Pooling identity documents and their infrastructures in e-Government programs

April 2013
Above all, the e-Government approach is a unifying and progressive one. While each central or local administration can move forward at its own pace, the e-Government program itself must strive to combine these initiatives into a cohesive whole, while generating savings by pooling resources. For secure ID documents, there is a threefold challenge to ensure they are long-lasting, adaptable and unifying.

This new challenge for ID documents will be all the more acute as more services become reliant on them, and especially with a move to pooling, where several administrations may be working with the same document. At this point the trust factor will extend into territories outside the conventional issuer / user relationship. These factors clearly point to considerable constraints in terms of security and durability.

If ID documents can be pooled, so can the infrastructures, processes and services linked to them, from the registration and issuance phase, through to verification and post-issuance.

Pooling new documents and infrastructures will provide considerable savings in terms of processing costs and cutting the potential sources of non-quality in back offices.

Pooling provides a greater capacity to modernize all or part of identity, travel, health or even driving license documents at minimal cost, and to improve and develop online public services.

Providing public and private stakeholders with a strong identification platform and providing a consistent level of security and trust will also foster the development of third-party services based on this pooled architecture. This trend will contribute to the underlying economic dynamic.

The organizations in charge will therefore need to implement technical and organizational solutions which promote this pooling approach. They will be faced with some challenges:

- in implementing a multi-application platform;
- in terms of scalability and adaptability of this platform, in particular the need to upgrade applications and data in the field after cards have already been deployed (post-issuance processes or add new);
- in terms of security, confidentiality and even trust between issuing bodies, and the constraints in choosing a multi-issuer structure.

On the strength of its experience in deploying more than 80 governmental programs, Gemalto makes three recommendations:

- Break down barriers and encourage initiatives towards pooling of documents at national level. Fragmented infrastructures with several different ID documents do not lend themselves, in the long-term, to the creation of a trusted national infrastructure able to support the requirements of e-ID, which is an essential vehicle for the modernization and digital development of a country.
- Don’t wait to reach critical mass before launching the initiative. The initiative will grow as the concrete benefits become apparent, even if they are small to begin with, since the first areas of application are naturally limited in scope during the start-up phase.
- Invest now in solutions that are at once totally flexible, confidence-inspiring and collaborative. Select a solution that secures the multi-application multi-issuance environment and the post-issuance capabilities. Having clear ideas about the program from the outset will give the project real potential for success.
CHAPTER 1:

The new constraints of e-Government programs

Above all, the e-Government approach is a unifying and progressive one

Many states have begun e-Government programs with the design, production or deployment of secure e-ID cards, often at the initiative of the interior ministry. Too often, the process has been approached from a technological standpoint, and many advanced countries are now attempting to demonstrate that, beyond the security benefits for both states and individuals, e-ID can provide citizens and businesses with real services and benefits, without infringing upon new rules on data protection and civil liberties.

This also makes it easier to garner the political support required to deploy these very costly projects.

Another challenge, particularly during these times of “economic crisis”, is to demonstrate that the e-Gov 2.0 approach and the associated use of smart cards yield a good return on investment, if not financially then at least politically.

Many states and local authorities are attracted by the versatility of these electronic ID documents and encourage their use in multiple everyday activities (transport, access to public buildings, payment for public services, etc.).

Within this context, the technical structure in place must be unifying.

But the scale of this undertaking means that simultaneous implementation is not possible, since each ministry, each administrative body moves at its own pace. Out of all government departments, finance ministries are the most comfortable with the notion of modernizing in order to gain a higher return on investment. Education, legal and defense ministries often do not have the budgetary resources for an in-depth transformation. Social services and welfare systems yield the most obvious return on investment in political terms, and can allow considerable savings to be made at a time when welfare systems are at breaking point. Local initiatives often progress at a faster rate than national programs, and can be useful testing grounds. It is therefore essential to ensure that each area of e-Government construction progresses at its own pace, according to its ability to adapt to the new rules, adopt modern digital tools and launch its own services.

Planning the stages of an e-Government program

The introduction of an e-Government program is a major political decision, involving all administrative bodies and resulting in a far-reaching cultural transformation in service relations practices between public service providers and users. This approach may continue over several years, so the different stages need to move forward in step, and trial projects should be launched, demonstrating the political will, potential for results and benefits generated by the program.
While each central or local administration can move forward at its own pace, the e-Government program itself must strive to combine these initiatives into a cohesive whole, while generating savings by pooling resources. For secure ID documents, there is a threefold challenge to ensure they are long-lasting, adaptable and unifying.
CHAPTER 2

Which services should be pooled?

