Electronic travel document programs

Successful migration to next-generation ePassport
Successful migration to next-generation ePassports

The first ePassport programs were launched between 2004 and 2006. Since that time, ICAO standard security mechanisms have been revised. More recently, new silicon platforms offering performance improvement and security enhancement have also become available. Today, governments must give consideration to the next generation of ePassport technologies. Gemalto can support them along the way, performing impact assessment to chart a roadmap to seamless migration.

Ongoing evolution of standards

Standards evolve on a regular basis, to remain apace of an ever-changing environment. For instance, new cryptographic algorithms are regularly implemented, helping to refine and enhance current security mechanisms. ICAO has been working on evolutions of the ePassport standard, initially implemented in 2004. Adopted in 2010 and recommended for deployment by December 2014, Supplemental Access Control improves the security mechanisms by addressing concerns with eavesdropping and skimming when using the Basic Access Control mechanism. With ICAO Logical Data Structure 2.0 (LDS2), visa and entry/exit information will be securely stored and updated in the microprocessor, expediting inspection while bolstering security.

From Korea to Sweden, from the USA to Singapore, Gemalto is currently powering 25 electronic passport programs around the world.

Impact on existing systems

Travel document programs comprise three main components:

- **Enrollment**: the decentralized infrastructure that captures the citizen’s passport application, covering administrative and biometric data. There is also a specific enrollment process for visa applications, which increasingly entail biometric capture.

- **Issuance**: the often-centralized infrastructure that manages passport applications and personalizes the document with the citizen's data.

- **Verification**: the decentralized infrastructure used at airports, seaports and land border checkpoints, which match the document to the passport holder through biometric verification.

The evolution of standards will impact all three of these components:

- **Enrollment** will require upgrades in order to capture new biometrics (fingerprints and iris scans).

- **New passport data groups** and enhanced security mechanisms usually require minor upgrades to the issuance scheme.

- **Document inspection** will include new procedures for accessing the passport’s microprocessor, a new cryptography algorithm and new access control rules for reading and authentication.

For security reasons, the forthcoming LDS2 would require all data written to the application to be signed by the inspection or visa issuance system storing the data on the microprocessor. This will enable verification of data authenticity and prevent storage of invalid data. This will have an impact on both enrolment (whether for visas or passports) and verification, bringing about a transition from mere verification (read only) to post-issuance (read and write).

LDS2 will be key to many new applications in the future

Management of access control rights to the microprocessor (reading and writing) will be handled under the supervision of the issuing member state, using the ICAO Public Key Directory as a credential broker. This will protect the passport from malicious writing and prevent any unauthorized access to citizens' personal data. Simplified security mechanisms are being considered for certain use cases of read and write, in order to facilitate adoption. Visa records will store information such as the issuing state, type of visa, place of issuance, period of validity, authorized maximum number of entries and visa number, as well as visa holder data (name, passport number, date of birth and citizenship).
**Gemalto: at the crossroads of secure printing and OS development**

Gemalto has 120 years of experience in secure printing (passports, national ID cards) and over 30 years of experience in operating system development. We have also deployed passport personalization solutions, in some cases operating these on behalf of our customers. This provides us with special insight into their needs and challenges.

**From Korea to Sweden, from the USA to Singapore, Gemalto is currently powering 25 electronic passport programs around the world.**

This puts us in a unique position to help governments integrate our products into an existing passport assembly and personalization system in the shortest lead-time. Our involvement in the standardization process at ICAO and ISO means we can anticipate forthcoming migrations and provide a head start to meet deadlines.

From 2008 to 2009, we supported our customers, mainly in the European Union, in their migration to Extended Access Control. We are currently assisting customers with ongoing migration to Supplemental Access Control and the latest Extended Access Control implementation (v2.10).

Our extensive offer includes delivery of samples for initial testing and qualification; impact assessment of issuance and verification systems; support from our technical consultants on ICAO requirements; and advice on cover materials, glues and binding from our passport booklet experts.

**Gemalto's portfolio of products, solutions and services**

Gemalto has the capabilities to address diverse needs:

- For governments that manufacture their own passports, Gemalto supplies electronic components. These can take the form of an inlay, cover or polycarbonate data page into which the electronic component is integrated.
- For governments that do not manufacture their own passports, Gemalto supplies complete booklets, including data page and electronic components.

We offer a wide range of solutions spanning citizen enrollment, document issuance and verification including border management and automated border control gates.

**About Gemalto**

Gemalto is the world leader in digital security with 2011 annual revenues of €2 billion and more than 10,000 employees, including 1,500 Research & Development engineers.

In the public sector, we help governments, national printers and integrators design and roll-out secure documents and robust digital identity solutions.

Beyond the traditional enrollment, personalization and issuance services, our eGovernment infrastructure and innovative applications will help win citizen’s acceptance and boost usage. A leader in digital identity solutions, we bring our contribution in over 60 government programs worldwide.