ETSI EN 319 411-2 V1.1.1 (2013-01)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Trust Service Providers issuing certificates;
Part 2: Policy requirements for
certification authorities issuing qualified certificates

Reference
DEN/ESI-000087

Keywords
e-commerce, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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://ipr.etsi.org).

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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.5].

The present document was previously published as TS 101 456 [i.11].

National transposition dates	
Date of adoption of this EN:	15 January 2013
Date of latest announcement of this EN (doa):	30 April 2013
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 October 2013
Date of withdrawal of any conflicting National Standard (dow):	31 October 2013

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 (CA).

For participants of electronic commerce to have confidence in the security of cryptographic mechanisms they need to have confidence that the CA has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with public key crypto systems.

The present document provides a baseline for policy requirements for certification authorities issuing qualified certificates in line with the Directive 1999/93/EC [i.1] of the European Parliament and of the Council on a Community framework for electronic signatures (hereinafter referred to as Directive 1999/93/EC [i.1]). Where requirements identified have general applicability on the operation and management practices of Trust Service Providers they are derived from the document EN 319 401 [6].

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 1999/93/EC [i.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 specific policy requirements relating to the CA include 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 Directive 1999/93/EC [i.1]). It specifically addresses the requirements for CAs issuing qualified certificates in accordance with annexes I and II of the Directive 1999/93/EC [i.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 TS 119 403 "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance" [i.2].

The present document references EN 319 401 [6] for generic policy requirements common to all classes of TSP service.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

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

[2] CEN Workshop Agreement 14167-2 (2004): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".

[3] CEN Workshop Agreement 14167-3 (2004): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)".

[4] CEN Workshop Agreement 14167-4 (2004): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - (CMCSO PP)".

NOTE: CEN Workshop Agreement 14167 is currently under revision to become the basis of a European Norm in CEN TC 224.

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

[6] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting electronic signatures".

[7] ISO/IEC 19790: "Information technology - Security techniques - Security requirements for cryptographic modules".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.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 1999/93/EC" in the present document.

[i.2] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance".

[i.3] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.4] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for qualified certificate profile".

[i.5] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Overview".

NOTE: This document is to be written.

[i.6] ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework".

[i.7] ISO/IEC 27002 (2005): "Information technology - Security techniques - Code of practice for information security management".

[i.8] 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.

[i.9] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

[i.10] CEN Workshop Agreement 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

NOTE: A replacement TS 14167-1 is under development in CEN.

[i.11] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.12] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[i.13] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[i.14] 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.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given EN 319 401 [6] and the following apply:

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

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

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

certification practice statement: statement of the practices which a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates

Certification Service Provider (CSP): entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

NOTE: This is a specific type of Trust Service Provider (TSP) supporting electronic signature as specified in EN 319 401 [6].

Qualified Certificate Policy (QCP): certificate policy which incorporates the requirements laid down in annex I and annex II of the Directive 1999/93/EC [i.1]

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in EN 319 401 [6] and the following apply:

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
CWA	CEN Workshop Agreement
EAL	Evaluation Assurance Level
OCSP	Online Certificate Status Protocol
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
SSCD	Secure Signature Creation Device
TSP	Trust Service Provider

4 General concepts

4.1 General Policy Requirements Concepts

The concepts described in EN 319 401 [6], clause 4 apply.

4.2 Certification authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the certification authority. The certification authority has overall responsibility for the provision of the certification services identified in clause 4.3. The certification authority is identified in the certificate as the issuer and its private key is used to sign qualified certificates.

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 sign 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 1999/93/EC [i.1].

A certification authority is a trust-service-provider, as described in EN 319 401 [6], and also a form of certification service provider as defined in the Directive 1999/93/EC [i.1], which issues public key certificates.

4.3 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, makes them available to relying parties. This service also makes available 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 may be based upon certificate revocation lists or a real time service which provides status information on an individual basis. The status information may be updated on a regular basis and hence may not reflect the current status of the certificate.

