ETSI EN 319 411-3 V1.1.1 (2013-01)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Trust Service Providers issuing certificates;
Part 3: Policy requirements for
Certification Authorities issuing public key certificates

Reference
DEN/ESI-000088

Keywords
e-commerce, electronic signature, Lightweight Certificate Policy, Normalized Certificate Policy, public key, security

ETSI

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

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

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

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://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 000314 (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 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.4].

The present document was previously published as TS 102 042 [i.6].

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, in its broadest sense, 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 and protect the confidentiality of electronic exchanges. This is commonly achieved by using cryptographic mechanisms which are supported by a Trust Service Provider issuing certificates, commonly called a Certification Authority (CA).

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

EN 319 401 [10] identifies general policy requirements for Trust Service Providers supporting Electronic Signatures regardless the service they provide. EN 319 411-2 [i.5] 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 "the Electronic Signature Directive"). The present document is based on the same approach as EN 319 411-2 [i.5] but is applicable to the general requirements of certification in support of cryptographic mechanisms, including other forms of electronic signature as well as the use of cryptography for authentication and encryption. Moreover, where requirements identified have general applicability they are carried forward into the present document. Annex A of the present document identifies significant differences to EN 319 411-2 [i.5] Both documents reference EN 319 401 [10] for the common general requirements.

Article 5.2 of the Electronic Signature Directive states that an electronic signature "*is not denied legal effectiveness … solely on the grounds that …[it is] not based on a qualified certificate …*". Hence, certificates issued by certification authorities operating in accordance with the present document are applicable to electronic signatures as described in article 5.2.

The present document includes options for supporting the same level of quality by certification authorities issuing qualified certificates (as required article 5.1 of the Electronic Signature Directive 1999/93/EC [i.1]) but "normalized" for wider applicability and for ease of alignment with other similar specifications and standards from other sources and institutions. Through such harmonization the quality level set by the Electronic Signature Directive can become embodied in more widely recognized and accepted specifications.

The present document applies also to certification authorities that include attributes in qualified certificates. Policy requirements for Attribute Authorities, i.e. for authorities that issue Attribute Certificate, are specified in TS 102 158 [i.9].

The present document is derived from the requirements specified in TS 102 042 "Policy requirements for certification authorities issuing public key certificates" [i.6]. Policy requirements relating to web server certificates previously covered in later versions of TS 102 042 [i.6] are to be addressed in a separate part of EN 319 411.

1 Scope

The present document specifies policy requirements relating to Trust Service Providers (TSP) issuing public key certificates. It defines policy requirements on the operation and management practices of certification authorities issuing and managing certificates such that subscribers, subjects certified by the TSP and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms.

The policy requirements are defined in terms of three reference certificate policies and a framework from which TSPs can produce a certificate policy targeted at a particular service.

The first reference policy defines a set of requirements for TSPs providing a level of quality the same as that offered by qualified certificates, without being tied to the Electronic Signature Directive (1999/93/EC [i.1]) and without requiring use of a secure user (cryptographic) device. This is labelled the "Normalized" Certificate Policy (NCP). It is anticipated that the NCP may be used as the basis for realizing the quality level set by the Qualified Certificate Policy (as defined in EN 319 411-2 [i.5]) but without the legal constraints of the Electronic Signature Directive (1999/93/EC [i.1]).

In addition to the NCP quality level, the present document specifies two alternative variants of NCP, the requirements of which may be used where alternative levels of service can be justified through risk analysis. The alternatives are referred to as:

- the Lightweight Certificate Policy (LCP) for use where a risk assessment does not justify the additional costs of meeting the more onerous requirements of the NCP (e.g. physical presence);
- the extended Normalized Certificate Policy (NCP+) for use where a secure user device is considered necessary.

Certificates issued under these policies requirements may be used in support of any asymmetric mechanisms requiring certification of public keys including electronic and digital signatures, encryption, key exchange and key agreement mechanisms.

The present document may be used by competent independent bodies as the basis for confirming that a CA provides a reliable service in line with recognized practices.

Subscribers and relying parties should consult the certificate policy and certification practice statement of the issuing TSP to obtain details of the requirements addressed by its certificate policy and how the certificate policy is implemented by the particular TSP.

The policy requirements relating to the TSP include requirements on the provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and if required, secure subject device provision. Support for other trusted third party functions such as time-stamping and attribute certificates 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 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 [i.2] for guidance on assessment of TSP processes and services against the present document. The present document references EN 319 401 [10] for policy general 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] FIPS PUB 140-1: "Security Requirements for Cryptographic Modules".

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

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

[4] 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)".

[5] 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)".

[6] 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.

