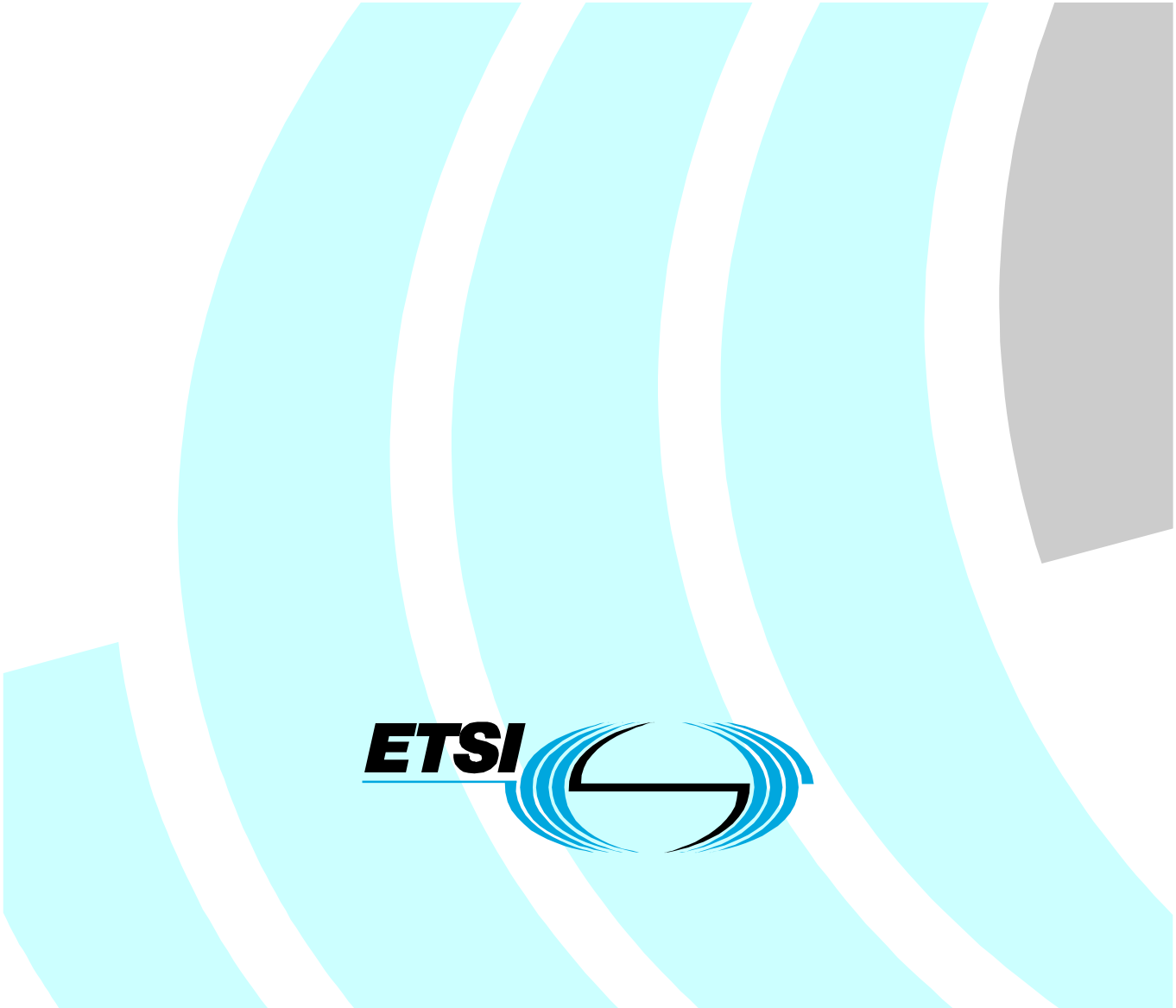
ETSI TS 101 456 V1.2.1 (2002-04)

Technical Specification

Policy requirements for certification authorities issuing qualified certificates



Reference
RTS/SEC-004013

Keywords
IP, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Security (SEC).

Introduction

Electronic commerce is emerging as a 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 a certification-service-provider issuing certificates, commonly called a certification authority.

For users of electronic signatures to have confidence in the authenticity of the electronic signatures they need to have confidence that the CA has properly established procedures and protective measure in order to minimize the operational and financial threats and risks associated with public key crypto systems.

The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive specifies requirements for qualified certificates. Annex II of the Directive specifies requirements on certification-service-providers issuing qualified certificates (i.e. certification authorities issuing **qualified** certificates). The present document specifies baseline policy requirements on the operation and management practices of certification authorities 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 present document.

1 Scope

The present document specifies policy requirements relating to certification authorities (CAs) issuing qualified certificates (termed certification-service-providers issuing qualified certificates in the Directive [1]). It defines policy requirements on the operation and management practices of certification authorities issuing qualified certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures.

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.

The policy requirements relating to the CA includes requirements on the provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and if required, signature-creation device provision. Other certification-service-provider functions such as time-stamping, attribute certificates and confidentiality support are outside the scope of the present document. In addition, the present document does not address requirements for certification authority certificates, including certificate hierarchies and cross-certification. The policy requirements are limited to requirements for the certification of keys used for electronic signatures.

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 [1]). It specifically addresses the requirements for CAs issuing qualified certificates in accordance with annexes I & II of this Directive [1]. Requirements for the use of secure-signature-creation devices as specified in annex III, which is also a requirement for electronic signatures in line with article 5.1, is an optional element of the policy requirements specified in the present 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.

The present document may be used by competent independent bodies as the basis for confirming that a CA meets the requirements for issuing qualified certificates.

It is recommended that subscribers and relying parties consult the certification practice statement of the issuing CA to obtain further details of precisely how a given certificate policy is implemented by the particular CA.

The present document does not specify how the requirements identified may be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE: See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance".

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 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 present document.

[2] IETF RFC 2527 (1999): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[3] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[4] 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.

[5] FIPS PUB 140-1 (1994): "Security Requirements For Cryptographic Modules".

[6] ETSI TS 101 862: "Qualified certificate profile".

[7] ISO/IEC 15408 (1999)(parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

[8] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

advanced electronic signature: electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable (see Directive 1999/93/EC).

