Designing the Provision of Public Key Infrastructure Services for eGovernment

Stefanos Gritzalis[1], Petros Belsis[1,2], Maria Karyda[1], Mike Chalaris[2],
Christos Skourlas[2], Ioannis Chalaris[2]

***Abstract*--The European Union has launched a comprehensive strategy framework and emerging actions on security and privacy issues. To this direction, a number of relevant initiatives have been put on (e.g. cyber security task force, awareness campaigns, promotion of good practices, improved exchange of information mechanisms, etc.). Their results will provide the basis for the work towards a secure information infrastructure. The key actions proposed for a secure information infrastructure, under the eEurope-2005 umbrella, include, between others, "Secure Communication between Public Services", e.g. examination of the possibilities to establish a secure communications environment for the exchange of government information. An important aspect towards this direction is the deployment of a Public Key Infrastructure (PKI). In this paper a good-practice guidance is described, on how a secure and efficient PKI can be developed to support secure and efficient Government-to-Government and Government-to-Citizen electronic communication**

***Index terms*— e-Government, Security, PKI**

I. INTRODUCTION

Establishing e-Government infrastructures heavily relies on the deployment of Public Key Infrastructures (PKI). However, the use of PKI by itself is not adequate. There is a necessity for the concurrent establishment of legislative framework. From a technical point of view, the creation of a PKI capable of supporting efficiently and securely the communication needs of e-government poses many challenges. Such a PKI should be capable of handling a heavy daily workload of transactions ranging in urgency as well as in the level of security requirements; of incorporating within its scope an increasing number of government agencies; and of supporting multiple entities wishing to provide certification services. In other words, such a PKI should be carefully designed in order to achieve flexibility, scalability and interoperability. In this paper we argue about the basic prerequisites for the establishment of both a secure and flexible PKI infrastructure, adoptable by citizens due to its accredited capability – based on the adoption of International standards - to provide reliable services, as well as the ability to eliminate the risk of transactions by incorporating secure communication channels. Furthermore, we discuss legislative issues that rule the provision of services, applications and communications. EU Member States and especially the public sector, should be prepared about the range of use and the capabilities of PKI services, as well as they should enforce the deployment of secure e-government services to citizens and provide secure and interoperable electronic communications between public services

The rest of the paper is organized as follows: after a brief introduction in Section I, Section II discusses the main issues that direct our architectural design, Section III addresses implementation choices, Section IV discusses regulatory issues, while Section V concludes the paper.

II. ARCHITECTURAL DESIGN

The creation and support of a PKI based infrastructure underlies a number of key issues, concerning operational design choices, capable of providing a secure and efficient Government-To-Government (G2G) and Government-To-Citizen (G2C) electronic communication. In fact, most of the ideas described here apply equally well to the design of PKI for use within any fairly sized organization that uses distributed, heterogeneous information systems across a number of domains.

Among the basic requirements for a PKI operating for the public sector should be the ability to handle a heavy daily workload of transactions ranging in urgency. Additively, security should be a main concern as well as its scalability potential. In other words, a PKI built for use in the public sector should be carefully designed in order to achieve the following, at a minimum:

- ***Flexibility***. Special measures should be taken in order to handle problems arising from the heterogeneity that characterizes the public sector. Therefore, both lower and higher levels of the infrastructure should be designed to be able to confront with these obstacles. For example on lower level, the hardware and software (smart cards,

[1] Laboratory of Information and Communication Systems Security (*Info-Sec-Lab*), Department of Information and Communication Systems Engineering, University of the Aegean, Samos, GR-83200, Greece
(sgritz, pbelsis, mka)@aegean.gr

[2] Department of Informatics, Technological Educational Institute (T.E.I.) of Athens, Egaleo, GR-12210, Greece
(mikehlr, cskourlas, ixalaris@teiath.gr)

operating systems etc) should be able to interoperate and to adhere to international standards. On higher level, specific attention should be paid on designing efficient organizational structures as well as security models to support secure interoperation between different organizations.

- ***Scalability***. The adoption and support of more and more e-government services, as well as the citizen's continuous participation raise continuously the demands for introduction of more and secure services. The regulatory framework according to EC Directive 99/93, poses no limit to their number. A PKI should be able to accommodate these increased demands for services.
- ***Interoperability***. The cornerstone of an expandable and functional PKI infrastructure is the possibility to be able to interoperate among the different ministries and agencies. The compliance of the infrastructures with international standards is the only choice towards this direction.

