It is requested that any comments on this document are submitted by 15th September to the ETSI EL-SIGN list on:

EL-SIGN@ETSI.ORG

With a copy to the editor on POPE@SECSTAN.COM

Please put "QCP" at the start of the Subject field of all e-mails relating to the document.

(You can subscribe to the list and obtain further information on related activities through:
HTTP://WWW.ETSI.ORG/SEC/EL-SIGN.HTM)

Policy Requirements for Certification Service Providers Issuing Qualified Certificates

ETSI STF 155 T1 Draft H
15th July 2000

Contents

Background

Electronic commerce is emerging as a future way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature. This is commonly achieved by using electronic signatures which are supported by certificates issued by a Certification Service Provider (CSP).

For users of electronic signatures to have confidence in the authenticity of the electronic signatures they need to have confidence that the CSP has properly established procedures and protective measure in order to minimise the operational and financial threats and risks associated with public key crypto systems. This document specifies baseline policy requirements on the operation and management of CSPs to give user this confidence.

The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (1999/93/EC) (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "Qualified Certificate". Annex II of the Directive specifies requirements on Certification Service Providers (CSPs) issuing Qualified Certificates. The current document specifies baseline policy requirements on the operation and management of CSPs issuing Qualified Certificates in accordance with the Directive. The use of a secure signature creation device, as required through Annex III of the Directive, is an optional element of the policy requirements specified in the current document.

1 Scope

This standard specifies minimum policy requirements relating to Certification Service Providers (CSPs) issuing Qualified Certificates. It defines policy requirements on the operation and management of CSPs issuing Qualified Certificates such that Subscribers certified by the CSP and Relying Parties may have confidence in the applicability of the certificate in support of electronic signatures.

The policy requirements relating to the CSP includes requirements on provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and if required, signature creation device provision. Other CSP functions such as time-stamping, key escrow and confidentiality support are outside the scope of this document. In addition, the current document does not address requirements for Certification Authority certificates, including certificate hierarchies and cross-certification.

These policy requirements are specifically aimed at Qualified Certificates issued to the public, and used in support of Qualified Electronic Signatures (i.e. electronic signatures that are legally equivalent to hand-written signatures in line with article 5.1 of the European Directive on a community framework for electronic signatures [Directive]). It specifically addresses the requirements for CSPs issuing Qualified Certificates in accordance with Annex II of this Directive. Requirements for the use of Secure-Signature-Creation Devices, which is also a requirement for electronic signatures in line with article 5.1, is an optional element of the policy requirements specified in this document.

Certificates issued under these policy requirements may be used to authenticate a person who acts on his own behalf or on behalf of the natural person, legal person or entity he represents.

These policy requirements are based around the use of public key cryptography to support electronic signatures.

This standard may be used by independent bodies as the basis for confirming that a CSP meets the requirements for issuing Qualified Certificates.

The policy requirements are defined in terms of:

a) The specification of two closely related Qualified Certificate Policies for Qualified Certificates issued to the public, one requiring the use of a secure signature creation device,

b) A framework for the definition of other Qualified Certificate Policies enhancing the above policies or for Qualified Certificates issued to non-public user groups.

Subscriber and relying parties should consult the Certification Practice Statement of the issuing Certification Service Provider to obtain further details of precisely how the certificate policy is implemented by the particular CSP for a particular certificate.

2 References

[BS 7799] BS 7799 Part 1 (1999): Code of Practice for Information Security Management

Editorial note: Use of ISO/IEC 13335 "Guidelines on the management of IT security" as an alternative to BS 7799 is under consideration.

[Directive] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Note: The above is referred to as "the Directive" in the current document.

[RFC 2527] RFC 2527, Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, S. Chokhani, W. Ford, March 1999

[X.509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: authentication framework".

[Data Protection] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[FIPS 140-1] FIPS PUB 140-1, Security Requirements For Cryptographic Modules, 1994 January 11

[Trustworthy systems] CEN/ISSS Workshop Agreement (to be completed) Requirements for Trustworthy Systems Managing Certificate for Electronic Signatures

[ETSI QCert] ETSI TS ???? (to be completed) Qualified Certificate Profile

NOTE: A general bibliography of related documents is given in annex E.

3 Definitions and Abbreviations

Certificate Policy: *A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [X509]*

Certification Authority*: An authority trusted by one or more users to create and assign certificates. [X.509]*

Certification Practice Statement: *A statement of the practices which a Certification Authority employs in issuing certificates. [RFC 2527]*

Certification Service Provider (CSP)*: An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. [Directive 2.11]*

Note: The current document is concerned with CSP's issuing Qualified Certificates (or component services for issuing Qualified Certificates – see 4.1). The current document is not concerned with other types of CSP functions such as time-stamping and key escrow.

Qualified Certificate: *a certificate which meets the requirements laid down in Annex I (of the Directive) and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II (of the Directive); [Directive]*

Qualified Certificate Policy (QCP)*: A certificate policy which incorporates the requirements laid down in Annex I and Annex II of the Directive;*

Qualified Electronic Signature: *advanced electronic signature which is based on a Qualified Certificate and which is created by a secure-signature-creation device as defined in Article 5.1 of the Directive.*

Relying Party: *A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. [RFC 2527]*

Signature-creation-data: *unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. [Directive]*

Note: In Qualified Certificates based on public key cryptography, as covered by the current document, the Signature Creation Data is a private key. Hence, within the current document the term private key is used for the Signature-creation data.

Signature-creation device (SCD): *configured software or hardware used to implement the signature-creation data [Directive]*

Secure-Signature-Creation Device (SSCD)*: a signature-creation device which meets the requirements laid down in Annex III (of the Directive); [Directive]*

Signature-verification-data: *data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature [Directive]*

Note: In Qualified Certificates based on public key cryptography, as covered by the current document, the Signature Verification Data is a public key. Hence within the current document the term public key is used for the Signature-verification data.

Subscriber: *An entity subscribing with a CSP to have its public key and identity certified in a public key certificate.*

4 General Concepts

4.1 Certification Services

The service of issuing Qualified Certificates is broken down in the current document into the following component services for the purposes of classifying requirements:

Registration Service: Verifies the identity and, if applicable, any specific attributes of a Subscriber. The results of this service are passed to the Certificate Generation Service.

Certificate Generation Service: Creates and signs Certificates based on the identity and other attributes verified by the registration service.

Certificate Dissemination Service: Disseminates Certificates to subscribers, and if the subscriber consents, to relying parties. This service also disseminates the CA's policy & practice information to Subscribers and Relying Parties.

Revocation Management Service: Processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.

Revocation Status Service: Provides certificate revocation status information to relying parties. This service may be a real-time service or may be based on revocation status information which is updated at regular intervals.

and optionally:

Subscriber SCD Provision Service: Prepares and provides a Signature Creation Device (SCD) to Subscribers.

Note: examples of this service are:

- A service which generates the subscriber' s key pair and distributes the private key to the subscriber;
- A service which prepares the subscriber' s Secure-Signature-Creation Device (SSCD) and device enabling codes and distributes the SSCD to the registered subscriber.

This subdivision of services places is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the CSP services.