The new roles of smart cards as secure national ID documents

The new generation of national ID cards (with microprocessors) therefore has a unifying role on two fronts:

> **Multi-service**: the card can have several different uses, both in the physical world and the digital world. It can be used as an identity card, driving license, health insurance card, poll card, public transport card, etc. It can also be used for identification, either face-to-face with a policeman, or over the internet on the government’s web portal, or even for private services.

> **Multi-operator**: the card is issued by one of the public authorities driving the e-Government program, but its electronic components can be updated or loaded with new applications by other public or private stakeholders (other ministry, region, town, bank, transport operator).

Pooling infrastructures

The cost of a smart card project within a governmental context can be broken down in a similar way to an ID card, health insurance card, or driving license project. The main components are:

> The cost of the infrastructure to register the data of citizens, to record their administrative data and potentially their biometric data (photos, fingerprints).

> The cost of the infrastructure to issue documents and secure cards, in general from a central site for optimization reasons.

> The cost of the infrastructure to check documents, with the infrastructure of readers in the various government locations, municipal buildings, town halls, prefectures, etc. This infrastructure is also used after documents have been issued, when the data in the chip needs to be updated.

> And of course the cost of the card, taking into account the technological choice (contact card such as a bank card, or a contactless card, such as an electronic passport or transport card, or a card which combine both types of technology).

In the case of multi-application cards, the issuing and verification components play a significant role, since they enable post-issuance services, such as adding to or updating data in the microchip throughout its entire lifecycle. So the data in the card is not fixed, but on the contrary changes in step with the life of the citizen (change of civil status, change of address, addition of other services in the card, updating security certificates, etc.).

Three cross-functional factors ensure secure ID cards are issued without problems:

> **Security**, which is essential to the credibility of the ID document. In addition to the document itself, the department, personnel and rules of operation need to comply with security principles which prohibit the implementation of fraudulent ID documents.

> **Consistency**, ensuring the quality of documents and their use. This plays a role according to an approach defining compliance criteria and verification procedures for the key stages of customization.

> **An organization** with management, operation, security and quality departments backed up by selected, qualified and experienced human resources.
A multi-issuer pooled system for citizen cards is represented in the diagram below.

It includes a central Trusted Service, used by the various issuers and operated by a cross-ministerial body – the Prime Minister’s Office, for example. This trusted service enables the various governmental bodies to issue their associated data and applications on the card in a secure and independent manner.

Therefore, the pooling of technology, systems, processes and organizations optimizes the implementation of secure document projects. Implementation schedules are also optimized: current status, definition of extensions and integration of changes. Risk management is improved thanks to the use of a proven architecture, and the immediate availability of a backup system.

These components are identical from a technical standpoint for most governmental projects implementing smart cards. Only the actual implementation differs.

The following table outlines the different areas affected by the pooling of infrastructures. The squares in green show components which are easy to pool.
Registration

Registration is carried out differently depending on the application, so each ministry keeps their own registration methods and infrastructure. Registrations need to be classified into several categories, depending on the location and type of information to record. The table below sums up the most common scenarios.

<table>
<thead>
<tr>
<th>Generic Registration Location</th>
<th>Specific Registration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording biographical data</td>
<td>Health Insurance (local health insurance authorities)</td>
</tr>
<tr>
<td>Identity card, passport, residency card, poll card (Town Hall, Local authority, Regional authority)</td>
<td></td>
</tr>
</tbody>
</table>

Town halls or regional authorities host citizen registration infrastructures for ID card, while local health insurance authorities host the infrastructure for healthcare cards.

This set-up is also possible for registration locations, in particular for ID cards and driving licenses. It would be possible to consider pooling registration systems for health insurance cards. In this respect, pooling would be of interest when it comes to taking pictures of users and taking their fingerprints, since the electronic devices required for this are costly.

The costs to acquire and operate equipment could therefore be shared. If the same public service employee could collect data for several governmental agencies, then money could be saved during operations.

The solution chosen must win the trust of users, and take into account the overall security of the project. Therefore, the Ministry of Transport should only be able to add data relating to the transport application, without being able to access data relating to identity or health insurance.