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

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

[9] ISO/IEC 17021: "Conformity assessment - Requirements for bodies providing audit and certification of management systems".

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

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

[12] CENELEC EN 45011: "General requirements for bodies operating product certification systems".

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.

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

[i.5] ETSI EN 319 411-2: "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 ".

[i.6] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

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

[i.8] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[i.9] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".

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

[i.11] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 319 401 [10] and the following apply:

attribute: information bound to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity

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

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

NOTE: This is a specific type of TSP Policy as specified in EN 319 401 [10].

Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

NOTE: See ITU-T Recommendation X.509 [7].

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

NOTE: See clause 4.2 for further explanation of the concept of Certification Authority.

Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates

NOTE: See RFC 3647 [i.3].

Lightweight Certificate Policy (LCP): certificate policy which offers a quality of service less onerous than the qualified certificate policy

NOTE: The qualified certificate policy is as defined in EN 319 411-2 [i.5].

Normalized Certificate Policy (NCP): certificate policy which offers a quality of service equivalent to the qualified certificate policy

NOTE: The qualified certificate policy is as defined in EN 319 411-2 [i.5].

Public-key certificate (PKC): public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it

NOTE: See ITU-T Recommendation X.509-200811 [7].

relying party: recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate

NOTE: See RFC 3647 [i.3].

secure user device: device which holds the user's private key, protects this key against compromise and performs cryptographic functions on behalf of the user

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

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

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in EN 319 401 [10] and the following apply:

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service provider

NOTE: The more general term Trust Service Provider is used in preference to CSP in the present document except in relation to external references.

EAL	Evaluation Assurance Level
LCP	Lightweight Certificate Policy
MLA	Multilateral Agreement
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
PDS	PKI Disclosure Statement
PIN	Personal Identifier Number
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority

3.3 Notation

The requirements identified in the present document include:

a) mandatory requirements strictly to be followed in order to conform to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements strictly to be followed if applicable to the services offered under the applicable certificate policy. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected depending on the quality of the service offered under the applicable certificate policy. Such requirements are indicated by markings by "[CHOICE]" with a subsequent indicator relating to the relative quality:

- "[LCP]", "[NCP]", "[NCP+]"

4 General concepts

4.1 General Policy Requirements Concepts

The concepts described in EN 319 401 [10] 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 certificates.

A Certification Authority is a Trust Service Provider, as described in EN 319 401 [10], and also a form of certification service provider as defined in the Electronic Signatures Directive 1999/93/EC [i.1], which issues public key certificates.

4.3 Certification services

The service of issuing 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.
- **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 TSP'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:

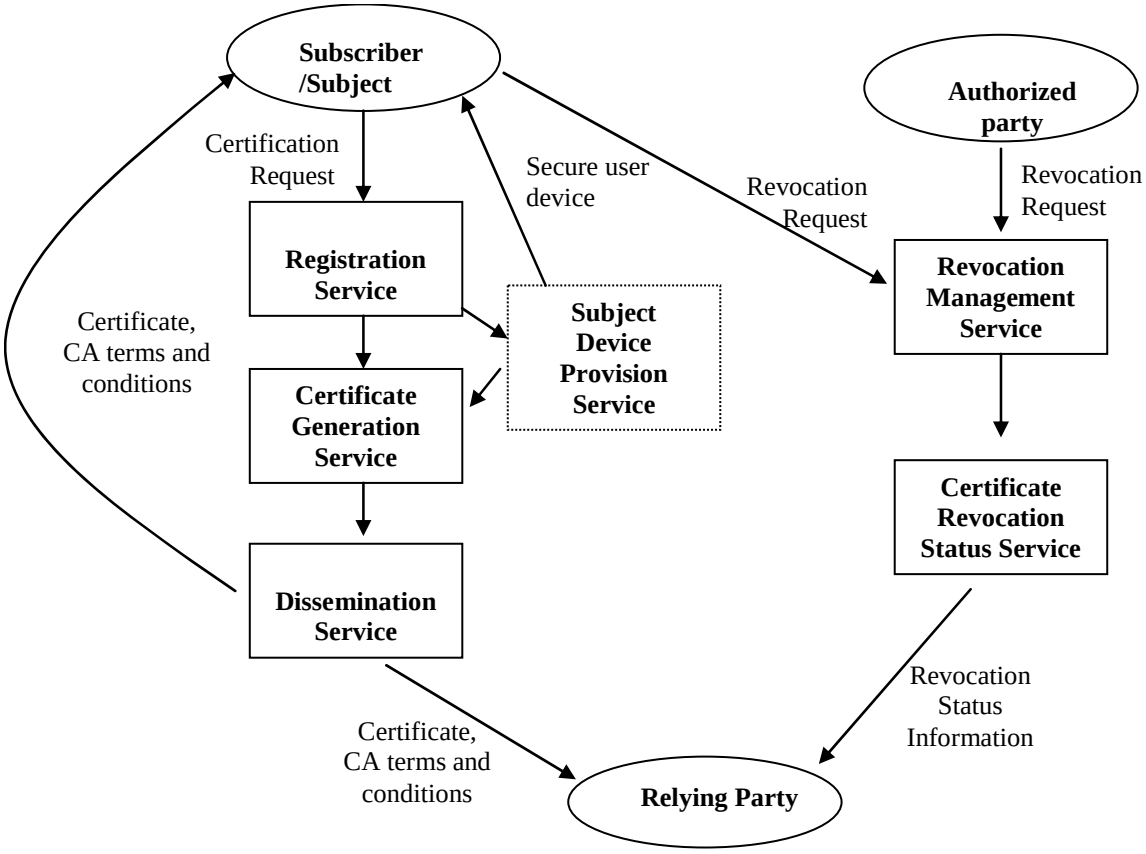
- **Subject device provision service:** prepares, and provides or makes available signature-creation devices, or other secure user device, to subjects.