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it (see ITU-T Recommendation X.509)

certificate policy: named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements (see ITU-T Recommendation X.509)

NOTE: See clause 4.3 for explanation of the relative role of certificate policies and certification practice statement.

certification authority: authority trusted by one or more users to create and assign certificates (see ITU-T Recommendation X.509)

NOTE: A certification authority is a certification-service-provider issuing certificates. See clause 4.2 for further explanation of the concept of certification authority.

certification practice statement: statement of the practices which a certification authority employs in issuing certificates (see IETF RFC 2527)

certification-service-provider (CSP): entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (see Directive 1999/93/EC)

NOTE: The present document is concerned with certification service providers issuing qualified certificates (or component services for issuing qualified certificates - see clause 4.1). The present document is not concerned with other types of CSP functions such as time-stamping and key escrow.

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data (see Directive 1999/93/EC)

qualified certificate: 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 1999/93/EC)

Qualified Certificate Policy (QCP): certificate policy which incorporates the requirements laid down in annex I and annex II of the Directive 1999/93/EC

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 1999/93/EC

relying party: recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate (see IETF 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 (see Directive 1999/93/EC)

NOTE: In qualified certificates based on public key cryptography, as covered by the present document, the signature-creation data is, for example, a private key. Hence, within the present document the term private key is used for the signature-creation data.

signature-creation device: configured software or hardware used to implement the signature-creation data (see Directive 1999/93/EC)

secure-signature-creation device: signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC

signature-verification data: data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (see Directive 1999/93/EC)

NOTE: In qualified certificates based on public key cryptography, as covered by the present document, the signature-verification data is, for example, a public key. Hence within the present document the term public key is used for the signature-verification data.

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subscriber: entity subscribing with a Certification Authority on behalf of one or more subjects

NOTE: The subject may be a subscriber acting on its own behalf.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
SSCD	Secure Signature Creation Device

4 General concepts

4.1 Certification authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the certification authority. The certification authority has overall responsibility for the provision of the certification services identified in clause 4.1. The certification authority's key is used to sign the qualified certificates and it 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, the certification authority always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. For example, a certification authority may sub-contract all the component services, including the certificate generation service. However, the key used to generate the certificates is identified as belonging to the CA, and the CA maintains overall responsibility for meeting the requirements defined in the present document and liability for the issuing of certificates to the public as required in the Directive [1].

A certification authority is a certification-service-provider, as defined in the Directive [1], which issues certificates.

4.2 Certification services

The service of issuing qualified certificates is broken down in the present 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 subject. The results of this service are passed to the certificate generation service.

NOTE 1: This service includes proof of possession of non-CA generated subject private keys.

- **Certificate generation service:** creates and signs certificates based on the identity and other attributes verified by the registration service.

- **Dissemination service:** disseminates certificates to subjects, and if the subject consents, to relying parties. This service also disseminates the CA's terms and conditions, and any published policy and 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:

- **Subject device provision service:** prepares and provides a signature-creation device to subjects.

NOTE 2: Examples of this service are:

- a service which generates the subject's key pair and distributes the private key to the subject;
- a service which prepares the subject's secure-signature-creation device (SSCD) and device enabling codes and distributes the SSCD to the registered subject.

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

The following diagram illustrates the interrelationship between the services.

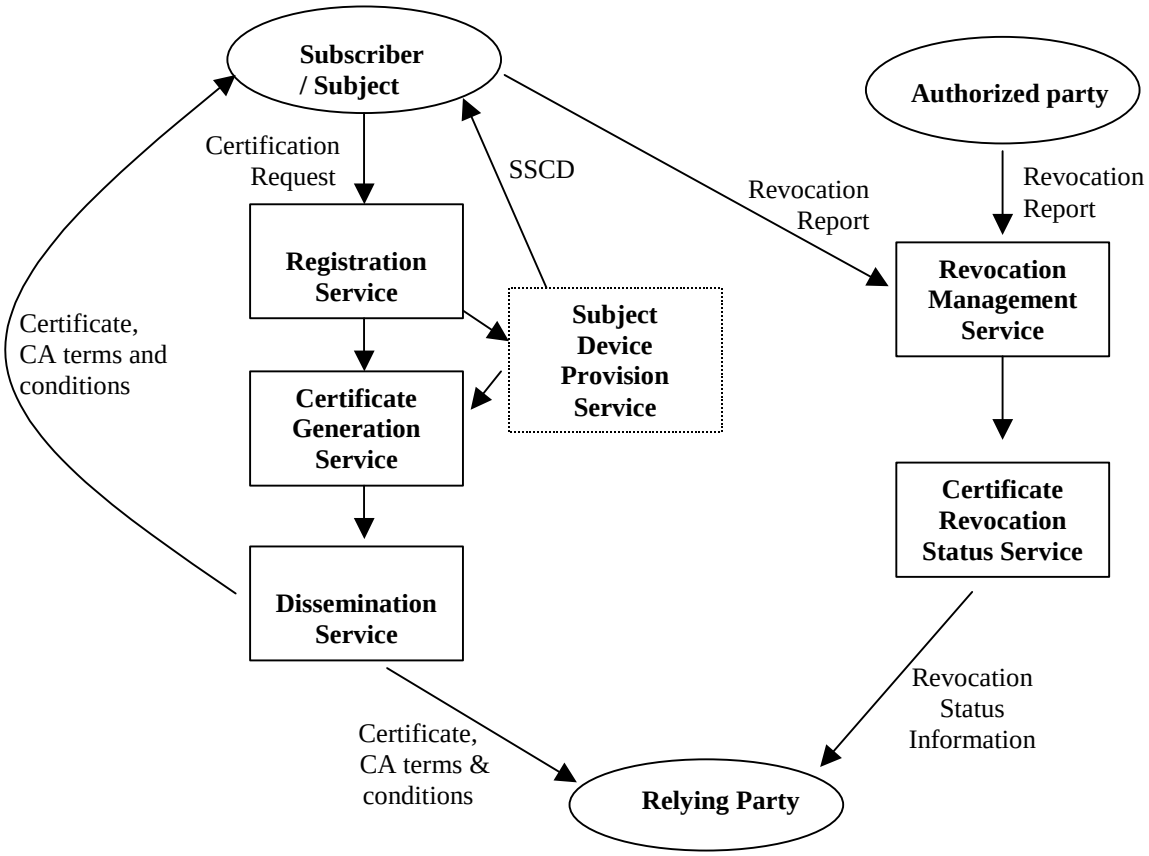


Figure 1: Illustration of subdivision of certification services used in the present document

4.3 Certificate policy and certification practice statement

This clause explains the relative roles of certificate policy and certification practice statement. It places no restriction on the form of a certificate policy or certification practice statement specification.