If registration processes are pooled, it would then be entirely possible to implement a very secure face-to-face registration process, requiring the presentation of several documents to guarantee the identity of the person receiving the card. Gemalto would recommend this type of procedure.
Customizing and issuing documents

Resources can also be pooled to issue documents. Indeed, this operation includes a data processing center and a card production facility; these components are part of all smart card projects. The issuance of secure documents (or ID cards) is based on a set of consistent principles, whatever the type of document in question [national ID card, social security card, passport or driving license]. An individual ID card needs to be provided in a secure manner to citizens, in line with requirements which can change over time.

The issuing process is the same for all projects:

- A data processing phase, transforming the information relating to the citizen collected during the registration phase into a format which can be processed by the machines performing the physical customization of the document.
- A phase to customize the microchip [electronic customization], and the front and back of the document [graphic customization].
- A phase to inspect the document. All customized documents are graphically and electronically inspected using inspection software. The aim is to ensure that all documents issued to citizens are in full working order.
- A phase to package documents. Either an individual package to be directly given to the citizen or in bundles to be given to a distribution center.
- An issuing phase; documents can be directly issued to the citizen, or via a distribution center. In that case, the identity of the citizen is checked before the document is handed over.

For a multi-issuer project, the various issuers are in charge of receiving citizen information. They each process their data in order to deliver customized applications to the customization center, with data that is confidential, since it is encrypted with their own encryption systems.

The customization center is a secure center, both physically and digitally. It houses customization machines. The customization, inspection and packaging phases described above take place in this customization center. Blank documents and the various confidential applications from issuers are required for the customization process.

The confidentiality and security of a multi-issuer document customization system relies on a trusted third party service. This trusted service is at the heart of the issuing process, and cements the partnership between application issuers and customization centers.

It enables:

- the definition of the applications which can be customized in documents;
- the secure storage of customization keys, for example the encryption keys of issued applications;
- the provision of authorizations to the customization center to load the applications supplied by issuers onto documents.
This highly secure trusted service is generally under the aegis of a cross-ministerial organization (under the Prime Minister), or reporting directly to the Ministry of the Interior. Below is a diagram of a potential customization process.

One of the advantages of this set-up is that it provides a shared document customization infrastructure. Indeed, only one customization center is needed to customize documents, whatever the issuer of the application and its nature (transport, health, driving license, etc.). Furthermore, the independence of application issuers is ensured, since each issuer is in charge of processing its own data and possesses its own encryption systems. Finally, in addition to issuer independence, data confidentiality and integrity is ensured by encryption and signature systems for applications, which issuers provide to the customization center. This center will then be able to decrypt and check the data thanks to the trusted third-party service.
CHAPTER 3

What constraints are there for secure identity documents?

More universal documents

The first task of a secure document is to gain people’s trust in the information or services which it hosts. This task will be difficult since services will rely on these documents, especially since pooling resources will entail several different bodies dealing with the same documents. The aspect of trust will thus take on a new aspect, surpassing the context of a classic issuer / user relationship. Naturally, this heightened trust will lead to the need for a document making no concessions in terms of security.

Demonstrable security

Inevitably, people’s trust in pooled documents will be won through an independent, recognized assessment of the security of the document. Since this assessment directly reduces the overall risks of the project, the lightweight methods that a single issuer could perhaps fall back on as part of its own program are no longer possible within a program involving several third parties.

Long-lasting security

The durability of security features is also key to gaining people’s trust. Whether to comply with regulations in force or reduce the risks of fraud, particular attention should be paid to the strength of the encryption features of these products. Security authorities cast a critical eye over the key security mechanisms in authentication or signature services, and often issue recommendations concerning the use this or that algorithm, and the estimated lifetime of protection features.

Complete and long-lasting integrity

Documents need to stand alone for their entire validity period. However, they must also display information required for a number of uses. Managing this limited amount of space, both in terms of the physical surface area of the document and the available memory in the microchip, will not only introduce the need for increased coordination between governmental stakeholders, but will also highlight the scalability offered by electronic use. Indeed, a microchip has the advantage that it can be updated several times, while preserving the integrity of each application, or even each set of data in the chip. In order to fit in with the pooling approach, documents need to be able to adapt to all types of administrative uses, and therefore must contain advanced functional capacities. Particular attention should be paid to the communication interface (a decisive factor for the document reading infrastructure), the applications platform for the card (conditioning the potential usefulness for citizens, as well as the implementation timeframes and risks for organizations), as well as the management features of the operating system (essential for the optimum use of the document’s electronic resources).

An adapted communication interface

All electronic documents require an infrastructure of readers, which will vary depending on planned uses. Most uses rely on two types of communication: contact communication, the most widespread and tried and tested, which requires the document to be inserted into a reader, or contactless communication, enabling the document to be read from a short distance.

