

Open Smart Card Infrastructure for Europe

V2



Volume 1: Application white papers and market oriented background documents

Part 1-1: eGovernment white paper on smart card applications and evolution: Analysis of developments

Authors: eESC TB10 eGovernment

NOTICE

This eESC Common Specification document supersedes all previous versions. Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document. Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Table of Contents

1. CURRENT SITUATION	3
1.1 STILL FEW SMART E-GOVERNMENT CARDS ISSUED IN EUROPE	3
1.2 AN IMPORTANT DIVERSITY IN EXISTING PROJECTS AND STRATEGIES.....	3
1.3 DIFFERENT POLITICAL, LEGAL, SOCIAL AND CULTURAL BACKGROUNDS.....	3
1.4 ATTRACTIVE SERVICES ARE REQUIRED	4
1.5 TECHNOLOGY ASPECTS IN EXISTING PROJECTS.....	4
2 HOW TO ADDRESS DIFFICULT ISSUES?	4
2.1 SMART CARDS AND SYSTEMS COSTS.....	4
2.2 INTEROPERABILITY: WHEN?	5
2.3 SECURITY: THE MAIN CONCERN IS PRIVACY	6
2.4 STANDARDS ARE AVAILABLE	6
2.5 THE STATUS OF BIOMETRY	6
3 HOW TO TACKLE EXISTING BARRIERS?	7
3.1 FOCUSING ON USER EXPERIENCE AND SERVICES	7
3.2 THE NEED FOR A GLOBAL, COMPREHENSIVE, STRATEGIC APPROACH	7
3.3 A STEP BY STEP APPROACH	7
3.4 THE FIRST SERVICE.....	8
3.5 DEMONSTRATING THE STABILITY OF STANDARDS	8
4 CONCLUSION: OVERCOMING UNREALISTIC EXPECTATIONS	8

1. Current situation

If e-government projects are basically on track, the large majority of those are not using smart cards. Yet, the technology exists and is mature. All these projects are very diverse and explore many different options.

1.1 Still few smart e-government cards issued in Europe

Today, despite the important interest raised by the use of smart cards in e-government applications, very few of these cards have actually been issued. For example, the deployments of ID cards going on in Sweden, Finland and Italy saw less than 1,000,000 cards issued. Still, there are numerous existing projects going on.

Compared to these limited deployments, health cards have already been massively deployed throughout Europe. E-government players therefore cannot avoid considering the possibility of sharing these existing infrastructures knowing that highly sensitive issues will be raised such as privacy.

1.2 An important diversity in existing projects and strategies

The e-government projects, as described in OSCIE Volume 1 Part 1-2 the other part of this document, encompass a huge diversity. Some projects are national; some are local. How do you compare the e-procedures developed by the French city of Quimper (50,000 inhabitants) with an Italian national ID cards rollout? How do you compare projects where cards are issued to citizens, to civil servants or to businesses? This illustrates the various options chosen in the deployment of these projects. Small local initiatives are very interesting as they provide valuable feedback.

Another observation is the very small amount of co-ordination between European countries. This is mainly due to the cultural differences in this sensitive field.

1.3 Different political, legal, social and cultural backgrounds

The services to be provided in the framework of e-government are very diverse. Nevertheless, one can notice that some services are always mentioned and appear to be universal while some other services only appear in a few projects.

Actually some services make common sense for everybody, in every country, for example, the case of VAT (and more generally tax) declarations and payments. There are no political or cultural issues raised by these services, which makes things easier both for the user and the provider (the administration). On the other hand, some services raise important issues that are complex to solve, because they are based on cultural or political beliefs.

The concept of an ID card is fully accepted in countries such as Finland, Sweden, France and Germany. Yet the United-Kingdom has historically been hostile to such a document that has long been regarded as contrary to individual rights, though recent developments show an evolution.

