Open Smart Card Infrastructure for Europe

v2

Volume 4: **Public Electronic Identity, Electronic Signature and PKI**

Part 3: **White Paper on Identification and Authentication in eGovernment**

Authors: **eESC TB2 Identification and Authentication**

Contacting *e*Europe Smart Cards Trailblazer 2
*e*Europe Smart Cards Trailblazer 2 on Identification and Authentication is an informal group of about 70 participating organisations and individuals interested in electronic signatures and smart cards that can be used for Identification and Authentication. *e*Europe Smart Cards Trailblazer 2 has been supported by EESSI (European Electronic Signatures Standardisation Initiative) that has largely promulgated the prevailing standards on electronic signatures in Europe pursuant to the European Directive 99/93/EC on a common framework for electronic signatures.

For information on *e*Europe Smart Cards Trailblazer 2 or this white paper you may contact:

Dr. Andreas Mitrakas
Chair, *e*Europe Smart Cards Trailblazer 2
Ubizen
Ubicenter
Philipssite 5
3001 Leuven, Belgium.
andreas.mitrakas@ubizen.com

Acknowledgement
In drafting this white paper, Trailblazer 2 acknowledge the contribution of Jan van Arkel (eEurope Smart Cards), Andrew Hinchley (CEN/ISSS, eWallet project), Dr. Lutz Martiny (eEurope Smart Cards), Hans Nilsson (Hans Nilsson Consulting), Henry Ryan (eEurope Smart Cards) and Peter Tomlinson (Iosis Associates) as well as of all its members.

Notice
This white paper can be quoted as:
*e*Europe Smart Cards Trailblazer 2, *White Paper: Identification and Authentication in eGovernment*, 2002.

Executive Summary

Implementations for eGovernments emerge as a significant application area for Identification and Authentication. Although standards developed for electronic signatures can still meet the requirements of Identification and Authentication, additional work is imminent to provide end users with consistent and interoperable solutions at an EU-wide level. Focusing on eGovernment applications this white paper aims at providing an essential pre-standardisation set of requirements as well as guidance for future work in the area of Identification and Authentication. This white paper concludes by highlighting some areas in which further work is necessary to better address the needs of eGovernment applications.

Table of Contents

1. Introduction

Identification and authentication has become an essential element to invoke Trust in electronic services. In Identification and Authentication the user requirements for Trust are often met by the usage of a combination of smart cards and Public Key Infrastructures (PKI).

Supporting four application domains including eGovernment, the scope of *e*Europe Smart Cards has been to identify the prevailing issues associated with the deployment of smart cards. The action plan focuses on both the needs of citizens and the business community alike in terms of business cases, multi-functionality and interoperability of systems and infrastructure, and the provision of trust in all aspects of service delivery. Failure to meet the promise of eGovernment applications might hamper the confidence of citizens and commercial end users alike who are likely to otherwise continue using traditional mechanisms to interact with the government to the detriment of electronic services. Furthermore, applications in the area of eGovernment are expected to represent a significant part of presently deployed on line applications.

The goal of this white paper is to tackle the problem of accessing readily accessible information with regard to common risks, trouble areas or shortcomings in setting up policies, strategies and implementations of identification and authentication solutions for eGovernment. This white paper also aims at providing an essential pre-standardisation set of requirements as well as guidance for future work in the area of identification and authentication. This white paper addresses issues such as:

- Basic assumptions on electronic signatures.
- Policy matters.
- Technical aspects to ensure designated trust levels.
- Common risks in implementing a smart card based PKI for the public sector.
- Aspects of Trust and assurance of the services.
- Selected aspects on risk and policy.

An additional goal for this white paper is to provide guidance to public administration agents and information technology providers alike with regard to the requirements for eGovernment applications.

Implementations for eGovernment inevitably play the role of putting public policy into practice. It is, therefore, necessary to allow for revisiting certain concepts and assertions of smart card based PKIs for Identification and Authentication before giving them a full-fledged effect in eGovernment. Such trial and testing are necessary to ensure compliance with the needs and expectations of large populations of end users and eGovernment for greater efficiency through electronic transactions. In this context, this white paper can be further used as initial input for e.g. best practices, model implementation plans on Identification and Authentication.

The remainder of this white paper addresses certain aspects of Trailblazer 2 within *e*Europe Smart Cards, and aspects of eGovernment applications that make use of smart cards and PKI, and provides guidance with regard to implementing smart card based PKIs in eGovernment and recommendation for future work.

2. Trailblazer 2 on Identification and Authentication

While *e*Europe Smart Cards has among other issues aimed at accelerating the pace of securing Internet based transactions, Trailblazer 2 on Identification and Authentication aims at supporting Trust services in need of identification, electronic signing and confidentiality. Identification and authentication technologies have widely been seen as essential to invoke Trust in open electronic commerce environments that require electronic signatures.