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 present document specifies certificate policies to meet the requirements for qualified certificates as laid down in annexes I and II of the Directive [1]. CAs specify in certification practice statements how these requirements are met.

4.3.2 Level of specificity

A certificate policy is a less specific 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. A certification practice statement defines how a specific certification authority meets the technical, organizational and procedural requirements identified in a 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 certification practice statement. This lower-level documentation is generally regarded as an internal operational procedure documents, which may define specific tasks and responsibilities within an organization. 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 the present document. 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 certification practice statement. A certificate policy is defined independently of the specific details of the specific operating environment of a certification authority, whereas a certification practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a certification authority. A certificate policy may be defined by the user of certification services, whereas the certification practice statement is always defined by the provider.

4.3.4 Other CA Statements

In addition to the policy and practice statements a CA may issue terms and conditions. Such a statement of terms and conditions is broad category of terms to cover the broad range of commercial terms or PKI specific, etc. terms that are not necessarily communicated to the customer, they may, nevertheless apply in the situation.

The PKI disclosure statement is that part of the CA's terms and conditions which relate to the operation of the PKI and which it is considered that the CA ought to disclose to both subscribers and relying parties.

4.4 Subscriber and Subject

In some cases certificates are issued directly to individuals for their own use. However, there commonly exist other situations where the party requiring a certificate is different from subject to whom the certificate applies. For example, a company may require certificates for its employees to allow them to participate in electronic business on behalf of the company. In such situations the entity subscribing to the certification authority for the issuance of certificates is different from the entity which is the subject of the certificate.

In the present document to clarify the requirements which are applicable to the two different roles that may occur two different terms are used for the **"subscriber"** who contracts with the certification authority for the issuance of certificates and the **"subject"** to whom the certificate applies. The subscriber bears ultimate responsibility for the use of the private key associated with the public key certificate but the subject is the individual that is authenticated by the private key.

In the case of certificates issued to individual for their own use the subscriber and subject can be the same entity. In other cases, such as certificates issued to employees the subscriber and subject are different. The subscriber would be, for example, the employer. The subject would be the employee.

Within the present document we use these two terms with this explicit distinction wherever it is meaningful to do so, although in some cases the distinction is not always crystal clear.

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" [3].

The policy requirements are defined in the present document in terms of certificate policies. These certificate policies are for qualified certificates, as defined the Directive [1], and hence are called qualified certificate policies. Certificates issued in accordance with the present 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 present document specifies two qualified certificate policies:

1) a qualified certificate policy for qualified certificates issued to the public, requiring use of secure signature-creation devices.

NOTE 1: The exact meaning of public is left to interpretation within the context on national legislation. A CA may be considered to be issuing qualified certificates to the public if the certificates are not restricted to uses governed by voluntary agreements under private law among participants.

2) a qualified certificate policy for qualified certificates issued to the public;

Clause 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 2: The present document makes use of the principles defined in IETF RFC 2527 [2] and the framework defined in ANSI X9.79 (see bibliography). The aim of the present document is to achieve best possible harmonization with the principles and requirements of those documents.

5.2 Identification

The identifiers for the qualified certificate policies specified in the present document are:

a) **QCP public + SSCD:** a certificate policy for qualified certificates issued to the public, requiring use of secure signature-creation devices

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public-with-sscd (1)
```

b) **QCP public:** a certificate policy for qualified certificates issued to the public

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public (2)
```

By including one of these object identifiers in a certificate the CA claims conformance to the identified qualified certificate policy.

A CA shall also include the identifier(s) for the certificate policy (or policies) being supported in the terms and conditions made available to subscribers and relying parties to indicate its claim of conformance.

5.3 User Community and applicability

5.3.1 QCP public + SSCD

The certificate policy QCP public + SSCD is for certificates:

a) which meet the requirements laid down in annex I of the Directive [1];

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive [1];

c) which are for use only with secure-signature-creation devices which meet the requirements laid down in annex III of the Directive [1];

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 [1].

5.3.2 QCP public

The certificate policy QCP Public is for certificates:

a) which meet the requirements laid down in annex I of the Directive [1];

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive [1];

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 [1].

5.4 Conformance

5.4.1 General

The CA shall only use the identifier for either of the qualified certificate policies as given in clause 5.2:

a) if the CA claims conformance to the identified qualified certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

b) if the CA has been assessed to be conformant to the identified qualified certificate policy by a competent independent party.

NOTE: See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance".

5.4.2 QCP public + SSCD

A conformant CA must demonstrate that:

a) it meets its obligations as defined in clause 6.1;

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

5.4.3 QCP public

A conformant CA must demonstrate that:

a) it meets its obligations as defined in clause 6.1;

b) it has implemented controls which meet the requirements specified in clause 7, excluding those specified in clause 7.2.9 and excluding the subscriber obligation given in clause 6.2 e) and f).

6 Obligations and liability

NOTE: This clause is applicable to both qualified certificate policies identified in clause 5: QCP public, and QCP public + SSCD, except where indicated.

6.1 Certification authority obligations

The CA shall ensure that all requirements on CA, as detailed in clause 7, are implemented as applicable to the selected qualified certificate policy (see clauses 5.4.2 and 5.4.3).

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

The CA shall provide all its certification services consistent with its certification practice statement.

6.2 Subscriber obligations

The CA shall oblige, through agreement (see clause 7.3.1 h)), the subscriber to ensure that the subject fulfils the following obligations:

a) submit accurate and complete information to the CA in accordance with the requirements of this policy, particularly with regards to registration;

b) only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber (see clause 7.3.4);

c) exercise reasonable care to avoid unauthorized use of the subject's private key;

d) if the subscriber or subject generates the subject's keys:

- generate subject's keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures;

- use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures;

NOTE 1: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive [1].