Another controversial application is e-voting. As mentioned in OSCIE Volume 1 Part 1-2, the other Part of this document, the French Right wing is in favour of such a service while the Left Wing is opposed to it.

E-government smart card promoters cannot ignore these issues nor can they solve them. They just have to cope with the situation.

Similarly, the adoption of the EU directive 1999/93/EC on digital signatures was transposed into national regulations in some more, some less ambitious extents throughout member countries.

1.4 Attractive services are required

Still the services proposed on government portals lack interest for their users despite the high expectations mentioned by them. This is true especially for citizens. Most services proposed today include the downloading of forms. Tax payment is used in most countries, with limited but increasing success.

For businesses, tele-procedures allow faster and less expensive processes. Schemes are beginning to be successful, mostly dealing with tax payment and benefits.

1.5 Technology aspects in existing projects

The existing projects and pilots have shown that the technology needed for e-government smart cards is available, mature and has had proven field experience.

The cards typically used are based on proprietary operating systems with an RSA crypto-processor to allow the card to carry digital signatures. Small memory sizes can be used (8 to 16 Kbytes) allowing for the storage of general ID data, fingerprint minutae, compressed photo, compressed paper signature image and two X509v3 digital certificates along with their associated keys.

The reasons that have prevented open systems such as JavaCard or Multos from being deployed could be: lack of experience, questions about their permanence, the cost/features ratio, intellectual property and fees issues. Outside Europe, we should still note that Multos has been chosen by Hong-Kong for their ID card.

There has been a lot of discussion around the infrastructures. The main lesson learnt from these first projects is the difficulty of deploying card readers. One can notice the very high number of users that do not succeed in installing their readers without calling the hotline (50%). Another finding is that this rate can be minimized by using USB interface readers.

Contactless smart cards encounter more and more success, mainly in mass transit. One million cards were reportedly issued in Japan, capable of generating electronic signatures.

The security of the readers is another much discussed issue. Secure readers (e.g. embedded finread) are unanimously chosen as being more secure. However, their high cost as compared with standard (transparent) readers increases the barrier to entry and prevents mass deployment.

2 How to address difficult issues?

There are several issues that prevent smart cards from being used more widely. Some are technical, such as using immature technologies or standards ; some are more generic such as the lack of interoperability or standard / format for interoperability. The most important one to be dealt with could be user acceptance – which varies from country to country, in line with the existence, or not, of deep rooted habits of use.

We believe that several of the issues are not critical: costs are no longer prohibitive, standards are available, security can be under control.

2.1 Smart cards and systems costs

Another much discussed issue is the price of the smart card. The additional cost due to the use of an embedded chip is around 2 euros, which is very low compared with the overall cost of the project.

The cost of the card (including the above mentioned price of the chip, but also the cost of the secure plastic card body and the general issuing costs) is considered to account for less than 10% of the global project cost, for large projects which include electronic certification

Administrations have to think about their e-services deployment in terms of social and economic return on investment (value added for the users). This approach had already been adopted by most of them and accompanied the evolution of the culture of administrations (more user centred).

This cost has to be estimated along with the overall project cost. More generally, best practices have to be found for assessing the global value (e.g. cost vs. efficiency) of e-government projects.

2.2 Interoperability: when?

To date, projects have started on an independent basis and do not make provision for interoperability. For example, the ID cards issued in Sweden, Norway or Italy and the projects in Germany, Netherlands or Belgium are not interoperable.

National administrations are currently thinking more about migrating their existing documents (chipless ID cards are currently not unique in Europe) than of creating a new unique document.

Considering the electronic signature, it has to be noted that the transposition of the Directive 1999/93/CE of Dec. 13 1999 is not uniform throughout the member nations, as far as article 5.1¹ is considered, and it never could be: indeed, the underlying legal traditions and frameworks may vary significantly from one country to another. For instance, the use of signatures (and certificates) meeting the requirements for article 5.1 can be compulsory for uses that may vary considerably from one country to another. The legal strength of article 5.1 signatures as proof may also vary in a significant manner.

