Final draft ETSI EN 319 411-1 V1.1.0 (2015-12)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

Reference
DEN/ESI-0019411-1

Keywords
e-commerce, electronic signature, extended validation certificate, public key, security, trust services

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights

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

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

Foreword

This final draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 1 of a multi-part deliverable covering policy requirements for Trust Service Providers issuing certificates, as identified below:

Part 1: "General requirements";

Part 2: "Requirements for trust service providers issuing EU qualified certificates";

Part 3: "Policy requirements for Certification Authorities issuing public key certificates".

The present document is derived from the requirements specified in ETSI TS 102 042 [i.6] "Policy requirements for certification authorities issuing public key certificates" that has been updated as detailed in annex B.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	12 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Electronic commerce, in its broadest sense, is 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 (TSP) 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 TSP has properly established procedures and protective measure in order to minimize the operational and financial threats and risks associated with public key cryptographic systems.

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.14] and those from CA/Browser Forum, BRG [5].

Bodies wishing to establish policy requirements for TSPs issuing certificates in a regulatory context other than the EU can base their requirements on those specified in the present document and specify any additional requirements in a manner similar to ETSI EN 319 411-2 [i.5], which builds on the present document requirements so as to benefit from the use of generally accepted global best practices.

1 Scope

The present document specifies generally applicable policy and security requirements for Trust Service Providers (TSP) issuing public key certificates, including trusted web site certificates.

The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates. These policy and security requirements support six reference certificate policies, defined in clause 5.

A framework for the definition of policy requirements for TSPs issuing certificates in a specific context where particular requirements apply is defined in clause 7.

The present document covers requirements for CA hierarchies, however this is limited to supporting the policies as specified in the present document. It does not include requirements for root CAs and intermediate CAs for other purposes.

The present document is applicable to:

- the general requirements of certification in support of cryptographic mechanisms, including digital signatures and seals;
- the general requirements of certification authorities issuing TLS/SSL certificates;
- the general requirements of the use of cryptography for authentication and encryption.

The present document does not specify how the requirements identified can 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 ETSI EN 319 403 [i.2] for guidance on assessment of TSP processes and services. The present document references ETSI EN 319 401 [8] for general policy requirements common to all classes of TSP services.

The present document however provides in annex C, a checklist of the policy requirements specific to TSP issuing certificates (as expressed in the present document) including the generic requirements which are independent of the type of service (as expressed in ETSI EN 319 401 [8]).

The present document includes provisions consistent with the requirements from the CA/Browser Forum in EVCG [4] and BRG [5].

2 References

2.1 Normative 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 referenced 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.

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

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

[2] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

[3] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

[4] CA/Browser Forum (V1.5.5): "Guidelines for The Issuance and Management of Extended Validation Certificates".

[5] CA/Browser Forum (V1.3.0): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

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

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

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

[9] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[10] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[11] IETF RFC 6960: "X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP".

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

2.2 Informative 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 referenced document (including any amendments) applies.

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

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 EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

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

[i.4] ISO 19005 parts 1 to 3: "Document management - electronic document file format for long-term preservation".

[i.5] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU 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 27002:2013: "Information technology -- Security techniques -- Code of practice for information security management".

[i.8] ISO/IEC 7498-2/ ITU-T Recommendation X.800: "Data communications network -- Open systems interconnection -- Security, structure and applications: Security architecture for open systems interconnection for CCITT applications".

[i.9] CEN TS 419 261: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures".

[i.10] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.11] IETF RFC 5246: "The Transport Layer Security Protocol Version 1.2".

[i.12] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.13] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.15] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.16] CEN TS 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup".

[i.17] CEN TS 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services".

[i.18] CEN TS 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup".

[i.19] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services".

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [8] and the following apply:

auditor: person who assesses conformity to requirements as specified in given requirements documents

NOTE: See ETSI EN 319 403 [i.2].

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

NOTE 1: The term certificate is used for public key certificate within the present document.

NOTE 2: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

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 1: See clause 4.2 for explanation of the relative role of certificate policies and certification practice statement.

NOTE 2: This is a specific type of trust service policy as specified in ETSI EN 319 401 [8].

NOTE 3: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

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

NOTE 1: Within the scope of the present document the set of certificates is related to end user certificates.

