gemalto
security to be free

European eServices:
What is missing for interoperability?

White Paper   **March 2009**

About Gemalto

Gemalto is the leader in digital security, with annual revenue of over €1.68 billion registered in 2008, more than 85 offices located in 40 countries and a workforce 10,000 strong that includes 1,300 R&D engineers.

Gemalto secure electronic documents are deployed in more than 50 government programs worldwide. Our firm is an acknowledged market leader in the field of smart card identity document technology. Gemalto is an active member of all standardization organizations relevant to smart card implementation.

European eServices:

What is missing for interoperability?

Dr. Bruno Rouchouze

April 2009

Introduction

European governments are increasingly motivated to reinforce security after the terrorist attacks of 11th September 2001. This is true for border control, as well as simple controls carried out in the street by police. At the same time, eServices are being developed, motivated by society's move from a paper world to a paperless one, and by the necessity for governments to reduce their budgets, and cut the cost of certain applications like citizen services offerings and government to government exchanges.

The main requirements for eID projects are travel functionalities and eServices, which are based on three key functions: Identification, Authentication, and digital Signature (IAS). As travel functionalities are well-covered by ICAO standards for ePassports, this paper focuses mainly on the requirement connected with eServices.

IAS can be used in relation to a host of diverse technologies, applications and projects. Interoperability between national systems is crucial in order to facilitate mobility for European citizens across the continent. However, there are several obstacles including relatively centralized and often proprietary architectures, fragmented responsibilities and a lack of simple collaboration, nationally-developed digital modernization programs and a diversity of ID and exchange security methods. Therefore, eServices interoperability must be based on a general framework agreed upon by all member states and must protect citizens' fundamental freedom and their personal data. It must cover legal, organizational and semantic aspects, as well as trust, security and technical frameworks.

This paper demonstrates that the technical choices are already in place for total eServices interoperability.

The main challenges anticipated are more about legal aspects and responsibilities. These aspects are detailed in this paper in order to give a complete overview and indicate the last key areas to be resolved for concrete European eService interoperability.

gemalto

eID: Overview

Since the Lisbon engagements on eID in 2000, seven European member states have already started national smart card-based eID projects, while 14 others have been analyzing this smart card technology for future national eID projects. National ID cards are issued by national government bodies or agencies for citizens of the respective country. These cards confirm the ID of individual citizens and thus are keys to rights related to citizenship. In this context, eID refers to a national ID card with visible and invisible security features and a secure microprocessor. These cards use the so-called ID-1 format which is well known from credit cards.

> *"By 2010, European citizens and businesses will be able to benefit from secure means of electronic identification that maximize user convenience while respecting data protection regulations. Such a means shall be made available under the responsibility of the member states but recognized across the EU. […] As our eGovernment services become more transactional, the need for secure electronic means of identification for use by people accessing public services is essential for citizen and business trust and in ensuring the effectiveness and efficiency of our public administrations."*
>
> Ministerial Declaration from the 25 member states
> Manchester eGovernment 2005

Traditionally, an ID card serves as personal document for visual identification. But by including a chip, the card's security is increased because smart card microprocessors are virtually impossible to counterfeit. These chips can also carry citizens' biographic data, and the additional storage of biometric features can create a strong link between card and holder as has been successfully done with ePassports. eIDs carry credentials in order to be used for either or both of the following:

- As an inter-European Union travel document
- To facilitate logical access to eGovernment or local administration services

The trend is set in Europe: electronic passports have been deployed successfully and most European countries have a national ID card and several, including Austria, Belgium, Estonia, Finland, France, Germany, Italy, Lithuania, Spain and Sweden, have adopted or are in the process of adopting an electronic contact technology-based national ID card.

Here the Lithuanian eID, the latest eID introduced in Europe in January 2009

Overview of technical tools for eServices in Europe

European Citizen Card: the standard for Europe

The requirements for a more secure ID document and for access to electronic services were the two main drivers for the European Committee for Standardization (CEN) when defining the European Citizen Card (ECC). Interoperability has always been important for the smart card industry. For any smart card program to be effective, the card must work seamlessly with readers, and the readers must in turn work seamlessly with PCs and networks. This is perhaps even more important when the cards and readers are supplied by different vendors or are used in multiple environments or geographical areas. The ECC standard gives technical answers regarding the requirement for interoperability.