And optionally:

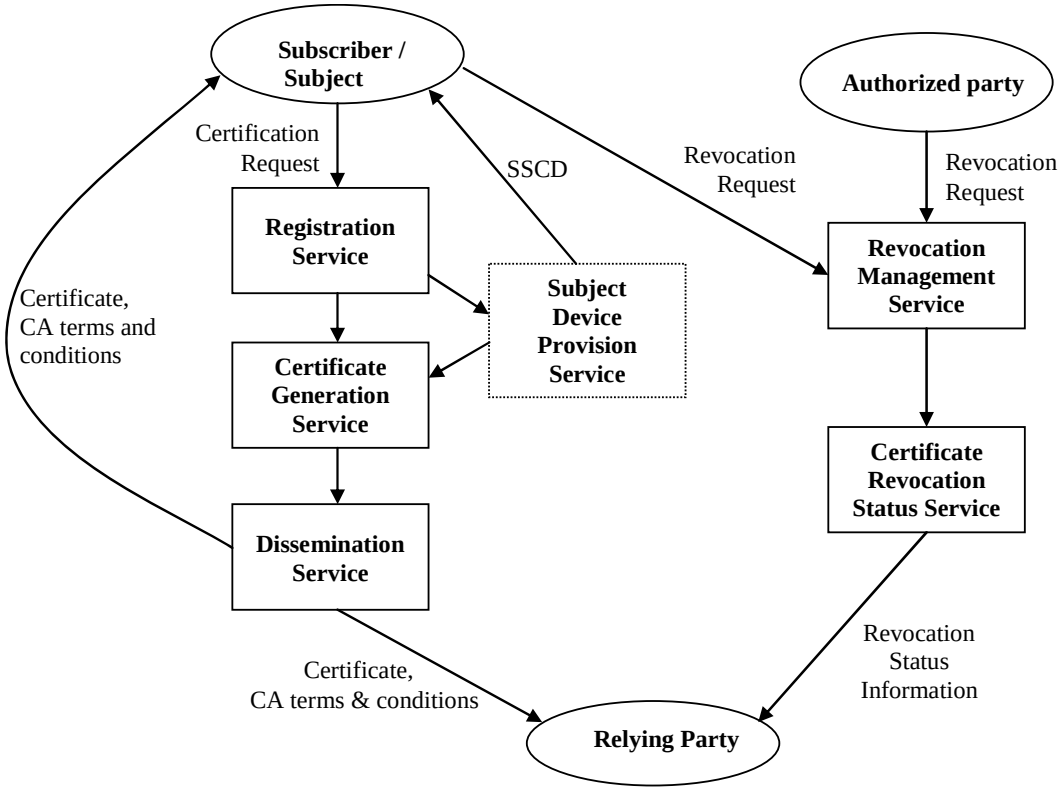
- **Subject device provision service:** prepares, and provides or makes available a signature-creation device to subjects.

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.

Figure 1 illustrates the interrelationship between the services.



NOTE: Figure 1 is for illustrative purposes. Clause 7 specifies the specific requirements for each of the services.

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

4.4 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.

A qualified certificate policy is a form of TSP Policy as specified in EN 319 401 [6] applicable to Certification Authorities issuing qualified certificates.

Certification Practice Statement is a form of TSP Practice Statement as specified in EN 319 401 [6] applicable to Certification Authorities issuing qualified certificates.

4.4.1 Purpose

The explanation and requirements identified in EN 319 401 [6], clause 4.3.1 apply.

4.4.2 Level of specificity

The guidelines identified in EN 319 401 [6], clause 4.3.2 apply.

4.4.3 Approach

The guidelines identified in EN 319 401 [6], clause 4.3.3 apply.

4.4.4 Other CA statements

In addition to, or as part of, the policy and practice statements a CA issues 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 relates to the operation of the PKI and which it is considered that the CA ought to disclose to both subscribers and relying parties.

4.5 Subscriber and subject

EN 319 401 [6] defines that a subscriber may be an organization comprising several end-users or an individual end-user. 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 the 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 for the **"subject"** to whom the certificate applies. The subscriber bears responsibility towards the CA 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 and that has control over its use.

In the case of certificates issued to individuals 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. Thus the situations described in the first paragraph can be restated in terms of subscriber and subject.

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 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*" [5].

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 1999/93/EC [i.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 certificate's 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 of 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 RFC 3647 [i.3] and the framework defined in ANSI X9.79 [i.6]. 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.

NOTE: EN 319 412-5 [i.4], clause 5.2.1, requires that the QcCompliance statement esi4-qcStatement-1 be included in a Qualified Certificate Statement extension, as defined in clause 5.2.1.