NOTE: 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 signature-creation module and enabling codes and distributes the module 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 certificate policy is a form of TSP Policy as specified in EN 319 401 [10] applicable to Certification Authorities issuing public key certificates.

Certification Practice Statement is a form of TSP Practice Statement as specified in EN 319 401 [10] applicable to Certification Authorities issuing public key certificates.

4.4.1 Other CA statements

In addition, or as part of, to 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 relate to the operation of the PKI and which it is considered that the CA ought to disclose to both subscribers and relying parties.

4.5 Subscriber and subject

EN 319 401 [10] 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 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, or a computer system may perform automated commerce on behalf of the owner organization. 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. Another common example is the case of server certificates, where the certificate is required for a computer system acting on behalf of the owner organization.

In the present document to clarify the requirements which are applicable to the two different roles that may occur two different terms are used for the **"subscriber"** who contracts with the Certification Authority for the issuance of certificates and the **"subject"** to whom the certificate applies. The subscriber bears responsibility towards the CA for the use of the private key associated with the public key certificate but the subject is the individual entity 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 owner organization. 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 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*" [7], [10].

The policy requirements are defined in the present document in terms of certificate policies. Certificates issued in accordance with the present document include a certificate policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. The present document specifies three certificate policies:

1) A Normalized Certificate Policy (NCP) which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in EN 319 411-2 [i.5] but without the legal constraints related to qualified certificates implied by the Electronic Signature Directive (1999/93/EC [i.1]) and without requiring the use of a Secure Signature Creation Device.

NOTE 1: The certificate policy NCP is particularly suited to the support of Advanced Electronic Signatures, as defined by the Electronic Signature Directive (1999/93/EC [i.1]), for legal entities if they use physical means to provide reasonable confidence that the signing key remains under their sole control.

2) An extended Normalized Certificate Policy (NCP+) which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in EN 319 411-2 [i.5] but without the legal constraints implied by the Electronic Signature Directive (1999/93/EC [i.1]) and, instead of requiring the use of a Secure Signature Creation, requires the use of a secure user device.

NOTE 2: The certificate policy NCP+ is particularly suited to the support of Advanced Electronic Signatures, as defined by the Electronic Signature Directive (1999/93/EC [i.1]), for human beings as well as legal entities since the use of a secure user device provides confidence that the signing key remains under the sole control of the signatory.

3) A Lightweight Certificate Policy (LCP) which incorporates less demanding policy requirements.

Clause 8 specifies a framework for other certificate policies which enhance or further constrain the above policies.

5.2 Identification

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

a) NCP: Normalized Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ncp (1)
```

b) NCP+: Normalized Certificate Policy requiring a secure user device

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ncpplus (2)
```