- only the subject holds the private key once delivered to the subject.

e) if the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), only use the certificate with electronic signatures created using such a device;

NOTE 2: The above item is NOT applicable to qualified certificate policy: QCP public.

f) if the certificate is issued by the CA under certificate policy QCP public + SSCD and the subject's keys are generated under control of the subscriber, generate the subject's keys within the SSCD to be used for signing;

NOTE 3: The above item is NOT applicable to qualified certificate policy: QCP public.

g) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

- the subject's private key has been lost, stolen, potentially compromised; or

- control over the subjects private key has been lost due compromise of activation data (e.g. PIN code) or other reasons; and/or

- inaccuracy or changes to the certificate content, as notified to the subscriber.

h) following compromise, the use of the subject's private key is immediately and permanently discontinued.

6.3 Information for Relying parties

The terms and conditions made available to relying parties (see clause 7.3.4) shall include a notice that if it is to reasonably rely upon a certificate, it shall:

a) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 7.3.4); and

NOTE 1: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay of up to 1 day in disseminating revocation status information.

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 clause 7.3.4; and

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

NOTE 2: The liability of CAs 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

CAs 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 CA practice

NOTE 1: This clause is applicable to both qualified certificate policies identified in clause 5: QCP public, and QCP public + SSCD, except where indicated.

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

NOTE 2: A reference to the article within the Directive on which the requirement is based is given after each paragraph.

The present document is concerned with CA's issuing qualified certificates. This includes the provision of services for Registration, certificate generation, certificate dissemination, revocation management and revocation status (see clause 4.2). Where requirements relate to a specific service area of the CA then it is listed under one of these subheadings. Where no service area is listed, or "CA General" is indicated, a requirement is relevant to the general operation of the CA.

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

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met. Each control objective is followed by a reference to the relevant requirement given in the Directive [1].

NOTE 3: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a CA may employ in issuing qualified certificates. In case of clause 7.4 (CA management and operation) reference is made to other more general standards which may be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic may vary.

7.1 Certification practice statement

The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive [1], annex II (a)).

In particular:

a) The CA shall have a statement of the practices and procedures used to address all the requirements identified in the qualified certificate policy.

NOTE 1: This policy makes no requirement as to the structure of the certification practice statement.

b) The CA's certification practice statement shall identify the obligations of all external organizations supporting the CA services including the applicable policies and practices.

c) The CA shall make available to subscribers and relying parties its certification practice statement, and other relevant documentation, as necessary to assess conformance to the qualified certificate policy.

NOTE 2: The CA is not generally required to make all the details of its practices public.

d) The CA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of the certificate as specified in clause 7.3.4.

e) The CA shall have a high level management body with final authority and responsibility for approving the certification practice statement.

f) The senior management of the CA has responsibility for ensuring the practices are properly implemented.

g) The CA shall define a review process for certification practices including responsibilities for maintaining the certification practice statement.

h) The CA shall give due notice of changes it intends to make in its Certification Practice Statement (CPS) and shall, following approval as in (e) above, make the revised Certification Practice Statement immediately available as required under (c) above.

7.2 Public key infrastructure - Key management life cycle

7.2.1 Certification authority key generation

Certificate generation

The CA shall ensure that CA keys are generated in controlled circumstances (see the Directive [1], annex II (g) and annex II (f)).

In particular:

a) Certification authority key generation shall be undertaken in a physically secured environment (see clause 7.4.4) by personnel in trusted roles (see clause 7.4.3) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

b) CA key generation shall be carried out within a device which either:

- meets the requirements identified in FIPS PUB 140-1 [5] level 3 or higher; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [8]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [7], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE 1: The rules of clause 7.2.2 (b to d) apply also to key generation even if carried out in a separate system.

c) Certification authority key generation shall be performed using an algorithm recognized as being fit for the purposes of qualified certificates.

d) The selected key length and algorithm for CA signing key shall be one which is recognized as being fit for the purposes of qualified certificates as issued by the CA.

NOTE 2: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive [1].

7.2.2 Certification authority key storage, backup and recovery

Certificate generation

The CA shall ensure that CA private keys remain confidential and maintain their integrity (see the Directive [1], annex II (g) and annex II (f)).

In particular:

a) The CA private signing key shall be held and used within a secure cryptographic device which:

- meets the requirements identified in FIPS PUB 140-1 [5] level 3 or higher; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [8]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [7], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

b) When outside the signature-creation device (see (a) above) the CA private signing key shall be encrypted using an algorithm and key-length that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part.

c) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

d) Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

e) 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 and certificate Distribution

The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties (see the Directive [1], annex II (g) and annex II (f)).

In particular:

a) CA signature verification (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: For example, certification authority public keys may be distributed in certificates signed by itself, along with a declaration that the key authenticates the CA, or issued by another CA. 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 source, is needed to give assurance of the correctness of this certificate.

7.2.4 Key escrow

CA and subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive [1], annex II (j)).

7.2.5 Certification authority key usage

The CA shall ensure that CA private signing keys are not used inappropriately.

In particular:

Certificate generation

a) CA signing key(s) used for generating certificates, as defined in clause 7.3.3, and/or issuing revocation status information, shall not be used for any other purpose.

b) The certificate signing keys shall only be used within physically secure premises.

7.2.6 End of CA key life cycle

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle (see the Directive [1], annex II (g) and annex II (f)).

In particular:

Certificate generation

a) all copies of the CA private signing keys shall be:

   - destroyed such that the private keys cannot be retrieved; or

   - retained 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

The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive [1], annex II (f)).

Certificate generation

In particular the CA shall ensure that:

a) certificate signing cryptographic hardware is not tampered with during shipment;

b) certificate and revocation status information signing cryptographic hardware is not tampered with while stored;

c) the installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees;

d) certificate and revocation status information signing cryptographic hardware is functioning correctly; and

e) CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement.

7.2.8 CA provided subject key management services

The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured (see the Directive [1], annex II (f) and (j)).

Certificate generation

If the CA generates the subject keys:

a) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures.

b) CA-generated subject keys shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of qualified electronic signatures.

NOTE: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive [1].

c) CA-generated subject keys shall be generated and stored securely before delivery to the subject.

d) The subject's private key shall be delivered to the subscriber or subject in a manner such that the secrecy of the key is not compromised and on delivery only the subject has access to its private key.

7.2.9 Secure-signature-creation device preparation

NOTE 1: This clause is NOT applicable to the qualified certificate policies: QCP public.

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive [1], annex III).