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 1999/93/EC [i.1];

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive 1999/93/EC [i.1];

c) which are for use only with secure-signature-creation devices which meet the requirements laid down in annex III of the Directive 1999/93/EC [i.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 1999/93/EC [i.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 1999/93/EC [i.1];

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive 1999/93/EC [i.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 1999/93/EC [i.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 either:

   i) the CA itself 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

NOTE 1: This evidence can be, for example, a report from an internal audit confirming that the CA conforms to the requirements of the identified policy. If the audit is internal to the CA organization the auditors should have no hierarchical relationship with the department operating the CA. See TS 119 403 [i.2].

   ii) the CA has a current assessment of conformance to the identified qualified certificate policy by a competent independent party. The results of the assessment shall be made available to subscribers and relying parties on request;

NOTE 2: This assessment can be carried out either under a "*voluntary accreditation*" scheme as defined in article 2.13 of the Directive [i.1], or other form of assessment carried out by a competent independent auditor, see TS 119 403 [i.2].

b) if the CA is later shown to be non-conformant in a way that significantly affects its ability to meet the requirements for qualified certificates identified in the Directive 1999/93/EC [i.1] it shall cease issuing certificates using the identifiers in clause 5.2, except for test purposes, until it has demonstrated or been assessed as conformant;

NOTE 3: Even if a CA is known to be critically non-conformant, it may issue certificates for internal and testing purposes provided that such certificates are not made available for any other uses.

NOTE 4: The means required to demonstrate conformance may depend on legal requirements for the country where the CA is established.

c) the CA conformance shall be checked on a regular basis and whenever major change is made to the CA operations.

NOTE 5: See TS 119 403 [i.2] for requirements relating to re-assessment period.

5.4.2 QCP public + SSCD

A conformant CA shall 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 shall 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

This clause is applicable to both qualified certificate policies identified in clauses 5.4.2 (QCP public) and 5.4.3 (QCP public+SSCD), except where indicated.

6.1 Certification authority obligations

The general obligations specified in EN 319 401 [6], clause 5.1 shall apply. In addition:

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, 5.4.3 and 8.4).

6.2 Subscriber obligations

The CA shall oblige through agreement (see clause 7.3.1 i)) the subscriber to address all the following obligations. If the subject and subscriber are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject (as listed below):

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 private key;

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

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

ii) use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate;

NOTE 1: See TS 102 176-1 [i.13] for guidance on algorithms and their parameters.

iii) the subject's private key is maintained under the subject's sole control.

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 or subject, 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:

i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key) or stolen; or

ii) the subject's private key has been potentially compromised or control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or

iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.

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

i) in the case of being informed that the CA which issued the subjects certificate has been compromised, ensure that the certificate is not used by the subject.

6.3 Information for relying parties

The general obligations specified in EN 319 401 [6], clause 5.3 shall apply.

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 1999/93/EC [i.1] 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 1999/93/EC [i.1] (see annex A for further guidance on liability).

7 Requirements on CA practice

This clause is applicable to both qualified certificate policies identified in clause 5.4.2: QCP public + SSCD, and clause 5.4.3: QCP public, except where indicated.

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

NOTE 1: If applicable, a reference to the article within the Directive 1999/93/EC [i.1] 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 objectives will be met. Each control objective is followed by a reference to the relevant requirement given in the Directive 1999/93/EC [i.1].

NOTE 2: 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 (CPS)

The requirements identified in EN 319 401 [6], clause 6.1 shall apply. In addition the following particular requirements apply:

a) The CA shall declare, through its CPS, how it achieves the reliability necessary for providing certification services (see the Directive 1999/93/EC [i.1], annex II (a)).

b) The CA shall document the signature algorithms and parameters employed.

7.2 Public key infrastructure - Key management life cycle

7.2.1 Certification authority key generation

Certificate generation

The requirements identified in EN 319 401 [6], clause 6.3.1 shall apply. In addition the following particular requirements apply (see the Directive 1999/93/EC [i.1], annex II (g) and (f)):

a) certification authority key generation shall be undertaken in a physically secure 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 ISO/IEC 19790 [7], level 3 or higher; or

NOTE 1: Demonstrated conformance to FIPS PUB 140-2 [i.9], level 3 is considered as fulfilment of this requirement.

- meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [2], CWA 14167-3 [3] or CWA 14167-4 [4]; or

- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national scheme. 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;

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: See TS 102 176-1 [i.13] for guidance on algorithms and their parameters.

e) a suitable time before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.

NOTE 3: These operations should be performed timely enough to allow all parties that have relationships with the CA (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be timely aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a CA which will cease its operations before its own certificate-signing certificate expiration date.

The rules of clause 7.2.2 (b to e) shall apply also to key generation even if carried out in a separate system.

7.2.2 Certification authority key storage, backup and recovery

The requirements identified in EN 319 401 [6], clause 6.3.2 shall apply. In addition the following particular requirements apply (see the Directive 1999/93/EC [i.1], annex II (g) and (f)):

Certificate generation

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

- meets the requirements identified in ISO/IEC 19790 [7], , level 3 or higher; or

NOTE: Demonstrated conformance to FIPS PUB 140-2 [i.9], level 3 is considered as fulfilment of this requirement.

- meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [2], CWA 14167-3 [3], CWA 14167-4 [4]; or

- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national scheme. 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 secure cryptographic device (see (a) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device;

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 secure 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

The requirements identified in EN 319 401 [6], clause 6.3.3 shall apply. In addition the following particular requirements apply: (see the Directive 1999/93/EC [i.1], annex II (g) and (f)).

Certificate generation and certificate distribution

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

The CA shall not hold subject private keys once they have been delivered to the subject (commonly called key escrow) (see the Directive 1999/93/EC [i.1], annex II (j)).

7.2.5 Certification authority key usage

The CA shall ensure that CA private signing keys are not used inappropriately (see the Directive 1999/93/EC [i.1], annex II (g) and (f)).

In particular:

Certificate generation

a) CA signing key(s) used for generating certificates, as defined in clause 7.3.3, may also be used to sign other types of certificates, as well as revocation status information, as long as operational requirements for the CA environment, as specified in clauses 7.2.1 to 7.2.3, 7.2.5 to 7.2.7 and 7.4, are not violated;

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 1999/93/EC [i.1], annex II (g) and (f)).

In particular:

Certificate generation

a) all copies of the CA private signing keys shall be destroyed or rendered unusable at the end of their life cycle.

7.2.7 Life cycle management of cryptographic hardware used to sign certificates

The requirements identified in EN 319 401 [6], clause 6.3.4 shall apply. In addition the following particular requirements apply (see the Directive 1999/93/EC [i.1], annex II (f)):

Certificate generation

The CA shall ensure that:

a) cryptographic hardware used to sign certificate and revocation status information is not tampered with during shipment;

b) cryptographic hardware used to sign certificate and revocation status information 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 two trusted employees;

d) cryptographic hardware used to sign certificate and revocation status information 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 1999/93/EC [i.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 during the validity time of the certificate;

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 during the validity time of the certificate;

NOTE: See TS 102 176-1 [i.13] for guidance on algorithms and their parameters.

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 subject, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control;

e) once delivered to the subject any copies of the subject's private key held by the CA shall be destroyed.

7.2.9 Secure-signature-creation device preparation

This clause is NOT applicable to the qualified certificate policies: QCP Public (see clause 5.4.3).

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive 1999/93/EC [i.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-creation 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 1: Separation may be achieved by ensuring distribution of activation data and delivery of secure-signature-creation device at different times, or via a different route.

NOTE 2: Requirement for SSCD preparation listed above may be fulfilled, for example, using a suitable protection profile, defined in accordance with ISO/IEC 15408 [1] or equivalent.

7.3 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 1999/93/EC [i.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 and, possibly, a role within that organization.

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 1999/93/EC [i.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 at time of registration 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 shall have been checked 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 example 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.

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

- full name (including surname and given names consistent with the applicable law and national identification practices);
- 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: The place should be given in accordance with 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;
- the association of the subject with the legal person or other organizational entity;

f) the CA shall record all the information used to verify the subjects' identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity;

g) if an entity other than the subject is subscribing to the CA services (i.e. the subscriber and subject are separate entities - see clause 4.5) then evidence shall be provided that the subscriber is authorized to act for the subject as identified (e.g. is authorized for all members of the identified organization);

h) the subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted;

i) 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;

  The 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 b), c), d)), subject device provision (see clause 7.4.11 items g), h) and any subsequent revocation (see clause 7.4.11 i)), identity and any specific attributes of the subject placed in the certificate, and the 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 7: The subscriber or the subject 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 8: Other parties (e.g. the associated legal person) may be involved in establishing this agreement.

NOTE 9: This agreement may be in electronic form.

j) the records identified above shall be retained for 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 according to the applicable law;

NOTE 10: The factors that need to be taken into account in identifying "applicable law" are:

i) the law of the country where the CA is established should always be considered;

ii) where subjects are registered through a registration authority in another country to where the CA is established then that RA should also apply its own country's regulations;

iii) where some subscribers are residing in another country then contractual and other legal requirements applicable to those subscribers should also be taken into account.

k) 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;

l) if the subject's key pair is not generated by the CA and the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), the certificate request process shall ensure that the public key to be certified is from a key pair effectively generated by a SSCD.

7.3.2 Certificate renewal and update

The CA shall ensure that requests for certificates issued to a subject who has already previously been registered are complete, accurate and duly authorized. This includes certificate renewals, issuing a certificate with a new subject key following revocation or prior to expiration, or update due to change to the subject's attributes (see the Directive 1999/93/EC [i.1], annex II (g)).