The following diagram illustrates the interrelationship between the services:

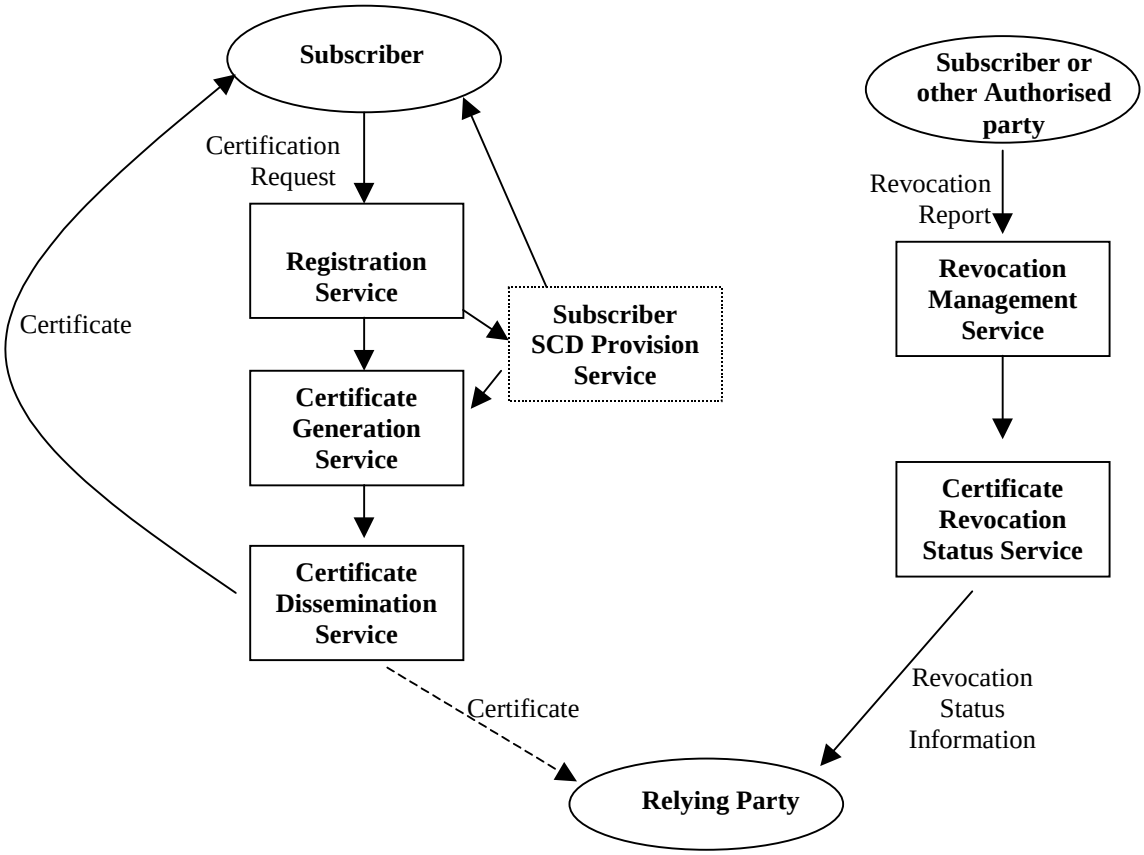

Figure 1: Illustration of Certification Component Services

4.2 Certification Authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and sign certificates is called the Certification Authority. The Certification Authority has overall responsibility for the provision of these services. The Certification Authority signs the Qualified Certificates and is identified in the certificate as the issuer.

The Certification Authority may make use of other parties to provide parts of the certification service. However, it always maintains overall responsibility and ensures that the policy requirements identified in the current document are met.

4.3 Certificate Policy & Certification Practice Statement

4.3.1 Purpose

In general, the purpose of the Certificate Policy, referenced by a policy identifier in a certificate, states "what is to be adhered to," while a Certification Practice Statement states "how it is adhered to", i.e., the processes it will use in creating and maintaining the certificate. The relationship between the Certificate Policy and Certification Practice Statement is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

The current document specifies Certificate Policies to meet the requirements for Qualified Certificates as laid down in Annex I and II of the Directive. CSPs specify in Certification Practice Statements how these requirements are met.

4.3.2 Level of Specificity

A Certificate Policy is a higher-level document than a Certification Practice Statement. A Certification Practice Statement is a more detailed description of the terms and conditions as well as business and operational practices of a

Certification Authority in issuing and otherwise managing certificates. The Certification Practice Statement of a Certification Authority enforces the rules established by entities subscribing a specific Certificate Policy.

Note: Even lower-level documents may be appropriate for a CA detailing the specific procedures necessary to complete the practices identified in the CPS. This lower-level documentation is generally regarded as an internal operational procedure documents, which may define specific tasks and responsibilities within an organisation. While this lower-level documentation may be used in the daily operation of the CA and reviewed by those doing a process review, due to its internal nature this level of documentation is considered private and proprietary and therefore beyond the scope of this standard. For example, the policy may require secure management of the private key(s), the practices may describe the dual-control, secure storage practices, while the operational procedures may describe the detailed procedures with locations, access lists and access procedures.

4.3.3 Approach

The approach of a Certificate Policy is significantly different from a Certificate Practice Statement. A Certificate Policy is defined independently of the specific details of the specific operating environment of a Certification Authority, whereas a Certificate Practice Statement is tailored to the organisational structure, operating procedures, facilities, and computing environment of a Certification Authority.

5 Introduction to Qualified Certificate Policies

5.1 Overview

A Certificate Policy is a “named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements” [X509].

The policy requirements are defined in current document in terms of Certificate Policies. These Certificate Policies are for Qualified Certificates, as defined the Directive, and hence are called Qualified Certificate Policies. Certificates issued in accordance with the current document include a Certificate Policy identifier which can be used by Relying Parties in determining the certificates suitability and trustworthiness for a particular application. The current document specifies two Qualified Certificate Policies:

a) A Qualified Certificate Policy for Qualified Certificates issued to the public,

b) A Qualified Certificate Policy for Qualified Certificates issued to the public, requiring use of Secure-Signature-Creation Devices.

Section 8 specifies a framework for other Qualified Certificate Policies which:

a) Enhance or further constrain the above policies, and/or

b) are for Qualified Certificates issued to “closed groups” other than the public.

Note: The current document makes use of the principles defined in RFC 2527 and the framework defined in ANSI X9.79. The aim of this document is to achieve best possible harmonisation with the principles and requirements of those documents.

5.2 Identification

The identifiers for the Qualified Certificate Policies specified in the current document are:

a) **QCP Public**: A Certificate Policy for Qualified Certificates issued to the public,

Editorial note: Object identifier to be added.

c) **QCP Public + SSCD**: A Certificate Policy for Qualified Certificates issued to the public, requiring use of secure signature creation devices

Editorial note: Object identifier to be added.

By including either of these object identifiers in a certificate the CSP claims conformance to the identified Qualified Certificate Policy.

5.3 Community and Applicability

5.3.1 QCP Public

This Certificate Policy is for certificates:

a) which meet the requirements laid down in Annex I of the Directive,

b) are issued by a CSP who fulfils the requirements laid down in Annex II of the Directive

c) are issued to the Public

Qualified Certificates issued under this policy may be used to support electronic signatures which "are not denied legal effectiveness and admissibility as evidence in legal proceedings", as specified in article 5.2 of the Directive.

5.3.2 QCP Public + SSCD

This Certificate Policy is for certificates:

a) which meet the requirements laid down in Annex I of the Directive,

b) are issued by a CSP who fulfils the requirements laid down in Annex II of the Directive

c) which are for use only with Secure Signature Creation Devices which meet the requirements laid down in Annex III of the Directive

d) are issued to the Public

Qualified Certificates issued under this policy may be used to support electronic signatures which "satisfy the 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", as specified in article 5.1 of the Directive.

5.4 Conformance

5.4.1 General

The CSP shall only use the identifier for either of the Qualified Certificate Policies as given in 5.2:

a) if the CSP claims conformance to the identified Qualified Certificate Policy and makes available on request the evidence to support the claim of conformance, or

b) if the CSP has been certified to be conformant to the identified Qualified Certificate Policy.

5.4.2 QCP Public

A conformant CSP must demonstrate that:

a) it meets its obligations as defined in 6.1,

b) it has implemented controls which meet the requirements specified in section 7, excluding those specified in: 7.2.8 (d), 7.2.9 and excluding the Subscriber obligation given in 6.2 (e). .

5.4.3 QCP Public + SSCD

A conformant CSP must demonstrate that:

a) it meets its obligations as defined in section 6.1,

b) it has implemented controls which meet all the requirements specified in section 7.

5.5 Contact Details

These Certificate Policies are published by:

(ETSI Secretariat Contact details to be added)

6 Obligations and Liability

Note: This section is applicable to both Qualified Certificate Policies identified in section 5: QCP Public, and QCP Public + SSCD, except where indicated.

6.1 Certification Authority Obligations

The Certification Authority shall ensure that all requirements on CSP, as detailed in Section 7, are implemented as applicable to the selected Qualified Certificate Policy (see section 5.4.2 and 5.4.3).