Subject device provision

In particular, if the CA issues a SSCD:

a) secure-signature-creation device preparation shall be securely controlled by the service provider;

b) secure-signature-creation device shall be securely stored and distributed;

c) secure-signature-creation device deactivation and reactivation shall be securely controlled;

d) where the secure-signature device has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure signature-creation device.

NOTE 2: Separation may be achieved by ensuring distribution and delivery at different times, or via a different route.

NOTE 3: Requirement for SSCD preparation listed above may be fulfilled, for example, using a suitable protection profile, defined in accordance with ISO/IEC 15408 [7] or equivalent.

7.3 Public key infrastructure - Certificate Management life cycle

7.3.1 Subject registration

The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive [1], annex II (d)).

In particular:

Registration

NOTE 1: When registering, a subject is identified as a person with specific attributes. The specific attributes may indicate, for example, an association within an organization possibly with a role.

a) Before entering into a contractual relationship with a subscriber, the CA shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 7.3.4 (see the Directive [1], annex II (k)).

b) The CA shall communicate this information through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

NOTE 2: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B.

c) The service provider 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. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.

NOTE 3: An examples of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.

NOTE 4: Attribute certificates are outside the scope of the present document as they contain no public signing key.

d) Where the subject is a person evidence shall be provided of:

- full name (including surname and given names);
- date and place of birth, a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

NOTE 5: It is recommended that the place be given in accordance to national conventions for registering births.

NOTE 6: The CA is liable as regards the accuracy "of all information contained in the certificate" (see annex A).

e) Where the subject is a person who is identified in association with a legal person, or other organizational entity, evidence shall be provided of:

- full name (including surname and given names) of the subject;
- date and place of birth, a nationally recognized identity number, or other attributes of the subject which may be used to, as far as possible, distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organizational entity;
- any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;
- evidence that the subject is associated with the legal person or other organizational entity.

f) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted.

g) The CA shall record all the information used to verify the subjects' identity, including any reference number on the documentation used for verification, and any limitations on its validity.

h) The CA shall record the signed agreement with the subscriber including:

- agreement to the subscriber's obligations (see clause 6.2);
- if required by the CA, agreement to use a SSCD;

NOTE 7: The above item above does not apply for QCP Public.

- consent to the keeping of a record by the CA of information used in registration (see clause 7.4.11 h), i), j)), subject device provision (see clause 7.4.11 items m), n) and any subsequent revocation (see clause 7.4.11 o)), and passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services;
- whether, and under what conditions, the subscriber requires and the subject's consents to the publication of the certificate;

- confirmation that the information held in the certificate is correct.

NOTE 8: 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.

NOTE 9: Other parties (e.g. the associated legal person) may be involved in establishing this agreement.

NOTE 10: This agreement may be in electronic form.

i) The records identified above shall be retained for at the period of time as indicated to the subscriber (see a) and b) above) and as necessary for the purposes for providing evidence of certification in legal proceedings.

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

NOTE 11: In order for the CA to obtain the assurance that the private key is really placed in a SSCD, the certificate request process may also ensure that the key pair has effectively been generated by a SSCD.

k) The CA shall ensure that the requirements of the national data protection legislation are adhered to (including the use of pseudonyms if applicable) within their registration process.

7.3.2 Certificate renewal, rekey and update

The CA shall ensure that requests for certificates issued to a subject who has already previously registered are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes (see the Directive [1], annex II (g)).

NOTE: The subscriber may, if the CA offers this service, request a certificate renewal for example where relevant attributes presented CA the certificate have changed or when the certificate lifetime is running out.

In particular:

Registration

a) The CA shall check that the information used to verify the identity and attributes of the subject is still valid.

b) If any of the CA terms and conditions have changed, these shall be communicated to the subscriber and agreed to in accordance with clause 7.3.1 a), b) and h).

c) If any information has changed, this is verified, recorded, agreed to by the subscriber in accordance with clause 7.3.1 c) to g).

d) The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's intended lifetime and no indications exist that the subject's private key has been compromised.

7.3.3 Certificate generation

The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive [1], annex II (g)).

In particular:

Certificate generation

a) the certificates are generated and issued in accordance with annexes I and II (g) of the Directive [1].

NOTE: A standard format for qualified certificates meeting the requirements of annex I of the Directive [1] is defined in TS 101 862 [6].

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

c) if the CA generated the subjects key:

- the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA;
- the private key (or SSCD - see clause 7.2.9) is securely passed to the registered subscriber or subject.

d) The CA shall ensure over time the uniqueness of the distinguished name assigned to the subject 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).

e) The confidentiality and integrity of registration data shall be protected especially when exchanged with the subscriber, subject or between distributed CA system components.

f) The CA shall verify that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are used.

7.3.4 Dissemination of Terms and Conditions

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see the Directive [1], annex II (k)).

In particular:

a) The CA shall make available to subscribers and relying parties the terms and conditions regarding the use of the certificate including the Directive [1], annex II (k):

- the qualified certificate policy being applied, including a clear statement as to whether the policy is for certificates issued to the public and whether the policy requires uses of a SSCD;
- any limitations on its use;
- the subscriber's obligations as defined in clause 6.2, including whether the policy requires uses of a SSCD;
- information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate (see clause 6.3);
- limitations of liability including the purposes/uses for which the CA accepts (or excludes) liability;
- the period of time which registration information (see clause 7.3.1) is retained;
- the period of time which CA event logs (see clause 7.4.11) are retained;
- procedures for complaints and dispute settlement;
- the applicable legal system; and
- if the CA has been certified to be conformant with the identified qualified certificate policy, and if so through which scheme.

b) The information identified in a) above shall be available 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. Alternatively this may be provided as part of a subscriber/relying party agreement. These terms and conditions may be included in a certification practice statement provided that they are conspicuous to the reader.

7.3.5 Certificate dissemination

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive [1], annex II (l)).

In particular:

Dissemination

a) upon generation, the complete and accurate certificate shall be available to subscriber or subject for whom the certificate is being issued;

b) certificates are available for retrieval in only those cases for which the subject's consent has been obtained;

c) the CA shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 7.3.4);

d) the applicable terms and conditions shall be readily identifiable for a given a certificate;

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 are not under the control of the CA, the CA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement;

f) The information identified in b) and c) above shall be publicly and internationally available.

7.3.6 Certificate revocation and suspension

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive [1], annex II (b)).