Trailblazer 2 has been a horizontal activity that can potentially impact a broad number of interest areas of *e*Europe Smart Cards. Trailblazer 2 has addressed Public Key Infrastructure (PKI) and smart cards to secure transactions in any given operational environment within the range of its activities. The choice of PKI and smart cards associates with the prevailing legislative and standardisation framework in the EU in the area of electronic signatures. To fulfil its objective, Trailblazer 2 has related its work with other Trailblazers such as Trailblazer 1 on Public Identity, Trailblazer 10 on eGovernment, Trailblazer 12 on advanced electronic signatures.

The scope of Trailblazer 2 has been to identify the functional requirements related to individual Trailblazer interest areas and respond to such functional requirements. In late 2001, Trailblazer 2 presented a *Pre-Inventory of Smart Card based PKI projects in the European Union*. By means of a questionnaire, this Pre-Inventory surveyed a number of large scale projects aiming at deploying smart card based PKIs by addressing technical, organisational as well as legal aspects of such deployments. This published pre-inventory draws useful conclusions for large-scale PKI implementations. Through this white paper Trailblazer 2 further builds on the conclusions and recommendations of this survey to crystallise certain conceptual requirements for smart card based PKI implementations. The focus on eGovernment associates with a burgeoning area of applications that address the requirements of at least two more *e*Europe Smart Cards Trailblazers, namely, Trailblazer 1 on Public Identity and Trailblazer 10 on eGovernment. While the focus of this white paper is the area of eGovernment at large, other large-scale implementation areas might find useful the conclusions drawn in the paper.

Supporting Trailblazer 2, the European Electronic Signatures Standardisation Initiative (EESSI) focuses on the standardisation of electronic signatures pursuant to the Directive 99/93/EC *on a Community framework for electronic signatures*. The EESSI standardisation deliverables have widely been acknowledged for being generic, flexible and applicable in a multitude of transactions. EESSI deliverables, however, can be further extended to reflect the specific needs of industry and governments. The Global Interoperability Framework for pan European interoperability of the functionality of end user identification, authentication and digital signature has worked closely together with the so-called Area K of EESSI and the GIF implementation guidelines completely rely on the work of Area K.

Trailblazer 2 contributes to the objectives of EESSI by bringing them closer to a significant user and application community associated with the usage of smart cards. The EESSI standards have been carried out by the European standardization organizations, namely the European Telecommunications Standards Institute (ETSI) and European Committee for Standardization/Information Society Standardization System (CEN/ISSS). The concrete results of the EESSI standardisation effort are referenced in annex I.

2.1. Identification and Authentication for eGovernment

Requirements for Identification and Authentication can be met in a number of ways and using various technologies or techniques. Also through the Directive 99/93/EC, for electronic signatures PKI has been given a significant primacy for meeting the requirements of electronic signature used by large populations that make use of public open networks. Working within the framework of Directive 99/93/EC, the EESSI standardisation effort added to the specificity of PKI with regard to electronic signatures. In maintaining a technology neutral stance this Directive has separated the legal recognition and conditions for the provision of electronic signatures from those of the technology of choice to deliver such service. While in the future other technologies might meet the requirements of the Directive 99/93/EC, the EESSI standards clearly focus on PKI and strongly support the usage of smart cards as a means to convey security and Trust in electronic communications within the meaning of the Directive 99/93/EC. Implementations for eGovernment may as well benefit from using existing standards for eSignatures that have been developed in a European context and are the outcome of broad consensus within the industry.

3. Applications for eGovernment

The envisaged transaction environment for eGovernment applications needs to meet the expectations of citizens and the businesses alike when interacting in an eGovernment transactions context (UNCTAD 01). Typical eGovernment applications for citizens include the ones below:

- Proof of identity
- Taxation
- Social Security
- Social Services
- Health care
- Registration Services of e.g. vehicle, boat etc.
- Permits e.g. building etc.
- Family status certificates
- Education enrolment
- Employment related services

Typical eGovernment applications for organisations include the ones below:

- Social security contributions
- Employment services
- Health and safety regulation
- Corporate tax
- VAT submissions
- Company registry
- Statistical and quota submissions
- Public procurement (also including invoicing and payment)
- Custom declarations

Some of these areas have already received significant attention in the past and in many cases technology infrastructures are already in place and successfully used for transactions. Customs declarations for example have greatly benefited from the evolution of Electronic Data Interchange (EDI) and subsequent Customs cooperation programmes. Typical roles within eGovernment applications include:

- Application owner: This is the eGovernment agency that owns and controls the eGovernment implementation that supports a smart card. The Application owner can also be the smart card issuer.
- PKI service provider: This is an outsourced provider of PKI services.
- Smart card vendor: This is an outsourced provider of smart card tokens.
- End user: End-users include typically citizens other categories of users might also be included, such as agents of public administrations, corporations, professionals etc.
- Other: This category includes the various brokers that might get implicated in an eGovernment smart card based implementation such as an identity broker, a privacy broker etc.