c) LCP: Lightweight Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) lcp (3)
```

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

5.3 User community and applicability

The policies defined in the present document place no constraints on the user community and applicability of the certificate.

5.4 Conformance

5.4.1 Conformance claim

The CA shall only claim conformance to the present document as applied in the certificate policy (or policies) identified in the certificate that it issues:

a) if either:

i) the CA itself claims conformance to the identified 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 certificate policy by a competent independent party (e.g. conformity assessment body). The results of the assessment shall be made available to subscribers and relying parties on request.

NOTE 2: See TS 119 403 "Policy Requirements and Guidance for TSP Conformity Assessment" [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 objectives identified in the present document, then it shall cease issuing certificates using the identifiers in clause 5.2 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) The CA conformance shall be checked on a regular basis and whenever major change is made to the CA operations.

NOTE 4: See TS 119 403 [i.2] for requirements relating to re-assessment period.

5.4.2 Conformance requirements

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, including options applicable to the implemented policies, as specified in clause 7.

6 Obligations, warranties and liability

6.1 Certification Authority obligations and warranties

The obligations specified in EN 319 401 [10] clause 5.1 shall apply.

The CA shall ensure that all requirements on CA, as detailed in clause 7, are implemented as applicable to the selected certificate policy (see clauses 5.4.2 and 8.3).

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

6.2 Subscriber obligations

The CA shall oblige through agreement (see clause 7.3.1 m)) 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) accurate and complete information is submitted to the CA in accordance with the requirements of this policy, particularly with regards to registration;

b) the key pair is only used in accordance with any limitations notified to the subscriber (see clause 7.3.4);

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

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

   i) subject keys are generated using an algorithm recognized by industry as being fit for the uses of the certified key as identified in the certificate policy;

   ii) a key length and algorithm is used which is recognized as being fit for the uses of the certified key as identified in the certificate policy during the validity time of the certificate.

NOTE: See TS 102 176-1 [i.11] giving guidance on algorithms and their parameters.

e) [CONDITIONAL] if the subscriber or subject generates the subject's keys and then the private key is for creating electronic signatures the subject's private key is maintained under the subject's sole control;

f) [NCP+] use the subject's private key for cryptographic functions within the secure user device only;

g) [NCP+] [CONDITIONAL] if the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the secure user device;

h) 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, 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.

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

j) in the case of being informed that the CA which issued the subject's 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 [10] 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: 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.

6.4 Liability

The CA shall specify any disclaimers or limitations of liability in accordance with applicable laws.

7 Requirements on CA practices

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

The present document includes the provision of services for registration, certificate generation, dissemination, revocation management and revocation status (see clause 4.3). Where requirements relate to a specific service area of the CA then it is listed under one of these subheadings. Where no service area is listed, or "CA General" is indicated, a requirement is relevant to the general operation of the CA.

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

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met.

NOTE: 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 certificates. In case of clause 7.4 (CA management and operation) reference is made to other more general standards which may be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic may vary.

7.1 Certification practice statement

The general requirements specified in EN 319 401 [10], clause 6.1 shall apply. In addition the following particular requirements apply:

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

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

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

c) The CA shall document the 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 [10], clause 6.3.1 shall apply. In addition the following particular requirements apply:

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

b) [CHOICE]:

   [LCP] CA key generation shall be carried out in a product, application or device which ensures that the keys are generated in a trustworthy manner and do not compromise the security of the private key and which:

   i) meets the requirements identified in ISO/IEC 19790 [11], FIPS PUB 140-1 [1] or FIPS PUB 140-2 [2] level 2 or higher; or

   ii) is a trustworthy system which is assured to EAL 3 or higher in accordance with ISO/IEC 15408 [3], or equivalent security criteria.

   [NCP] CA key generation shall be carried out within a device which either:

   iii) meets the requirements identified in ISO/IEC 19790 [11], FIPS PUB 140-1 [1], or FIPS PUB 140-2 [2] level 3 or higher; or

   iv) meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [4], CWA 14167-3 [5] or CWA 14167-4 [6]; or

   v) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [3], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

c) Certification Authority key generation shall be performed using an algorithm recognized by industry as being fit for the CA's signing purposes.

d) The selected key length and algorithm for CA signing key shall be one which is recognized by industry as being fit for the CA's signing purposes. TS 102 176-1 [i.11] giving 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: In order to meet this requirement these operations need to 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

Certificate generation

The requirements identified in EN 319 401 [10], clause 6.3.2 shall apply. In addition the following particular requirements apply:

a) [CHOICE]:

[LCP] The CA private signing key shall be held and used in a product, application or device which does not compromise the security of the private key and which:

i) meets the requirements identified in ISO/IEC 19790 [11], FIPS PUB 140-1 [1] or FIPS PUB 140-2 [2], level 2 or higher; or

ii) is a trustworthy system which is assured to EAL 3 or higher in accordance with ISO/IEC 15408 [3], or equivalent security criteria.

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

iii) meets the requirements identified in ISO/IEC 19790 [11], FIPS PUB 140-1 [1], or FIPS PUB 140-2 [2] level 3 or higher; or

iv) meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [4], CWA 14167-3 [5], CWA 14167-4 [6]; or

v) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [3], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

b) [CHOICE]:

[LCP] When outside the signature-creation product, application or device, the secrecy of the CA's private key shall be ensured.

NOTE: This may be achieved using physical security or encryption.

[NCP] When outside the signature-creation 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 signature creation 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 secured environment (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

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

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

7.2.3 Certification Authority public key distribution

Certificate generation and certificate distribution

The requirements identified in EN 319 401 [10] clause 6.3.3 shall apply. In addition the following particular requirements apply:

The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.

In particular:

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

NOTE: For example, Certification Authority public keys may be distributed in certificates signed by itself, along with a declaration that the key authenticates the CA, or issued by another CA. By itself a self signed certificate cannot be known to come from the CA. Additional measures, such as checking the fingerprint of the certificate against information provided by a trusted source, is needed to give assurance of the correctness of this certificate.

7.2.4 Key escrow

a) [CONDITIONAL] If the subject's key is to be used for electronic signatures with the meaning of Directive 1999/93/EC [i.1], then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow).

b) [CONDITIONAL] If a copy of the subject's key is kept by the CA then the CA shall ensure that the private key is kept secret.

7.2.5 Certification Authority key usage

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

In particular:

Certificate generation

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

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

7.2.6 End of CA key life cycle

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle.

In particular:

Certificate generation

a) The use of the corresponding CA's private key, shall be limited to that compatible with the hash algorithm, the signature algorithm and signature key length used in the generating certificates, in line with current practice as in clause 7.2.1 d).

b) 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 [10], clause 6.3.4 shall apply. In addition the following particular requirements apply:

Certificate generation

In particular the CA shall ensure that:

a) cryptographic hardware is not tampered with during shipment;

b) cryptographic hardware is not tampered with while stored;

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

d) cryptographic hardware is functioning correctly; and

e) CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement. This destruction does not affect all copies of the private key. Only the physical instance of the key stored in the cryptographic hardware under consideration will be destroyed.

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.

Certificate generation

[CONDITIONAL] If the CA generates the subject's keys:

a) CA-generated subject keys shall be generated using an algorithm recognized by industry as being fit for the uses identified in the certificate policy 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 are recognized by industry as being fit for the purposes stated in the certificate policy during the validity time of the certificate.

NOTE: See TS 102 176-1 [i.11] giving 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 in a manner such that the secrecy and integrity of the key is not compromised.

e) [CONDITIONAL] If a copy of the subject's private key is not required to be kept by the CA, or other authorized entity, (see clause 7.2.4), once delivered to the subject, the private key can be maintained under the subject's sole control. Any copies of the subject's private key held by the CA shall be destroyed.

7.2.9 Secure user device preparation

[NCP+] The CA shall ensure that if it issues to the subject secure user device this is carried out securely.

Subject device provision

[CONDITIONAL]: In particular, if the CA issues a secure user device:

a) Secure user device preparation shall be securely controlled by the service provider.

b) Secure user device shall be securely stored and distributed.

c) Secure user device deactivation and reactivation shall be securely controlled.

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

NOTE: 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.

7.3 Certificate management life cycle

7.3.1 Subject registration

The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

In particular:

Registration

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.

b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.

c) 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 1: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B.

d) The service provider shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be at time of registration by appropriate means and in accordance with national law.

e) [CHOICE]:

   i) [LCP] No requirement.

   ii) [NCP] If the subject is a physical person evidence of the subject's identity (e.g. name) 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 2). Evidence for verifying other entities shall involve procedures which provide the same degree of assurance.

NOTE 2: 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.

f) [CONDITIONAL] If the subject is a physical person, evidence shall be provided of:

   i) full name (including surname and given names consistent with the applicable law and national identification practices);

   ii) date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

NOTE 3: It is recommended that the place be given in accordance with national conventions for registering births.

g) [CONDITIONAL] If the subject is a physical person who is identified in association with a legal person, or organizational entity (e.g. the subscriber), evidence shall be provided of:

   i) full name (including surname and given names, consistently with the applicable law and national identification practices) of the subject;

   ii) date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name;