A basic question refers to the possibility of outsourcing several parts of the PKI infrastructure. Relative to it, we could notice the following: First the possibility of outsourcing the activities of a Certification Service Provider (CSP) eliminates the risk of failure. Second, in addition to the usual requirements a CSP should be able to meet in order to provide services to the general public, it is necessary to be able to verify the validity of the signatures essentially for indefinite time, even after the revocation or expiration of the corresponding certificate and even after the signer has retired or his/her certificate is revoked, for whatever reason. The key is in archiving the validation chain, i.e. to store the certificate of the signatory along with a proof of its validity at the time of signing. This, in turn, requires that signing a document is immediately followed by a signature verification procedure and an archiving action of (a) the signed document, (b) the signatory's certificate, and (c) proof of validation of the certificate. This key creation and maintenance scheme has been adopted by EU directives and has been embedded in the national legislation of almost all European Union countries [3].

A number of issues related to the presented design challenges are directed by EU directives. Such issues include:

- Establishment of trust between participating parties
- Required legal status of a CSP providing services to the public sector.
- Certification hierarchy levels and cross-certification capabilities, which are necessary for proper operation within the public sector.
- Types of certificates most appropriate for civil servants.

Directions to be followed may refer to the following (good) practices:

A. Voluntary accreditation scheme

This issue refers to whether it should be obligatory for a CSP to undergo an accreditation process before providing services on behalf of the public sector. The fact that this is not explicitly directed by EU legislation, has led to different approaches from the member states.

Relative to what the best practice is we could notice that differentiation between the provision of qualified and unqualified certificates is recommended. Qualified certificates issuing is equivalent to compliance with Annex I of Directive 99/93. Thus, the establishment of an evaluation framework supervised by a superior authority is essential in order to verify that the CSP will issue certificates of the expected strength and quality required by qualified certificates.

If the CSP is not willing to issue qualified certificates, then the accreditation should not be obligatory, but it should only be stated in the CSP's Certification Practice Statement (CPS) that the certificates it provides are unqualified.

In general, it is a good practice for the public sector to prefer CSP that have elected to undergo the voluntary accreditation process.

B. Certificate types

An integral part of the PKI that acts as an entity's identity in everyday transactions with or within the government is a digital certificate.

In accordance to the Directive, qualified and unqualified certificates are both recommended with the annotation "advanced" in cases where the certificates are signed by an accredited CSP, regardless of whether the CSP is private or public. However, civil servants should preferably use only qualified certificates (as dictated by Annexes I-IV of Directive 99/93) for their communication needs.

As a useful option we could consider to distinguish certificates into classes depending on the *effort* expended into ascertaining that the individual is the one she claims to be as well as the *level* of provided security. A first classification could be based on the following: Class 1 certificates (where a simple check is required to verify uniqueness of the civil servant's data within the CSP domain), Class2 (the identity of the civil servant is verified against data held by his/her department), and Class3 certificates (the identity is verified through the physical presence of the civil servant before a registration representative) [5]. Another possible classification could be into Low class (e.g. support of digital signatures for classified information on encrypted networks), Medium Class (e.g. digital signatures for unclassified mission critical and national security information on encrypted networks), and High Class (e.g. digital signatures for authentication of subscriber identity for accessing classified information over unprotected networks) certificates [6].

III. IMPLEMENTATION CHOICES

Due to the high sensitivity of the data and to the necessity of assuring the correct implementation of an e-Government

PKI based infrastructure, it is of primary concern to verify the robustness of the implemented architecture. A number of issues that handle with both higher and lower level details should be taken under consideration for these reason. Such issues include the determination of a supervisor body that provides control and audit over the CSP's, the determination of physical devices that create and store the digital certificates efficiently, the determination of procedures for key-pair creation.

A. *Supervisory body*

A supervisory body will be responsible fro verifying that the potential CSP complies with a number of regulations before it receives permission to operate. In cases of audit, it will be verified that the CSP follows a number of predefined standards.

Among the main duties of the supervising body we can distinguish:

- The obligation to perform annual auditing over accredited CSP's that provide services to the public sector. This audit may be performed by the supervising authority itself or it can be outsourced to contractors.
- Provisions of a publicly available auditing frame-work, explaining in detail all procedures relevant to CSP monitoring and auditing.

Finally, there should be mandatory provision under law that before the government signs a contract with a CSP, the CSP should be evaluated by the supervisory body for conformance to predefined quality standards.

B. *Secure devices*

Magnetic media are not suitable for keeping sensitive data, therefore are not suitable for storing private keys. Private keys used within the public sector should be kept in smart cards and other, similar tokens, compliant with Annex III of Directive 99/93. Their reliability and tamper-resistance is much higher comparing to magnetic media such as diskettes. The use of smart cards is suggested for storing the users' private key, as well as the use of the ITU X.509 v.3 standard for the format of certificates.

As far as the signature creation system is concerned, this can be any one of the following, as long as it complies with the provisions of Annex III of Directive 99/93: (a) a personal computer with the appropriate software, provided by the CSP, (b) a Personal Digital Assistant with appropriate software, provided by the CSP, (c) the smart card itself, and (d) a hardware appliance running a signature creation application.