A clear definition of roles is a prerogative for eGovernment implementations to allow for a separation of duties and areas off responsibilities.

4. European Union Directive on electronic signatures

The advent of the Directive 99/93/EC *on a Common framework for electronic signatures* has made an impact on eGovernment applications. The Directive introduces three classes of electronic signatures, namely:

- A general class of electronic signatures;
- Advanced electronic signatures;
- Advanced electronic signatures based on qualified certificates and created by a secure signature creation device.

A specific type of electronic signatures, often dubbed under the term introduced by EESSI as qualified signatures, can meet certain formal requirements and are granted the same legal effect as hand-written signatures, according to article 5.1 of the Directive. The effect of advanced electronic signatures which are based on a qualified certificate and are created by a secure-signature-creation device is that they:

a. Satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data.
b. Are admissible as evidence in legal proceedings.

Advanced electronic signatures, are a more generic type of an electronic signature that meets the following requirements:

a. It is uniquely linked to the signatory;
b. It is capable of identifying the signatory;
c. It is created using means that the signatory can maintain under his sole control;
d. It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Article 5.2 of the Directive 99/93/EC addresses the legal effect of signatures that do not meet the requirements of qualified signatures. These signatures are not to be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that they are:

a. In electronic form.
b. Not based on a qualified certificate.
c. Not based on a qualified certificate issued by an accredited certification-service provider.
d. Not created by a secure signature-creation device.

The signatures of Article 5.2 can also be used for identification and authentication, like when using S/MIME, for example. These signatures are within the focal area of Trailblazer 2, and can be used for certain eGovernment applications where hand-written signatures are not needed.

This far a relatively small number of deployments and applications have characterised the deployment of qualified signatures. In a paper-based environment law requires hand-written signatures in a relatively small number of formal transactions, a tendency that might be projected in electronic transactions also. It can be argued that the assertions on qualified signatures have thus far paid little service to the general usage of electronic signatures. This tendency can be amended by improvements in the available technology and a higher rate of penetration of electronic transactions also for eGovernment.

Electronic signatures that can also be used for Identification and Authentication have successfully been used within Closed User Groups (CUG) for a number of

years. These CUG solutions remain largely out of the scope of the Directive 99/93/EC, they may, however, benefit from the formal requirements with regard to qualified signatures. Some CUG implementations of electronic signature could also be enhanced to use qualified signatures.

Directive 99/93/EC allows Certification Service Providers to provide their services without prior authorisation by Member States' authorities. Member States may, however, decide how they may ensure the supervision of compliance with the provisions of the Directive. The Directive does not preclude the establishment of private sector based supervision systems or oblige certification service providers to apply to be supervised under any applicable accreditation scheme. However, Member States are obliged to notify the EC of any approved provision of certification services. The Directive also foresees provisions for the recognition of certification service providers based beyond the EU.

By means of this Directive eGovernment services can be used within Member States' and EU administrations and in communications between those administrations citizens and businesses. The practical market impact that the regulation of electronic signatures will bring about still remains to be seen.

5. Observations on Identification and Authentication for eGovernment

In 1997, the first law on electronic signature was enacted in a EU Member State. Italy and almost simultaneously, Germany picked up on the trend set out in several US states that followed the first digital signature law enactment of the state of Utah (1995). The high level of legislative responsiveness in a matter as fundamental to transactions as electronic signatures has been probably unparalleled in the regulation of information technology in general, signalling a high degree of responsiveness from the legislator. Nevertheless, there are a number of issues associated with implementations in the area of Identification and Authentication that can further be considered such as the ones addressed in the non-exhaustive list below.

5.1. Multi-level effect of electronic signatures

Electronic signature legislation pursuant to the implementation of Directive 99/93/EC and subsequent standardisation has resulted in three levels of electronic signatures:

- The level of requirements set out in several member states that have shifted implementations to a high-level and demanding framework likely to meet specific public law requirements.
- The qualified signatures' level in the meaning of the Directive 99/93/EC.
- A general level of electronic signatures that does not necessarily follow any broadly applicable normative guidelines.

It might be beneficial for end users to determine clear equivalence criteria among these varying levels that also associate with the specific application they are used for.

