Chapter 6

Good Practices

Greek Presidency of the European Union
1. Introduction

This chapter aims at developing good-practice guidance on how a secure and efficient PKI can be designed and built for supporting secure and efficient G2G and G2C electronic communication.

Specifically, the aim of this chapter is the following:

✓ To record the framework for the exploitation of e-signatures in establishing secure e-government services within member states.

✓ To review certificate management practices and procedures in the public sector.

✓ To make recommendations that take into account the current situation in member states and constitute good practice.
2. Towards an efficient PKI in the Public Sector

I. Challenges of PKI design

Creating a PKI capable of supporting efficiently and securely the communication needs of the public sector poses many challenges. A PKI operating in the public sector 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, a PKI built for use in the public sector should be carefully designed in order to achieve the following, at a minimum:

✓ **Flexibility.** Due to the multifaceted nature of the public sector, as well as the entities that provide services within its domain, PKIs are inevitably destined to operate in heterogeneous environments. Thus, a basic provision of every PKI design should be to ensure that the components chosen to implement the PKI (e.g. smart cards, software and hardware systems, certificate directory organization and operation etc.) are able to communicate with each other, by virtue of incorporated interoperability features and of adherence to internationally accepted standards.

✓ **Scalability.** This issue is related to the expansion of the public sector in order to provide more services and in many places. As e-government services receive wider acceptance by citizens, there will be a necessity to introduce more services with increased security requirements. Moreover, entities providing certification services to governments will accordingly increase and, as directed in the EC Directive 99/93, no limit to their number can be assumed. A PKI should be able to accommodate these increased demands for services.

✓ **Interoperability.** A PKI for the public sector should adopt appropriate standards (e.g. for certificate formats, public directory maintenance, revocation list handling, etc.). This will increase the PKI’s interoperability and robustness.
II.

The discussion herein addresses the design challenges stated above and follows the EU Directive 99/93 article by article (when possible). The focus is on the main or most controversial issues regarding the introduction and use of PKIs in the public sector.

These issues are the following:

- Trust architecture and technologies needed in a PKI environment within the public sector.
- Interoperability.
- Required legal status of a Certification Service Provider (CSP) providing services to the public sector.
- Certification hierarchy levels and cross-certification capabilities that are necessary for proper operation within the public sector.
- Types of certificates most appropriate for civil servants.
- Certificate revocation and expiration policy.
- Operation and placement within the public sector of Registration Authorities (RA) and their relation with the Certification Authority (CA).

In the sequel, a number of recommendations that address the above issues will be presented, according to the following structure:

- Reference to EU Directive 99/93 article. This is simply the article number and name as stated in the EU Directive.
- Reference to EU Directive 99/93 item within the article in hand. This is a title that reflects the content of a paragraph, within the article stated above in the EU Directive 99/93 that addresses a specific issue.
- An explanation of each item discussed and its importance within a PKI
- A review of the situation in member states as recorded in the responses to the questionnaires as well as in the available governmental documentation of each country.
- Recommendations for good practice concerning the issue referred to by the article item.
###Directive 99/93 Voluntary accreditation scheme

####III.

####III.1

This issue pertains to whether a potential Certification Service Provider (CSP) should be obliged to undergo a special accreditation procedure established by the government before it is allowed to provide services in the public sector or whether this accreditation procedure should be voluntary and undertaken only at the CSP’s discretion.

The EU Directive 99/93 leaves open the issue of whether a potential CSP should undergo a compulsory accreditation process in order to be authorized to provide certification services. Thus, it was observed that different approaches among member states exist, as evidenced by the responses to the questionnaires. Moreover, some countries relate the issue of accreditation to the intention of the CSP to provide qualified or unqualified certificates as defined in Annex I of the Directive 99/93. Some other countries treat these two types of certificates identically as far as accreditation is concerned. Thus, for instance, Austria allows voluntary accreditation for CSPs regardless of whether they provide qualified or unqualified certificates and so do Germany, Greece, The Netherlands, Sweden, Spain, and Luxembourg. The UK, on the other hand, allows voluntary accreditation only for CSPs issuing unqualified certificates and so do Finland and Belgium. Additionally, Denmark, Finland and the UK mandate for compulsory accreditation for CSPs issuing qualified certificates. Finally, Italy follows a scheme requiring compulsory accreditation for issuing unqualified certificates and voluntary accreditation for qualified certificates.

Differentiation between the provision of qualified and unqualified certificates is recommended. Issuing qualified certificates means that the certificates should comply with certain requirements stated in Annex I of Directive 99/93. Thus, there should be an evaluation framework established by the supervisory body for ascertaining that the CSP will issue certificates of the expected strength and quality required by qualified certificates.

Should the CSP intend to only issue unqualified certificates of any type, it should not be obliged to undergo a formal accreditation process. Its obligation is restricted to stating specifically in the Certification Policy Statement (CPS) that the certificates it provides are unqualified.