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

In particular:

Registration

a) the CA shall check the existence and validity of the certificate to be renewed and 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 i);

c) if any certified names or attributes have changed, or the previous certificate has been revoked, the registration information shall be 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 validity period 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 1999/93/EC [i.1], annex II (g)).

In particular:

Certificate generation

a) Qualified certificates shall contain (see annex I of the Directive 1999/93/EC [i.1]):

   i) an indication that the certificate is issued as a qualified certificate;

   ii) the identification of the CA [Certification Service Provider] and the State in which it is established;

   iii) the name of the signatory or a pseudonym, which shall be identified as such;

   iv) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

   v) signature-verification data which correspond to signature-creation data under the control of the signatory;

   vi) an indication of the beginning and end of the period of validity of the certificate;

   vii) the identity code of the certificate (e.g. certificate serial number);

   viii) the advanced electronic signature of the certification service provider issuing it;

   ix) limitations on the scope of use of the certificate, if applicable; and

   x) limits on the value of transactions for which the certificate can be used, if applicable;

NOTE 1: A standard format for qualified certificates meeting the requirements of annex I of the Directive 1999/93/EC [i.1] is defined in EN 319 412-5 [i.4].

b) the CA shall take measures against forgery of certificates, and, in cases where the CA generates signature-creation data, guarantee confidentiality during the process of generating such data; (see II (g) of the Directive 1999/93/EC [i.1]);

c) the procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject generated public key;

d) if the CA generated the subject's key:

   - the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA;

   - the private key (or SSCD - see clause 7.2.9) shall be securely passed to the registered subject;

e) 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);

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

NOTE 2: See also clause 7.4.10 on Data Protection requirements.

g) 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 general obligations specified in EN 319 401 [6], clause 6.2 shall apply. In addition, this statement shall also specify for each qualified certificate policy supported by the CSP the following:

a) 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;

b) any limitations on its use;

c) 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);

d) the period of time during which registration information (see clause 7.3.1) is retained.

NOTE 1: 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.

NOTE 2: Regarding contractual terms and conditions for certificates issued to the public attention is drawn to requirements of consumer legislation including implementation of Directive 93/13/EEC [i.12] on unfair terms in consumer contracts.

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 1999/93/EC [i.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 shall be 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 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 1999/93/EC [i.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 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 the certification authority or an entity designated by the CA;

NOTE 3: In order to maximize interoperability the CA should issue Certificate Revocation Lists as defined in ISO/IEC 9594-8 [5].

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 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 not unavailable for longer than a maximum period of time as denoted in the certification practice statement;

NOTE 4: 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;

l) revocation status information shall include information on the status of certificates at least until the certificate expires.

7.4 CA management and operation

7.4.1 Security management

The requirements identified in EN 319 401 [6], clause 6.4.1 shall apply.

7.4.2 Asset classification and management

The requirements identified in EN 319 401 [6], clause 6.4.2 shall apply.

7.4.3 Personnel security

The requirements identified in EN 319 401 [6], clause 6.4.3 shall apply.

7.4.4 Physical and environmental security

The requirements identified in EN 319 401 [6], clause 6.4.4 shall apply. In addition the following particular requirements apply:

Certificate generation, subject device provision (in particular preparation) and revocation management

a) the facilities concerned with certificate generation, subject device preparation (see clause 7.2.9) and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data;

b) any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person;

c) physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, subject device preparation (see clause 7.2.9) and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter;

d) 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 preparation (see clause 7.2.9) 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.;

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

NOTE: 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 requirements identified in EN 319 401 [6], clause 6.4.5 shall apply. In addition the following particular requirements apply:

System Planning

a) capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available;

Incident reporting and response

b) audit processes, meeting requirements specified in clause 7.4.11, shall be invoked at system startup, and cease only at system shutdown.

Certificate generation, revocation management

Operations procedures and responsibilities

The requirements identified in EN 319 401 [6], clause 6.4.5 item i) shall apply to the above service components.

7.4.6 System Access Management

The requirements identified in EN 319 401 [6], clause 6.4.6 shall apply. In addition the following particular requirements apply:

NOTE 1: With regards general requirement "*Sensitive data shall be protected*" [6] sensitive data includes registration information.

Certificate generation

a) 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;

b) 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 2: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

Dissemination

c) dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information;

Revocation management

d) 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 3: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

Revocation status

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

7.4.7 Trustworthy Systems Deployment and Maintenance

The requirements identified in EN 319 401 [6], clause 6.4.7 shall apply.