5.2. Authentication vs. signing

Directive 99/93/EC has built on a dichotomy between high-grade performative signatures and the general electronic signing capability that can easily be purchased through present day commercial grade implementations, supporting S/MIME. This approach accommodates the varying approaches among the legal systems of the EU member states with regard to electronic signatures.

Implementations for eGovernment need a high degree of clarity of the exact scope of the implementation in order to ascertain that the desired function also serves the legal purpose of the transaction performed.

5.3. Qualified signatures, for eGovernment

At present, private applications and CUGs might face some difficulty in becoming users of qualified signatures. The formal requirements for qualified signatures largely serve the needs of applications that replace procedures requiring hand-written signatures. Without underestimating the value qualified signatures might have for private transactions it might be argued that the implementation of Directive 99/93/EC on electronic signatures and the subsequent standardization of qualified signatures greatly facilitate the deployment of electronic signatures that meet formal requirements, such as those of eGovernment.

The widespread usage of qualified signatures relates to the number and type of implementations that become available in a way that these signatures are mandated. The immediate effect for eGovernment is that while the installation of

a qualified signature based system is demanding, the effort might not be entirely justified should the user community be limited to a confined number of users or applications.

5.4. The function of signatures

The Directive on electronic signatures implies a certain level of public policy when using electronic signatures. The subsequent standardisation effort led by EESSI has also concluded that natural persons only can use qualified signatures and they can only use those signatures to carry out signing tasks. Other traditional functions of electronic signatures might slowly pass in the background, at least as far as the current level of eGovernment applications is concerned. (Kuner et al. 1999, Aalberts et al. 1999). The immediate effect for eGovernment implementations might be that the function of electronic signatures should be monitored at the national level to rationalise on the exact functions performed by applying a signature and subsequently adapt the requirements to the usage of qualified signatures.

5.5. Remove any residual barriers to eGovernment transactions

For eGovernment applications it is necessary to remove any specific legal barriers to electronic signatures that might still remain at the local or application levels. Certain transactions might remain out of scope of present day national laws on electronic signatures, which might, nevertheless, affect electronic signatures. One goal of additional legal review in this area may include addressing and if necessary removing any such uncertainty. Special attention could also be attached to the evidential value and legal effect of electronic signatures in a particular context.

5.6. Contractual freedom

When acting in a private law transaction framework, eGovernment applications should take into account private law requirements. One such requirement is the principle of contractual freedom, also addressed in Directive 00/31/EC *on certain legal aspects of information society services, in particular electronic commerce in the Internal Market*. Contractual freedom might result in variations of electronic signature implementation requirements, which eGovernment applications should be in the position to conditionally accommodate under certain circumstances.

5.7. A link to eGovernment transactions

The current model for electronic signatures provides limited links to transaction procedures. Aspects such as the role under which a signature is made, or authorisation limits have only marginally been addressed. Signature policies and attribute certificates are likely to improve the present situation (Mitrakas 02). The eWallet work alongside some work on multi-function smart cards is one work item aiming to establish consistent links between identification and authentication and personal and role information required for any associated transactions.

Implementations for eGovernment might take transactions better into perspective when designing on line processes to ensure that the desired function is well served by the signature implementation. The eWallet area is a critical area in need of further development.

5.8. A complex area

Risks and benefits of using a particular technology for electronic signatures might have to be better explained to the end-users who might also need additional training. The widespread adoption of formal quality management techniques (e.g. ISO 9000) by businesses will require them to provide that training to their staff and to ensure that the services that they provide to their clients are fully explained.

Government has been relatively slow to adopt formal quality management methods, and might thus be much less prepared to introduce the citizen and business users to eGovernment process changes. Implementations for eGovernment might require a dedicated action on end-user awareness with regard to the semantics of electronic signing and associated applications.

5.9. Public administration awareness

Understanding the implications of technology and linking them to regulatory requirements has been challenging for most lawmakers for the better part of the past decade. Although significant work has been accomplished at the EU level, there might still be a need to further train administrators and create awareness in using electronic signatures technologies through large-scale projects within public administrations.

5.10. Operation and collaboration

Requirements for eGovernment applications need to recognise that PKI implementations function better when used in public open networks. Alternative technologies do exist that better appeal to the priorities of closed user groups (e.g. Pretty-Good-Privacy). To reap the full benefits of PKI it is important to strive for open interoperable PKI implementations.

Implementations for eGovernment can benefit from being interoperable with non-domestic providers in order to facilitate cross-country interchanges. In this regard provisions for the recognition of non-EU based service providers, are needed to set out requirements according to national accreditation conditions.