Regardless of the type of the signature creation mechanism, the evaluation of signature creation devices should be carried out using the *Common Criteria Security Evaluation* framework [1, 2] for IT security evaluation (CC Version 2.1 or ISO/IEC 15408 Parts 1-3). Evaluation using this framework is mandatory under a decision reached by the Electronic Signature Committee, as stated in Article 9 of the EU Directive 99/93, on July 2002.

C. *Key pair generation*

In order to generate and distribute key pairs in a secure manner, a possible solution could depend upon their storage within a Secure Signature Creation Device (SSCD) device and hand this device over to the RA, which should then hand it over to the requesting civil servant. The private key should never leave the smart card, in any form, and the CSP should be obliged under law not to extract and store such keys in their premises.

This practice contributes, also, to the increase of the cryptanalysis lifetime of the private key, since this key cannot be extracted from the smart card and stored elsewhere. Private key disclosure is not easy to detect but the provision that the private key is generated and stored *in* the smart card decreases significantly the likelihood of such an event.

Relative to the provision of an efficient cross certification scheme between CSP's, a solution could rely upon the development of a simple hierarchical architecture [1] with a single Certification Authority (CA) and multiple Registration Authorities (RA) per sector, whereby a sector is meant as an integrated organizational entity. This does not mean that all CAs should be supported by a single CSP. Where multiple CAs are already operating these can also operate as a root CA in the subordinate certification architecture. In this architecture, all CAs operating below the bridge certification authority possess a self-signed certificate.

For countries that have not yet developed a PKI, the development of *a simple hierarchical architecture with a single CA and multiple* RA per sector could be recommended, whereby a sector is meant as a ministry or as a government agency, as dictated by the government structure. This does not mean that all CA should be supported by a single CSP. On the contrary, it is desirable to have many CSP operating these CA.

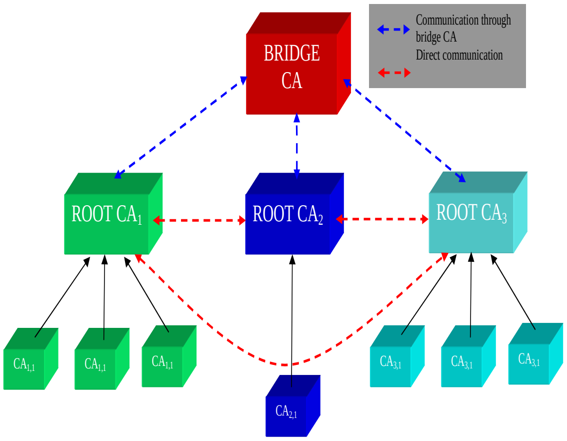

Figure 1: Connecting different CA hierarchies

For countries where multiple CA are already operating in the public sector, every such CA can also operate as a root

CA in the subordinate certification architecture, as shown in Figure 1. In this architecture, all CA's operating below the bridge certification authority possess a self-signed certificate that is generated according to the procedures and provisions laid down in the national legislation as well as in the EU Directive 99/93. It is important that the private key of each root CA is guarded against disclosure; this should be verified by the supervisory body of each country.

Relative to establishing communication channels CA's we could consider the following two alternative solutions: (a) communicate directly, and alternatively (b) through the Bridge Certification Authority (BCA) [7]. For (a), all CSP operating in the public sector should accept and support cross-certification. This is not only for convenience but, also, for ensuring interoperability between CSP. To support (b) it is necessary to have a BCA providing online services with high availability and to adopt specific communication protocols, such as OCSP.

However, cross-certification within an international "virtual" PKI [8] interconnecting many different CSP and operating in different countries, is not a simple task. There are many issues that should be resolved, including:

- Achieving interoperability between CSP.
- Willingness of involved CSP as well as of users subscribed to specific CSP to offer trust certification services offered by other CSP.
- Willingness and effort of involved CSP to comply with complex CPS, or imposed by the need to participate and support cross verification in complex trust architectures.

Usually every CA operating under different CSP either does not adopt the same certification technologies or do not adopt the same certification practices. Interoperability enforcement may be difficult to achieve between many cooperating CA's. This is when a BCA can be useful (Figure 1). One may view this scheme as a form of cross-certification that places the burden for supporting mutual trust and interoperability of technologies and processes to a single entity, as all other CA cross-certify with the bridge certification authority. However, there are still more aspects to consider, as this scheme introduces a single-point-of-failure; thus entities such as back-up BCA and means for the fast transition to these should be studied in detail before such a trust architecture can be supported.