NOTE: Requirements for the trustworthy systems may be ensured using, for example, systems conforming to CWA 14167-1 [i.10] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [1].

7.4.8 Business continuity management and incident handling

The requirements identified in EN 319 401 [6], clause 6.4.8 shall apply (see the Directive 1999/93/EC [i.1], annex II (a)). In addition the following particular requirements apply:

CA systems data back up and recovery

a) CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of incident/disasters.

NOTE 1: In line with ISO/IEC 27002 [i.7], clause 10.5.1: Back-up copies of essential information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

b) Back-up and restore functions shall be performed by the relevant trusted roles specified in clause 7.4.3.

NOTE 2: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

CA key compromise

c) 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

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

- inform the following of the compromise: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties;
- indicate that certificates and revocation status information issued using this CA key may no longer be valid;
- when a CA is informed of the compromise of another CA, any CA certificate that has been issued for the compromised CA is revoked.

Algorithm compromise

e) Should any of the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage then he CA shall:

- inform all subscribers and relying parties with which the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties;
- revoke any affected certificate.

7.4.9 CA termination

The requirements identified in EN 319 401 [6], clause 6.4.9 shall apply. In addition the following particular requirements apply:

a) Regarding the requirement "The TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period;" this shall apply to registration information (see clause 7.3.1), revocation status information (see clause 7.3.6) 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).

b) Regarding the requirement "The TSP shall state in its practices the provisions made for termination of service" this shall also include:

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

7.4.10 Compliance with Legal Requirements

The requirements identified in EN 319 401 [6], clause 6.4.10 shall apply. In addition the following particular requirements apply:

a) 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);

NOTE: Data protection issues specific to this policy are addressed in:

   i) Registration (including use of pseudonyms) (see clause 7.3.1).

   ii) Confidentiality of records (see clauses 7.4.11 a) and 7.3.3 f)).

   iii) Protecting access to personal information (see clause 7.4.6).

   iv) User consent (see clause 7.3.1 i)).

b) 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;

c) 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 requirements identified in EN 319 401 [6], clause 6.4.11 shall apply. In addition the following particular requirements apply:

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

a) with regards requirement "*Records concerning the operation of services shall be made available if required for the purposes of providing evidence*". 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;

Registration

b) the CA shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged;

c) 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 i));
- any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 7.3.1 i);
- 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;

d) the CA shall ensure that privacy of subject information is maintained;

Certificate generation

e) the CA shall log all events relating to the life-cycle of CA keys;

f) the CA shall log all events relating to the life-cycle of certificates;

Subject device provision

g) 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;

h) if applicable, the CA shall log all events relating to the preparation of SSCDs;

Revocation management

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

7.5 Organizational

The requirements identified in EN 319 401 [6], clause 6.5 shall apply. In addition the following particular requirements apply:

Certificate generation, revocation management

a) 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, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides;

b) 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.

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) the certificate policy shall identify which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply;

b) there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the qualified certificate policy;

c) 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;

d) certificate policy(s) shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the qualified certificate policy;

e) a defined review process shall exist to ensure that the qualified certificate policies are supported by the CAs Certification Practices Statement (CPS);

f) the CA shall make available the qualified certificate policies supported by the CA to all appropriate subscribers and relying parties;

g) revisions to qualified certificate policies supported by the CA shall be made available to subscribers and relying parties;

h) 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;

i) a unique object identifier shall be obtained for the certificate policy of the form required in ITU-T Recommendation X.509 [5].

8.2 Exclusions for non public QCPs

Certificates issued under a 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 6.4;

b) independence of providers of certificate generation and revocation management services as specified in clause 7.5 a), b);

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 either

   i) 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

NOTE 1: This evidence can be, for example, a report from an internal audit confirming that the CA conforms to the requirements of the identified policy. If the audit is internal to the CA organization the auditors should have no hierarchical relationship with the department operating the CA.

   ii) the CA has a current assessment of conformance to the identified qualified certificate policy by a competent independent party. The results of the assessment shall be made available to subscribers and relying parties on request;

NOTE 2: This assessment can be carried out either under a "voluntary accreditation" scheme as defined in article 2.13 of the Directive 1999/93/EC [i.1], or other form of assessment carried out by a competent independent auditor. See TS 119 403 [i.2].

b) if the CA is later shown to be non-conformant in a way that significantly affects the ability of the CA to meet the requirements for qualified certificates identified in the Directive 1999/93/EC [i.1] it shall cease issuing certificates using the qualified certificate policy, until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period;

NOTE 3: Even if a CA is known to be critically non-conformant, it may issue certificates for internal and testing purposes provided that such certificates are not made available to for any other uses.

c) if the CA conformance is checked on a regular basis and whenever major change is made to the CA operations.