The ECC standard is an open application standard, defining logical data structure, and security and privacy mechanisms of the data and interface, and communication protocols. It is open and allows governments to select different options. For instance, both contacts and contactless smart card interfaces are defined as well as biometrics and/or PINs for 2-factor authentication. The complete framework for an electronic signature is specified. There is no limitation on this standard in the project quantity scale and/or in the type or number of online services. The ECC standard is key for an interoperable and cross-border eServices solution. It is open for a wide range of services including eGovernment, eBusiness, eVoting, eDemocracy and eBanking.

With the decision to take this application standard into a national government and/or industry program, the decision maker reduces development time, decreases technical risks as well as the necessary budget for the period of definition, specification and tendering. Moreover, with the European Citizen Card standard, the European Union can take a leadership role in eID/eServices as it has done in the past with the GSM standard for mobile communication.

The European Citizen Card (ECC) standards have already been issued. The illustration shows the very first ECC product issued in August 2008 by Gemalto.

gemalto

IAS-ECC: Off-the-shelf technical specifications based on the ECC

The standards define the services and mechanisms that need to be adopted in order to provide product features that comply with functional requirements, user capability to use the product and integration within the environment. The standards provide a certain level of interoperability, but the high level of definition introduces different interpretations and the options that can be part of a standard may introduce interoperability difficulties.

The IAS-ECC specification has been published by the GIXEL association (GIXEL is the French association for electronic components systems and smart card industries). The technical specifications contain an implementation plan that determines choices left open by the standards and thus lead to a high level of interoperability. They comply fully with ECC standards while providing a high level of interoperability. This ECC standard is a central element for an interoperable eID management system. It is a key enabler for the achievement of the i2010 objectives proposed by the European Commission and it is already used by some member states.

Even if harmonization at a European level must be based on agreed legal, semantic and technical requirements, the IAS-ECC technical specification focuses on technical concerns only.

It is anticipated this will:

- Improve security of ID documents security by adding security features and secure electronic components

- Reduce costs for businesses and administration activities by simplifying procedures and optimizing resources

- Improve the quality and accessibility of public services by making the public sector more open and transparent, and facilitating transactions between administrations and citizens

- Pick out services with clear added-values to citizens and governments, i.e. increase the quality and accessibility of public services and offer accessibility for all users and not only for some experts

- Harmonize data and security architecture in the EU-area for a complete intra-European interoperability motivated by European citizens' mobility

The IAS ECC technical specification allows the smart token to be connected directly to the server where eServices must be used. This reduces risk management, ensuring security and privacy, and avoids legacy difficulties. Identity cards have been in common use throughout numerous countries around the world for some time now. They have been introduced for several reasons, including acting as proof of identity and age and for voting. Building on the technologies introduced for the implementation of ePassports, eID cards use microprocessor technology to store personal information, to enable electronic identification and/or holder authentication and allow secure digital signatures. The cards become an efficient and secure platform and interface for the receipt of government services. This is the first significant advantage from Gemalto's point of view.

Test suite for full interoperability

Interoperability starts with compliance in terms of specifications, but is proven by the results from test suites that check both compatibility to the specifications and interoperability, with the cards on test showing how they respond to external requests. Such test suites exist for eTravel applications at the ICAO level.