Fulfilling Member State law requirements might not necessarily be sufficient for the international recognition of collaborative large-scale eGovernment applications. At a more practical level the often-diverging notion of signatures in an international environment might mean that certain steps be made to enhance convergence. The mutual recognition of accreditation schemes in Europe might further be enhanced by achieving a level of harmonization that also invokes international recognition (ETSI TR 102 040). It is, however, further required to strive for convergence of the legal meaning of signatures at an international level such as that invoked by Article 7(1)(b) of the 1996 UNCITRAL Model Law on Electronic Commerce, which determines the security level an electronic signature must meet as a method "*as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement*". Balancing the requirements between prescriptive approaches in Europe and minimalist ones as most of the times can be found in the US is a challenge still to surmount.

5.11. Industry involvement

When combining smart cards with PKI it is not always clear what practices prevail in each specific area of application like user registration and profiling for example. Such requirements may vary across different industries that still lack proper definition of the terms used, the date to be collected and the processes in support of the deployments.

Greater industry involvement might further become necessary to invoke the prevailing practices in those areas that require the identification and authentication of large distributed communities that make the potential users of smart card based PKIs.

5.12. Market driven standards

The industry has proved to be a valuable resource in setting up standards for electronic signatures. For eGovernment implementations it is important to avoid repetition while making the most out of using public open standards (e.g. EESSI).

5.13. Functional cooperation

While technical interoperability might hinder deployment, the level of usage of technical standards might vary across different application areas. Addressing the specific needs of new transaction areas such as in mobile commerce is also a shortcoming of the present situation in which the interest of service providers is likely to increase.

In eGovernment, technical standards may not necessarily address all aspects that functional areas require; hence, increased interaction with acting organisations in certain areas (e.g. Radicchio) may further be required. Liaisons in this field have already been established between such organisations and selected *e*Europe Trailblazers, and interoperability frameworks have been exchanged between the *e*Europe Steering Committee and Radicchio.

5.14. Ancillary requirements vs. hard coded provisions

Seeking compliance with existing legislation on electronic signatures is a basic requirement for certain types of smart card based PKI projects that target the area of qualified electronic signatures. Seeking legal interoperability and satisfying the legal requirements including privacy still remains a challenge. Additionally it is often the case that consumer protection legislation is further taken into account. To date consumer requirements have only marginally been taken into account although the risks for consumers using a complex technology such as electronic signatures are far greater than the risks businesses face (Kaufman Winn 1998).

5.15. Technology agnosticism

Although legislation in Europe has evolved on the basis of technology neutrality, standardisation takes a firm stance in favour of PKI. Nevertheless, eGovernment applications need to recognise that technology changes might occur in the future and be neutral at the level of design requirements.

5.16. Open models

Large-scale implementation might not be able to remain confined within the isolated barriers of closed implementations. The needs of eGovernment can better be met if an open transaction model and subsequent Trust hierarchies is put in place early enough. Leveraging on the value of PKI requires an open business approach that supports open electronic transactions on public open networks.

A feature of open PKI hierarchies associates with embedding the top root key in specific applications. As commercially available software is by far what is preferred by both consumers and organisations eGovernment application are likely to benefit from associating with roots that are "Trusted" by such commercial grade applications. Implementations of eGovernment might in this regard consider seeking:

- Having their roots embedded through direct inclusion in commercial grade software
- Recognition and subsequent support by an entity whose top root has been embedded in commercial grade software
- Root key storage on smart cards that also allows for easy distribution in the target area.

5.17. Standardisation

Close monitoring of the results of standardisation at national as well as European levels is essential for eGovernment applications, like for example the standards on certificate profile for specific applications. It is also necessary to consider the possibility of synchronising the requirements between physical tokens and digital certificates especially for applications that might require EU wide harmonisation. Public identity might be considered as an example in this area because of the requirements to address issues pertaining in both the physical token and the associated digital certificate. Monitoring and providing feedback to standards' organisations is necessary in order to keep standards in this area focused.

5.18. The technology experience

While technology is the facilitator of the surge in electronic services for eGovernment implementations, it might however, turn to a reason of concern. Certain industry features might impact eGovernment projects on issues like, smart card operating systems, smart card readers, interoperable certificate profiles, policy mapping etc. Certain aspects such as the installation and deployment time and costs for smart card readers might become critical much like drivers and application software that may not feature the required user friendliness needed.

5.19. Risk assessment

Although risk assessment is a background requirement for PKI policy implementations emanating from the prevailing standards (e.g. ETSI TS 101 456), it might be increasingly difficult to put risk assessment into its proper perspective without proper consideration of the transaction model that the signature infrastructure might be used for. The role of risk assessment becomes ever more important considering the typical requirement to provide service insurance for transactions using digital certificates. Pinning down Euro values to digital certificates might just be presumptuous without taking the transaction model into perspective.

For implementations in eGovernment it can be suggested that insurance that is made available within an eGovernment context reflects a pre-determined transaction model to be defined at an early stage of the eGovernment implementation planning.