NOTE 2: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

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

NOTE 1: A CA can be:

1) a trust service provider that creates and assigns public key certificates; or

2) a technical certificate generation service that is used by a certification service provider that creates and assign public key certificates.

NOTE 2: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

Certification Authority Revocation List (CARL): revocation list containing a list of CA-certificates issued to certification authorities that are no longer considered valid by the certificate issuer

NOTE: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

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

NOTE 1: See IETF RFC 3647 [i.3].

NOTE 2: This is a specific type of Trust Service practice statement as specified in ETSI EN 319 401 [8].

Coordinated Universal Time (UTC): As indicated in ETSI EN 319 401 [8].

Cross Certificate: certificate that is used to establish a trust relationship between two certification authorities

digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

NOTE: See ISO/IEC 7498-2/Recommendation ITU-T X.800 [i.8].

Domain Validation Certificate (DVC): certificate which has no validated organizational identity information for the subject, only identifying the subject by its domain name

EV certificate: See Extended Validation certificate.

Extended Validation Certificate (EVC): As indicated in the EVCG [4].

high security zone: specific physical location of the security zone (see ETSI EN 319 401 [8], clause 7.8) where the Root CA key is held

Organizational Validation Certificate(OVC): certificate that includes validated organizational identity information for the subject

Publicly-Trusted Certificate (PTC): certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly

NOTE 1: An RA can assist in the certificate application process or revocation process or both.

NOTE 2: See IETF RFC 3647 [i.3].

registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests

revocation officer: person responsible for operating certificate status changes [i.8]

root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

NOTE 1: A Root CA certificate is generally self-signed but the Root-CA can also be certified by a (Root)CA from another domain (e.g. cross-certification, Root-Signed in the context of a root-signing program, etc.).

NOTE 2: A Root CA can be used as the Trust Anchor for many applications (e.g. browsers) but nothing prevents the TSP to present subordinate CAs for this purpose, according to the business context.

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

secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP

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

NOTE: Relationship between subscriber and subject is described in clauses 5.4.2 and 6.3.5.

subordinate CA: certification authority whose Certificate is signed by the Root CA, or another Subordinate CA

NOTE: A subordinate CA normally either issues end user certificates or other subordinate CA certificates.

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

NOTE 1: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

NOTE 2: A Trust Anchor can also be a Root CA.

NOTE 3: Examples of trust anchors are as in a trusted List [i.12] or a list of trusted CA certificates distributed by an application software provider.

3.2 Abbreviations

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

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB	CA/Browser
CAB Forum	CA/Browser Forum
CARL	Certification Authority Revocation List
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.

DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
EV	Extended Valuation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
LCP	Lightweight Certificate Policy
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy

PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTC	Publicly-Trusted Certificate

NOTE: Within the context of the present document PTC is used synonymously with EVC, DVC and OVC as per CAB Forum documents.

RA	Registration Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol

NOTE: IETF RFC 5246 [i.11] or earlier equivalent Secure Socket Layer protocol.

TSP	Trust Service Provider
UTC	Coordinated Universal Time

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any CP. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements applicable to the services offered under the applicable CP. Such requirements are indicated by clauses marked by the applicable CP as follows:

   i) "[LCP]", "[NCP]", "[NCP+]", "[EVCP]", "[OVCP]" and "[DVCP]";

   ii) [PTC] is used to denote requirements applicable to EVCP, OVCP and DVCP for CAB Forum requirements.

4 General concepts

4.1 General policy requirements concepts

See ETSI EN 319 401 [8], clause 4 and IETF RFC 3647 [i.3], clauses 3.1 and 3.4 for guidance.

4.2 Certificate policy and certification practice statement

4.2.1 Overview

The present document serves as a basis for the TSP to develop, implement, enforce, and update:

- a CPS that describes the practices and procedures used to address all the requirements identified for the applicable TSP policy;
- a CP document that includes all rules valid for a given CP as specified in clause 5 or clause 7.

NOTE 1: The CP document contains additional information which is out of scope of the present document (e.g. the description of the certificate profile).

NOTE 2: The CP generally refers to the CPS to indicate how the TSP implements the policy requirements for the selected CP.

This clause explains the relative roles of CP and CPS. It places no restriction on the form of a CP or CPS specification.

CPS is a form of TSP Statement as specified in ETSI EN 319 401 [8], clause 6.1 applicable to CAs issuing certificates.