These types of communication should be considered in the following cases:

- contact cards will be mainly used for health insurance and applications over the internet (e-Government);
- contactless cards can be used within some infrastructures for identity checks (at border crossings for example), public transport, or payment in university cafeterias; driving licenses can be designed to be checked either using a contact or contactless interface.

A range of governmental applications

Governments can take full advantage of the electronic features of documents by using applications in the card which can link up with issuance and checking infrastructures. These applications are often essential to ensure projects run smoothly. They need to ensure they comply with standards and regulations (ICAO, EU, ISO/IEC, etc.), combine security, performance and compactness while integrating with various systems, with the major constraint for any embedded system deployed nationwide: requiring as little maintenance as possible in the field.

Astute management of memory

In order to ensure there are sufficient resources for the applications of all bodies, particular attention should be paid to the issue of the total available memory in documents. This resource cannot be increased once the document has been issued, and has a considerable effect on costs. Therefore, prior consultation and research should be carried out by organizations, in order to not only choose the best size for their project, but also to implement the technical means to avoid the duplication of information in the document. Our recommendation would be to provide enough space for the storage of data to identify the cardholder (photograph, name, address, civil status, fingerprints), and three digital certificates. In this case, a minimum of 72 kB is required, especially if the document will also be used as a travel document, according to the ICAO standards.
A longer lifecycle

Pooling introduces the need for the effective management of the lifecycle of documents, including updating or upgrading them in the field. Indeed, in contrast to traditional secure document, which is issued just once by a single body, a pooled document will need to be altered by various bodies (organizations) at various stages. This means that after being issued, certain tasks still need to be performed in an effective and secure manner, in particular:

- **The ability to load applications as well as data:**
  Since cards do not just include data, but also keys / certificates and applications, these three components must be easy to update, to avoid an increase in the rate of card renewals.
- **A flexible and reliable method to check update entitlements:**
  Gemalto recommends entitlement checks based on an infrastructure of private keys, which will also ensure that third parties can be trusted, and avoid costly investment (SAM, HSM, etc.) to make the transportation of sensitive keys secure.
- **Advanced resource sharing features for documents, ensuring that each organization has a balanced and controlled use**
  Since document resources (in particular memory space) are limited and therefore costly, organizations will surely request guarantees concerning the resources allocated to them. For this purpose, documents will need to manage memory quotas, ensuring amongst other things that no organizations exceed their allocated quota.

Verification and post-issuance

This component can be pooled to a certain extent. First of all, it should be noted that all these cards are not checked and updated at the same rate. A health insurance card for example will probably be checked more often (when used with healthcare professionals or in social security agencies) than a driving license.

**Post-issuance requirements vary depending on the type of document:**
- **National ID Card:** except a change of address or a renewal of an essential certificate for digital signatures (every two to three years), ID cards are not frequently updated. In some cases (name change following a marriage), a new card will be issued.
- **Driving License:** in general, these are updated relatively infrequently because of the regulations in force, in particular the requirement to visibly display the types of vehicles which the holder is authorized to drive on the card. For the implementation of a points system or fines, updates could be more frequent, and would mainly rely on a system involving mobile terminals.
- **Health Insurance Card:** this is probably the most frequently updated card. Therefore, depending on the case, insurance entitlements are updated each quarter or year. The list of beneficiaries could also require more frequent updates.
- **Poll card:** in general, this card is updated for each election, to include the polling station where the holder is registered to vote, and a stamp attesting that the holder voted.

Furthermore, the post-issuance location varies greatly depending on the application. From a technical standpoint, the infrastructure is the same whatever the application, but requires the user management systems for each application to be networked (the national database of driving licenses, health insurance database, etc.) and a link to the PKI (for the renewal of certificates).

In a multi-application approach, the equipment for this can be shared, even if the locations are different. It is therefore possible to pool the verification and post-issuance infrastructure according to a geographical factor; the updating location. Therefore, all cards issued by the government (national ID card, driving license, or even health insurance card), could use the same infrastructure. Eventually, it will be possible to push this approach further, offering self-service booths where users can update several different types of cards.

Connecting systems together also makes issuing new cards easier, in the event of theft or loss. All data and applications could be reloaded onto the new card in one fell swoop.
CHAPTER 4

What concrete results should we expect from pooling?

The benefits of pooling

These types of initiatives are not new, since pooling new documents and their infrastructures means sharing costs, which provide direct savings.