NOTE 4: The means required to demonstrate conformance may depend on legal requirements for the country where the CA is established.

A conformant CA shall 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:

   - 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;

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

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

e) it meets the additional requirements specified in clause 8.3.

Annex A (informative): Potential liability in the use of electronic signatures

This annex provides a conceptual framework considering the potential liability of various actors involved in issuing and using qualified certificates as defined in the Directive 1999/93/EC [i.1].

The liability requirements of CAs issuing qualified certificates (or certification service providers issuing qualified certificates using the terminology defined in the Directive 1999/93/EC [i.1]) to the public are stated in the Directive 1999/93/EC [i.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 1999/93/EC [i.1], it is advised that reference is 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.

I) Liability of CAs

A) Liability of CAs to relying parties Governed by the Directive 1999/93/EC [i.1**]**

Consideration of liability under the Directive 1999/93/EC [i.1] 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 1999/93/EC **[**i.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 1999/93/EC [i.1] implies that the liability provisions also reach reckless and intentional misconduct on the part of the CA.) Thus, to avoid liability, a CA needs to 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 1999/93/EC [i.1].

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.

Directive 1999/93/EC [i.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 are 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 needs to 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 1999/93/EC [i.1]

Where a CA does not fall into the liability scheme established by the Directive 1999/93/EC [i.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 case law 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 [i.12]) and the Distance Selling Directive 97/7/EC [i.14] 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 [i.14] 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 [i.8) and article 8 of the electronic signatures Directive 1999/93/EC [i.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 1999/93/EC [i.1], 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 1999/93/EC [i.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 statement.

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.	See clause 7.4.10 for issues relating to Data Protection.
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 address the requirements of CAs issuing qualified certificates as defined in annex II of the Directive 1999/93/EC [i.1].

Table C.1

Directive 1999/93/EC [i.1], annex II requirement	Qualified certificate policy reference
"a) demonstrate the reliability necessary for providing certification services;"	Clauses 7.1, 7.4.8, 7.4.9 and 7.5
"b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;"	Clauses 7.3.5, 7.3.6 and 7.4.6 (d)
"c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;"	Clause 7.4.11 EN 319 401 [6], clause 6.4.11 (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;"	Clauses 7.3.1 and 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;"	Clauses 7.4.1, 7.4.3 and 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;"	Clauses 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;"	Clauses 7.2.2, 7.2.3, 7.2.8, 7.3.1, 7.3.2 and 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;"	EN 319 401 [6], clause 6.5 (d, e)
"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;"	Clauses 7.4.11 and 7.4.9
"j) not store or copy signature-creation data of the person to whom the certification service provider provided key management services;"	Clause 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;"	Clauses 7.3.1 and 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."*	Clauses 7.2.3, 7.3.5, 7.3.6, 7.4.6 and 7.4.7

Annex D (informative): IETF RFC 3647 and qualified certificate policy cross-reference

NOTE: There is a difference in organization between RFC 3647 [i.3] and the present document, and in some cases RFC 3647 [i.3] is more detailed. The same clause from the present document may be related to several sections in RFC 3647 [i.3].