In general, it is a good practice for the public sector to prefer CSPs that have elected to undergo the voluntary accreditation process.
III.2

A digital certificate is an integral part of the PKI that acts as an entity’s identity in everyday transactions with or within the government. A description of digital certificates was given in Chapter 2. It is important to decide whether some keyless certificates (called attribute certificates) are also needed. Examples of such certificates are role and permission certificates that define the duties of the certificate bearer. The use of such certificates is not recommended for the near future; in any case, such certificates should, be used always in conjunction with the identity certificate of the individual. In the case of attribute certificates, the privileges corresponding to the physical entity are included within the certificate, while with role-based certificates the privileges are concluded on the basis of the role of the entity rather than on the basis of its identity. In both cases an extra administrative overhead is added to the CSP, since frequent certificate renewals are needed every time an entity changes role or privileges. On the other hand, identity-based certificates place the overhead of privilege definition on the applications.

All member states recognize at least two types of certificates: qualified and unqualified as described in Annex I of Directive 99/93. There is also another type of certificate in use, called advanced certificate. This type of certificate, adopted by Germany, is defined as a qualified certificate that can be traced back to a national Root Certification Authority. Some other countries also classify certificates into three separate classes depending on the security strength of the certificate as well as the security of the device bearing the user’s keys (e.g. Spain’s Class 1, Class 1S and Class 2CA). On the other hand, Belgium classifies certificates according to their intended use: signature (qualified certificate for non-repudiation), authentication (SSL/MIME authentication certificate) and encryption (SSL/MIME encryption certificate).

In view of the Directive, the use of both qualified and unqualified certificates is 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.

Finally, it is useful to consider a further distinction of certificates into classes depending on the effort expended into ascertaining that the individual is the one he/she claims to be as well as the level of provided security.
Using the former criterion, one may classify certificates into Class 1 (only a simple check is done for uniqueness of the civil servant’s data within the CSP domain), Class 2 (the identity of the civil servant is verified against data held by his/her department), and Class 3 certificates (the identity is verified through the physical presence of the civil servant before a registration representative) ([13, 22]). Using the latter criterion, a 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.3

This aspect pertains to the establishment of a special supervisory body whose aim will be to ascertain that potential CSPs comply with a number of regulations and requirements before they are allowed to operate, or (in cases of voluntary accreditation) to periodically audit already operating CSPs in order to verify that their mode of operation follows a set of predefined standards.

This was one of the aspects on which there was unanimous agreement among member states, at least as far as the necessity of having such a supervisory body is concerned. Some differences exist only with respect to the organization of such a body.

In The Netherlands, for instance, there is a special governmental agency called Policy Authority (currently operating in pilot stage) that is responsible for setting CSP operation requirements as well as checking their compliance with them. Also in The Netherlands, there is a separate accreditation body (TTPNL) that is responsible for handling accreditation applications. TTPNL closely co-operates with the Policy Authority. In Sweden there are two supervisory bodies (National Tax board and Swedish Agency for Public Management) that are responsible for the control, coordination, and identification of common practices for CSPs, (e.g. Certificate Practice Statement), a supervisory authority responsible for regulating, monitoring and auditing the operation of CSPs issuing qualified certificates (the Swedish National Post and Telecom Agency) as well as a separate accreditation body (SWEDAC) that is responsible for handling accreditation applications. On the other hand, other countries (e.g. Belgium, Greece, Germany, Finland, Luxembourg, Italy, Portugal) have a single body that not only supervises the operation of CSPs, but handles their accreditation as well.
A variation of such a scheme is followed by Austria, where there is a single body, called RTR, handling both the accreditation applications and the supervision of the operation of CSP but, as far as the latter duty is concerned, it receives consultation from the Secure Information Technology Centre - Austria (A-Sit).

Regarding possible recommendations, all member states should preferably continue, or establish the operation of a single (if possible, for simplicity and efficiency) supervisory body, assembled and operating within the public sector, with the possibility of outsourcing specific activities to the private sector, if technological expertise is missing or scarce. It seems a good idea to keep this supervisory body distinct in nature, as well as in duties, from the Accreditation Body, which is responsible for handling the accreditation of CSPs for reasons of efficiency as well as of separation of duties. There should be a close cooperation between them, as the accreditation body should apply guidelines and assess accreditation applications according to the policy and technological standards set by the supervisory body. As far as the legal and organizational status of the supervisory body are concerned, these may vary according to each country’s specific needs.

The following should be among the duties of this body:

- Annual audit of accredited CSPs that provide services to the public sector. This audit may be performed either by members of the supervision body or by subcontracted external experts.

- In order to facilitate the above, a publicly available auditing framework should be developed, which should be adopted by all CSPs after public consultation. This framework should explain 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.
### Secure signature creation devices (SSCD)

#### III.4

This issue pertains to the nature of the devices used for creating and storing the users’ private keys.

Regarding the generation/storage of users’ private key, there is also an agreement among all member states: all propose the use of smart cards conforming to specific standards, mainly the minimum requirements listed in Annex III of Directive 99/93 (e.g. Belgium has SSCD type 1, 2 and 3 EAL5+ accredited smart cards, while Germany has smart cards evaluated to ITSEC E4/high). Some countries allow other alternative devices: in Denmark the signature creation is done on a PC client where the signature creation data are also kept (the system is software based). France allows a combination of smart cards and software. In the UK, on the other hand, there is no central policy on this issue and each government agency may decide on its own. Finally, Austria, Luxemburg and Ireland did not respond to the corresponding question.