Today, the market for electronic signatures meeting the requirements of article 5.1 is very small. However, the Directive states that an electronic signature cannot be denied before the court, on the ground that it is electronic (article 5.2), and there is a large quantity of applications where electronic signatures could prove very useful, even if they don't meet the requirements of article 5.1. To sum up, imposing the use of signatures meeting the requirements of article 5.1 for e-government purposes has to be carefully weighted against security requirements and legal obligations, otherwise it could prove counter productive (price and / or loss of time for implementation and / or confusion for users).

If Europe sees interoperability as a key issue, it should encourage the migration to the chip of those documents where a consensus already exist. For example, the driving licence (a directive² has already been voted) has long been seen as the perfect document for a common European e-government card.

¹ Advanced electronic signatures (based on a qualified certificate and created by a secure-signature-creation device).

² 91/439/EEC: Council Directive of 29 July 1991 on driving licences

2.3 Security: the main concern is privacy

Security is, and has always been, the main justification for using smart cards. Cards are available now with an excellent level of security, for a very low cost.

There are two aspects of equal importance about card security: using a smart chip on a card increases the cost of defrauding it by a factor that had never been seen before.

We can assume that, for the first time in history, criminals will not be able to counterfeit it.

The second important aspect in security is privacy. As the cards will contain personal data, defrauding the card means breaking privacy. All surveys carried out in Europe have shown a real interest and high expectations from the citizens for smart e-government cards but also pointed out a real concern about privacy.

Privacy is an essential issue as it is directly linked with democracy.

Cards are available now with an excellent level of security, for a low cost, which is relatively small compared with the benefit of the level of trust they can provide, as a cornerstone for security. This does not preclude the use of rigorous communication and managing procedures.

We therefore advise an investment in security, security management and communication to keep fraud under control and enhance confidence.

2.4 Standards are available

The integration of smart cards in e-government, in accordance with existing legal requirements required an important number of standards to be published. These standards deal with the format (physical, electrical, protocols) of the card and of the reader, the reader / computer interface, the security architecture, the format of certificates, of security protocols, etc.

Today, we believe a sufficient basic set of standards is available (ISO 7816, PC/SC, EESSI, WIM, etc.), to cover almost any kind of situation and they are globally accepted, at least in Europe.

However developing either internationally shared formats for interoperability, and / or open software and APIs is a priority.

2.5 The status of biometry

There is no consensus, today on the maturity of biometry. The failure rate is around 1%, which prevents this technology from being used in commercial applications where it cannot be allowed to deny service to a customer.

For e-government projects, the benefits of using biometry (creating a unique link between the individual - biologically speaking - and his/her card) could compensate for this drawback. But the potential of biometry – maybe associated with smart cards – has to be explained to users and project managers, and the justifications of biometry have to be more explicit.

3 How to tackle existing barriers?

In order to ease the adoption of smart cards in e-government, we propose 6 action items: demonstrating the stability of standards, adopting a phased approach (which has already been done in most cases), mandating the use of smart cards for at least one service, focusing on user experience, adopting a global, comprehensive, strategic approach and defining a minimum set for interoperability of European e-government cards.

3.1 Focusing on user experience and services

The acceptance of smart cards by the end user is key for the success of e-government projects. It is possible to convince end-users of their interest in taking part in the project, by taking into account their user experience. A consistent user experience should be defined³ together with usage scenarios. Such scenarios could be filling in an online form, paying tax online, requesting online documents, etc.

For example, users may be interested in being able to do their administrative procedures outside opening hours, or from their home; kiosks may also be proposed. Once the user has learnt how to use one service, he/she can use them all.

3.2 The need for a global, comprehensive, strategic approach

There is an important need for coordination and more, for a global, comprehensive, strategic approach. This approach should, in every country be defined at the highest political level in order to allow for real collaboration between the different ministries. At the European level, a coordination between member prime ministers will allow the definition of a common strategic vision where a global ID smart card system could be proposed.