The Certification Authority has the responsibility for conformance with the procedures prescribed in this policy, even when the CSP functionality is undertaken by sub-contractors.

The Certification Authority shall also carry out any additional obligations indicated in the certificates either directly or incorporated by reference.

6.2 Subscriber Obligations

The Subscriber shall:

a) submit accurate and complete information to the CSP during Subscriber registration in accordance with the requirements of this policy;

b) only use the key pair for Electronic Signatures and in accordance with any other limitations notified to the Subscriber.

c) exercise reasonable care to avoid unauthorised use of its private key;

d) if the Subscriber generates its keys:

- generate Subscriber keys using an algorithm recognised as being fit for the purposes of Qualified Electronic Signatures,
- use a key length and algorithm which is recognised as being fit for the purposes of Qualified Electronic Signatures.

Note: It is currently proposed that the recognition of algorithms being fit for the purposes of Qualified Certificates is through a cryptographic advisory panel under the committee identified in Article 9 of [Directive].

e) if the Certificate Policy requires use of a SSCD , use a secure signature-creation device conforming to Annex III of the Directive.

Note: The above item is NOT applicable to Qualified Certificate Policy: QCP Public.

f) submit accurate and complete information to the CSP;

g) notify the CSP without any delay in case of compromise, or risk of compromise, of the Subscriber's private key, and/or inaccuracy of the certificate content, as notified to the Subscriber, that occur at least up to the end of its validity period.

Note: The CSP requires that the Subscriber agrees to these obligation during registration as defined in 7.3.1.

6.3 Relying Party Obligations

The Relying Party cannot reasonably rely on a certificate if it has failed to:

a) verify the validity, suspension or revocation of the certificate; or

b) take account of any limitations on the usage of the certificate indicated to the Relying Party either in the certificate or the terms and conditions supplied as required in 7.3.5.

c) take any other precautions prescribed in agreements or elsewhere.

Note: The liability of CSPs issuing Qualified Certificates to the public specified in Article 6 of the Directive applies to parties who “reasonably rely” on a certificate.

6.4 Liability

CSPs issuing Qualified Certificates to the public are liable as specified in Article 6 of the Directive. (see Annex A for further guidance on liability)

7. Requirements on CSP Practice

Note: This section is applicable to both Qualified Certificate Policies identified in section 5: QCP Public, and QCP Public + SSCD, except where indicated.

The CSP shall implement the controls that meet the following requirements.

Note 1: A reference to the article within the Directive on which the requirement is based is given in square brackets after each paragraph.

The current document is concerned with CSP's issuing Qualified Certificates. This includes the provision of services for Registration, Certificate Generation, Certificate Dissemination, Revocation Management and Revocation Status (see 4.1). Where requirements relate to a specific service area of the CSP then it is listed under one of these headings. Where no service area is listed, or "CSP General" is indicated, a requirement is relevant to the general operation of the CSP.

The subdivision of CSP services implied by the following subdivision of requirements is not a part of this policy. There is no requirement for any particular division of services provided that the requirement relating to a certain aspects of the CSP services are met.

These policy requirements are not meant to imply any restrictions on charging for CSP services.

7.1 Certification Practice Statement

The Certification Authority shall ensure that the Certification Service Provider's certification practices and procedures are effective. [Directive Annex II (a)].

In particular:

a) A risk assessment shall be carried out to evaluate business risks and determine the necessary security requirements and operational procedures.

b) The CA shall have a Certification Practice Statement which identifies the practices and procedures used to address all the requirements identified in the Qualified Certificate Policy, as considered necessary through the risk analysis.

Note: This policy makes no requirement as to the structure of the Certification Practice Statement.

c) The CA's Certification Practice Statement shall identify the obligations of all external organisations supporting the CSP services including the applicable policies and practices.

d) The CA shall make available details of its Certification Practice Statement as necessary to assess conformance to the Qualified Certificate Policy either:

- To an external auditor who is able to certify conformance to the Qualified Certificate Policy, or
- To all appropriate Subscribers and Relying Parties

Note: The CA is not generally required to make all of its practices public.

e) The CA shall have a management body with final authority and responsibility for approving the Certification Practice Statement.

f) There shall be a defined review process for Certification Practice Statement including responsibilities for maintaining the Certification Practice Statement.

g) Revisions to the Certification Practice Statement shall be made available to the auditors or to all appropriate Subscribers and Relying Parties as in (d) above.

7.2 Public Key Infrastructure - Key Management Life Cycle

7.2.1 Certification Authority Key Generation

Certificate Generation

The Certification Authority shall ensure that Certification Authority keys are generated in accordance with industry standards. [Directive Annex II (g)] [Directive Annex II (f)]

In particular:

a) Certification Authority key generation shall be undertaken by properly authorised personnel under, at least, dual control.

b) Certification Authority key generation shall be carried out within a device meeting FIPS 140-1 level 3, or equivalent, as a minimum.

c) Certification Authority key generation shall be performed using an algorithm recognised as being fit for the purposes of Qualified Certificates.

d) The selected key length and algorithm for Certification Authority signing key shall be one which is recognised as being fit for the purposes of Qualified Certificates and appropriate for the expected lifetime of the keys used by the CA.

Note: It is currently proposed that the recognition of algorithms being fit for the purposes of Qualified Certificates is through a cryptographic advisory panel under the committee identified in Article 9 of [Directive].

7.2.2 Certification Authority Key Storage, Backup and Recovery

Certificate Generation

The Certification Authority shall ensure that Certification Authority private keys remain confidential and maintain their integrity. [Directive Annex II (g)] [Directive Annex II (f)]

In particular:

Technical control procedures

a) The Certification Authority private signing key shall be stored within a secure cryptographic device meeting FIPS 140-1 level 3, or equivalent, as a minimum.

b) The Certification Authority private key shall be backed up, stored and recovered only by authorized personnel using dual control in a physically secured environment.

c) Backup copies of the Certification Authority private keys shall be subject to the same or greater level of security controls as keys currently in use.

d) Certification Authority Private Keys if stored in software, shall be encrypted. Otherwise they shall be stored in a dedicated key processing hardware module.

e) Where the keys are stored using software and encryption, the keys shall be held in clear form only whilst they are in use, after this time the memory used to hold them shall be purged.

f) Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

7.2.3 Certification Authority Public Key Distribution

Certificate Generation & Certificate Distribution

The Certification Authority shall ensure that the integrity and authenticity of the Certification Authority public key and any associated parameters are maintained during initial and subsequent distribution. [Directive Annex II (g)] [Directive Annex II (f)].

In particular:

a) CA public keys shall be made available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.

Note 1): Certification Authority public keys may be distributed in certificates signed by itself or issued by another Certification Authority. By itself a self signed certificate cannot be known to come from the CA. Additional measures, such as checking the fingerprint of the certificate against information provided by a trusted route, is needed to give assurance of the correctness of this certificate.

2) Requirements for CSP issuing Certification Authority certificates, cross certification and certification hierarchies are outside the scope of this standard.

7.2.4 Key Escrow

Key Escrow shall not be applied to Certification Authority and Subscriber signature keys.

7.2.5 Certification Authority Key Usage

Certificate Generation

The Certification Authority shall ensure that Certification Authority keys are used only for their intended functions in their intended locations. [Directive Annex II (g)] [Directive Annex II (f)]

7.2.6 End of Certification Authority Key Life Cycle

Certificate Generation

The Certification Authority shall ensure that, at the end of their life cycle, all copies of the Certification Authority private keys are either [Directive Annex II (g)] [Directive Annex II (f)]:

a) completely destroyed, or

b) are archived in a manner such that they are protected against being put back into use.

7.2.7 Life Cycle Management of Cryptographic Hardware used to Sign Certificates

Certificate Generation

The Certification Authority shall ensure that [Directive Annex II (f)]:

i) Certificate signing cryptographic hardware is not tampered with during shipment;

ii) Certificate signing cryptographic hardware is not tampered with while stored;

iii) access to Certificate signing cryptographic hardware requires a minimum of two trusted employees throughout its life cycle;

iv) Certificate signing cryptographic hardware is functioning correctly; and

v) Certificate signing keys stored on Certification Authority cryptographic hardware are destroyed upon device retirement.