In addition, the level of definition in IAS-ECC specifications allows for the production of test suites provided by SOLIATIS, an innovative company created in 2002 specialized in solutions based on smart card technology. These test suites will be used for interoperability evidence. Such test suites already exist for IAS-ECC. European member states can already apply them to their cards.
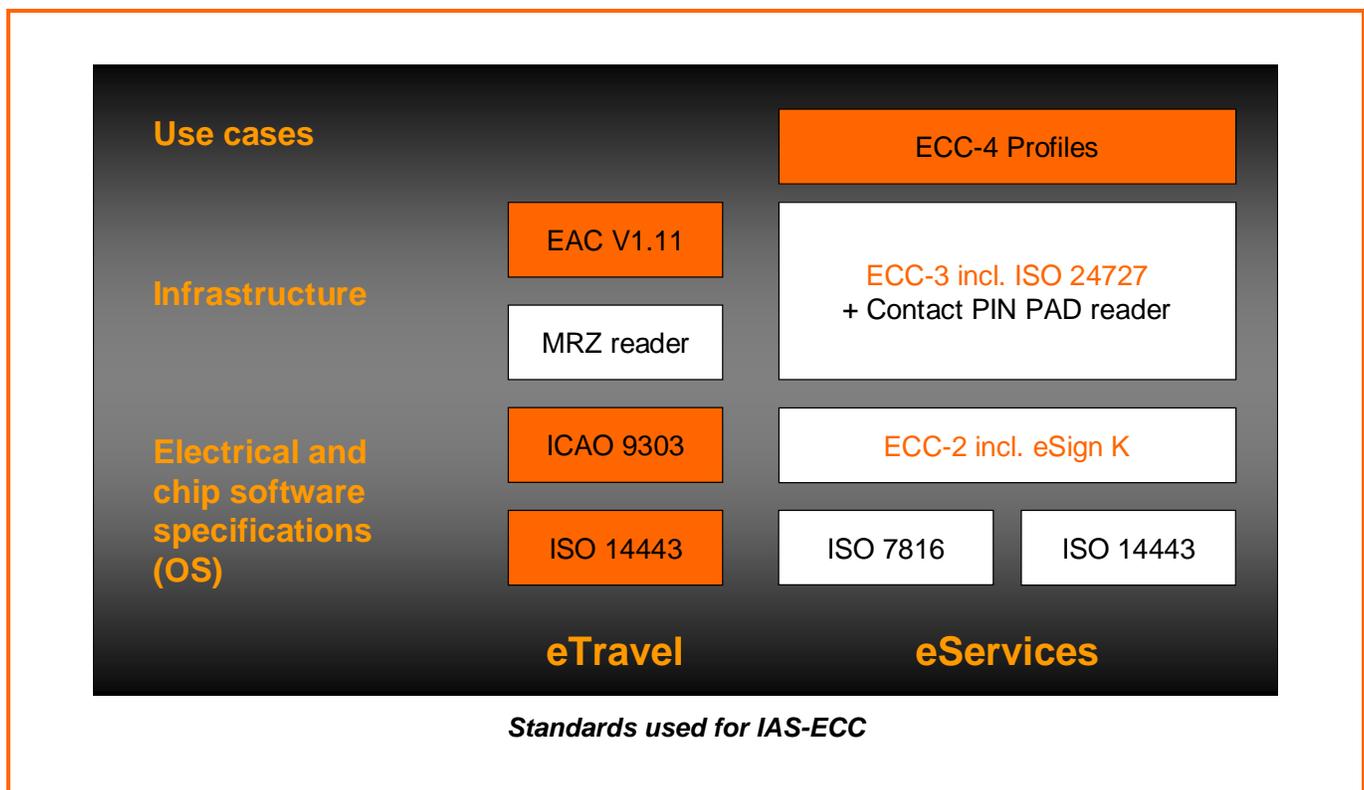
Instant connectivity for citizens

Smart cards need specific tools for communicating with the external world. The first issues to emerge have been solved with middleware-based solutions.
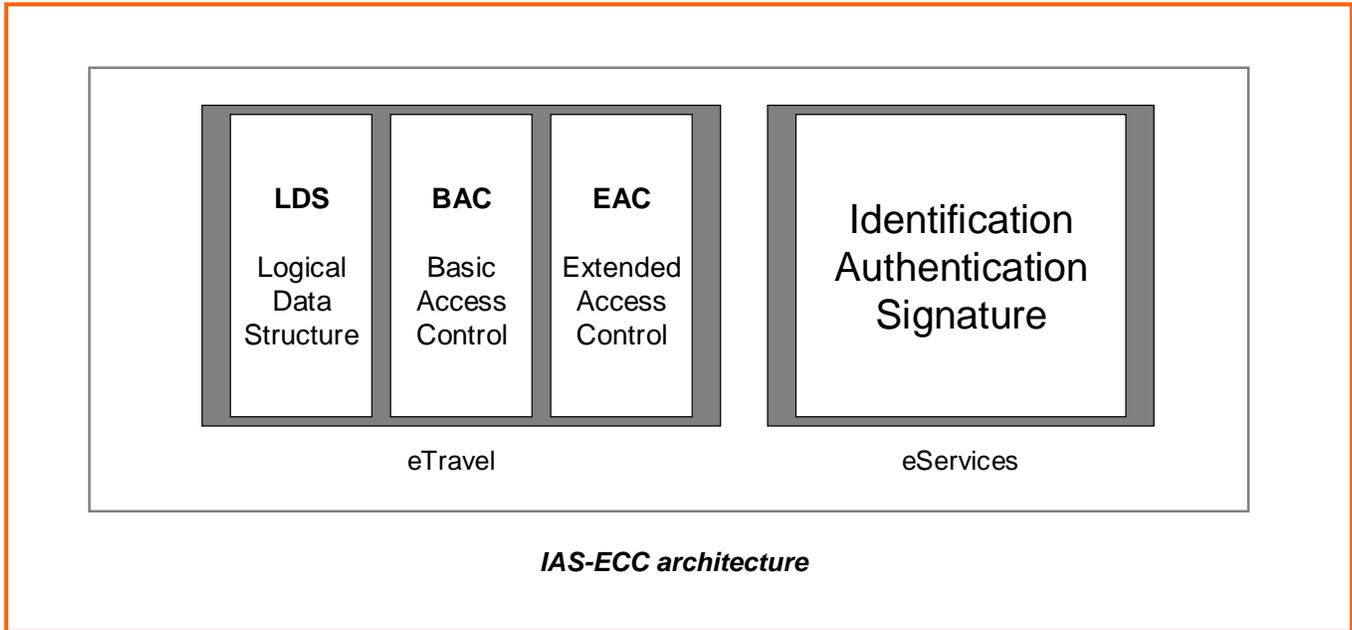
A complete IAS-ECC is already in place and can be downloaded at the French ANTS website. This governmental tool allows all existing IAS-ECC cards proposed by different manufacturers to communicate with PCs and servers. A second version will soon be available and will integrate the ECC's part three requirements in order to accept not only IAS-ECC cards but also smart cards with others operating systems. This will guarantee complete interoperability between IAS-ECC smart cards and also between IAS-ECC smart cards and all existing eID cards that have already been deployed which will be able to dialogue with this kind of IAS-ECC middleware.