3.3 A step by step approach

We strongly recommend administrations willing to implement e-government services to follow a step by step high-level approach, accompanying the citizens in their experience. The first step is about online information on public services, the second step (interaction) allows the user to download digital versions of already existing paper forms, the third step (two-way interaction) adds the processing of forms - including authentication - and then the fourth step (transaction) is about case handling, decision and delivery, including payment (Carcenac report).

For example, today everyone can easily notice that e-government services have started, without mandating the usage of smart cards. When digital certificates are needed, they can be provided as a file to be stored on the computer or as a token (including smart cards). Because, users are threatened by the complexity of connecting a new device to their computer, they generally use software certificates. In the short/mid term, security and the necessity of ensuring a sufficient level of confidence will certainly be a driver for administrations to promote or mandate the use of smart cards.

³ Such a definition has been made, for example, in MeT ("MeT Consistent User Experience", version 1.1, 20 November 2001, URL: <http://www.mobiletransaction.org/>).

3.4 The first service...

Administrations should recommend the smart card as a token for e-government and invent some strong incentive schemes for users to adopt the first services and get accustomed to a new and enjoyable type of relationship with the administration.

This has been done, for example, in many bank card projects where consumers were offered a card to pay for parking. This has trained them to use their card and they now use it for many other payments at many kinds of merchants. Another example related to electronic signature, is the French TeleTVA procedure for VAT processing. The administration mandated the use of electronic signatures for this application, allowing businesses to get a first experience of digital signatures and to be able to use them for many other applications. This also meant the industry was ready to support them.

3.5 Demonstrating the stability of standards

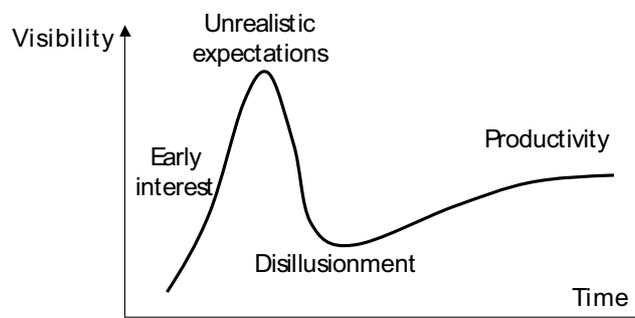
We recommend the development of a platform to demonstrate the availability and the stability of standards. This demonstration would allow a user to do some e-government procedures such as filling in an online form, paying tax online, requesting online documents. All the developments will be based on standards.

This would have the advantage making a clear point on the availability and stability of standards for a low investment.

Member states and the European institutions should also promote strongly the creation and adoption of a minimum set for interoperability, leaving open to the maximum possible extent the possibility that each member nation follows its own development strategy, as well as encouraging fair and socially positive competition between solution providers in which smart cards will certainly play a key role.

4 Conclusion: overcoming unrealistic expectations

Any application, based on a new technology, is known to go through the hype cycle. First, the applications gain early interest, where specialists begin to understand the benefit this application could bring. Then, as more people get involved in the development, enthusiasm grows and generates unrealistic expectations. As a consequence of this second phase appears a third and often long phase of disillusionment. As the application continues to be developed on a solid basis, the productivity phase sees its mass deployment.



Today, e-government applications come in the unrealistic expectations phase, where we would like to see all state of the art technologies doing everything possible for e-government and we tend to lose the vision of what is actually needed to address

citizens, businesses and administrations needs. In order to go as fast as possible to the productivity phase, a pragmatic approach should be adopted.

The use of smart cards should be pushed in a limited number of highly visible environments, a minimum set of interoperability should be defined, and consistent user experience should be preserved.

These factors are key to the success of smart card based e-government.
