Electronic travel document programs

Successful migration to next-generation ePassports
You may be looking to introduce electronic passports in your country. You may be facing the end of a current contract and therefore anticipating contract renewal, either for the electronic components of the passport or for a technological overhaul of an issuance platform. You may be seeking to increase the security of your passport project by transitioning to a new generation of platforms. Given the emergence of new security threats, there is a need for more advanced platforms, with enhanced security.

You may be seeking to introduce new security mechanisms:

- From Basic Access Control (BAC) to Supplemental Access Control (SAC)
- From BAC to Extended Access Control (EAC)
- From EAC v1.11 to EAC v2.10 (part 1)

You may want to introduce or enforce a multi-sourcing policy to prevent disruption in passport issuance to citizens.
Enrolment
Enrolment will require upgrades in order to capture new biometrics and perform on-the-spot new quality checks when migrating to biometric passports.

Passport
When transitioning to an electronic passport, the migration will require the inclusion of a microprocessor for the passport, with a new secure embedded software in an inlay that must be qualified to integrate properly with your manufacturing process, or a complete passport booklet, depending on your needs. Passport durability is then impacted by the overall resistance of the inlay.

The post-personalization quality control stations will need to be updated as well to perform SAC authentication

Issuance
It all starts with an audit of the existing system, to assess the infrastructure and hardware used, as well as the data workflow and business processes. The objective is to maximize the use of legacy hardware and the migration plan (gradually phasing out the existing system while phasing in the new one). It is also important to understand the maintenance contract in place on the hardware. New passport data groups and enhanced security mechanisms usually require minor upgrades to the issuance scheme.

Document inspection
When introducing electronic passports, 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. SAC protocol upgrade will require only software upgrades of the readers.
Gemalto: at the crossroads of secure printing and embedded software development

Gemalto has 120 years of experience in secure printing (passports and national ID cards among others) and over 30 years of experience in secure embedded software development. We have also deployed passport personalization solutions, in some cases operating these on behalf of our customers.

From Korea to Sweden, from the United States to Singapore, Gemalto currently powers 30 electronic passport programs around the world.

This places Gemalto 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.

Controlling the end-to-end value chain
Gemalto offers all relevant expertise under a single roof:
> In-house manufacturing
> 120 years of experience in secure printing
> In-house software development, with over 30 years’ experience in secure embedded software and crypto libraries development
> Expertise in Common Criteria certification and intellectual property
> Development of personalization solutions and issuance services
> Development and deployment of enrolment and verification infrastructures

No disruption in deliveries for your project
With its world-class supply chain, Gemalto has the capabilities to deliver large volumes to support national rollouts of electronic passports:
> Thanks to our multi-sourcing policy, we can source microprocessor from more than one manufacturer.
> Our in-house manufacturing allows for maximum efficiency and reduced lead times.
> We have high-capacity manufacturing and disaster recovery plans enforced.
Security and performance: our key values at your service

We have been developing smart card secure embedded software since the 1980s and electronic passport operating systems since 2004. Today, the Operating System lies at the heart of the security of an electronic passport program.

Our product range is constantly evolving, with both security enhancements and performance improvements, the availability of new silicon platforms and the implementation of a multi-sourcing policy. This enables availability of our secure embedded software on several interchangeable microprocessor sources for guaranteed delivery while offering transparency at personalization and usage level (functionality and performance).

Gemalto has recognized expertise in cryptography, with an industry-leading group of crypto-analysts, several hundred patents in cryptography and security and over 40 products with Common Criteria and ITSEC certification. We also develop our own crypto libraries to ensure timely counter measure update guaranteeing resistance to the latest-known attacks and specially designed to meet current needs. In term of microprocessor qualification, we carefully select the most suitable platform on which to develop secure and reliable embedded software. Intense tests and component qualification are done by our R&D team from Radio Frequency performance to security and cryptographic performance. The related hardware security guidelines are used by Gemalto’s Operating System and application developers.

With over 160 millions of electronic travel documents in circulation in 2015, Gemalto will deliver the solution you expect for your project.

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.

The International Civil Aviation Organization (ICAO) introduced new cryptographic protocols for the ePassport standard, which was initially implemented in 2004. Adopted in 2010 and recommended for deployment by December 2014, Supplemental Access Control (SAC) improves the security mechanisms by ensuring a higher level of protection against eavesdropping and skimming when using the Basic Access Control (BAC) 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.

Gemalto is actively involved in the standardization committees of ICAO and the International Organization for Standardization (ISO), which allows us to rapidly integrate all new protocols for speedy time to market.