   iii) full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);

iv) any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;

v) the association of the subject with the legal person or other organizational entity.

h) [CONDITIONAL] If the subject is an organizational entity, evidence shall be provided:

i) of full name of the organizational entity (private organization, government entity or non-commercial entity);

ii) of reference to a nationally recognized registration, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name.

i) [CONDITIONAL] If the subject is a device or system operated by or on behalf of an organizational entity, evidence shall be provided of:

i) identifier of the device by which it may be referenced (e.g. Internet domain name);

ii) full name of the organizational entity;

iii) a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name.

j) The CA shall record all the information necessary to verify the subject's 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.

k) 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).

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

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

i) agreement to the subscriber's obligations (see clause 6.2);

ii) if required by the CA, agreement by the subscriber to use secure user device;

iii) consent to the keeping of a record by the CA of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clause 7.4.11), the identity and any specific attributes 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;

iv) whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;

v) confirmation that the information held in the certificate is correct.

NOTE 4: The subscriber may agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct may be carried out subsequent to other aspects of the agreement.

NOTE 5: This agreement may be in electronic form.

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

NOTE 6: 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.

o) [CONDITIONAL] 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.

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

q) The CA's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

7.3.2 Certificate renewal and update

The CA shall ensure that requests for certificates issued to a subject who has previously been registered with the same CA 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.

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 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 are 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), c) and m).

c) If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the subscriber in accordance with clause 7.3.1 d) to l).

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.

In particular:

Certificate generation

a) The certificates shall include, in accordance with X.509 [7] and RFC 5280 [8]:

i) identification of the CA and the country in which it is established;

ii) the name of the subject, or a pseudonym which shall be identified as such;

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

iv) the public key which corresponds to the private key under the control of the subject;

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

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

vii) the electronic signature of the Certification Authority issuing it;

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

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

b) The CA shall take measures against forgery of certificates, and, in cases where the CA generates the subjects' private key, guarantee confidentiality during the process of generating such data.

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

d) [CONDITIONAL] if the CA generated the subject's key:

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

ii) [LCP], [NCP] the private key shall be securely passed to the registered subject;

iii) [NCP+] the secure user device containing the subject's private key shall be securely passed to the registered subject.

e) The CA shall ensure that over the life time of the CA a distinguished name which has been used in a certificate by it is never 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.

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 [10] clause 6.2 shall apply. In addition the CA shall ensure that the terms and conditions are made available to subscribers and relying parties.

In particular:

a) The indication of the certificate policy being applied shall include:

i) the 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 the use of any particular product, application or device for the purposes of applying the key-pair associated with the certificate being issued;

ii) any limitations on its use;

iii) the subscriber's obligations as defined in clause 6.2, including whether the policy requires the use of any particular product, application or device for the purposes of applying the key-pair associated with the certificate being issued;

iv) 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);

v) any limitations of liability, including the purposes/uses for which the CA accepts (or excludes) liability;

vi) the period of time which registration information (see clause 7.3.1) is retained;

vii) the period of time which CA event logs (see clause 7.4.11) are retained;

viii) procedures for complaints and dispute settlement.

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

NOTE 1: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B. Alternatively this communication 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.8] 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.

In particular:

Dissemination

a) Upon generation, the complete and accurate certificate shall be available to the 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) [CHOICE]:

   i) [LCP] the information identified in b) and c) above shall be available as specified in the CA's Certification Practice Statement;

   ii) [NCP] 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 apply 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) [CONDITIONAL] If the CA is issuing certificate to the public 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.

In particular:

Revocation management

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

   i) who may submit revocation reports and requests;

   ii) how they may be submitted;

   iii) 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.

iv) whether and for what reasons certificates may be suspended;

v) the mechanism used for distributing revocation status information;

vi) the maximum delay between receipt of a revocation report and the change to revocation status information being available to all relying parties.
This shall be at most [CHOICE]:

- [LCP] 72 hours;
- [NCP] 24 hours.

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 the certificate.

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