In particular:

Revocation management

a) The CA shall document as part of its certification practice statement (see 7.1) the procedures for revocation of certificates including:

   - who may submit revocation reports and requests;
   - how they may be submitted;
   - any requirements for subsequent confirmation of revocation reports and requests;

NOTE 1: For example, a confirmation may be required from the subscriber if a compromise is reported by a third party.

   - whether and for what reasons certificates may be suspended;
   - the mechanism used for distributing revocation status information;
   - the maximum delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties. This shall be at most 1 day.

b) Requests and reports relating to revocation (e.g. due to compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations) shall be processed on receipt.

c) Requests and reports relating to revocation shall be authenticated, checked to be from an authorized source. Such reports and requests will be confirmed as required under the CA's practices.

d) A certificate's revocation status may be set to suspended whilst the revocation is being confirmed. The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.

NOTE 2: Support for certificate suspension is optional.

e) The subject, and where applicable the subscriber, of a revoked or suspended certificate, shall be informed of the change of status of its certificate.

f) Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

g) 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;
- the CRL shall be signed by a the certification authority or an authority designated by the CA.

h) Revocation management services shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this service is be not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

Revocation status

i) 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 CA, the CA shall make best endeavours to ensure that this information service is be not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

NOTE 3: Revocation status information may be provided, for example, using on-line certificate status service or through distribution of CRLs through a repository.

j) The integrity and authenticity of the status information shall be protected.

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

7.4 CA management and operation

7.4.1 Security management

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive [1], annex II (e), 2nd part).

In particular:

CA General

a) The CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures.

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

c) The CA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy.

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

NOTE 1: See ISO/IEC 17799 for guidance on information security management including information security infrastructure, management information security forum and information security policies. Other alternative guidance documents are given in bibliography.

e) The security controls and operating procedures for CA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained.

NOTE 2: It is recommended that this documentation (commonly called a system security policy) identifies 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 is recommended that the documentation describes 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.

f) CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.

7.4.2 Asset classification and management

The CA shall ensure that its assets and information receive an appropriate level of protection. (see the Directive [1], annex II (e)).

In particular:

CA General

a) The CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

7.4.3 Personnel security

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see [1], annex II (e) 1st part).

In particular:

CA General

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

NOTE 1: It is recommended that CA personnel 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 CA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified.

c) CA personnel (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 CA specific functions. It is recommended that the job descriptions include skills and experience requirements.

d) Personnel shall exercise administrative and management procedures and processes that are in line with the CA's information security management procedures (see clause 7.4.1).

NOTE 2: See ISO/IEC 17799 for guidance.

Registration, certificate generation, subject device provision, revocation management

e) Managerial personnel shall be employed who possess expertise in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment.

f) All CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations.

g) Trusted roles include roles that involve the following responsibilities:

- Security Officers: Overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of Certificates;
- System Administrators: Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management;
- System Operators: Responsible for operating the CA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery;
- System Auditors: Authorized to view and maintain archives and audit logs of the CA trustworthy systems.

h) CA personnel shall be formally appointed to trusted roles by senior management responsible for security.

i) The CA 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 affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

NOTE 3: In some countries it may not be possible for CA to obtain information on past convictions. However, the employer 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 CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see Directive 1999/93/EC [1] annex II (f)).

In particular:

CA General

a) Physical access to facilities concerned with certificate generation, subject device provision, and revocation management services shall be limited to properly authorized individuals.

b) Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities; and

c) Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

Certificate generation, subject device provision and revocation management

d) The facilities concerned with certificate generation, subject device provision and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

e) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, subject device provision and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

f) 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 CA's physical and environmental security policy for systems concerned with certificate generation, subject device provision and 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 and entering, and disaster recovery, etc.

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

NOTE 1: See ISO/IEC 17799 for guidance on physical and environmental security.

NOTE 2: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

7.4.5 Operations management

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive [1], annex II (e)).

In particular:

CA General

a) The integrity of CA systems and information shall be protected against viruses, malicious and unauthorized software.

b) Damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures.

c) Media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access.

NOTE 1: Every member of personnel with management responsibilities is responsible for planning and effectively implementing the certificate policy and associated practices as documented in the certification practice statement.

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

Media handling and security

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

System Planning

f) 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

g) The CA shall 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.

Certificate generation, revocation management

Operations procedures and responsibilities

h) CA security operations shall be separated from normal operations.

NOTE 2: CA 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 CA security operations, but, may actually be performed by, non-specialist, operational personnel (under supervision); as defined within the appropriate security policy, and, roles and responsibility documents.

7.4.6 System Access Management

The CA shall ensure that CA system access is limited to properly authorized individuals (see [1], annex II (f)).

In particular:

CA General

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

NOTE 1: It is recommended that firewalls be configured to prevent protocols and accesses not required for the operation of the CA.

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

NOTE 2: Sensitive data includes registration information.

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

e) CA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.

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

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

NOTE 3: Sensitive data includes registration information.

Certificate generation

h) The CA shall ensure that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CA.

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

NOTE 4: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

Dissemination

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

Revocation management

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

NOTE 5: This may used, for example, an intrusion detection system, access control monitoring and alarm facilities.

Revocation status

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

7.4.7 Trustworthy Systems Deployment and Maintenance

The CA shall use trustworthy systems and products that are protected against modification (see the Directive [1] , annex II (f)).

NOTE 1: Requirements for the trustworthy systems may be ensured using, for example, systems conforming to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [7] or equivalent.

NOTE 2: It is recommended that the risk analysis carried out on the CA's services (see clause 7.4.1) identifies its critical services requiring trustworthy systems and the levels of assurance required.

In particular:

CA General

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the CA or on behalf of the CA to ensure that security is built into IT systems.

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 CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible (see the Directive [1], annex II (a)).

In particular:

CA General

CA key compromise

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

Revocation status

b) In the case of compromise the CA shall as a minimum provide the following undertakings:

- inform all subscribers, relying parties and other CAs with which it 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.

NOTE: It is recommended that when another CA with which a compromised CA has an agreement is informed of the compromise, any a CA certificate that has been issued for the compromised CA is revoked.

7.4.9 CA termination

The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive [1], annex II (i)).

In particular:

CA General

a) Before the CA terminates its services the following procedures shall be executed as a minimum:

   - the CA shall inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations.

