gemalto-based French, Portuguese and Swedish passports) at the interoperability test held in Prague in March 2007.

The Gemalto Coesys eBorder system is able to manage all the security features of a second generation inspection station:

- Propagation and verification of Document Signer Certificates according to the relevant Country Certificates
- Storage of the Document Verifier keys and exchange of Document Verifier Certificates
- Propagation and verification of Inspection System Certificates for border control terminals
- EAC terminal and microprocessor authentication and the granting of access rights to biometric data.

Gemalto is also introducing Coesys eBorder Gate for automatic biometric identification. Coesys eBorder Gate slashes inspection time and human intervention, and allow checking time to be spent focusing on potentially sensitive travelers.

Gemalto in brief

Gemalto is a leader in digital security with pro forma 2006 annual revenues of €1.7 billion, operations in about 100 countries and over 10,000 employees including 1,500 R&D engineers.
Gemalto was formed in June 2006 by the combination of Axalto and Gemplus.

In the public sector, Gemalto aims to make each interaction between citizens and public sector organizations and agencies more secure, easier and private. Security, durability, reliability of exchanges and the protection of citizen's privacy are non-negotiable when it comes to digital identity.

Gemalto supports key identity applications in the public sector such as ePassports, eIdentity and other international and national identification initiatives as well as in healthcare and social security. Gemalto serves the market with secure documents, solutions and managed services, covering enrolment, issuance, authentication and complementary applications.
Our solutions are tailored to local markets in partnership with local players.

Our considerable practical experience - in major ePassport and eID card projects; some of the world's biggest eHealthcare programs; and numerous driving license, vehicle registration and tachograph projects – is at your service.

Glossary

AA	Active Authentication
BAC	Basic Access Control
BIG	Brussels Interoperability Group
BSI	German Bundesamt für Sicherheit in der Informationstechnik
CVCA	Country Verifying Certification Authority
DCSSI	French Direction Centrale de la Sécurité des Systèmes d'Information
DV	Document Verifier
DVCA	Document Verifying Certification Authority
EAC	Extended Access Control
EC	European Commission
ECC	European Citizen Card
ePassport	Electronic Passport
EU	European Union
ICAO	International Civil Aviation Organization
IS	Inspection System
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PA	Passive Authentication
PKD	Public Key Directories
PKI	Public Key Infrastructure
VWP	Visa Waiver program

More information:
email: eric.billiaert@gemalto.com

www.gemalto.com

• Pictures: Kari Koskinen - DR • june 2007 • Design: Blend.fr

gemalto
security to be free