NOTE 3: Subscribers and relying parties can consult the CP and CPS of the issuing TSP to obtain details of the requirements addressed by its CP and how the CP is implemented by the particular TSP.

4.2.2 Purpose

In general, the purpose of the CP, referenced by a policy identifier in a certificate, states "what is to be adhered to", while a CPS states "how it is adhered to", i.e. the processes it will use in creating and maintaining the certificate.

4.2.3 Level of specificity

A CP is a higher level document than a CPS; it can apply to a community to which several CAs belong that abide by the common set of rules specified in that CP. A CPS defines how one specific CA meets the technical, organizational and procedural requirements identified in a CP.

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

4.2.4 Approach

The approach of a CP is significantly different from a CPS. A CP is defined independently of the specific details of the specific operating environment of a CA, whereas a CPS is tailored to the organizational structure, operating procedures, facilities, and computing environment of a CA. A CP can be defined by the provider, by standards, by national (e.g. government) or international organizations, by the customers (subscribers) of the CA or by the users of certification services, whereas the CPS is always defined by the provider.

4.2.5 Certificate Policy

As described in IETF RFC 3647 [i.3], clause 3.3, certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. The present document defines six CPs:

1) A Normalized Certificate Policy (NCP) which meets general recognized best practice for TSPs issuing certificates used in support of any type of transaction.

2) An extended Normalized Certificate Policy (NCP+) which offers the same quality as that offered by the NCP for use where a secure cryptographic device (signing or decrypting) is considered necessary. The requirements for this CP include the policy requirements for the issuance and management of NCP certificates.

3) A Lightweight Certificate Policy (LCP) offering a quality of service less onerous than the NCP (requiring less demanding policy requirements) for use where a risk assessment does not justify the additional burden of meeting all requirements of the NCP (e.g. physical presence), for certificates used in support of any type of transaction (such as digital signatures, web authentication or electronic seal).

4) An Extended Validation Certificate Policy (EVCP) for TLS/SSL certificates offering the level of assurance required by CAB Forum for EVC. The requirements for this CP are built on the policy requirements for the issuance and management of NCP certificates, enhanced to refer to requirements from EVCG [4]. It includes, except where explicitly indicated, all the Normalized Certificate Policy (NCP) requirements, plus additional provisions suited to support EVC issuance and management as specified in EVCG [4].

5) A Domain Validation Certificate Policy (DVCP) for TLS/SSL certificates offering the level of assurance required by CAB Forum for DVC. The policy requirements for this CP are built on the policy requirements for the issuance and management of LCP certificates, enhanced to refer to requirements from the BRG [5] as applicable to domain validation certificates. It includes, except where explicitly indicated, all the Lightweight Certificate Policy (LCP) requirements, plus additional provisions suited to support DVC issuance and management as specified in BRG [5].

6) An Organizational Validation Certificate Policy (OVCP) for TLS/SSL certificates offering the level of assurance required by CAB Forum for OVC. The policy requirements for this CP are built on the policy requirements for the issuance and management of LCP certificates, enhanced to refer to requirements from BRG [5] as applicable to organizational validation certificates. It includes, except where explicitly indicated, all the Lightweight Certificate Policy (LCP) requirements, plus additional provisions suited to support OVC issuance and management as specified in BRG [5].

Clause 7 specifies a framework for other CPs which enhance or further constrain the above policies.

4.3 Other Trust Service Providers statements

In addition to, or as part of, the CP and CPS a TSP issues terms and conditions. Terms and conditions can cover a broad range of commercial terms or PKI specific terms that are not necessarily communicated to the customer, etc.

The PKI disclosure statement is that part of the CA's terms and conditions which relate to the operation of the PKI.

4.4 Certification services

NOTE 1: The present document does not mandate any sub division of the services of a TSP. Requirements are stated in subsequent clauses.

The certification services are broken down in the present document into the following component services for the purposes of classifying requirements:

- **Registration service:** verifies the identity and if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.

NOTE 2: This service includes proof of possession of non-CA generated subject private keys.

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

- **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.

- **Subject device provision service (optional):** prepares, and provides or makes available secure cryptographic devices, or other secure devices, to subjects.

NOTE 3: Examples of this service are:

i) a service which generates the subject's key pair and distributes the private key to the subject;

ii) 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.