5.20. Policy and life-cycle management

In eGovernment applications citizen identity management for users of public services emerges as a major challenge. Indispensable stakeholders in this area include the eGovernment initiatives and the service providers alike. The underlying operation of technology for citizen identity management and associated procedures requires high-grade definition to be able to cope with requirements for public services that include transparency, wide, seamless and non-discriminatory accessing, interoperability, accountability, security and simplicity. More specific critical requirements for eGovernment based citizen identity management include:

- Policy based systems to position them with regard to security and application requirements within their operational context.
- Managing the identity lifecycle, because relying on identity information requires the management of, for example, the issuance and revocation of identity elements. An additional difficulty pertains in large distributed implementations as opposed to closed user groups.

Selecting reliable and transparent sources on identity data is essential for the reliability of the implementation and the accuracy of the information supplied. This is an integral part of the Trailblazer 1 and GIF part 2 requirements.

Data protection aspects to counter user concerns with regard to the handling of their personal data and the management of their electronic identities and invoke trust therein. For this purpose eEurope Smart Cards has developed a privacy code of conduct for interoperability of multi application smart cards supporting Authentication.

It is necessary to provide a link to the transaction and transmission platform to enable interoperability of various applications and platforms. Present day concepts for electronic services might soon need to be re-evaluated in the perspective of mobile transactions and contact less smart cards. Hence, providing support for multiple platforms becomes an essential requirement.

Maintaining the confidentiality of certain policies, while ensuring the openness and publicisation of others depending on the scope, is a matter to be resolved in certain cases. While a key management policy must remain highly confidential, certificate policy must be as widely disseminated as possible.

5.21. Products and services

The Trailblazer 2 survey has concluded that large-scale projects may benefit from selecting readily available, off the shelf products and services to the extent they are available rather than going for high risk customised solutions. Implementations for eGovernment will certainly benefit from such an approach.

The combination of hardware such as a smart card, a reader and a software solution has an impact on the deployment phase of the project (e.g. more technical problems to resolve, support skills required etc.).

Any additional services that are not part of the initial implementation (e.g. secure archival, validation, time stamping) must at least be included in the planning.

5.22. Business model

In the interest of transparency and accountability it is necessary to identify the designated business model for the specific smart card based PKI implementation to also support to a certain level return on the investment made. The Trailblazer 2 survey has identified a major shortcoming of present day smart card based PKI projects in this area.

5.23. Project management and planning

Planning of the smart card and certificate management cycles is necessary to take place in conjunction with the overall project management. It is also important to reconcile any differences between the smart card management process cycle and certificate management process.

5.24. End-user considerations

The end user is no expert; hence, any application he may use must work together with the smart card through appropriate software and a smart card reader. The end-user needs a "pre-packaged" and user-friendly solution.

5.25. Data protection and consumers' rights

In spite of the specific referencing of data protection in the directive 99/93/EC, there is some concern associated with the privacy assertions of certain PKI infrastructures. While a general concern on this subject is widely shared the lack of standards or best policies to put formal legal privacy requirements into practice characterises the requirements in this field. The need for awareness in this area has been highlighted in the Trailblazer 2 survey.

5.26. A specific legal framework

A specific legal framework must be properly put in place to support the eGovernment implementations. Matters of liability with regard to issuers, vendors, manufacturers, users etc. also have to be taken into account and put in the perspective of eGovernment usage.

Further harmonisation might also be in the order with regard to application areas such as electronic identity cards, electronic payments, electronic invoicing and digital signatures. The Directive 01/115/EC *On the simplification, modernisation and harmonisation of the conditions laid down for invoicing in respect of VAT* is a valid example in this respect. Taking into account the format of the physical token and electronic certificate this is necessary in order to achieve interoperability in the usage of public identity.

5.27. Risk management

Especially for classes of certificates other than qualified in the meaning of Directive 99/93/EC on electronic signatures, it is necessary to consider aspects of risk and liability associated with the provision of such service. Implementations of eGovernment are required to consider apportionment of liability among the various actors such as the issuing authority, repository, certificate manufacturer, the certification authority, registration authority, application service provider,

smart card vendor etc. Implementations of eGovernment need to seek a risk model where liability is addressed in a way commensurate with the risk incurred.

A risk approach might be a way to treat the liability aspects that lie beyond the limits drawn in Directive 99/93/EC.

5.28. Insurance matters

Insurance models for electronic signatures used to be rare in the early days of commercial PKI. Catching up quickly, insurance industry now provides comprehensive coverage models for PKI risks.