Gemalto has also recently introduced a similar tool as a pioneering solution enabling citizens to instantly connect to eServices using eID smart cards. This solution requires no software on the citizen's computer. It radically simplifies the rollout of value-added secure services and boosts take-up. Coesys eGov 2.0 runs on any browser on any operating system, and allows plug-and-play connectivity from any computer. The core technology at work – Gemalto's SConnect smart card neutral connectivity – won the **Sesame Award for Software** at the Cartes & Identification trade show in 2007. This solution spearheads the increasingly popular citizen-centric approach, also described as eGovernment 2.0 and represents a paradigm shift in smart card-based service delivery over the web.

Profile for concrete usage

France has made the choice to be ECC-compliant and has selected IAS-ECC as the specification for its national eID card. The specification represents the concrete implementation of the ECC and freezes some technical options proposed by the ECC. As an association of several standards (see table below), IAS-ECC allows for complete interoperability between smart card manufacturers and also with previous IAS versions. The architecture is built as shown in the following diagram and can be easily upgraded with new coming functionalities or security features.

Use cases		ECC-4 Profiles	
Infrastructure	EAC V1.11	ECC-3 incl. ISO 24727 + Contact PIN PAD reader	
	MRZ reader		
Electrical and chip software specifications (OS)	ICAO 9303	ECC-2 incl. eSign K	
	ISO 14443	ISO 7816	ISO 14443
	eTravel	**eServices**	

Standards used for IAS-ECC

IAS-ECC architecture

The travel functionality is contactless as for the ePassport when the eService uses contact mode. This is driven by the opportunity to reuse both existing infrastructures (ePassport & RSA PKI). Nevertheless, the eService side could easily incorporate a contactless approach.

Security evaluation

Security will be evaluated, compared within Europe and certified. A Common Criteria scheme is already in place and is widely used in the smart card industry. The Common Criteria define the methodology of evaluation and European member states have agreed on mutual recognition of certificates delivered by their certification bodies.

Evaluation of a smart card refers to Protection Profile (PP) documents that explicitly guide the process of evaluation, taking into consideration the security needs for each of the card's different uses. Gemalto has contributed to the writing of several PPs. Security evaluation of the eTravel application refers to ICAO and EAC PPs, and security evaluation of ePassports is already carried out according to them. For eServices, several PPs already offer a good base for authentication and digital signature features in contact communication mode.

.

eServices: Next steps for full European interoperability

The EU has recognized that eGovernment offers European citizens important opportunities for improved access to better governmental services. When implemented and used correctly, eGovernment offers national governmental systems substantial productivity gains and helps them to cope with increasing demand for high-quality governmental services.

Interoperability is a basic requirement for systems and applications. The European eGovernment world is rather scattered and uncoordinated at the moment and requires some effort to consolidate it. First steps taken by the STORK consortium are taking things in the right direction, but interoperability is not only technical; it also involves standards, security, legal and semantic issues. The current eGovernment situation may be summarized as in the following subsections.