**Noteworthy initiatives**

> The smart ID card in Portugal is a good example of ID document federation. The new ID document (citizen card) replaces five older documents (for identity, tax, healthcare, welfare, voting), and displays several identifiers on the front and back of the document. Although the Portuguese constitution prohibits a single centralized database for all areas, and therefore a single identifier, the Portuguese solution to combine all identifiers on a single physical card provides direct savings, and this simplification is very popular with citizens.

> Launched in 2001, the MyKad card in Malaysia is one of the very first multi-function ID cards (ID, driving license, healthcare, welfare, micropayments, transport), and was driven forwards by the Prime Minister at the time. The historical and structural economic conditions in the country made this approach a good choice.

> The work carried out to register users and issue documents such as electronic passports can also be transferred to new programs for ID cards, driving licenses or even residency cards. This has happened in France, Sweden, and many other countries in Europe, Asia or the Middle East.

> In the Gulf countries in particular, the secure national ID card is also the driving license.

> In terms of healthcare, the registration process is just as essential. The identification of the insured party, due to the healthcare coverage entitlements linked to it, highlights the importance of upstream processes, in particular the quality of registration procedures and verified identity data.

In Finland, the national ID card is also used as a healthcare card. In Belgium, the national smart ID card will eventually replace the old SIS card (social security card).

**The effects of pooling**

In addition to economies of scale, reducing the number of documents to be carried by citizens, and the number of production, registration and issuance procedures, pooling speeds up the deployment of new services for existing members or newcomers.

It provides organizations with access to resources which they could not access previously. It eliminates barriers to entry which have been impeding certain organizations because of issues relating to equipment, resources and scale: local and regional authorities or other public or semi-public organizations.

Pooling improves the quality of pooled documents and services due to the organizational or even contractual requirements inherent to this approach. It also promotes the improvement of the services offered to citizens.
In particular, pooling the infrastructures for new secure documents will lead to:

- considerable savings, in terms of processing costs, reducing sources of non-quality in back offices, and most of all notable time savings for all, which could potentially lead to increased productivity;
- greater availability of public service employees, to improve front office services;
- a sharing of knowledge and best practices, in particular in terms of data protection and security, to develop collective expertise;
- a greater ability to modernize all or part of ID documents, at minimal cost;
- a secure identification system for public and private stakeholders, ensuring a consistent level of security and trust at minimal cost;
- the possibility to develop new regional public services, local assistance and welfare services, and ultimately, a considerable range of services strengthening social cohesion and e-inclusion, which are the cornerstones of a sustainable society;
- the creation of private companies offering innovative services based on this pooled architecture, thus contributing to overall economic growth;

For purposes of comparison and to approximate a measurement of the potential gains to be derived from pooling of resources, below we hypothesize a country of 10 million people. It should be borne in mind that, because the figures are often highly confidential and strongly dependent on the specific conditions of the project, the approach remains a conceptual one.

The estimated costs are projected over 5 years and include chronological issuance of:

- An electronic ID card
- An electronic signature certificate plus its renewal after 2 years
- A health card
- A voter registration card

According to Gemalto estimates, the extra initial investment necessary to be able to offer federated documents represents about +10% compared to the estimated cost of an isolated eID project. From the very first pooled secure document, the ROI threshold is passed. The economy on the document itself is significant, typically representing the majority of the cost of an issuance program.

Over the 5-year period, the savings achieved are very significant. A conventional non-pooled program, according to our hypothesis, would have cost 55% more than the pooled project.

Looking at the detail, we observe that the estimated marginal costs for adding a document type to a pooled document represents at the most 30% of the outlay on a complete isolated project.

These substantial economies of scale on the follow-up projects are to be set against the initial 10% extra outlay.
Legitimacy of pooled infrastructures

The aim of pooling the technical resources and infrastructures for secure documents is to reach a level of efficiency and a quality of service commensurate with citizens’ new requirements in terms of the social and economic functioning of states and their local, regional and central administration. This undertaking affects countries as a whole, and it is therefore perfectly normal and legitimate to optimize the resources of a country at all levels.

It should be noted that requirements for identity protection, security and the fight against fraud, archetypal collective and state matters, are well accepted by citizens. Making documents consistent, modernizing them, and cutting administrative procedures are really seen as proof of progress, showing a state using its resources more astutely, valuing the time of its citizens and being more attentive to their practical needs. These are the natural counterparts to trust, and ways to ensure trust is always present in exchanges between citizens and the authorities. Essentially, identifying is being able to verify that a person is who he or she claims to be when exercising his or her rights and duties as a citizen. This is truly a universal need, and in particular on the internet in today’s world.