7.2.8 CSP Provided Subscriber Key Management Services

Certificate Generation

If the CSP generates the Subscriber keys, the Certification Authority shall ensure that [Directive Annex II (f)] [Directive Annex II (j)]:

a) CSP-generated Subscriber keys are generated using an algorithm recognised as being fit for the purposes of Qualified Electronic Signatures.

b) The selected key length and algorithm for CSP-generated Subscriber keys shall be one which is recognised as being fit for the purposes of Qualified Electronic Signatures.

Note: It is currently proposed that the recognition of algorithms being fit for the purposes of Qualified Certificates is through a cryptographic advisory panel under the committee identified in Article 9 of [Directive].

c) CSP-generated Subscriber keys are not stored or copied by the CSP subsequent to delivery to the Subscriber.

d) In the case of a Secure Signature Creation Device being used CSP-generation of keys shall be an integral part of Secure Signature Creation Device Preparation (see 7.2.9).

Note: The above item is NOT applicable to Qualified Certificate Policy: QCP Public.

7.2.9 Secure Signature Creation Device Preparation

Note: This sub-section is NOT applicable the Qualified Certificate Policies: QCP Public.

Subscriber SCD provision

If the CSP issues a Secure-Signature-Creation Device [Directive Annex III] to the Subscriber, the Certification Authority shall ensure that:

i) secure signature-creation device preparation is securely controlled by the CSP;

ii) secure signature-creation device is securely stored and distributed;

iii) secure signature-creation device deactivation and reactivation are securely controlled.

7.3 Public Key Infrastructure - Certificate Life Cycle

7.3.1 Subscriber Registration

The Certification Authority shall ensure that [Directive Annex II (d)]:

i) Subscribers are properly identified and authenticated and

ii) Subscriber certificate requests are accurate, authorized and complete.

In particular:

Registration

a) When registering, a Subscriber is identified as a person with specific attributes.

Note: The specific attributes may indicate, for example, an association within an organisation possibly with a role.

b) Before entering into a contractual relationship with a Subscriber the CSP shall inform the Subscriber of the precise terms and conditions regarding use of the certificate including [Directive Annex II (k)]:

- Any limitations on its use;
- The Subscriber's obligation as defined in 6.2
- The procedures for complaints and dispute settlements;
- The period of time for which CSP event logs (see 7.4.11) are maintained;
- The applicable legal system;
- Qualified Certificate Policy being applied,
- If the CSP has been certified to be conformant with the identified Qualified Certificate Policy, and if so through which scheme.

c) The CSP shall communicate such an agreement through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

Note: A Model PKI Disclosure Statement which may be used as the basis of such a communication is given in Annex B.

d) The CSP shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a Qualified Certificate is issued. This information shall be checked against the physically present person (either directly or indirectly through submitted documentation which provides equivalent assurance). Checks shall use documentation (paper or electronic) that at least verifies the Subscriber's:

- Full name (Including family name and first names),
- Physical address by which the Subscriber may be contacted,
- Date and place of birth, a nationally recognised identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

Notes 1: The place should be given in accordance to national conventions for registering births.

2: The CSP is liable as regards the accuracy "of all information contained in the certificate" (see Annex A).

e) The CSP shall record all the information used to verify the Subscribers identity, including any reference number on the documentation used for verification, and any limitations on its validity.

f) The CSP shall record the signed agreement with the Subscriber including:

- agreement to the Subscriber's obligations,
- if required by the CSP, agreement by the Subscriber to use a Secure Signature Creation Device,
- consent to the keeping of a record by the CSP of information used in registration (see 7.4.11 h, i, j) and any subsequent revocation (see 7.4.11 k), and passing of this information to third parties under the same conditions as required in by this policy in the case of the CA terminating its services
- whether the Subscriber requires and consents to the publication of its certificate,
- that the information held in the certificate as being correct.

Note: The Subscriber may agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct may be carried out subsequent to other aspects of the agreement.

g) If the Subscriber's key pair is not generated by the CSP, the certificate request process shall ensure that the Subscriber has possession of the private key associated with the public key presented for certification.

h) The CSP shall ensure that the requirements of the national its national data protection legislation are taken into account (including the use of pseudonyms if applicable) within their registration process.

Certificate Generation

i) The CA shall ensure over time the uniqueness of the distinguished name assigned to the Subscriber within the domain of the CA. (i.e. over the life time of the CA a distinguished name which has been used in an issued certificate shall never be re-assigned to another entity.)

j) The confidentiality and integrity of registration information shall be protected whenever exchanged with the Subscriber or between distributed CSP services.

k) The CSP shall verify registration data is exchanged with recognised registration authorities in the event that external registration service providers are used.

Certificate Dissemination

l) The CSP shall inform Subscribers by a durable means of communication the precise terms and conditions regarding use of the certificate including items as listed in (c) above.

m) The CSP shall communicate such an agreement through a durable means of communication, which may be transmitted electronically, and in readily understandable language.

7.3.2 Certificate Renewal and Rekey

The Certification Authority shall ensure that [Directive Annex II (g)]:

i) Requests for Certificates issued to a Subscriber who has already previously registered (e.g for renewal or rekey) are accurate, authorised and complete;

ii) Certificates renewal and rekey following certificate revocation or expiration are accurate, authorised and complete.

In particular:

Registration

a) The CSP shall check that the information used to verify the identity and attributes of the Subscriber is still valid,

b) If any of the CSP terms and conditions have changed, these shall be communicated to the Subscriber and agreed to in accordance with 7.3.1 (b), (c), (f)

c) If any information has changed, this is verified, recorded, agreed to by the Subscriber in accordance with 7.3.1 (d), (e), (f), (g)

7.3.3 Certificate Generation

The Certification Authority shall ensure that new, renewed and rekeyed certificates are issued securely. [Directive Annex II (g)]

In particular:

Certificate Generation

a) the certificates are generated and issued in accordance with Annex I of the Directive. [Directive Annex II (g)]

Note: A standard format for Qualified Certificates meeting the requirements of Annex I of the Directive is defined in standard ES (reference to ETSI QC format standard to be inserted).

b) the procedure of issuing the certificate is securely linked to the associated registration, certificate renewal or rekey, including the provision of any Subscriber generated public key.

c) if the CSP generated the Subscribers key:

- the procedure of issuing the certificate is secure linked to the generation of the key pair by the CSP;
- the private key (or Secure Signature Creation Device – see 7.2.9) is securely passed to the registered Subscriber.

7.3.4 Certificate Dissemination

The Certification Authority shall ensure that Certificates and associated information are made available as necessary to Subscribers and Relying Parties. [Directive Annex II (l)]

In particular:

Certificate Dissemination

a) Upon generation complete and accurate certificates are available to Subscribers;

b) Certificates are available for retrieval in only those cases for which the Subscriber's consent has been obtained. [Directive Annex II item (l)].

c) The CSP shall make available to Relying Parties the terms and conditions regarding the use of the certificate including: [Directive Annex II (k)]:

- any limitations on its use
- when the relying party is considered to "reasonably rely" on the certificate (see 6.3);
- limitations of liability (see 5.3)
- the procedures for complaints and dispute settlements;
- the period of time which CSP event logs (see 7.4.11) are maintained;
- procedures for complaints and dispute settlement;
- the applicable legal system, and
- the Qualified Certificate Policy being applied,
- If the CSP has been certified to be conformant with the identified Qualified Certificate Policy, and if so through which scheme.

d) The information identified in (c) above shall be available through a durable means of communication, which may be transmitted electronically, and in readily understandable language.

Note: A Model PKI Disclosure Statement which may be used as the basis of such a communication is given in Annex B.

e) The information identified in (b) and (c) above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which is not under the control of the CSP, this information service may be unavailable for a maximum period of time as denoted in the Certification Practice Statement.

f) This information shall be publicly and internationally available.