OUR APPROACH TO INLAY AND E-COVER DURABILITY

> Greater resistance of our products and subsequent long passport lifetime and durability are enabled by enhanced tests above ICAO standards.
> Beyond a reinforced standard warranty, Gemalto offers extensive warranty options matching your specific document’s issuance and lifetime.
Coesys Enrolment: quality, speed, security
Enrolment is the moment when the secure document that proves an individual’s identity is created so there can be no room for error.

Coesys Enrolment offers a time-saving generic enrolment engine designed to speed up data capture, to verify an applicant’s identity and to ensure the quality of data captured. The centralized or decentralized workflow can be tailor-made to fit with your environment and requirements. Working in over 20 national enrolment programs, our solutions have already registered millions of citizens.

Gemalto’s Coesys Enrolment provides all the software and hardware components to capture citizen data, with a focus on speed and accuracy. Our solution is available as mobile units, desktop units and kiosks to suit the requirements of all situations.

Coesys Issuance Platform
Gemalto’s solution is equipment-agnostic and works with all major brands of personalization equipment. Its flexible design is suitable for both centralized and decentralized issuance and works with both desktop and industrial personalization machines.

It can also be easily linked to one of the many Gemalto personalization sites around the world to enable business continuity and disaster-recovery policies.

This solution was initially developed to serve Gemalto’s own needs and is used in our factories to issue over 2 billion secure documents per year. This guarantees a clear roadmap for new features, support for new mechanisms and new personalization equipment.

Document lifecycle management
Registration and issuance are bundled so that the status of a document can be followed up throughout its life cycle.

The workflow is flexible and when a document is reported lost or stolen, it can be added to a watch list (such as the Interpol database of lost or stolen documents) while an automated renewal is processed.

In order to facilitate the citizen’s experience, we offer SMS gateway services to provide SMS notification (to let them know their passport is ready for pick up) and delivery and renewal services through self-service kiosks.

The system can also be configure to facilitate the transfer of certificates to the ICAO Public Key Directory to allow other countries to verify the signature used by the issuing authority at the time of passport issuance to trace its origin and authenticity.
Mobile verification terminal
Conventional mobile inspection is usually limited to visual inspection. The officer checks document authenticity and compares the physical appearance of the document holder with the ID photo and age, height and eye color data mentioned on the datapage. Special equipment (magnifier, UV lamp) and proper training are crucial to accurately identify visual features. There is generally no automated data processing of Machine Readable Travel Documents (MRTD), nor a link with back-end infrastructure (visa, entry/exit).

The Mobile Verification Terminal features a fingerprint scanner, contact and contactless readers, and Machine Readable Zone (MRZ) swipe reader. It is a universal and versatile reader that can read passports, national ID cards, residence permit cards, driver’s licenses and electronic visa cards.

It is a fully mobile border inspection system, with most of the same features, such as online/offline verification, biometric matching and the support of all security mechanisms defined by ICAO (Passive Authentication, Basic Access Control, Supplemental Access Control, Terminal Authentication, Active Authentication) and the European Union (Extended Access Control).

It displays citizen data on-screen (administrative data and facial image) and can perform biometric verification. Linked to the border control back-end infrastructure, it can perform searches in an array of databases (Interpol watch list, visa applicant database, entry/exit).

Overall, it also offers better data processing, through cross-referencing of existing databases and reliable retrieval of data stored to the microprocessor (compared to manual entry by border control staff, which can inadvertently misspell citizen names).

The Mobile Verification Terminal is designed for field operations, with its IP 65 protection against dust and water, high-capacity battery, additional data storage capacity (SD card) and full communication range (Wi-Fi, GPRS).

It has a cradle for charge and synchronization and comes with a Terminal Management System solution that can manage watch lists and the keys and certificates needed to access the passport microprocessor.
Operated services
Gemalto delivers end-to-end issuance services with personalized passports and ancillary services.

This flexible solution provides significant cost savings while eliminating costly investments (facilities, IT infrastructure, hardware, operations), lowering operational costs and optimizing human and financial capital (turning fixed costs into variable costs).

It allows governments to focus on their core competencies, simplify their interfaces and outsource passport issuance to a reliable partner capable of providing local facilities, infrastructure and workforces that are ready to operate.

Operated issuance of passports is already in place in Northern Europe. Gemalto is proud to supply operated services to Denmark, Norway and Sweden.

SWEDEN’S CHOICE
Outsourcing production and personalization services to Gemalto is a model that combines the use of latest technology with technical expertise.

The Swedish police put paramount importance to expertise in performing service functions, treating each citizen as a customer who needs to be served with utmost competence and efficiency. This is precisely what Gemalto offers to Sweden through its operation center in Stockholm.