Table D.1: Cross-reference RFC 3647 [i.3] sections and policy references

RFC 3647 [i.3] section	Present document reference
1 INTRODUCTION	
1.1 Overview	Clause 5.1
1.2 Document name and identification	Clause 5.2
1.3 PKI participants	Clause 5.3 7 Introductory text
1.4 Certificate usage	Clause 5.3
1.5 Policy administration	ETSI see covering pages
1.5.1 Organization administering the document	ETSI
1.5.2 Contact person	See cover pages
1.5.3 Person determining CPS suitability for the policy	Clause 7.1
1.5.4 CPS approval procedures	Clause 7.1
1.6 Definitions and acronyms	Clause 3
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	
2.1 Repositories	Clause 7.3.5
2.2 Publication of certification information	Clauses 7.3.5, 7.3.6 and 7.3.4
2.3 Time or frequency of publication	Clauses 7.3.5 and 7.3.6
2.4 Access controls on repositories	Clause 7.4.6
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Naming	Clause 7.3.3
3.2 Initial identity validation	Clause 7.3.1
3.3 I Identification and authentication for re-key requests	Clause 7.3.2
3.4 Identification and authentication for revocation request	Clause 7.3.6
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	Clause 7.3.1
4.2 Certificate application processing	Clause 7.3.3
4.3 Certificate issuance	Clause 7.3.3
4.4 Certificate acceptance	Clause 7.3.1
4.5 Key pair and certificate usage	Clauses 6.2 and 6.3
4.6 Certificate renewal	Clause 7.3.2
4.7 Certificate re-key	Clause 7.3.2
4.8 Certificate modification	Clause 7.3.2
4.9 Certificate revocation and suspension	Clause 7.3.6
4.10 Certificate status services	Clause 7.3.6
4.11 End of subscription	
4.12 Key escrow and recovery	Clause 7.2.4
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	
5.1 Physical controls	Clauses 7.4.1, 7.4.4 and 7.4.5
5.2 Procedural controls	Clauses 7.4.5, 7.4.3 and 7.4.6
5.3 Personnel controls	Clause 7.4.3
5.4 Audit logging procedures	Clause 7.4.11
5.5 Records archival	Clause 7.4.11
5.6 Key changeover	Clause 7.2
5.7 Compromise and disaster recovery	Clause 7.4.8
5.8 CA or RA termination	Clause 7.4.9
6 TECHNICAL SECURITY CONTROLS	
6.1 Key pair generation and installation	Clauses 7.2.1, 7.2.3, 7.2.8 and 7.2.9
6.2 Private Key Protection and Cryptographic Module Engineering Controls	Clauses 7.2.1, 7.2.2, 7.2.6 and 7.2.7
6.3 Other aspects of key pair management	Clause 7.2

RFC 3647 [i.3] section		Present document reference
6.4	Activation data	Clauses 7.2.7 and 7.2.9
6.5	Computer security controls	Clauses 7.4.5, 7.4.6 and 7.4.7
6.6	Life cycle technical controls	Clauses 7.4.5, 7.4.6 and 7.4.7
6.7	Network security controls	Clause 7.4.6
6.8	Time-stamping	N/A
7	CERTIFICATE, CRL, AND OCSP PROFILES	
7.1	Certificate profile	Clause 7.3.3 a)
7.2	CRL profile	Clause 7.3.6
7.3	OCSP profile	
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	
8.1	Frequency or circumstances of assessment	Clause 5.4.1
8.2	Identity/qualifications of assessor	TS 119 403 [i.2]
8.3	Assessor's relationship to assessed entity	TS 119 403 [i.2]
8.4	Topics covered by assessment	Clauses 5.4.2, 5.4.3 and 8.4
8.5	Actions taken as a result of deficiency	Clauses 5.4.1 and 8.4
8.6	Communication of results	Clause 5.4.1
9	OTHER BUSINESS AND LEGAL MATTERS	
9.1	Fees	Clause 7 intro
9.2	Financial responsibility	Clause 7.5
9.3	Confidentiality of business information	
9.4	Privacy of personal information	Clauses 7.3.1 k), 7.3.3 e), 7.4.10 and 7.4.11 i)
9.5	Intellectual property rights	Cover pages
9.6	Representations and warranties	
9.7	Disclaimers of warranties	
9.8	Limitations of liability	Clause 6.4
9.9 I	Indemnities	
9.10	Term and termination	
9.11	Individual notices and communications with participants	Clause 7.3.4
9.12	Amendments	ETSI Procedures
9.13	Dispute resolution provisions	Clause 7.5
9.14	Governing law	
9.15	Compliance with applicable law	Clause 7.4.10
9.16	Miscellaneous provisions	
9.17	Other provisions	Clause 7.5

Annex E (informative): Revisions made since TS 101 456 version 1.4.3 (2007-05)

Requirements are the same as in TS 101 456 [i.11] but restructured. For general requirements applicable to TSPs refer to EN 319 401 [6].

Annex F (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/.

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

ITU-T Recommendation 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".

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

NIST SP 800-78: "Cryptographic Algorithms and Key Sizes for Personal Identity Verification", Tim Polk, Donna Dodson and William Burr.

IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

History

Document history				
V1.1.1	December 2000	Publication as TS 101 456		
V1.2.1	April 2002	Publication as TS 101 456		
V1.3.1	May 2005	Publication as TS 101 456		
V1.4.1	February 2006	Publication as TS 101 456		
V1.4.2	December 2006	Publication as TS 101 456		
V1.4.3	May 2007	Publication as TS 101 456		
V1.0.0	April 2012	Public Enquiry	PE 20120731:	2012-04-02 to 2012-07-31
V1.1.0	November 2012	Vote	V 20130115:	2012-11-16 to 2013-01-15
V1.1.1	January 2013	Publication		