7.3.5 Certificate Revocation & Suspension

The Certification Authority shall ensure that certificates are revoked in a timely manner based on authorised and validated certificate revocation requests. [Directive Annex II (b)]

In particular:

Revocation Management

a) Requests and reports relating to revocation (e.g. due to compromise of Subscriber's private key) shall be processed immediately,

b) Requests and reports relating to revocation shall be validated.

c) A certificate's revocation status may be set to suspended whilst the revocation is being validated.

d) The Subscriber, which is the subject of a revoked or suspended certificate, shall be informed of the change of status of its certificate.

e) Once a Certificate is revoked it cannot be reinstated.

f) Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used these shall be published at least daily and:

- every CRL shall state a time for next CRL issue; and
- a new CRL may be published before the stated time of the next CRL issue.

g) Revocation management services shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which is not under the control of the CSP, this information service may be unavailable for a maximum period of time as denoted in the Certification Practice Statement.

Revocation Status

h) Revocation status information, shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which is not under the control of the CSP, this information service may be unavailable for a maximum period of time as denoted in the Certification Practice Statement.

Note: Revocation status information may be provided, for example, using on-line certificate status service or through distribution of CRLs through a repository.

i) Revocation status information shall be publicly and internationally available.

7.4 CSP Management and Operation

7.4.1 Security Management

The Certification Authority shall ensure that [Directive Annex II (e) 2nd part]:

i) management direction and support for information security is provided;

ii) information security is properly managed within the organization;

iii) the security of CSP facilities, systems and information assets accessed by third parties is maintained; and

iv) the security of information is maintained when the responsibility for CSP functions has been outsourced to another organization or entity.

In particular:

CSP General

a) The CSP management information security forum shall define an information security policy and ensure it is published and communicated to all employees.

b) The information security infrastructure necessary to manage the security within the CSP shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the CSP management forum.

Note: See BS 7799 for guidance on information security management including information security infrastructure, management information security forum and information security policies.

c) The CSP shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to third parties. Responsibilities of third parties shall be clearly defined by the CSP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the CSP. The CSP shall retain responsibility for the disclosure of relevant practices of all parties.

Registration, Certificate Generation, Revocation Management

d) The technical security controls and operating procedures for systems providing these certification services shall be documented and maintained. This documentation (commonly called a System Security Policy) should identify all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats. It should describe the rules, directives and procedures regarding how the specified services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

7.4.2 Asset Classification and Management

The Certification Authority shall ensure that CSP assets and information receive an appropriate level of protection. [Directive Annex II (e)]

In particular:

CSP General

a) The CSP shall implement information classification and associated protective controls for information that take account of security, regulatory and business needs for sharing or restricting information, and the impacts associated with such needs.

7.4.3 Personnel Security

The Certification Authority shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CSP's operations. [Directive Annex II (e) 1st part]

In particular:

CSP General

a) The CSP shall employ personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;

Note: CSP staff should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two.

b) Security roles and responsibilities, as specified in the CSP's security policy, shall be documented in job descriptions.

c) Staffing: CSP staff (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and CSP specific functions. These should include skills and experience requirements.

d) Staff shall exercise administrative and management procedures and processes that are adequate and which correspond to recognised standards.

Note: See [BS 7799] for guidance.

Registration, Certificate Generation, Subscriber SCD Provision, Revocation Management

e) Managerial staff shall possess expertise in the electronic signature technology and familiarity with proper security procedures for personnel with security responsibilities.

f) All CSP staff in trusted roles shall be free from conflicting interests.

Note: Trusted roles include security officer with overall responsibility for administering the implementation of the security practices defined in the Certification Practice Statement, the administrators in charge of the registration, certificate generation service and revocation management services, operators for systems carrying our registration, certificate generation service and revocation management services.

g) CSP staff shall be formally appointed to trusted roles by an appropriate senior management group

h) The CSP shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which effects his/her suitability for the position. Staff shall not have access to the trusted functions until any necessary checks are completed.

Note: In some countries it may not be possible for CSP to obtain information on passed convictions. However, the employed may be able to ask the candidate to provide such information and turn down an application in case of refusal.

7.4.4 Physical and Environmental Security

The Certification Authority shall ensure that:

i) physical access to facilities concerned with Certificate Generation, Subscriber SCD Provision, and Revocation Management services is limited to properly authorized individuals and certificate issuance facilities are protected from environmental hazards;

ii) loss, damage or compromise of assets and interruption to business activities are detected, and as far as possible, prevented; and

iii) compromise or theft of information and information processing facilities are detected and as far as possible prevented.

In particular:

Certificate Generation, Subscriber SCD Provision & Revocation Management

a) The facilities concerned with key management, certificate issuance and certificate revocation status services shall be operated in an environment which physically protects the services from compromise through unauthorised access to systems or data.

b) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate management service. Any parts of the premises shared with other businesses shall be outside this perimeter.

c) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CSP's physical and environmental security programs concerned with Certificate Generation, Subscriber SCD Provision & Revocation Management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking, entering, and disaster recovery, etc.

d) Controls shall be implemented to protect against equipment, information and software relating to the CSP services being taken off-site without authorization.

7.4.5 Operations Management

The Certification Authority shall ensure that [Directive Annex II (e)]:

i) the correct and secure operation of CSP systems is ensured;

ii) the risk of CSP systems failure is minimized;

iii) the integrity of CSP systems and information is protected against viruses and malicious software;

iv) damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures;

v) media are securely handled to protect media from damage, theft and unauthorized access.

In particular:

CSP General

Note: Every member of staff with management responsibilities is responsible for planning and efficiently implementing the certificate policy and associated practices as documented in the Certification Practice Statement.

a) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of certification services.

Media handling and security

b) All media shall be handled securely in accordance with requirements of the information classification scheme (see 7.4.2). Media containing sensitive data shall be securely disposed of when no longer required.

System Planning

c) Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Incident reporting and response

d) Parties should act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

Note: The responsibilities of Subscribers are defined in the terms conditions as defined in 7.3.1.

Registration

e) Registration shall be operated by responsible and suitably skilled staff..

Certificate Generation, Revocation Management

Operations procedures and responsibilities

f) Certificate Generation and Revocation Management shall be operated by responsible and suitably skilled staff..

g) CSP security operations shall be separated from normal operations.

Note: CSP security operations' responsibilities include:

- operational procedures and responsibilities
- secure systems planning and acceptance
- protection from malicious software
- housekeeping
- network management
- active monitoring of audit journals, event analysis and follow-up
- media handling and security

- data and software exchange

These responsibilities will be managed by CSP security operations, but, may actually be performed by, non-specialist, operational staff (under supervision); as defined within the appropriate security policy, and, roles and responsibility documents.

7.4.6 System Access Management

The Certification Authority shall ensure that CSP system access is limited to properly authorized individuals [Directive Annex II (f)].

Note: Requirement for trustworthy systems indicated below may be fulfilled using, for example, using systems conforming to the protection profiles defined in [Trustworthy Systems].

In particular:

CSP General

a) Controls (e.g., firewalls) shall be implemented to protect the CSP's internal network domains from external network domains accessible by third parties

Note: Firewalls should be configured to prevent protocols and accesses not required for the operation of the CSP.

b) Sensitive data shall be protected when exchanged over networks which are not secure.

Note: Sensitive data includes Subscriber registration information.

c) The CSP shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.

d) The CSP shall ensure access to information and application system functions are restricted in accordance with the access control policy and that the CSP system provides sufficient computer security controls for the separation of trusted roles identified in CSP's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs are restricted and tightly controlled.

e) Users shall be successfully identified and authenticated to the application before all other interactions with the application.

f) Users shall be accountable for their activities, for example by retaining event logs (see 7.4.11).

g) Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorised users.

Note: Sensitive data includes Subscriber registration information.

Registration

h) Registration shall operate on a trustworthy system.

Certificate Generation

i) The CSP shall ensure that local network components (e.g. routers) are kept in a secured environment and their configurations periodically audited.

j) Continuous monitoring and alarm facilities shall be provided to enable the CSP to detect, register and react in a timely manner upon any authorised and/or irregular attempts to access its resources.

Note: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

k) Certificate Generation shall operate on a trustworthy system.