NOTE: The CA is not required to have a prior relationship with the relying party.

   - the CA shall terminate all authorization of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing certificates;

   - the CA shall perform necessary undertakings to transfer obligations for maintaining registration information (see clause 7.3.1) and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4);

   - the CA shall destroy, or withdraw from use, its private keys, as defined in clause 7.2.6.

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

c) The CA shall state in its practices the provisions made for termination of service. This shall include:

   - the notification of affected entities;

   - the transfer of its obligations to other parties;

   - the handling of the revocation status for unexpired certificates that have been issued.

7.4.10 Compliance with Legal Requirements

The CA shall ensure compliance with legal requirements (see the Directive [1], article 8).

In particular:

CA General

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 (see clause 7.4.11).

b) The CA shall ensure that the requirements of the European data protection Directive, as implemented through national legislation, are met.

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

d) The information that users contribute to the CA shall be completely protected from disclosure without the user's agreement, a court order or other legal authorization.

7.4.11 Recording of Information Concerning Qualified Certificates

The CA shall ensure that all relevant information concerning a qualified certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings (see the Directive [1], annex II (i)).

NOTE 1: Records concerning qualified certificates include registration information (see clause 7.3.1) and information concerning significant CA environmental, key management and certificate management events.

In particular:

General

a) The confidentiality and integrity of current and archived records concerning qualified certificates shall be maintained.

b) Records concerning qualified certificates shall be completely and confidentially archived in accordance with disclosed business practices.

c) Records concerning qualified certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, shall have access to registration and other information relating to the subject.

NOTE 2: This may be used, for example, to support the link between the certificate and the subject.

d) The precise time of significant CA environmental, key management and certificate management events shall be recorded.

NOTE 3: It is recommended that the CA states in its practices as the accuracy the clock used in timing of events, and how this is accuracy ensured.

e) Records concerning qualified certificates shall be held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures.

NOTE 4: 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 realized until after a lengthy time elapses, if ever.

NOTE 5: Where differing periods of times are applied to certificates being used for different purposes, they shall be clearly identified they should have different specific qualified certificate policy identifiers. Where differing periods are applied to different parts of the registration and event log records, this shall be indicated to the subscriber and relying party as specified in clauses 7.3.1 and 7.3.4.

f) The 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 6: 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.

g) The specific events and data to be logged shall be documented by the CA.

Registration

h) The CA shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged.

i) The CA shall ensure that all registration information including the following is recorded:

- type of document(s) presented by the applicant to support registration;
- record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable;
- storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 h));
- any specific choices in the subscriber agreement (e.g. consent to publication of certificate);
- identity of entity accepting the application;
- method used to validate identification documents, if any;

- name of receiving CA and/or submitting Registration Authority, if applicable.

j) The CA shall ensure that privacy of subject information is maintained.

Certificate generation

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

l) The CA shall log all events relating to the life-cycle of certificates.

Subject device provision

m) The CA shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

n) If applicable, the CA shall log all events relating to the preparation of SSCDs.

Revocation management

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

7.5 Organizational

The CA shall ensure that its organization is reliable (see [1], annex II (a)).

In particular that:

CA general

a) Policies and procedures under which the CA operates shall be non-discriminatory.

b) The CA shall make its services accessible to all applicants whose activities fall within its declared field of operation.

c) The CA is a legal entity according to national law.

d) The CA has a system or systems for quality and information security management appropriate for the certification services it is providing.

e) The CA has adequate arrangements to cover liabilities arising from its operations and/or activities.

f) The CA has the financial stability and resources required to operate in conformity with this policy.

g) The CA 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.

h) The CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters.

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

Certificate generation, revocation management

j) The parts of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

k) The parts of the CA concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

8 Framework for the definition of other qualified certificate policies

This clause provides a general framework for other policies for CAs issuing qualified certificates. A CA may claim conformance to this general framework as defined in clause 8.4. In general terms this requires conformance to the requirements in clauses 6 and 7 excluding those applicable only to CAs issuing certificates to the public.

NOTE: This clause is NOT applicable to either qualified certificate policies identified in clause 5: QCP public, and QCP public + SSCD.

8.1 Qualified certificate policy management

The CA shall ensure that the certificate policy is effective.

In particular:

a) There shall be a body (e.g. 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 requirements 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 policies are supported by the CAs Certification Practices Statement (CPS).

e) The CA shall make available the qualified certificate policies supported by the CA 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 clauses 6 and 7 with the exclusions indicated below. In the case of any conflict the requirements of the present document prevail.

h) A unique object identifier shall be obtained for the certificate policy of the form required in ITU-T Recommendation X.509 [3].

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 clause 6.3.

b) Independence of providers of certificate generation and revocation management services as specified in clause 7.5 j), k).

c) Dissemination of certificates publicly as specified in clause 7.3.5 f).

d) Public availability of revocation status information as specified in clause 7.3.6 k).

8.3 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 7.3.4:

a) If the policy is not for public use and whether exclusions identified in clause 8.2 apply.

b) Whether the policy includes requirements for use of 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 present document.

8.4 Conformance

The CA shall only claim conformance to the present document and the applicable qualified certificate policy:

a) if the CA claims conformance to the identified qualified certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

b) if the CA has been assessed to be conformant to the identified qualified certificate policy by an independent party.

A conformant CA must demonstrate that:

c) it meets its obligations as defined in clause 6.1;

d) it has implemented controls which meet the requirements specified in clause 7, excluding:

- clause 7.2.9 if the CA does not require use of a SSCD;
- those clauses specified in clause 8.2 if the CA is not providing a service to the public;

e) uses a qualified certificate policy which meets the requirements specified in clause 8.1;

f) it has implemented controls which meet the additional requirements of the qualified certificate policies employed;

g) it meets the additional requirements specified in clause 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 [1].

The liability requirements of CAs issuing qualified certificates (or certification-service-providers issuing qualified certificates using the terminology defined in the Directive [1]) to the public are stated in the Directive [1] 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 recognizable 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 recognizable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

A CA may be considered to be issuing qualified certificates to the public if the certificates are not 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 Member States of the EU. Even where liability is governed by the electronic signatures Directive (the "Directive" [1]), 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. It should also be noted that in some cases, in particular those involving closed systems, liability is governed by the agreement between the CA and the parties using and relying upon the certificate.

l) Liability of CAs

A) Liability of CAs to relying parties Governed by the Directive [1]

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

Article 6 of the Directive [1] requires Member States to incorporate certain minimum liability provisions in national law. These provisions apply to CAs that issue qualified certificates to the public. They do not apply to CAs operating in closed systems or issuing non-qualified certificates. In particular, article 6 requires a CA 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 CA generated both of them; and
- that it registers any revocation of the certificate.