Hardware tokens (e.g. smart cards, complying with Annex III of Directive 99/93) should be used within the public sector for storing private keys. Hardware tokens are more reliable and tamper-resistant storage media compared 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: (i) a personal computer with the appropriate software, provided by the CSP, (ii) a Personal Digital Assistant with appropriate software, provided by the CSP, (iii) the smart card itself, and (iv) 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 [II] 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.
<table>
<thead>
<tr>
<th>Key pair generation</th>
<th>III.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the scene</td>
<td>A major issue with regard to certificates is the generator of the various key pairs (private, public) used in the community of a PKI in the public sector. An additional issue is what methods or devices will be used to this end.</td>
</tr>
<tr>
<td>Current situation</td>
<td>Most of the countries that use certificates provided by CSPs let this issue be resolved by the CSPs themselves and only check for compliance of the key generation process with certain international standards. In some countries it is desired that users should not be allowed to specify their own keys. However, it is required that the keys for non-repudiation purposes are created under the full control of the subscriber. The fact that CSP provide the means (hardware and software) to generate the key-pair for every civil servant may not leave the suspicion to the users that their private keys may be in danger to be illegally used. CSPs should take extreme care in order to ensure that stealing key pairs and impersonating a legal user is not possible.</td>
</tr>
<tr>
<td>Good practice</td>
<td>An adequately secure solution for the generation of the key pairs is to generate them within a SSCD device and hand this device over to the Registration Authority, 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 CSPs 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.</td>
</tr>
</tbody>
</table>
### III.6

This issue pertains to special requirements that should be fulfilled by a CSP wishing to provide certification services to the public sector. Although the Directive 99/93 covers most aspects of appropriateness of a CSP, it is rather generic at certain points and leaves several issues open for further consideration.

Member states seem to place considerable importance to additional requirements that a CSP should fulfill before it can cooperate with the state. Most of them are not included in the Directive 99/93 and stem from the high quality demands of e-government. Thus, Austria and France do not require that a CSP undergoes a formal risk analysis and assessment of its assets. Austria and France do not require that a CSP take measures for the physical security of its assets and premises. Austria and France do not require that the device used for generating the keys complies with stringent security standards. Austria, Denmark, Finland, France, Germany, Luxemburg, and The Netherlands do not require ISO 9000 certification of the CSP. Austria and France do not require compliance of the CSP with laws regarding personal information. They also do not require that the CSP staff meet high expertise standards. Moreover, Austria allows only the use of qualified certificates as described in Annex II of Directive 99/93, Belgium requires the CSP to use the national registration number for e-government purposes, i.e. the CSP should use this (unique per civil servant) number as part of the credentials necessary for verifying an applicant’s identity. Germany requires that it is possible to verify a signature up to 35 years after its placement in an electronic document, as it is necessary to preserve signed documents for as long a time interval as possible. Italy requires that a CSP is insured so that it can compensate the state in case of damages. The Netherlands requires that the Certificate Revocation Lists (CRL) be updated every four hours and Spain requires compliance with special security requirements.

It is necessary for the public sector to be able to verify the validity of the signatures of electronic documents even after the civil servant has retired or his/her certificate is revoked for any reason. Therefore, long and secure storage of all certificates that have ever been created and assigned to a civil servant should be ensured, along with an indication of the period for which they were valid.

An additional technical requirement of a CSP offering services to the public sector is that the certificate of each root Certification Authority (which is self-signed) should be signed using a private key long enough to ensure its maximum possible lifetime, its practical usability notwithstanding. This is because when the private key of a Certification Authority is compromised, the whole certification hierarchy collapses and no certificate can be considered valid.
It is also important to minimize the usage and consequently the exposure of the Root CA private key and therefore it is desirable that the Root CA signs only certificates of subordinate CAs rather than the certificates of the end-entities.

Moreover, it is recommended that the CSP complies, as a minimum, with the following:

- Perform a formal risk analysis assessment of its assets using a well-established formal or semi-formal risk assessment framework, using widely accepted pertinent methodologies and tools (see [6, 21]).
- Provide guarantee for preserving certificates in a form that enables them to be verified for an indefinite period of time.
- Provide a publicly available Certification Practice Statement for approval by the supervision body.
- Be insured, to be able to compensate the state for damages inflicted either to citizens or to civil servants from both malpractice of the CSP itself and from external malicious intervention.
- Maintain log information and undergo a regular auditing process carried out by the supervisory body.
- Update Certificate Status Information (CSI) on predefined time limits (e.g. frequent update of Certificate Revocation Lists (CRL))
- Obtain an ISO 9000 certification.
<table>
<thead>
<tr>
<th><strong>Trust architecture</strong></th>
<th><strong>III.7</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setting the scene</strong></td>
<td>An important issue that should be settled before any efforts for designing a PKI begin is the architecture of the certification structure. To this effect, the following parameters should be set:</td>
</tr>
<tr>
<td>✓ The number of Certification Service Providers (CSPs) that provide services to the public sector.</td>
<td></td>
</tr>
<tr>
<td>✓ The number of certification entities that exist in each CSP. It is usual to have two kinds of such entities: i) one or more Certification Authorities and (ii) one or more Registration Authorities.</td>
<td></td>
</tr>
<tr>
<td>✓ The appropriate CSP interconnection topology - trust chain. The provisions to allow cross-certification in situations with many CSPs and many operating CAs providing services to the public sector.</td>
<td></td>
</tr>
</tbody>
</table>