Subscriber SCD Provision

l) Subscriber SCD Provision shall operate on a trustworthy system

Certificate Dissemination

m) Certificate Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

Revocation Management

n) Revocation Management shall operate on a trustworthy system.

o) Continuous monitoring and alarm facilities shall be provided to enable the CSP to detect, register and react in a timely manner upon any authorised and/or irregular attempts to access its resources.

Note: This may used, for example, an intrusion detection system, access control monitoring and alarm facilities.

Revocation Status

p) Revocation Status application shall enforce access control on attempts to modify revocation status information.

7.4.7 Systems Development and Maintenance

The Certification Authority shall ensure that CSP systems development and maintenance activities are properly authorized to maintain CSP system integrity [Directive Annex II (f)].

In particular:

CSP General

a) Prior to deployment of any operational software, the CSP shall perform adequate checks to ascertain that the integrity of the software has not been compromised in any way. This includes ensuring that products are protected against modification so that they cannot be used to perform functions other than those for which they have been designed.

b) Change control procedures exist for releases, modifications and emergency software fixes for any operational software.

7.4.8 Business Continuity Management and Incident Handling

The Certification Authority shall ensure [Directive Annex II (a)]:

i) that operations can be quickly restored in the event of a disaster;

ii) that operations can be quickly restored in the event of the compromise of the Certification Authority's private signing key; and

In particular:

CSP General

CA Key compromise

a) The CSP's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a Certification Authority's private signing key as a disaster.

Revocation Management

b) When informed of a compromise of another CA's key, for which a CA Certificate has been issued, that CA Certificate shall be revoked.

Revocation Status

c) In such case the CSP shall as a minimum provide the following undertakings:

- Inform all Subscribers, relying parties and other CSPs with which the CSP has agreements or other form of established relations of the compromise.
- Indicate that Certificates and revocation status information issued using this CA key may no longer be valid.

7.4.9 CA Termination

The Certification Authority shall ensure that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of the CSP's services, and in particular ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings [Directive Annex II (i)].

In particular:

CSP General

a) The CSP shall maintain procedures for the termination, notification of affected entities, and for transferring archived CSP event logs to a custodian

b) Before the CSP terminates its services the following procedures shall be completed as a minimum:

- Inform all Subscribers, relying parties and other CSPs with which the CSP has agreements or other form of established relations.
- CSP shall terminate all authorization of subcontractors to act on behalf of the CSP in the process of issuing certificates.
- The CSP shall perform necessary undertakings to maintain event log archives according to 7.4.11
- Certification Authority private keys are destroyed, or withdrawn from use, as defined in 7.2.6.

c) The CSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the CSP becomes bankrupt or for other reasons is unable to cover the costs by itself.

7.4.10 Monitoring and Compliance Checking

The Certification Authority shall ensure that:

i) the CSP complies with legal requirements;

ii) compliance with the CSP's security policies and procedures is ensured;

iii) the effectiveness of the system audit process is maximised and interference to/from the system audit process is minimised.

In particular:

CSP General

Compliance with legal requirements

a) Important records shall be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities

b) The CSP shall ensure that the requirements of the European Data Protection Directive, as implemented through National legislation, are met.

c) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

d) Users must be assured that the information they contribute to the CSP is completely protected from disclosure unless with their agreement or by court order or other legal requirement.

7.4.11 Event Logging

The Certification Authority shall ensure that [Directive Annex II (i)]:

i) significant CSP environmental, key management, and certificate management events are accurately and completely logged

ii) the confidentiality and integrity of current and archived event logs are maintained

iii) event logs are completely and confidentially archived in accordance with disclosed business practices

iv) event logs can be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings

v) event logs are held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures

Note 1) The duration of the record retention period is difficult to pinpoint, and requires weighing the need for reference to the records against the burden of keeping them. The records could be needed at least as long as a transaction relying on a valid certificate can be questioned. For most transactions, statutes of limitation will eventually place a transaction beyond dispute. However, for some transactions such as real property conveyances, legal repose may not be realised until after a lengthy time elapses, if ever.

2) Where differing periods of times are applied to certificates used for different purposes they shall be clearly identified as different classes of certificate (e.g. using different Specific Qualified Certificate Policy Identifiers).

vi) the precise time of events is recorded.

In particular:

General

a) The following events shall be logged in a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Note: This may be achieved, for example, through the use of write only media, a record of each removable media used and the use of off site backup.

b) The specific events and data to be logged shall be documented by the CSP.

Registration

c) The CSP shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged;

d) The CSP shall ensure that all registration information including the following is recorded:

A) type of identification document(s) presented by the applicant;

B) record of unique identification data, numbers, or a combination thereof (e.g., applicant's drivers license number) of identification documents, if applicable;

C) storage location of copies of applications and identification documents

D) identity of entity accepting the application;

E) method used to validate identification documents, if any; and

F) name of receiving Certification Authority and/or submitting Registration Authority, if applicable.

e) The CSP shall ensure that privacy of Subscriber information is maintained.

Certificate Generation

f) The CSP shall log all events relating to the life-cycle of CA keys.

g) The CSP shall log all events relating to the life-cycle of certificates.

h) The CSP shall not record the plain text value of any private keys.

Subscriber SCD Preparation

i) The CSP shall log all events relating to the life cycle of keys managed by the CSP, including any Subscriber keys generated by the CSP.

j) If applicable, the CSP shall log all events relating to the preparation of Secure Signature Creation Devices.

Revocation Management

k) The CSP shall ensure that all requests and reports relating to revocation, as well as the resulting action, are logged.

7.5 Organisational

The Certification Authority shall ensure that the CSP organisation is reliable. [Directive Annex II (a)].

In particular that:

CSP General

a) the CSP is a legal entity;

b) the CSP has quality systems and information security management systems appropriate for the certification services it is providing;

c) the CSP has adequate arrangements to cover liabilities arising from its operations and/or activities, in particular to bear the risk of liability for damages;

d) it has the financial stability and resources required to operate in conformity with this policy;

Note: "sufficient": As between a CSP and its client, the Subscriber, the sufficiency of the CSP's financial basis is apparent from their willingness to do business with each other in a setting where the Subscriber could have retained the services of another. In relation to third parties, however, the sufficiency of a CSP's financial basis should be evaluated according to a reasonableness standard.

e) it employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide certification services;

f) it has policies and procedures for the resolution of complaints and disputes from customers received from customers or other parties about the provisioning of electronic trust services or any other related matters;

g) it has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

h) It must have no record of prior intentional wrongdoing.

Certificate Generation, Revocation Management

i) the CSP is independent of others for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive and staff, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides;

j) the CSP has a documented structure which safeguards impartiality of operations;

8 Framework for the Definition of Other Qualified Certificate Policies

Note: This section is NOT applicable to either Qualified Certificate Policies identified in section 5: QCP Public, and QCP Public + SSCD.

8.1 Qualified Certificate Policy Management

The Certification Authority shall ensure that the Certificate Policy is effective.

In particular:

a) There shall be a Policy Management Authority with final authority and responsibility for specifying and approving the Qualified Certificate Policy.

b) A risk assessment shall be carried out to evaluate business and determine the security requirements to be included in the Qualified Certificate Policy for all the areas identified above.

c) Certificate Policy(s) shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the Qualified Certificate Policy.

d) A defined review process shall exist to ensure that the Qualified Certificate Policy are supported by the CSPs Certification Practices Statement.

e) The CSP shall make available the Qualified Certificate Policies supported by the CSP to all appropriate Subscribers and Relying Parties.

f) Revisions to Qualified Certificate Policies supported by the CA shall be made available to Subscribers and Relying Parties.

g) The Qualified Certificate Policy shall incorporate, or further constrain, all the requirements identified in section 6 and 7 with the exclusions indicated below. In the case of any conflict the requirements of this standard prevail.