g) [CHOICE]:

i) [LCP] Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least every 72 hours.

ii) [NCP] Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours.

h) Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used as the sole means of providing revocation status information:

i) every CRL shall state a time for next scheduled CRL issue; and

ii) a new CRL may be published before the stated time of the next CRL issue;

iii) the CRL shall be signed by the Certification Authority or an authority designated by the CA.

NOTE 3: In order to maximize interoperability the CA should issue Certificate Revocation Lists as defined in ITU-T Recommendation X.509 [7].

Revocation status

i) [CHOICE]:

i) [LCP] Revocation status information shall be available as specified in the CA's Certification Practice Statement.

ii) [NCP] Revocation status information, 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.

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) If a CA supports multiple methods (CRL and on-line certificate status service) to provide Revocation Status, any updates to revocation status shall be available for all methods.

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

l) [CONDITIONAL] If the CA is issuing certificates to the public, Revocation status information shall be publicly and internationally available.

m) 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 [10], clause 6.4.1 shall apply.

7.4.2 Asset classification and management

The requirements identified in clause EN 319 401 [10], clause 6.4.2 shall apply.

7.4.3 Personnel security

The requirements identified in EN 319 401 [10], clause 6.4.3 shall apply.

7.4.4 Physical and environmental security

The requirements identified in EN 319 401 [10], 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 [10] clause 6.4.5 items a) to h) shall apply for all service components. In addition the following particular requirements apply.

System planning

a) [CHOICE]:

i) [LCP] no requirement;

ii) [NCP] 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) The CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

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

d) Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.

Certificate generation, revocation management

Operations procedures and responsibilities

The requirements identified in EN 319 401 [10], 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 [10], clause 6.4.6 shall apply. In addition the following particular requirements apply:

NOTE 1: With regards general requirement "*Sensitive data shall be protected*" [10], 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.

NOTE 2: TS 119 403 [i.2] defines audit framework and period.

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 3: 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 4: 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 [10], 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 [3].

7.4.8 Business continuity management and incident handling

The requirements identified in EN 319 401 [10], clause 6.4.8 shall apply. In addition the following particular requirements apply:

CA systems data backup 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 and the planned processes shall be in place.

d) Following a disaster the CA shall, where practical, take steps to avoid repetition of a disaster.

NOTE 3: ISO/IEC 27002 [i.7] gives advice about the procedures to avoid it.

Revocation status

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

   i) 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;

   ii) indicate that certificates and revocation status information issued using this CA key may no longer be valid;

   iii) 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

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

   i) inform all subscribers and relying parties with whom the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties;

   ii) revoke any affected certificate.

7.4.9 CA termination

The requirements identified in EN 319 401 [10], 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 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 [10], 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 these policy requirements are addressed in:

i) registration (including use of pseudonyms) (see clause 7.3.1);

ii) confidentiality of records (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 m)).

7.4.11 Recording of information concerning certificates

The requirements identified in EN 319 401 [10], clause 6.4.11 shall apply. In addition the following particular requirements apply:

NOTE 1: Records concerning 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:

i) type of document(s) presented by the applicant to support registration;

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

iii) storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 m));

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

v) identity of entity accepting the application;

vi) method used to validate identification documents, if any;

vii) 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 secure user devices.

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 [10], 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 conformance with the applicable certificate policies; 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 certificate policies

This clause provides a general framework for other policies for CAs issuing public key certificates. A CA may claim conformance to this general framework as defined in clause 8.3. 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.

8.1 Certificate policy management

The authority issuing the certificate policy 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 certificate policy.

c) A risk assessment shall be carried out to evaluate business requirements and determine the security requirements to be included in the certificate policy for the stated community and applicability.

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

e) A defined review process shall exist to ensure that the certificate policy is supported by the CA's Certification Practice Statement.

f) The CA shall make available the certificate policies supported by the CA to its user community.

NOTE: The CA's user community includes the subscribers/subjects eligible to hold certificates issued under the policy and any parties which may require relying upon those certificates.

g) Revisions to certificate policies supported by the CA shall be made available to subscribers and relying parties.

h) The certificate policy shall incorporate, or further constrain, all the requirements identified in clauses 6 and 7.

i) A unique object identifier shall be obtained for the certificate policy of the form required in ITU-T Recommendation X.509 [7].

8.2 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 7.3.4, of the ways in which the specific policy adds to or further constrains the requirements of the certificate policy as defined in the present document.