IV. LEGISLATIVE ISSUES

The establishment of a PKI e-Government framework, except from the technical dimension, mainly raises a number of questions of legislative nature. Such issues may refer to the time expiration of certificates, the formulation of Certification Practice Statement (CPS) etc. [4]

A. Determining the Certificate lifetime

Determining a secure certificate lifetime is related to the lifetime of the private key used in the certificate. This is largely determined by two factors; Cryptographic lifetime, that is, loosely, the average time required to determine the private key from the public key, given the specific signature scheme and Disclosure lifetime, which is the average time that passes before a user's private key is disclosed [2].

B. Certification Practice Statement (CPS)

The creation and continuous availability both in printed and electronic form is necessary so as to enable the citizen to ensure the continuous compliance of the CA with international standards.

The CPS should address, among others issues, the following important ones:

- Statement on whether the CSP is accredited or not and, if accredited, when the accreditation took place and by whom.
- List of CSPs already operating with which there is mutual trust.
- Description of the certificate contents and extensions.
- Description of certificate types offered.
- Statement of estimates of private key robustness as well as a reference to the models that lead to these estimates.
- Statement of practices towards the support of cross-certification.
- CA's obligations.
- Cooperation protocols with the RA.
- Subscriber obligations.
- Relying party's obligations.
- Statement of Insurance against damages caused by the CSP.
- Offer of value added services (e.g. time-stamping, notarization, encryption of information, certificate repository).

C. Revoked certificates handling

It is within the CSP's obligations to create a new certificate for a civil servant prior to its expiration. The renewal procedure as well as the time prior to the servant's key expiration that triggers the creation of a new key is a matter of internal agreement between the state and the CSP. Relative to the revocation of certificates and the policy that government agencies should follow upon the occurrence of a misconduct or misuse incident involving a certificate, the following should apply:

- It is within the civil servants obligation to notify that they suspect for potential misuse of their certificate
- Agencies should notify CSP's when such a notice is made by a civil servant.
- Last, the CSP should handle all the necessary procedures for revocation of the certificate of all directories containing valid entries and notify all the interested parties about the certificate's invalidity.

There is also necessity for the establishment of a mechanism between government agencies when a certificate holder resigns, retires, or in general there is any role re-assignment between the holder and the assigned certificate's attributes.

D. *Cease of CSP's operation*

Before a CSP starts providing certification services to the public sector, it should comply with a minimum set of compatibility/CSP-interoperability standards. If all CSP comply with these standards then it will be easier for a CSP to undertake resigning CSP's duties.

This is, also, another argument in favor of having more than one CSP providing certification services to the state. Indeed, if there is only one such CSP and it resigns, it will be difficult for the government to appoint another CSP, as there should be a public call, sufficient time to evaluate the applications, assurance that the new CSP conforms with standards etc.

V. CONCLUSIONS

In this paper, we deal with a number of technical, regulatory and legislative challenges relative to the provision of secure and reliable e-government PKI based infrastructures. We discussed key issues that direct our architectural design, in order to perform adequately from a technical point of view, as well as to conform with the established EU regulatory principles. We provide directions for a resilient and robust implementation of a PKI based eGovernment framework. We also discuss the formulation of good practice guidelines and relative to the provision of superior quality services.

VI. REFERENCES

[1]. J. J. Marchesini, S. Smith. Virtual hierarchies – An Architecture for Building and Maintaining Efficient and Resilient Trust Chains. *NORDSEC 2002*

[2]. R.D. Silverman. A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths *RSA Laboratories Bulletin*, No. 13, April 2002 (revised November 2001).

[3]. Department of Trade and Industry (DTI) of United Kingdom, Consultation on Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signature – answers to questionnaires www.dti.gov.uk/cii/datasecurity/electronicsignatures/signatures2.shtml

[4]. W. Ford. Straw-man certificate policy definitions: mid-level policies for digital signature and encryption. 1997 European Telecommunications Standards Institute (ETSI). *Electronic Signature Formats*. ETSI TS 101 733 v.1.3.1 (2002-02).

[5] The Netherlands Land Registry and Registry of Deeds. *Delivering Property Registration Services in the e-Government* era (Future electronic registration of deeds in the Netherlands http://www.gov.ie/landreg/netherlands presentation.htm

[6]. V.-V. Patriciu and A. Serb. Deploying a Certification Authority for Networks Security. *2nd International Conference on Security and Protection of Information*, 2003, www.vabo.cz/spi/ostatni/3day/01patric.ppt

[7]. S. van Den Eyden. Trusted Archival Services: Safety on the Internet. In *J. Du Mortier, F. Robben, M. Tayemans (Eds.), A decade of research at the crossroads of Law and ICT*, pp. 343-363, Brussels, Larcier, 2001.

[8]. J. Marchesini, S. Smith. Virtual hierarchies – An Architecture for Building and Maintaining Efficient and Resilient Trust Chains. *NORDSEC 2002*, 2002, www.dartmouth.edu/~pkilab/slides/NORDSEC6Nov02.pdf