A CA is liable for damages resulting from failures to fulfil these obligations unless it has not acted negligently (subject to its ability to limit its liability, as discussed below). In other words, liability is predicated on the CA making an error, and that error being the result of negligence on the part of the CA. (The structure of the Directive implies that the liability provisions also reach reckless and intentional misconduct on the part of the CA.) Thus, to avoid liability, a CA 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 CA. Indeed, some failures on the part of the relying party may render its reliance on the certificate unreasonable under the circumstances, relieving the CA of liability under the Directive.

Member State courts frequently look to industry standards in determining whether certain conduct is negligent. Although compliance with an industry standard, such as the policy requirements defined in the present document, is not conclusive evidence that a CA has fulfilled its duty of care, in most Member State it is *prima facie* evidence that a CA is not negligent. Likewise, failure to comply with an industry standard, such as defined in the present document, may be *prima facie* evidence of negligence in most Member States.

The Directive [1] permits CAs 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 CA may not be able to control the number of transactions for which it becomes liable, the CA 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 CA 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 CA'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 CA negligently issues an inaccurate revocation list that the relying party fails to check. In that case, the CA 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 realized that the certificate had been revoked.

B) Liability of CAs to relying parties Not Governed by the Directive [1]

Where a CA does not fall into the liability scheme established by the Directive [1], 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 CA 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 CA and the subscriber; thus, a CA'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 CA and the subscriber does not designate the relying party as a third party beneficiary, however, national law will be the only source of a CA's liability to third parties.

C) Liability of CAs to subscribers

A CA'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 CA 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 CAs 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 CA 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 CA engaged in wilful misconduct. In some Member States, it is possible that CAs, 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 CA in the performance of the duties it owes to the subscriber.

CAs 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 [4]) and article 8 of the electronic signatures Directive [1]. At the same time, CAs may be required to disclose personal data to the authorities, particularly where the subscriber uses a pseudonym.

D) Liability of CAs to unrelated third parties

A CA could be liable to an unrelated third party if the CA 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 CA 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 CA; 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 CA

The liability, if any, of a subscriber to a CA for the provision of false, misleading, or inaccurate information is governed by the contract between the subscriber and the CA. If the subscriber intentionally provided false or misleading information, it may be liable to the CA 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 CA 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 CA 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 CA issuing certificates as a supplemental instrument of disclosure and notice. A PKI disclosure statement may assist a CA to respond to regulatory requirements and concerns, particularly those related to consumer deployment and in particular meet the requirements of the Directive [1], 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 clause for each defined statement type. Each clause of a PDS contains a descriptive statement, which MAY include hyperlinks to the relevant certificate policy/certification practice statement sections.

Table B.1

Statement types	Statement descriptions	Specific Requirements of qualified certificate policy (see clause 7.3.4)
CA 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 registration information and CA event logs (see clause 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 clause 6.2, including whether the policy requires use of a SSCD
Certificate status checking obligations of relying parties:	The extent to which relying parties are obligated to check certificate status, and references to further explanation.	information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate (see clause 6.3).
Limited warranty and disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see clause 6.4).

Statement types	Statement descriptions	Specific Requirements of qualified certificate policy (see clause 7.3.4)
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: CAs 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 International Chambers of Commerce'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 CA 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

Table C.1 identifies how the security controls objectives and other parts of the Qualified Certificate Policies (QCP) defined in the present document addresses the requirements of CAs issuing qualified certificates as defined in annex II of the Directive [1].

Table C.1

Directive annex II requirement	Qualified certificate policy reference
a) demonstrate the reliability necessary for providing certification services;	7.1, 7.4.8, 7.4.9, 7.5
b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;	7.3.5, 7.3.6, 7.4.6 (k)
c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;	7.4.11 (d)
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 recognized standards;	7.4.1, 7.4.3, 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, 7.2.1, 7.2.2 and 7.2.8
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;	7.2.2, 7.2.3, 7.2.8, 7.3.1, 7.3.2, 7.3.3
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 (e, f)
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 authorized 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.	7.2.3, 7.3.5, 7.3.6, 7.4.6, 7.4.7

Annex D (informative): IETF RFC 2527 and qualified certificate policy cross reference

Table D.1: Cross-reference IETF RFC 2527 [2] clauses and policy references

IETF RFC 2527 [2]	Qualified certificate policy reference
1.1 Overview	5.1
1 INTRODUCTION	
1.2 Identification	5.2
1.3 Community and Applicability	5.3
1.4 Contact Details	back of title page
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	7.3.5, 7.3.6
2.7 Compliance Audit	N/A
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	N/A
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
5.2 Procedural Controls	7.4.5
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	7.3.3
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

TTP.NL Part 1: "Requirements and Guidance for the Certification of the Public Key Infrastructure of Certification Service Providers".

TTP.NL Part 2: "Requirements and Guidance for the Certification of Information Security Management of Certification Service Providers".

TTP.NL Part 3: "General Requirements and Guidance for the Accreditation of Certification Service Providers issuing Qualified Certificates".

"Scheme approval profiles for Trust Service Providers".

NOTE: See http://www.tscheme.org/.

ISO/IEC 17799 (2000): "Information technology - Code of practice for information security management".

ITU-T X.843 | ISO/IEC 15945: "Information technology - Security techniques - Specification of TTP services to support the Application of Digital Signatures".

ITU-T X.842 | ISO/IEC 14516: "Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services".

ISO/IEC TR 13335-1 (1996): "Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security".

ISO/IEC TR 13335-2 (1997): "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security".

ISO/IEC TR 13335-3 (1998): "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security".

ISO/IEC TR 13335-4 (2000): "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards".

ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework".

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts - Statement by the Council and the Parliament re article 6 (1) - Statement by the Commission re article 3 (1), first indent.

CEN Workshop Agreement 14172: "EESSI Conformity Assessment Guidance".

History

Document history		
V1.1.1	December 2000	Publication
V1.2.1	April 2002	Publication