Deciding on the above should take into account both the existing situation in each country, as well as the necessity for cross-country interoperability and cross-certification capabilities for the benefit of European citizens. According to the Directive 99/93 (article 3, item 7), care should be taken so as to avoid creating obstacles to citizens with regard to cross-border services.

| **Current situation** | Regarding the trust architecture, the situation in member states is as follows: Nearly all of them, with the exception of Belgium, obtain certification services from several CSPs. Belgium allows only one CSP, which essentially is part of the government itself (i.e. the government has, itself, the role of the CSP). In one country (Spain), three government sectors, namely Ministry of Economic affairs, Treasuring, and Social Security, each obtain certification services from a single CSP. Luxemburg is still in the planning phase with regard to this issue. A major problem is that most of the member states seem to have settled on a number of different CA with no specific architecture and no consideration for cross-country certification of CAs selected by other countries. Most of them provide for multiple CSPs serving the needs of each government sector. A few others will only allow a single CSP in their planned PKI. Although none of the member states commented precisely on the adopted certification architecture, The Netherlands stated that it is already operating with a hierarchical architecture, which CSPs can join freely after they have been certified by the government Policy Authority (PA) for compliance with a predefined set of regulations and requirements. Moreover, Denmark states that the architecture is hierarchical with a public Certification Policy already defined, insuring interoperability; Germany states that it has a hierarchical trust chain with a bridge-CA. |
A promising solution for countries that have not yet developed a PKI, could be the development of a simple hierarchical architecture with a single CA and multiple RAs per sector, 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 CAs should be supported by a single CSP. On the contrary, it is desirable to have many CSPs operating these CAs. For countries where multiple CAs 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 CAs 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.

As far as the communication between participating CAs is concerned, there can be two alternative solutions: (i) directly, and (ii) through the Bridge Certification Authority. To support (i), it is important that all CSPs operating in the public sector should accept and support cross-certification. This is not only for convenience but, also, for ensuring interoperability between CSPs. To support (ii) it is necessary to have a Bridge CA providing online services with high availability and to adopt specific communication protocols, such as OCSP.

However, providing for cross-certification within an international “virtual” PKI, interconnecting many different CSPs and operating in different countries, is not a straightforward task. There are many issues that should be resolved, including:

- Technology interoperability between CSPs.
- A positive disposition of involved CSPs as well as of users subscribed to specific CSPs to trust certification services offered by other CSPs.
Ability and interest of involved CSPs to create and unconditionally comply with complex Certification Practice Statements that may, in addition, contain obligations that a CSP can accept only with reluctance, as they are imposed by the need to provide cross-certification in a complex trust architecture.

In practice, CAs operating under different CSPs either do not adopt the same certification technologies or do not adopt the same certification practices. Thus, it may be difficult in practice to enforce interoperability among many CSPs that are required to be members of the same trust architecture. This is when a bridge certification authority 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 CAs 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 bridge certification authorities and means for the fast transition to these should be studied in detail before such a trust architecture can be supported.

### III.8

Another important issue that should be resolved before a PKI is developed is the determination of the lifetimes of certificates. A certificate should not have an unlimited lifetime in order to minimize the exposure of the public keys to potential cryptanalysis aiming at revealing the corresponding private keys. This is handled by certificate expiration and revocation mechanisms.

Regarding the situation in member states, the answers to the questionnaires showed a variety of different opinions on this issue. Belgium has a certificate update interval of 5 years for any certificate type and for any possible use of certificates. In Denmark, the OCES certificates are updated every 12 months or more. (The OCES certificates, issued by TDC, which is the largest Danish telecommunication company, are the national certificates of Denmark and OCES stands, in Danish, for Public Certificates for Electronic Services.) The same update interval is also adopted by Greece (unqualified certificates), Italy (qualified certificates), Portugal (qualified certificates) and Sweden. Sweden, however, states that server certificates should typically be valid for 12-24 months and so should be software-based certificates while the lifetime of smart card certificates should be 3-5 years.

The Netherlands have an update interval of 3 years for qualified certificates. France has the same update interval but for qualified certificates while this interval is at least 12 months for Germany (qualified certificates), with typical value equal to 3 years.
The lifetime of a certificate should depend on its use as well as on the security level of its owner. A good practice approach follows (it pertains to the trust architecture of Figure 1).

- Certificate of the Bridge Authority. An indicative average lifetime is between 5 and 8 years.
- Certificate of a subordinate CA. An indicative average lifetime is between 3 and 5 years.
- Certificate of a civil servant. It can have a lifetime between 2 and 3 years, depending on their position and duties (too frequent revocations can create unnecessary certificate management overhead).