Insurance for digital certificates might not be entirely justified at all times, though. It is necessary to assess insurable risks in the light of specific applications together with insurers and application providers. Although it is a present day practice for many commercial certification service providers to provide insurance on a per certificate basis, this might not suffice for eGovernment transactions. Additionally to certificates, insurance might also be linked to the application it is used for after assessing the risks that the parties involved might run to.

5.29. Certificate Policy

Certificate policies and certification practice statements have been introduced as an essential element in current Trust centric PKI models. This approach favours mostly a high level Trust specific definition. Policy matters, however, have to be additionally addressed from an application perspective through an application centric policy framework.

Policies need to be linked to aspects specific to the transactions and usages of the end users. Additionally, Policies have to be drafted in a manner better apprehended by non-technical audiences and better focused on the end user products and services they are intended for. This requirement is specifically relevant to the rigid structure policy formats such as RFC 2527 that do not necessarily provide a framework understood by non-technical end users. A more product centric approach is therefore recommended (e.g. GlobalSign Certification Practice Statement version 4.1, Sections 11 to 21).

5.30. Assurance of services

Service assurance and accreditation has been early enough part of electronic signatures initiatives. Implementations for eGovernments might lead to useful conclusions with regard to the usage of accreditation services and the relevance thereof in order to achieve specific goals, in transactions for commerce and the administration. The specific application areas in the interest of eGovernment might additionally require that assurance services and accreditation schemes be further extended to meet their requirements.

5.31. Legal amendments

As Directive 99/93/EC enters its review phase, the eGovernment experience might prove to be a valuable resource in order to identify any additional requirements that can only be met through an amendment to the present Directive. Looking closely into aspects of the transposition of the Directive in the member states, and the impact it has made in the Candidate Countries and the

market will lead to valuable conclusions for the future of identification and authentication services.

5.32. Pragmatic approach

It is important to underline that the electronic signature regulation might be due for a moderate update pursuant to the revision term foreseen after mid 2002. Any implementations have to be aware of any changes that might be subsequently adopted in this area and try to maintain a level of flexibility in order to accommodate changes.

6. Way forward

Future activity in this area might focus on addressing the needs of eGovernment implementations, without loosing track of the end-user requirements. In this regard some of the following suggestions could be considered:

6.1. A Code of practice

A Code of practice could be considered with regard to coordinating the requirements for smart card based PKI projects for eGovernment. The experience of the early entrants in this area is likely to be valuable to followers who might benefit from an outline of high-level implementation guidelines. In spite of the practical significance potential users of a Code of practice in the area of Identification and Authentication in eGovernment might recognise the limited binding effect such codes have.

6.2. A project methodology

A project methodology has been recommended in the Trailblazer 2 Pre-Inventory as a requirement to bring smart card based PKI implementations closer to real-life implementation. In this way those to follow can leverage on the experience of the first wave of implementations.

6.3. PKI and smart cards

Looking carefully into the practical aspects of the implementation, planning for eGovernment projects needs to recognise the complexities emerging from combining PKI and smart cards. The Trailblazer 2 survey revealed that the combination of PKI and smart cards, adds yet another layer of complexity in an eGovernment implementation. This requirement can be seen in conjunction with the previous recommendation on a project methodology.

6.4. Legal barriers

National administration rules need to be parsed to ensure consistency with Directive 99/93/EC on electronic signatures. Legal barriers that have been removed as a result of the implementation of the Directive 99/93/EC might still be hidden in rare cases within possibly outdated administrative rules. The specific legal effect of electronic signatures also has to be studied in the specific area of implementation.

6.5. Policy frameworks

Policy has been in the focus of the EESSI standardisation plan through wok conducted by ETSI. Implementations for eGovernment might have additional requirements that have yet to be defined. General commercial applications might not necessarily meet the policy standards for implementations that address the needs of the general public. Hence, policy requirements have to be addressed in a framework specific to eGovernment.

6.6. Accreditation

In an effort to address accreditation requirements eGovernment implementations might further support the customisation of existing accreditation schemes.

Sharpening the focus of present day accreditation schemes for the provision of certification services, will better match the needs of specific application areas in eGovernment.

6.7. Interoperability and cross recognition

Interoperability and cross recognition of eGovernment PKIs is essential in order to make the most of a powerful technology that delivers Trust in opens networks. The IDA (Interchange of Data between Administrations) initiative on a European Bridge CA might yield valuable results in this regard. This recommendation can be seen in relation with the previous recommendation on accreditation schemes for eGovernment.

6.8. Risk models

Developing new risk models for smart card based PKIs including aspects of liability and insurance is critical for the success of eGovernment implementations. The certificate centric insurance model might still have to be reviewed in the light of implementations that focus on the delivery of a service to a distributed user community. Such models need also to take into account the specific requirements of the application areas they intend to service.