Pooling to exceed critical mass

e-Government is recognized as a powerful catalyst to drive society towards its integration into the digital world. While e-ID is the key to building a modern social contract, it nonetheless remains subject to the fundamental need to win public acceptance.

The success of e-Government therefore depends on how frequently the services are used and on public acceptance of new tools such as smart cards, PINs, or electronic signatures. What could be seen in a negative light can be used to positive effect, if people are shown that the system offers real benefits, enduring quality of service and ease of access in return for little financial outlay.

Pooling physical and electronic infrastructures and documents will also have an effect here. Over the course of the e-Government program, partners will naturally appear who are able to speed up the distribution and take-up of the new uses of secure documents, in particular the use of online services.

Studies performed by Gemalto in 2007 and 2009 systematically show the most popular services are “proximity” services, in the fields of healthcare, education, finance or welfare, with services relating to transport and access to public leisure services also popular. The success of online taxes is real and spectacular, but really only generates a few connections per year per user.

Pooling requirements

Pooling infrastructures relating to secure documents can bring together public stakeholders, or even private ones, most often at the initiative of a governmental central service.

**Pooling combines two notions:**

- the sharing of technical resources;
- the sharing of experiences and best practices.

Therefore, as in any partnership agreement, there are rules and principles, in particular subsidiarity, solidarity, the sharing of resources and reciprocal trust.

Online taxes, online schooling, voting, healthcare, transport, various social security applications, etc. Secure ID documents no longer need to prove their ability to combine central and local services into a single document, whether in Asia, the Middle East or Europe. The challenges faced by these modernization programs remain long-term security, the ability to integrate new applications and how simple it is to manage the system as a whole.
Pooling new secure documents and their infrastructures, in addition to economies of scale, cutting costs and appeasing citizens’ practical concerns, aims to facilitate and speed up the deployment of e-services and the emergence of a digital society. The challenge is to improve the deployment of remote services while ensuring citizens take up these services. This change must enable public services to join the ranks of the best services in the private sphere, such as in the insurance, banking, or financial sectors.

Pooling secure documents and their infrastructures will then help to promote national economic growth.

The organizations in charge therefore need to implement technical and organizational solutions which promote this pooling approach.

On the strength of its involvement in the deployment of more than 80 governmental programs, drawing from the lessons learned over the years from the implementation of technical solutions deployed as part of multi-application, multi-issuer platforms, Gemalto makes three recommendations:

- Break down barriers and encourage initiatives towards pooling of ID documents at national level. Fragmented infrastructures with several different ID documents do not lend themselves, in the long-term, to the creation of a national infrastructure of trust able to support the requirements of e-ID, an essential vehicle for the modernization and digital development of a country.

- Don’t wait to reach critical mass before launching the initiative. The initiative will grow as the concrete benefits become apparent, even if they are small to begin with, since the first areas of application are naturally limited in scope during the start-up phase. Starting out with a large number of people and organizations involved is sure to lead to interminable theoretical discussions and exposure to electoral calendar risks and constraints.

- Invest now in solutions that are at once totally flexible, confidence-inspiring and collaborative. Select a solution that secures the multi-application multi-issuance environment and the post-issuance capabilities. Having clear ideas about the program from the outset will give the project real potential for success.
  - flexibility is essential for any long-term project;
  - trust and collaboration are essential when several parties are involved.

Gemalto invite you to find out more about how the new secure documents and the associated infrastructures are designed with the capabilities required to support pooling and integration.

They are faced with several challenges:
- in implementing a multi-application platform;
- in terms of scalability and adaptability of this platform, in particular the need to upgrade applications and data in the field when cards have already been deployed (post-issuance processes);
- in terms of security, confidentiality and even trust between issuing bodies, and the constraints in choosing a multi-issuer structure.
About Gemalto

Gemalto is the world leader in digital security with pro-forma 2012 annual revenues of €2.2 billion and more than 10,000 employees, including 1,700 Research & Development engineers.

Gemalto has been involved in the deployment of more than 80 government programs, and has drawn on its substantial experience in implementing technical solutions deployed over multi-application, multi-issuer platforms, to propose ID Motion, an innovative solution to rise to the challenges of pooling the new secure identity documents and their infrastructures.

In particular, this range of cards, solutions and services meets the issuing bodies’ need for independence, meets security requirements, and provides the flexibility required to cater for applications deployed after the initial launch.