The Police bottom-line of providing quality service and optimizing taxpayers’ money were the primary drivers for outsourcing. The Police are also maintaining a fundamental characteristic of its own operations: authority and the control that such authority guarantees.

The Swedish police have been able to free their resources from being bogged down by functions that do not enhance their core competencies such as printing documents and management the logistics to distribute them. In addition, the increasing complexity of the technical environment; the difficulty hiring qualified candidates, particularly for IT operations; and the lengthy procurement cycle to upgrade technology were all valid reasons for the Swedish police to consider outsourcing to Gemalto.
Border control authorities can:
> Apply systematic, reliable controls
> Reduce operating costs in automated mode (eGates), moving from a ratio of 1 officer for 1 traveler to a more efficient ratio of 1 officer for 4 to 8 travelers. Current projects show that security check operating costs can be dramatically reduced when migrating to an automated system.
> Free staff to focus on travelers requiring special attention

For visa applications, authorities can increase security, preventing visa counterfeiting and using biometrics to match the visa to the traveler at the time of border crossing. Paperless visa applications can reduce paperwork, reducing operating costs and expediting visa processing and issuance.

Airport operators can:
> Improve the flow of airport foot traffic
> Optimize floor space and throughput
> Project a modern image of airports, attracting more travelers
> Increase the time spent by travelers in duty-free shops rather than in queues

Travelers can:
> Cross borders more rapidly, with reduced queuing and stress
> Enjoy a more pleasant travel experience

Gemalto's border control solutions, a win-win situation for border control authorities, airport operators and travelers.

Gemalto provides turnkey solutions for border control, including front-end and back-end components such as:
> Databases to handle entry/exit and biometric data
> PKI (for inspection system certificate management)
> Interfaces with other systems (ministries of the interior, ministries of foreign affairs, Interpol, Schengen visa, Advanced Passenger Information Systems)
> eGates (automated border control)
> Biometric readers
References in over 100 Government Programs

Over 100 e-Identity projects, including
30 ePassport, 40 National eID/eRP, 25 Driving License, 18 eHealth

Over 70 turnkey solutions / managed services
20 Enrolment, 40 Issuance, 10 e-Verification, 10 e-Gov

### ePassports
- African Union
- Algeria
- Azerbaijan
- Belgium
- Burundi
- Cap Verde
- Czech Republic
- Denmark
- Gabon
- Estonia
- France
- Hong Kong
- Italy
- Ivory Coast
- Kenya
- Latvia
- Lithuania
- Luxembourg
- Macau
- Malaysia
- Malta
- Moldova
- Morocco
- Norway
- Oman
- Poland
- Portugal
- Qatar
- Turkey
- Singapore
- Slovenia
- South Africa
- Sudan
- Sweden
- Taiwan
- USA

### Driving Licenses
- Australia eDL
- (Queensland)
- El Salvador (eDL)
- Greece (DL)
- India (eDL)
- Mexico (eDL)
- Norway (DL)
- United Kingdom (DL)

### eHealthcare
- Algeria
- Antigua
- Azerbaijan
- Bulgaria
- China
- France
- Gabon
- Germany
- Italy
- Mexico
- Puerto Rico
- Sweden

### ID & Resident Permits
- El Salvador (eID)
- Greece (ID)
- India (eID)
- United Kingdom (eID)

### Other
- El Salvador (eID)
- India (Mobile ID)
- Kuwait (eID)
- Lithuania (eID)
- Mongolia (eID)
- Nigeria (eID)
- Oman (eID/eRP/Mobile ID)
- Portugal (eID/eRP)
- Qatar (eID/eRP)
- Saudi Arabia (eID)
- Singapore (ID)
- Spain (eID)
- South Africa (eID)
- Sweden (eID/eRP)
- Switzerland (ID)
- Tunisia (ID)
- UAE (eID)
- UK (eRP - 2013)
- Uruguay
- Benin (Voter Registration)
- Burkina Faso (Voter Registration)
- Gabon (Voter Registration)
- USA: DoD cards (military)
- Tachographs in 10 countries
EXPERTISE AT YOUR SERVICE. Gemalto is the world leader in digital security with 2014 revenues of €2.5 billion. In the public sector, Gemalto provides secure documents, robust identity solutions and services for governments, national printers and integrators in the service of citizens. Its products and solutions are deployed in more than 100 government programs worldwide. Gemalto is contributing to more than 40 eID initiatives and over 30 ePassport programs with specific expertise in border and visa management projects. The company is active in major eHealthcare schemes and numerous e-driving license and vehicle registration projects. Gemalto also collaborates with its clients to report and share best practices from around the world.