6.9. Data protection and consumer rights

Highlighting data protection and consumer protection aspects comes as a pressing need of services offered to the general public. It has been indicated in the Trailblazer 2 Pre-Inventory that pilot phase projects could claim limited understanding only of the requirements of these two areas, a situation worth every attention.

6.10. Additional regulation?

If necessary, additional regulation could be considered as a result of the review phase of Directive 99/93/EC. In this regard the eGovernment experience might prove to be a valuable resource of input to enhance the legally recognised certification services in Europe.

Annex I

Deliverables that have been approved within the EESSI programme include the following:

ETSI standards

- Time Stamping Profile - TS 101 861 v 1.1.1 (September 2001)
- Qualified Certificate Profile - TS 101 862 v 1.2.1 (June 2001)
- Policy requirement for certification authorities issuing qualified certificates TS 101 456 v 1.1.1 (December 2000)
- Qualified Certificate Profile - TS 101 862 v 1.1.1 (December 2000)
- Electronic Signature Formats - TS 101 733 v 1.2.2 (December 2000)
- Electronic Signature Formats - ETSI ES 201 733 v 1.1.3 (May 2000)
- XML format for signature policies - TR 102 038 (April 2002)
- Policy requirements for time-stamping authorities - TS 102 023 (April 2002)
- Policy requirements for certification authorities issuing public key certificates - TS 102 042 (April 2002)
- Policy requirements for certification authorities issuing qualified certificates - TS 101 456 v 1.2.1 (April 2002)
- Provision of harmonized Trust Service Provider status information - TR 102 030 (April 2002)
- Frequently Asked Questions (March 2002)
- International Harmonization of Policy Requirements for CAs issuing Certificates - TR 102 040 (March 2002)
- Time stamping profile - TS 101 861 v1.2.1 (March 2002)
- Signature Policies Report - TR 102 041 (February 2002)
- XML Advanced Electronic Signatures (XAdES) - TS 101 903 (February 2002)
- Electronic Signature Formats - TS 101 733 v 1.3.1 (February 2002)

CEN/ISSS standards

- CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)
- CWA 14168 Secure Signature-Creation Devices, version 'EAL 4'
- CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+
- CWA 14170 Security Requirements for Signature Creation Systems
- CWA 14171 Procedures for Signature Verification
- CWA 14172 EESSI Conformity Assessment Guidance - Parts:1-5
- CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices
- CWA 14365 Guide on the Use of Electronic Signatures

References

B.P. Aalberts & S. van der Hof, *Digital Signature Blindness, Analysis of legislative approaches toward electronic authentatio*n, November 1999, http://cwis.kub.nl/~frw/people/hof/ds-fr.htm.

T. Arcarese, *Status of e-ID cards in Europe, European Commission, DG Information Society*, Draft version December 2001.

L. Blivet, A. Mitrakas, M. Moyal, *Pre-Inventory of Smart Card based PKI projects in the European Union*, eE SC, 2001.

EESSI, *First Set of Deliverables*, http://www.ict.etsi.fr/eessi/ddd.doc

Policy requirements for certification authorities issuing qualified certificates, ETSI TS 101 456, 2001.

J. Eymeri, *The electronic identification of citizens and organisations in the European Union: State of Affairs*, 37th Meeting of the Directors-General of the Public Service of the Member States of the European Union, 26-27 November 2001, Bruges.

GlobalSign, *Certification Practice Statement,* version 4.1, 1 April 2002.

J. Kaufman Winn, *Couriers without luggage: Negotiable instruments and digital signatures*, 1998, http://faculty.smu.edu/jwinn/ecouriers.html

C. Kuner, A. Miedbrodt, Written Signature Requirements and Electronic Authentication: A Comparative Perspective OECD workshop on electronic commerce, 1999.

C. Megglé, J. Ajdenbaum, N. Lipszyc, Y. Le Roux, *Network Authentication Module for internet End-users – Electronic Signature*, Version: 2.1, 1 October 2002

A. Mitrakas, *It's all in the cards: Large-scale smart card based PKI deployments in Europe*, ISSE 2002, Conference proceedings, Paris, 2-4 October 2002.

A. Mitrakas, *Citizen Centric Identity Management: Chip Tricks?*, Network Security, MCC International, July 2002.

A. Mitrakas, *PKI based signing ceremonies: The case of signature policies*, Information Security Bulletin, March 2002.

H. Nilsson, M. Pohjolainen, *Requirements for European Public EID-card's Issuers, Supporting PKI and Certificate contents*, eEurope Smart Card Charter Trailblazer 1, January 2002.

Trailblazer 10, *Survey of Secure Smart Card based e-Government Applications*, eEurope, Smart Cards, 2002.

UNCTAD, *E-Commerce and Development Report 2001*, United Nations 2001.