Standards: challenge 1

Even if governments and smart card industries have developed ECC standards at CEN, there are always opportunities to select others standards. The lack of widely-used standards implies that standards often conflict and interoperability problems often occur. Many of the conflicting standards are software-based. There may also be differences involving flawed implementations of the same standard that are not interoperable. In some cases, even different versions of a same standard may conflict. This is due to the freedom given to all European member states to select their own national solutions without any current key recommendations at a European level for facilitating interoperability. This flexibility is a barrier to generic and useful interoperable solutions and paves the way for complex and expensive bridges between national eGovernment solutions. Are European citizens prepared to pay for such complex solutions when simpler ones already exist? Probably not.

Business analysts suggest the market for eService information systems in Europe is huge and largely untapped. However, interoperability problems may be one reason for governments and other eService providers to hold off from investing in information and communication technology (ICT). Consequently, growth in companies supplying ICT for the eServices sector is lower than it could be. Furthermore, economic growth related to standardization may accrue predominantly in the country or part of the European continent where a particular standard has been developed. Other economic implications of a lack of commonly-used eService standards are lost opportunities for cost reduction and compromised quality of eServices. In terms of cost, given the lack of commonly used standards, opportunities for streamlining governmental and private eService processes and for delivering activity data go unexploited. And as regards the quality of eServices, a lack of integrated information systems could introduce failures in a Europe-wide system of interoperability where European citizens – the final user – will be the victims.

There is now a powerful process in place to harmonize existing standards. Recently, however, there have been major advances made in such activities from the smart card industry with ECC and IAS-ECC. The large-scale member states eID pilot planned to start in 2008 and funded by the ICT Policy Support Program (PSP) is expected to become a further catalyst. It is hoped some guidelines will thus be defined at a European level and will limit the standards used. This is a first step for assuming complete interoperability at a European level.

Security level requirements: challenge 2

The security levels of deployed solutions may differ from one member state to another, creating conflicts for interoperable eServices. Given that cyber criminals and terrorists will always attack the weakest link in the European defense chain, pan-European security is only achievable if all eID projects are equally strong, but this is not the case for the more popular secure smart card-based approach and the purely software-based approaches used in some national infrastructures.

gemalto

For example, the European Digital Signature Directive has concrete requirements. But some pure software approaches cannot be used for strong secure signatures because they do not meet protection profile requirements for a level EAL4 augmented (also referred to as EAL4+) signature. What would happen if a document from Country A was signed in Country B with a login-password combination and then delivered for eServices by Country C but was hacked when Countries A or B requested a strong authentication mechanism for digital signature?

No European country would want to weaken national security and break down their economical efforts further to unsecured foreign choices that could introduce a major risk into their global interoperable system. Member states must therefore evaluate and compare security levels of all national implementations.

European mobility necessitates total interoperability everywhere in Europe but harmonization is not really applied to security level requirements for concrete functions such as identification, authentication digital signature, data memory protection or privacy management. Even if technical solutions already exist, there is no consensus on such crucial and fundamental elements of complete and applied interoperability. The method for measuring security levels already exists with Common Criteria, which is an ISO standard and widely adopted in Europe. It would be highly satisfactory to harmonize security level requests by using common protection profiles for common security targets where security objectives, threats and security function requirements are strongly defined. Depending on these security requirements, some unsecured approaches would be definitively stopped in favor of common secure solutions. Smart card technology solutions based on IAS ECC would probably emerge as favorites, which would guarantee a complete secure chain of eServices systems and for member states that have already invested in such secure technology for their own national eServices needs.

Semantics: Challenge 3

The interoperability of ICT systems is indispensable for efficient business processes. However, such interoperability for eServices is a big challenge. Those who provide eServices use ICT from different manufacturers from different technology generations and in Europe, from countries with different eService systems, languages and semantics. This means that eServices information systems are often unable to exchange data in a meaningful way.

The eServices deployed in different European countries serve similar needs, being used for tax declarations, healthcare services, police declarations, secure private or public transactions, etc. However, the implementation of such eServices differs from one country to the next, and different semantics determine that different input data is required for similar fundamental eServices in different countries. This generates conflict in terms of interoperability.

For services such as eHealth where patient medical history or emergency data need to be harmonized at a European level, it would be helpful for strong interoperability to define common terminology and common

semantics. If EU member states are to seek cross-border eServices and, in the long run, an internal market for eServices, such interoperability issues need to be solved at an international level.