Determining a secure certificate lifetime is ultimately related to estimating the lifetime of the private key used in the certificate. The lifetime of a private key is determined by two components (see [4]):

- Cryptographic lifetime. This is, loosely, the average time that is required to determine the private key from the public key, given the specific signature scheme (e.g. RSA).
- Disclosure lifetime. This is the average time that passes before a user’s private key is disclosed and it is a function of the vulnerability of the entity that stores the key, the frequency at which the entity storing the key is publicly exposed as well as how profitable it will be for an attacker to disclose the private key of a specific user.

Considering the above, models can be formed that produce an estimate of the probability of loss or theft of a key as a function of time and usage. It is important that a CSP undertakes the effort to produce such estimates and publish them in its CPS along with a reference to the methodology that led to the estimates. In [18] one may find a very interesting discussion on such estimation models for RSA and Elliptic Curve based cryptography.

Another major issue regarding certificates as used in the public sector is that the state should be able to verify a signature for an indefinite time period. The EU Directive 99/93 states in Annex II, item (i), that the certificates should remain valid for a period of 30 years. As with all other aspects of the Directive 99/93, the European Commission decided to provide standards to also deal with this aspect of certificates. According to EESSI, trusted archival services (see also [22]) are of central importance in establishing the validity of signatures long after their creation and placement in electronic documents. At the same time, the European Telecommunications Standards Institute (ETSI) defined the standard Electronic Signature Formats (see [7]) that suggest necessary ingredients for proving the validity of a signature for, essentially, indefinite time even after the revocation or expiration of the corresponding certificate.
This is desirable in the public sector as a hand-written signature remains valid for indefinite time and the electronic signature is supposed to be an equivalent replacement. The key is in archiving the validation chain (also [22]). This does not mean simply to archive the document along with the signature. It is not enough that just the electronic signature and the content of the document are present in an archive to perform the validation at any time after the document was signed. It is necessary to also ascertain that the certificate of the signatory is also stored along with a proof of certificate validity at the time of signing (certificate status information). This, in turn, requires that signing a document is immediately followed by a signature verification procedure and an archiving action of (i) the signed document, (ii) the signatory’s certificate, and (iii) proof of validation of the certificate. Alternatively, there could be timing information (i.e. proof of time when the document was signed) in the archived document. To this end, the CSP should provide time stamping services in general and for archiving signature validation proofs in particular.

### III.9

This issue pertains to the exact procedures that should be followed for processing new certificate applications and for making a decision about whether the certificate application should be rejected or approved issuing a new certificate. First of all, there should be a clear description of what kind of documentation is required and should be maintained locally at the registration point. This will help the civil servant understand his/her obligations as far as the use of certificates is concerned. There should also be unambiguous description of the necessary credentials that the civil servant should produce in order to apply for a certificate. The application registration task should, normally, be assigned to an authority other than the Certification Authority (CA), called Registration Authority (RA) and the registration application, in the public sector, should preferably be automatic. This means that, upon employment, a civil servant does not need to be aware of any CSP operating in his/her sector or to apply for a certificate. Rather, as a part of the employment process, the sector employing the civil servant (e.g. the personnel office) should provide the necessary credentials to the local Registration Authority, informing the civil servant about this action.

Among all member states, only Belgium has a single RA. Belgium is notable in this respect as the only CSP is the government itself and it is only the government that provides, also, the registration services. Among other member states, Finland and France create Registration Authorities per sector and level, while in Denmark, Finland, France, Germany, Portugal, Sweden, Italy, and the UK each government organization may choose its own RA. In Austria each government organization may choose only from within a list of RAs while in Sweden a CSP may be used that also provides RA services.
**Good practice**

The RA is responsible for determining the level of the required identity proof, depending on the certificate type and its security level. After validating the applicant’s proof of identity and the correctness of the supplied details, the RA sends all the material to the CA requesting the issuance of the certificate for the applicant. Then, the CA makes the final decision of whether to approve the application or reject it and, in the former case, it creates the secret key within a secure smart card and forwards it to the RA which, in turn, forwards it to the applicant.

**Distribution of certificates**

**III.10**

**Setting the scene**

In order to support the trust architecture proposed in Figure 1 as well as various audit processes, there should be a way for CSP to make their certificates (for civil servants, at least) publicly available to other CSP and supervision bodies.

Some member states (Austria, Belgium, Finland, Germany, and Luxembourg) have or plan to have (in the case of Luxembourg), a central certificate repository. Austria will base the central repository on the LDAP standard. Belgium has a central repository for certificates of all citizens including those of civil servants. Ireland did not respond to the relevant question.

There are many uses for a central certificate repository that makes it an indispensable component of any PKI. A publicly available certificate repository enables government agencies and CSPs to have immediate access to Certification Status Information (CSI), and it provides a means to enforce interoperability of certificate formats. In general, a central repository enables the CSP site to put contact information (e.g. e-mail addresses) of civil servants as well as their certificate information into the hands of the public sector. Larger government agencies may also use an LDAP server that implements referrals of requests to various subunits of the agency. Another use case of public certificate directories came from France in the questionnaires where for online VAT declaration, enterprises can see the list of CSPs that have been referenced by the Ministry of Economy on its Internet site where each CSP name is linked to its certification policy.