8.2 Exclusions for Non Public QCPs

Certificates issued under a Qualified Certificate Policy for Qualified Certificates not issued to the public need not apply the following Qualified Certificate Policy requirements:

Note: A CA is not considered to be issuing Qualified Certificates to the public if the certificates are restricted to uses governed by voluntary agreements under private law among participants.

a) liability as defined in 5.3

b) independence of providers of Certificate Generation and Revocation Management services as defined in 7.5 (i) and (j).

c) Dissemination of certificates publicly as defined in 7.3.4 (f)

d) Public availability of revocation status information as defined in 7.3.5(i).

8.3 Additional Requirements

Subscribers and Relying Parties shall be informed, as part of implementing the requirements defined in 7.3.1 (b) and 7.3.5 (iii):

a) if the policy is not for public use and whether exclusions identified in 8.2 apply;

b) whether the policy includes requirements for use a SSCD;

c) the ways in which the specific policy adds to or further constrains the requirements of the Qualified Certificate Policy as defined in the current document.

8.4 Conformance

The CSP shall only claim conformance to the current document and the applicable Qualified Certificate Policy:

a) if the CSP has been certified to be conformant to the Qualified Certificate Policy; or

b) if the CSP claims conformance to the Qualified Certificate Policy and makes available on request the evidence to support the claim of conformance.

A conformant CSP must demonstrate that:

a) it meets its obligations as defined in 6.1,

b) it has implemented controls which meet the requirements specified in section 7, excluding

- those specified in 5.4.2 (b) if the CSP does not require use of a SSCD
- those specified in 8.2 if the CSP is not providing a service to the public.

c) uses a Qualified Certificate Policy which meets the requirements specified in 8.1,

d) it has implemented controls which meet the additional requirements of the Qualified Certificate Policies employed.

e) it meets the additional requirements specified in 8.3.

Annex A (Informative): Potential Liability in the Use of Electronic Signatures

This annex provides a conceptual framework considering of the potential liability of various actors involved in issuing and using Qualified Certificates as defined in the Directive on Electronic Signatures [Directive].

The liability requirements of CSPs issuing Qualified Certificates to the public are stated in the Directive as follows:

Directive - Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.

The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

A CA is not considered to be issuing Qualified Certificates to the public if the certificates are restricted to uses governed by voluntary agreements under private law among participants.

Liability in most cases is governed by national law, which varies across the 15 Member States of the EU. Even where liability is governed by the Electronic Signatures Directive (the "Directive"), reference must be had to Member State implementation of its liability provisions. Therefore, any entity thinking of engaging in the provision of certification services should consult local counsel in the countries in which it intends to operate to learn where possible exposure exists.

I. Liability of CSPs

A. Liability of CSPs to Relying Parties Governed by the Directive

Consideration of liability under the Directive begins with Recital 22, which provides that "[c]ertification service providers providing certification services to the public are subject to national rules regarding liability". Thus, CSP liability is governed by Member State law.

Article 6 of the Directive requires Member States to incorporate certain minimum liability provisions in national law. These provisions apply to CSPs that issue Qualified Certificates to the public. They do not apply to CSPs operating in closed systems or issuing non-Qualified Certificates. In particular, Article 6 requires a CSP issuing Qualified Certificates to the public to ensure

- the accuracy of the information contained in the certificate at the time of issuance;
- that the certificate contains all information required for a Qualified Certificate at the time of issuance;
- that the signatory holds the signature creation data corresponding to the signature verification data identified in the certificate;
- that the signature creation data and signature verification data work together where the CSP generated both of them; and
- that it registers any revocation of the certificate.

A CSP is liable for damages resulting from failures to fulfil these obligations unless it has not acted negligently. In other words, liability is predicated on the CSP making an error, and that error being the result of negligence on the part of the CSP. (The structure of the Directive implies that the liability provisions also reach reckless and intentional misconduct on the part of the CSP.) Thus, to avoid liability, a CSP must prove only that its own actions were not negligent. Failures on the part of the relying party – for example, to check a revocation list – should not give rise to liability on the part of the CSP. Indeed, some failures on the part of the relying party may render its reliance on the certificate unreasonable under the circumstances, relieving the CSP of liability under the Directive.

The Directive permits CSPs to limit their liability by limiting both the use of a certificate and the value of transactions for which it is valid. It is important that these limits be conspicuous, or they may be held invalid under consumer protection or general contract law. These limits also need to be placed on closed system certificates, to protect them from "leaking" into other environments.

Note that because liability limits is on a transaction basis, and the CSP may not be able to control the number of transactions for which it becomes liable, the CSP may not have control over its overall liability.

Damages are governed by Member State law. Generally, in order for negligence to give rise to damages, the negligence must be the cause of the loss. For example, where a CSP negligently fails to issue a timely revocation list, but the relying party fails to check whether the revocation list exists, the legal cause of any loss suffered by the relying party probably is not the CSP's negligence, but the relying party's failure to check. Had the relying party checked, it would have noticed that the revocation list was out of date and acted accordingly. The result is less clear, however where the CSP negligently issues an inaccurate revocation list that the relying party fails to check. In that case, the CSP could argue that the relying party's failure to check was the cause of the loss, as the relying party was not reasonable in relying on a certificate that it had not checked. The relying party could argue, however, that its failure to check did not contribute to the loss, on the theory that, had it checked, it would not have realised that the certificate had been revoked.

B. Liability of CSPs to Relying Parties Not Governed by the Directive

Where a CSP does not fall into the liability scheme established by the Directive, either because it is not issuing Qualified Certificates, or not issuing them to the public, liability generally derives from one of two sources: contract or statutory law. In closed systems, the CSP will likely have a contractual relationship with the relying party. In that case, questions of liability will be governed in the first instance by the contract. Where consumers are involved, statutory protections may also apply.

In open systems, the relying party may be designated a third party beneficiary of the contract between the CSP and the subscriber; thus, a CSP's liability vis-à-vis the relying party will be governed by its contract with the subscriber. Whether a contract creates liabilities to third parties may depend upon its interpretation in light of relevant caselaw and statutory provisions. Where the contract between the CSP and the subscriber does not designate the relying party as a third party beneficiary, however, national law will be the only source of a CSP's liability to third parties.

C. Liability of CSPs to Subscribers

A CSP's liability to a subscriber for failure to provide service (such as not issuing timely revocation lists) or for improperly suspending or revoking a certificate is governed by the contract between the CSP and the

subscriber. If the subscriber is a consumer, both the Unfair Contract Terms Directive (93/13/EEC) and the Distance Selling Directive (97/7/EC) apply, and will constrain the CSPs ability to limit its liability. The Unfair Contract Terms Directive prohibits terms that have not been individually negotiated and which cause a significant imbalance in the parties' rights and obligations to the detriment of the consumer. The Distance Selling Directive applies to contracts where the supplier and the consumer do not meet in person during the formation of the contract.

In a case where the CSP obtained the subscriber by making false promises, it may be liable to the subscriber under the law of fraud. However, a fraud claim probably would require proof that the CSP engaged in wilful misconduct. In some Member States, it is possible that CSPs, as a partially-regulated business, might be subject to heightened duties of care or fiduciary responsibilities, as are doctors and lawyers. In that case, a remedy similar to malpractice might be available either at common law or by statute for the negligence of the CSP in the performance of the duties it owes to the subscriber.

CSPs also face liability to subscribers if they do not comply with data protection laws enacted to implement the Framework Data Protection Directive (95/46/EC) and Article 8 of the Electronic Signatures Directive (99/93). At the same time, CSPs may be required to disclose personal data to the authorities, particularly where the subscriber uses a pseudonym.

D. Liability of CSPs to Unrelated Third Parties

A CSP could be liable to an unrelated third party if the CSP issues a certificate to a subscriber in the name of the third party. Liability in this case would not be governed by the Directive, because the unrelated third party would not have reasonably relied on the certificate. Nor would liability be governed by contract law, as there is no contract between the CSP and the third party. However, Member States may have provided statutory or tort/delict law remedies for this type of harm – for example, an action against a person who aids in the theft of identity. In these situations, liability is likely to be predicated on the negligence or wilful misconduct of the CSP; however, some legal systems might choose to impose strict liability for issuance of certificates to a subscriber in the name of an unrelated third party.