8.3 Conformance

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

a) if either

i) the CA claims conformance to the identified 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 certificate policy by an independent party. The results of the assessment shall be made available to subscribers and relying parties on request;

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 objectives identified in the present document, it shall cease issuing certificates using its certificate policy identifier 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 2: 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.

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

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;

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

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

e) it meets the additional requirements specified in clause 8.2.

Annex A (informative): Model PKI disclosure statement

A.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. 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.

A.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.

Statement types	Statement descriptions	Specific Requirements of 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 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 secure user device.
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).
Applicable agreements, certification practice statement, Certificate:	Identification and references to applicable agreements, certification practice statement, certificate policy and other relevant documents.	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 certificate policy, and if so through which scheme.

Annex B (informative): IETF RFC 3647 and present certificate policy document 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 B.1: Cross-reference RFC 3647 [i.3] clauses and policy references

RFC 3647 [i.3] section	Present document reference
1 INTRODUCTION	
1.1 Overview	5.1
1.2 Document name and identification	5.2
1.3 PKI participants	5.3 7 Introductory text
1.4 Certificate usage	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	-
1.5.4 CPS approval procedures	7.1
1.6 Definitions and acronyms	3
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	
2.1 Repositories	7.3.5
2.2 Publication of certification information	7.3.5, 7.3.6, 7.3.4
2.3 Time or frequency of publication	7.3.5, 7.3.6
2.4 Access controls on repositories	7.4.6
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Naming	7.3.3
3.2 Initial identity validation	7.3.1
3.3 Identification and authentication for re-key requests	7.3.2
3.4 Identification and authentication for revocation request	7.3.6
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1
4.2 Certificate application processing	7.3.3
4.3 Certificate issuance	7.3.3
4.4 Certificate acceptance	7.3.1
4.5 Key pair and certificate usage	6.2, 6.3
4.6 Certificate renewal	7.3.2
4.7 Certificate re-key	7.3.2
4.8 Certificate modification	7.3.2
4.9 Certificate revocation and suspension	7.3.6
4.10 Certificate status services	7.3.6
4.11 End of subscription	-
4.12 Key escrow and recovery	7.2.4
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	
5.1 Physical controls	7.4.1, 7.4.4, 7.4.5
5.2 Procedural controls	7.4.5, 7.4.3, 7.4.6
5.3 Personnel controls	7.4.3
5.4 Audit logging procedures	7.4.11
5.5 Records archival	7.4.11
5.6 Key changeover	7.2
5.7 Compromise and Disaster Recovery	7.4.8
5.8 CA or RA termination	7.4.9
6 TECHNICAL SECURITY CONTROLS	
6.1 Key pair generation and installation	7.2.1, 7.2.3, 7.2.8, 7.2.9
6.2 Private Key Protection and Cryptographic Module Engineering Controls	7.2.1, 7.2.2, 7.2.6, 7.2.7
6.3 Other aspects of key pair management	7.2.1, 7.2.2, 7.2.5
6.4 Activation data	7.2.7, 7.2.9
6.5 Computer security controls	7.4.5, 7.4.6, 7.4.7
6.6 Life cycle technical controls	7.4.5, 7.4.6, 7.4.7

RFC 3647 [i.3] section	Present document reference
6.7 Network security controls	7.4.6
6.8 Time-stamping	N/A
7 CERTIFICATE, CRL, AND OCSP PROFILES	
7.1 Certificate profile	7.3.3 a)
7.2 CRL profile	7.3.6
7.3 OCSP profile	-
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS	
8.1 Frequency or circumstances of assessment	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	5.4.2, 5.4.3, 8.3
8.5 Actions taken as a result of deficiency	5.4.1, 8.3
8.6 Communication of results	5.4.1
9 OTHER BUSINESS AND LEGAL MATTERS	
9.1 Fees	7 intro
9.2 Financial responsibility	7.5
9.3 Confidentiality of business information	
9.4 Privacy of personal information	7.3.1 o), 7.3.3 e), 7.4.10
9.5 Intellectual property rights	Cover pages
9.6 Representations and warranties	6
9.7 Disclaimers of warranties	6
9.8 Limitations of liability	6.4
9.9 Indemnities	-
9.10 Term and termination	-
9.11 Individual notices and communications with participants	7.3.4
9.12 Amendments	ETSI Procedures
9.13 Dispute resolution provisions	7.5
9.14 Governing law	-
9.15 Compliance with applicable law	7.4.10
9.16 Miscellaneous provisions	-
9.17 Other provisions	7.5

Annex C (informative): Revisions made since TS 102 042 V2.1.3

Requirements are the same as in TS 102 042 [i.6] but restructured. For general requirements applicable to TSPs refer to EN 319 401 [10].

Annex D (normative): Auditors qualification

This annex states requirements of bodies that may audit conformance of implementations of the present document if conformance is to be certified.

The body carrying out the audit shall be accredited for the purpose of auditing organisations implementing the present document by an official accreditation body (such as the signatories to the Multilateral Agreement (MLA) of the European Cooperation for Accreditation http://www.european-accreditation.org and International Accreditation Forum http://www.iaf.nu) as conforming to ISO/IEC 17021 [9] or EN 45011 [12].

The auditing body shall also be accredited as having the necessary competence for carrying out the audit such as specified in TS 119 403 [i.2], clause 6.

The "Independent Auditors Report" shall confirm that "the examination was conducted in accordance with European Standards/Specifications, in particular EN 319 411 part 3" followed by a list of other applicable standards e.g. TS 119 403 [i.2].

Annex E (informative): Bibliography

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".

ANS X9.79: "Public Key Infrastructure - Practices and Policy Framework".

History

Document history				
V1.1.1	April 2002	Publication as TS 102 042		
V1.2.1	May 2005	Publication as TS 102 042		
V1.2.2	June 2005	Publication as TS 102 042		
V1.2.3	December 2006	Publication as TS 102 042		
V1.2.4	March 2007	Publication as TS 102 042		
V1.3.4	December 2007	Publication as TS 102 042		
V2.1.1	May 2009	Publication as TS 102 042		
V2.1.2	April 2010	Publication as TS 102 042		
V2.2.1	December 2011	Publication as TS 102 042		
V2.3.1	November 2012	Publication as TS 102 042		
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		