**Current situation**

Publicly available certificate directories should be organized in order to provide high-availability. CSPs that provide services in the public sector should demonstrate that the software and hardware components implementing the LDAP and referrals are certified as highly available. Moreover, special provision must be taken for the distribution of self-signed certificates of Root Certification Authorities. Since there is no third party that signs and verifies the information contained in these certificates, they must be distributed by means of trusted mechanisms or through trusted secure locations.
### Value added services

#### Setting the scene

Certification of individuals’ identities can be considered as the main function of a CSP; it is, nevertheless, necessary within the e-government domain to have additional services that can cover daily needs of civil servants in their G2G and G2C transactions.

In this respect there is a mixed situation within the EU. Some countries (Austria, Belgium, France, Spain) do not offer services other than identity certification within the government domain. Other countries (Luxembourg) plan such services while other countries (e.g. Germany, France, Italy, The Netherlands, Sweden) offer these services while in some situations (as mentioned by Sweden) the demand for them is low. For example, notary services are planned by Luxemburg and are already provided by Portugal and Sweden. Time-stamping services are planned by Luxemburg and are already provided by Denmark, Germany, Italy, Portugal, Sweden, and the UK. Non-repudiation of receipt services are planned by Greece and Luxemburg and are already provided by Sweden and UK. Finally, Belgium has already scheduled the introduction of all value-added services listed below. Regarding auditing, all member states except Finland, France and Spain require that audit information be kept by a CSP providing services to the public sector. In Germany, in particular, the organization responsible for keeping audit information about the operation of CSPs providing qualified certificates is the designated body (along with the CSP).

#### Current situation

It is recommended that, as a minimum, a CSP should provide the following services beyond certification:

- **Timestamping services**: In many cases it is necessary for the recipient of a signed electronic document to know when the document was signed by the sender (e.g., when the signed document should have been sent before a specific deadline date). Thus function, called time-stamping, can be performed by the Certification Authority of a CSP itself or by a separate authority called Time Stamping Authority (TSA) although the former option is preferable to keep things simple. The time-stamping function requires the applicant to possess a valid certificate through the CSP offering the service.

- **Non-repudiation of receipt**: A particularly desirable function that can be provided by a CSP, besides certifying the identity of a civil servant or preventing him/her of denying having sent a message, is also to prevent denial of having received a certain message. This is called non-repudiation of receipt. Thus, the non-repudiation service as a whole should ensure that a civil servant can deny neither having sent nor having received an electronic message and that this can be proved with sufficient evidence before a court, if necessary.
Notary services: As the use of electronic signatures permeates the public sector, it is unavoidable that there will also be a need for more demanding services than simple identity certification, such as signing contracts of property transfer, transferring property to relatives, signing of wills etc. The electronic support of all these activities (mostly of financial nature), collectively called notary services, is an important value added service that can be supported by a CSP. Some ideas on ways to organize notary services in the public sector can be found in [13] by the Netherlands Land Registry and Registry of Deeds. Along these ideas, it is possible for a CSP to undertake the creation of an electronic contract (or will, for that matter) along with a traditional handwritten one still necessary to be created by the notary public (according to the Dutch, very reasonable, idea of notary services). The electronic contract will be accompanied by a declaration of equivalence whereby the notary public accepts liability for differences between the electronic version and the original hand-written deed kept by the notary public. The declaration of equivalence is authenticated by means of an electronic signature using the CSP. With this signature the notary public accepts liability for any damages arising from the lack of equivalence. In this way, the electronic document may be thought of as being of the same legal status and effect as the hand-written one, but more easily accessible and presentable as proof of property when the need arises (e.g. disputes over property ownership).

Audit capability: After the development and deployment of a PKI it is evident that the whole public sector of a country relies on using the certificates of the CSPs employed by the PKI. Ministries, government agencies, and third parties require some assurance with regard to the quality of the operation of the whole infrastructure and provided services. For example, as remarked in the very informative article [12], possible concerns include the following: Are the PKI systems and processes trustworthy? Are requirements specified in the certificate policy (CP) and certification practice statement (CPS) being followed consistently, etc? PKI audit services are necessary in order to resolve these questions. These services pertain to logging most of the crucial events that take place in a PKI (e.g. applications sent by a RA to a CA, certification chaining, etc.). All the above, presuppose the establishment of a well-defined auditing framework by the supervision body that states: (i) the frequency of CSP auditing, (ii) the structure and the format of the audit results report, (iii) the actions to be taken in case an improper event is found to have been logged.
### Setting the scene

This issue is related to the design and public availability of the Certification Practice Statement (CPS) that states the regulations, policies and services related to a CSP.