The European Commission must implement a roadmap for further semantic definitions regarding eServices. Current and future wide-scale pilots taking place in member states should be extended to other key applications with clearly defined semantics.

Legislation: Challenge 4

Legislation covers national requirements but legislation on a European level for electronic services is still being drafted. Certain definitions of failed responsibility could mean complex responsibility analysis in the case of eService fraud.

A first example is privacy. Privacy is defined as the right of an individual to keep his life and personal affairs out of public view, and to control the flow of their personal information. As a substrate of anonymity, privacy is sometimes related to anonymity and could be seen as an aspect of security. An invasion of privacy is a legal term essentially defined as a violation of the right to be left alone. There are different types of privacy, including bodily privacy, political privacy, medical privacy and privacy from corporations or from government interfaces but for our purposes, we will talk about ePrivacy. This is defined as a person's right to keep their electronic life and business out of public view, and to control the flow of their personal electronic information. In order to protect our ePrivacy, the necessary functionality must be part of our digital experience: eIdentification, eAuthentication, eSignature and data eStorage.

Article 12 of the **Universal Declaration of Human Rights** is clear: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*" In some countries, privacy is explicitly protect by a constitution. For example, France's Declaration of the Rights of Man and the Citizen and the right to freedom of speech granted in the first amendment of the US Constitution have limited the effects of lawsuits for breach of privacy. Other countries without constitutional privacy protection have laws protecting privacy such as the United Kingdom's Data Protection Act of 1998 or Australia's Privacy Act of 1988. In many countries, if an individual's privacy is breached, the individual may bring a lawsuit asking for monetary damages.

Europeans are acutely familiar with the risks associated with the uncontrolled use of personal information from their experiences in World War II, with fascist governments and with post-war Communist regimes. In general, they are highly suspicious and fearful of the unchecked use of personal information. The right to privacy is a highly-developed area of law in Europe. The European Commission understands that diverging data protection legislation in EU member states would impede the free flow of data within the EU zone and all member states have also validated the **European Convention on Human Rights**, in which Article 8 provides a right to respect for an individual's "private and family life, their home and their correspondence". It is completed with the harmonization of data protection regulation with the **Directive on the Protection of Personal Data**. The EU Directive 95/46/EC limits and regulates the collection of personal information on individuals, including workers.

Even if the European Union requires all member states to legislate to ensure that citizens have a right to privacy through means such as Directives 95/46, national data privacy laws still vary greatly across Europe. This means privacy concerns are often viewed as a barrier, and there is a complex landscape of privacy within Europe which could have a very negative impact upon European interoperability. Even if privacy issues are seen as generally more difficult to tackle as technical issues, it is nonetheless critical to focus on them. There is currently no clear procedure governing the response to the loss of privacy in one country by a citizen from another country using eServices from a third. It is critical that Europe-wide legislation is completed.

Digital signatures can also pose similar problems. The potential security issues outlined in the **conflict of security level requirements** section is still pending in terms of European legislation. It is not clear how to manage such security issues in terms of legal and engaged responsibilities between member states, ICT eServices providers, companies supplying ICT for eServices sector and European citizens themselves.

Both examples show that national and European legislation is not sufficiently clear to satisfy the requirements of future cross-border interoperable eServices. In addition to educating citizens about eServices, it is crucial that we focus on such international legal aspects if member states wish to avoid confusing and complex situations linked to the future use of cross-border eServices.

Conclusions

The pan-European emerging eServices IT infrastructure is a huge opportunity for improving the lifestyles of European citizens. But these eServices must be developed and deployed in harmony within Europe and interoperability requirements must always be kept in mind. The goal must be a combination of interoperability and security mixed with privacy for the introduction of cross-border eID-based eServices. One solution for the interoperability challenge in terms of eServices may be the common use of a more confined and harmonized number of well-developed standards. European member states now have the chance to benefit from IAS-ECC solution for rolling out eID within their national program. There are already product offers proposed by different providers in the field that guarantee fast deployment and cost effectiveness with continuity of supply. Some deployments have already started.

But the solution is not only technical. Europe cannot forget other key challenges regarding interoperability. Security, semantics and legislation are probably the three key drivers for a completely harmonized and truly global European system based on national or regional sub-systems. Effort must be made in future in these areas as well as being directed at anticipating cyber threats and attacks. This is the path towards readiness for EU i2010 objectives. This interoperability will be the cornerstone of European eServices and will become an everyday reality within organizations, between different providers, within regional and national eServices systems, and last but not least, everywhere in Europe for all European citizens alike.