II. Liability of Subscribers

A. Liability of Subscriber to CSP

The liability, if any, of a subscriber to a CSP for the provision of false, misleading, or inaccurate information is governed by the contract between the subscriber and the CSP. If the subscriber intentionally provided false or misleading information, it may be liable to the CSP under the law of fraud.

B. Liability of Subscriber to Relying Party

The liability, if any, of a subscriber to the relying party for the provision of false, misleading, or inaccurate information to a CSP that results in the issuance of a certificate upon which the relying party relies is governed by the contract between the subscriber and the relying party. If the subscriber intentionally provided false or misleading information, it may be liable to the relying party under the law of fraud. The subscriber is also liable for the acts of its agents acting within express or implied authority, and in some circumstances may be liable for the acts of an agent possessing apparent authority to act on its behalf based on the subscriber's manifestations to the relying party.

C. Liability of Subscriber to Unrelated Third Party

The liability of a subscriber to an unrelated third party for providing information to a CSP that results in a certificate being issued to the subscriber in the name of the third is governed by a Member State's statutory, tort/delict, or fraud law. In most cases, the attempt to impersonate the third party will be intentional, and thus actionable as fraud. Member States may also have created statutory or common law tort/delict remedies for theft of identity.

Annex B (Informative): Model PKI Disclosure Statement

B.1 Introduction

The proposed Model PKI Disclosure Statement is designed for use by a CSP issuing certificates as a supplemental instrument of disclosure and notice. A PKI Disclosure Statement may assist a CSP to respond to regulatory requirements and concerns, particularly those related to consumer deployment and in particular meet the requirements of the Directive Annex II. Further, the aim of the Model PKI Disclosure Statement is to foster industry "self-regulation" and build consensus on those elements of a Certificate Policy and/or Certification Practice Statement that require emphasis and disclosure.

Although Certificate Policy and Certification Practice Statement documents are essential for describing and governing certificate policies and practices, many PKI users, especially consumers, find these documents difficult to understand. Consequently, there is a need for a supplemental and simplified instrument that can assist PKI users in making informed trust decisions. Consequently, a PKI Disclosure Statement is not intended to replace a Certificate Policy or Certification Practice Statement.

This Annex provides an example of the structure for a PKI Disclosure Statement, illustrating the harmonized set of statement types (categories) that would be contained in a deployed.

B.2 The PDS structure

The PDS contains a section for each defined statement type. Each section of a PDS contains a descriptive statement, which MAY include hyperlinks to the relevant Certificate Policy / Certification Practice Statement sections.

STATEMENT TYPES	**STATEMENT DESCRIPTIONS**	**Specific Requirements of Qualified Certificate Policy (see 7.3.1(b) and 7.3.4(c))**
CSP contact info:	The name, location and relevant contact information for the CA/PKI.	
Certificate type, validation procedures and usage:	A description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage.	Any limitations on its use; Whether the policy is for Qualified Certificate issued to the public.
Reliance limits:	The reliance limits, if any.	Indication that the certificate is only for use with electronic signatures the period of time which CSP event logs (see 7.4.11) are maintained (and hence are available to provide supporting evidence)
Obligations of Subscribers:	The description of, or reference to, the critical Subscriber obligations.	The Subscriber's obligations as defined in 6.2.2.
Certificate status checking obligations of Relying Parties:	The extent to which Relying Parties are obligated to check certificate status, and references to further explanation.	When the relying party is considered to "reasonably rely" on the certificate (see 6.2.3);

Limited warranty & disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see 5.3)
Applicable agreements, Certification Practice Statement, Certificate	Identification and references to applicable agreements, Certification Practice Statement, Certificate Policy and other relevant documents.	Qualified Certificate Policy being applied
Privacy policy:	A description of and reference to the applicable privacy policy.	Note: CSP's under this policy are required to comply with the requirements of Data Protection Legislation.
Refund policy:	A description of and reference to the applicable refund policy.	
Applicable law, complaints and dispute resolution:	Statement of the choice of law, complaints procedure and dispute resolution mechanisms (anticipated to often include a reference to the ICC's arbitration services).	The procedures for complaints and dispute settlements; The applicable legal system;
CA and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	If the CSP has been certified to be conformant with a Qualified Certificate Policy, and if so through which scheme.

Annex C (informative): Electronic Signature Directive and Qualified Certificate Policy Cross-reference

The following table identifies how the security controls objectives and other parts of the Generic Qualified Certificate Policy defined in the current document addresses the requirements of CSPs issuing Qualified Certificates as defined in Annex II of the Directive:

Directive Annex II requirement	Qualified Certificate Policy Reference
a) demonstrate the reliability necessary for providing certification services;	7.1, 7.4.8, 7.4.10, 7.5
b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;	7.3.4, 7.3.5
c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;	7.4.11
d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a Qualified Certificate is issued;	7.3.1, 7.3.2
e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;	7.4.1 to 7.4.5
f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the processes supported by them;	7.4.6, 7.4.7, 7.2
g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;	7.2, 7.3.3, 7.2.8
h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;	7.5
i) record all relevant information concerning a Qualified Certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;	7.4.11, 7.4.9

j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;	7.2.8
k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature, inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;	7.3.1, 7.3.4
l) use trustworthy systems to store certificates in a verifiable form so that: - only authorised persons can make entries and changes, - information can be checked for authenticity, - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and – any technical changes compromising these security requirements are apparent to the operator.	7.3.4, 7.3.5

Annex D (Informative): RFC 2527 and Qualified Certificate Policy Cross Reference

Table 1: Cross-Reference RFC 2527 Sections and Policy References

RFC 2527	Qualified Certificate Policy Reference
1 INTRODUCTION	
1.1 Overview	5.1
1.2 Identification	5.2
1.3 Community and Applicability	5.3
1.4 Contact Details	5.4
2 GENERAL PROVISIONS	
2.1 Obligations	6.1, 6.2, 6.3
2.2 Liability	6.4
2.3 Financial Responsibility	7.5
2.4 Interpretation and Enforcement	5.4
2.5 Fees	N/A
2.6 Publication and Repositories	7.3.4, 7.3.5
2.7 Compliance Audit	7.4.10
2.8 Confidentiality Policy	7.3.1
2.9 Intellectual Property Rights	N/A
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Initial Registration	7.3.1
3.2 Routine Rekey	7.3.2
3.3 Rekey After Revocation -- No Key Compromise	7.3.2
3.4 Revocation Request	7.3.5
4 OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1
4.2 Certificate Issuance	7.3.3
4.3 Certificate Acceptance	7.3.1
4.4 Certificate Suspension and Revocation	7.3.5
4.5 Security Audit Procedures	7.4.10
4.6 Records Archival	7.4.11
4.7 Key Changeover	7.3.2
4.8 Compromise and Disaster Recovery	7.4.8
4.9 CA Termination	7.4.9
5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	
5.1 Physical Security Controls	7.4.4

RFC 2527	Qualified Certificate Policy Reference
5.2 Procedural Controls	7.4.1
5.3 Personnel Security Controls	7.4.3
6 TECHNICAL SECURITY CONTROLS	
6.1 Key Pair Generation and Installation	7.2.8, 7.2.9
6.2 Private Key Protection	7.2.8
6.3 Other Aspects of Key Pair Management	7.2
6.4 Activation Data	7.2.9
6.5 Computer Security Controls	7.4.6
6.6 Life Cycle Security Controls	7.3
6.7 Network Security Controls	7.4.6
6.8 Cryptographic Module Engineering Controls	7.2
7 CERTIFICATE AND CRL PROFILES	
7.1 Certificate Profile	N/A
7.2 CRL Profile	N/A
8 SPECIFICATION ADMINISTRATION	
8.1 Specification Change Procedures	7.1
8.2 Publication and Notification Procedures	7.1
8.3 Certification Practice Statement Approval Procedures	7.1

Annex E (Informative): Bibliography

Reference to all the relevant national scheme documentation to be inserted here.

ISO/IEC 15945 “Information technology - Security techniques - Specification of TTP services to support the Application of Digital Signatures”

ISO/IEC 14516 “Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services”.

ISO/IEC 13335 “Guidelines on the management of IT security”.

ANS X9.79 Public Key Infrastructure – Practices and Policy Framework