All member states pay particular attention to the issue of CPS publicity as well as to that of making perspective users of a CSP’s services aware of its CPS. In Belgium, the electronic identity cards that contain the certificates (authentication and signature) contain a certificate policy extension pointing to an official WWW page where all policies and procedures related to the use of certificates are published, in all official languages. In Denmark, awareness about the CPS is effected through government awareness projects as well as through official government sites focusing on PKI (National IT and Telecom Website). In Germany, information regarding CPSs is published by the Bundesamt für die Sicherheit in der Informationstechnik (BSI) at [www.bsi.bund.de](http://www.bsi.bund.de) and by the Regulierungsbehörde für Telekommunikation und Post at [www.regtp.de](http://www.regtp.de). In Italy, the CPS of voluntarily accredited CSPs is published on the web site of the accreditation body. In Luxembourg, only the CPSs of CSPs issuing qualified certificates are published (through OLAS). In The Netherlands there is a national Data Center of the Dutch Government PKI that provides information on CSPs and services for those seeking services supporting qualified certificates. In Portugal the legislation that implements the Directive 99/93 states that the national accreditation/supervision authority should ensure the availability through electronic means (e.g. Web site), of any information regarding the operation and policies of CSPs issuing qualified certificates. Spain states that CSPs should ensure the availability of their CPSs over the Internet. Sweden publicizes information regarding available CSPs through the web site of the Swedish Agency for Public Management ([www.statskontoret.se](http://www.statskontoret.se)). Moreover, Sweden publicizes information on regulations for the use of electronic identification as well as on signatures within the public sector on the SAM-SET project Web site ([www.rsv.se](http://www.rsv.se)). Finally, the UK provides information on the operation and policies of CSPs through various government, departmental, and transactional Web sites.

### Current situation

The existence of a CPS as well as its continuous availability both in electronic and in printed form, should be a prerequisite for a CSP wishing to offer services to the public sector. Moreover, there should be an automatic dispatch of the CPS to anyone who files an application for services provided by the CSP. Some mechanism for notifying all government agencies upon a modification of any part of a CSP should also exist; this is the responsibility of the CSP.
The content of a CPS for a CSP providing services in the public domain should address, among others issues, the following ([D]):

✓ Statement on whether the CSP is accredited or not and, if accredited, when the accreditation took place and by which government agency.
✓ List of CSPs already operating within the public sector 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.
✓ CAs’ obligations.
✓ Cooperation protocols with RAs (which are established within government agencies and operate in the public sector).
✓ Subscriber (government’s) obligations.
✓ Relying party’s obligations.
✓ Statement of Insurance against damages caused by the CSP to the state.
✓ Offer of value added services (e.g. time-stamping, notarization, encryption of information, certificate repository).
✓ Obligations of the CSP against the state in case of resignation before the end of the contract.
### Setting the scene

It is important to put forward rules governing certificate revocation and expiration. Note that there is an important difference between revocation and expiration that dictates a difference in handling the two cases. An *expired* certificate can be used up to the expiration date for its intended use. A revoked certificate is terminated prematurely, before the expiration date, due to some reason that ranges from an individual being promoted to another position that requires a different type of certificate to an individual being fired due to misconduct or misuse of the certificate. All revoked and expired certificates should be stored along with data regarding the termination of their validity.

In many member states automatic revocation or renewal of a civil servant’s certificate is performed when s/he is transferred to another post (Denmark, France, Italy, Portugal). France, Italy, and Portugal have stated that among the attributes used in the certificate is the role of the civil servant; thus, the revocation or renewal of the certificate of a civil servant upon transfer to another post is possibly due to the need to change the role in the attributes. Sweden states that revocation or renewal depends on what kind of certificate the civil servant uses. If s/he uses identification certificates only the certificate is not revoked or renewed upon a transfer to another post. Rather, the civil servant is (possibly) moved to another rights list depending on the new post. The UK, on the other hand, has adopted a more open approach, according to which there is no central policy on this issue and each governmental agency decides by itself. The Netherlands, Finland, Sweden and Belgium do not revoke or renew the certificate upon transfer to another post, while Greece’s plans are similar. The fact that these countries do not include roles in certificates possibly explains why automatic revocations or renewals do not occur. Germany answered that whether revocation or renewal will be invoked depends on the case; however no further information is given (Germany includes roles in certificates). Finally, Austria, Ireland, and Spain do not have specific plans on this issue for the time being, although Spain states that certificates include roles.

The CSP should create automatically a new certificate (invocation of the certificate renewal procedure) some time (to be specified upon agreement between the CSP and the state) *before* the expiration of the certificate of a civil servant.

As far as the revocation of certificates is concerned and the policy that government agencies should follow upon the occurrence of a misconduct or misuse incident involving a certificate, the following should apply:

- Civil servants should immediately notify their organization if they suspect that their certificate may be illegally used by someone else.
✓ The government agency should notify the CSP upon the filing of such a notice by a civil servant.
✓ The CSP, in turn, should revoke the suspect certificate from the Directory and notify all users who use it.

Government agencies should form specific procedures to be followed with respect to the certificate when its subject retires, transfers to another position - only when role-based certificates are used – resigns, etc.

### CSP: Cease of operation

#### Setting the scene

An important issue with regard to the operation of a CSP in the public sector is how to handle the possibility of the CSP ceasing offering certification services before the date stated in the contract with the state. This may occur, for example, due to the CSP going out of business or due to dissatisfaction stemming from deterioration of the quality of the services provided by the CSP.

As stated in Annex II article c of Directive 99/93, the CSP is obliged to issue a warning to the state three months before it stops providing its services. The problem, then, is how the transition to another CSP takes place without disrupting the functioning of the public sector. In order for this transition to take place in a fast and inexpensive way, it is obvious that interoperability between the resigning CSP and the CSP that takes over should be established.

The member states seem to have imposed several compatibility requirements for CSPs providing services to the public sector, although they do not state explicitly in their response to the questionnaire that they do so in order to provide a smooth transition of services between CSPs. Thus, for example, Denmark has established a public Certification Policy that ensures interoperability; Germany requires conformance with the ISIS-MTT standard; in Italy if no voluntarily accredited CSP replaces a terminating CSP, all certificates issued by the latter will be revoked.

In The Netherlands, a CSP wishing to join the CSP hierarchy of the public sector should fulfill specific requirements, while in the UK certain government sectors require digital certificates provided by a specific organization, tScheme, or an equivalent organization. Belgium takes a unique position as it has only one CSP, essentially the government itself, which excludes the possibility of CSP resignation. In addition, 8 out of the 15 countries have special legislation that handles the legal issues of CSP resignation.

### III.14

The government agency should notify the CSP upon the filing of such a notice by a civil servant.

The CSP, in turn, should revoke the suspect certificate from the Directory and notify all users who use it.

Government agencies should form specific procedures to be followed with respect to the certificate when its subject retires, transfers to another position - only when role-based certificates are used – resigns, etc.
In Denmark the resigning CSP is obliged to make its revocation list available until all certifications ever issued by the resigning CSP expire, while it should also provide an archive service for six years after the date of release of the last issued certificate. In Greece the CSP informs the National Telecommunications and Posts Commission (EETT), the subscribers and all the other CSPs 3 months before the termination, according to EETT regulation 248-71/15.3.2002. The CSP revokes the issued certificates, unless otherwise specified in the contract between the CSP and the subscriber or within the CSP’s CPS. For Qualified Certificates the CSP transfers its records to other CSPs. The CSP taking over informs EETT within 7 days of this transfer. If this transfer was not performed properly, the terminating CSP transfers its records to EETT. Moreover, most countries provide for regulations that ensure some compatibility level among CSPs providing e-government services. Germany, Italy and The Netherlands impose interoperability of technology. Belgium, Denmark, Germany and Italy impose compatibility of CPSs. Denmark, Italy, The Netherlands, Portugal and the UK dictate that a CSP should first apply for voluntary accreditation.

The conclusion is that: (i) interoperability is the key to overcome problems that arise due to CSP termination of operation, and (ii) the government is responsible for establishing a legal framework that handles the case of premature CSP termination of 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 CSPs comply with these standards then it will be easier for a CSP to undertake resigning CSP’s duties.

This is, also, another argument in favour 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.
Compliance with Data Protection legislation and individual privacy from CSPs is a prerequisite for strengthening, consolidating and increasing user confidence in electronic communications and e-government services. A person's right to data protection is guaranteed as a basic right in the legislation of member states and it is additionally anchored in the European Charter of Fundamental Rights. CSPs should respect not only the provisions laid down in Article 8, items 2 and 3 of the Directive 99/93 as enacted in the national legislation of member states, but the data protection principles and the relevant legislation as a whole. In relation to data protection requirements, attention must be paid to the dissemination of PKI information (certificate information and revocation information) as well as to the regulation of lawful access to data available at CSPs. Guaranteeing adequate safeguards for personal privacy requires the aspect of personal privacy to be taken into account from the earliest stages of the designing phase of technologies and infrastructures (see, for further details, International Working Group on Data Protections in Telecommunications, Working Paper on Data Protection aspects). In order to enter into a contract with a CSP it must be verified that the CSP respects and applies the data protection regulation in force. Compliance with the data protection framework pertains to legal requirements as well as to data security measures (as foreseen in Art. 17 of the EU Data Protection Directive 95/46). It is recommended that Data Protection Authorities provide assistance to public authorities to monitor the CSP privacy policy. It is further recommended that obligations and requirements specifying the obligations laid down in data protection acts, are included in contracts concluded between the Public Sector and CSPs.

Generally, in the contractual relationship between the Public and the CSPs, specific provision should be included, so as to cover cases of liability of CSPs towards authorities, due to CSPs’ any kind of default, provided that such liability causes direct or indirect damage to the citizen, or impedes the exercise of legal rights or the exploitation of opportunities on the part of citizens.
Bibliography

1. Bundesamt für Sicherheit in der Informationstechnik (BSI): Protection Profiles (PPs) for Secure Signature Creation Devices and Smart Cards: [http://www.bsi.de/cc/pplist/pplist.htm#schutzprofilpp10]


14. PKI in the Swedish public sector, [http://forvaltningsnett.dep.no/dok/pki/int_meeting/Sweden.ppt]