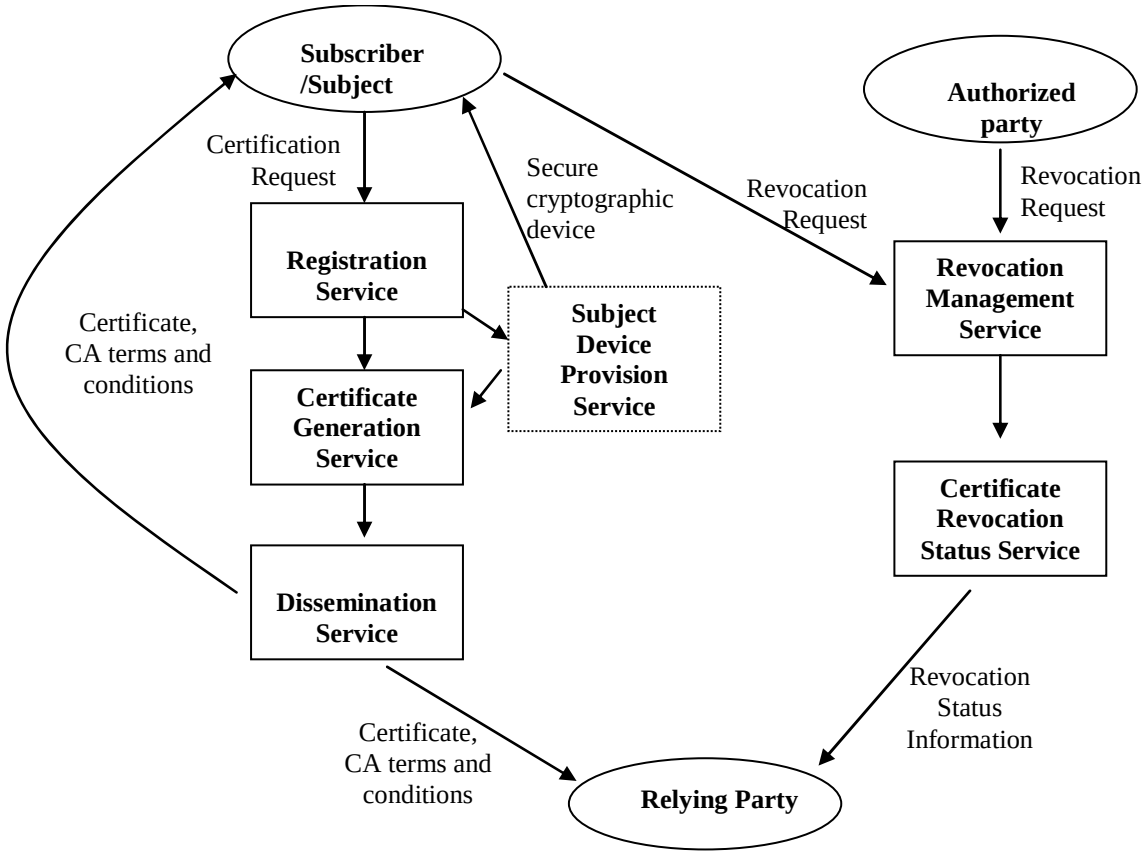

Figure 1: Illustration of subdivision of certification services used in the present document

NOTE 4: Figure 1 is for illustrative purposes. Clause 6 specifies the specific requirements for each of the services.

NOTE 5: Italicized and underlined sub headings in clause 6 are used to identify where the subsequent requirements relate to a specific service component as described in clause 4.4 (e.g. certificate generation).

5 General provisions on Certification Practice Statement and Certificate Policies

5.1 General requirements

The present document is structured broadly in line with IETF RFC 3647 [i.3] to assist TSPs in applying these requirements to their own CP and CPS documentation.

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 TSP then it is listed under one of these subheadings. Where no service area is listed, or "General" is indicated, a requirement is relevant to the general operation of the TSP.

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 1: 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 TSP can employ in issuing certificates. In some cases reference is made to other more general standards which can be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic can vary.

NOTE 2: Italicized sub headings in this clause are used to identify where the subsequent requirements relate to a specific service component as described in clause 4.4 (e.g. certificate generation).

[NCP+, EVCP]: all requirements specified for [NCP] shall apply.

[DVCP, OVCP]: all requirements specified for [LCP] shall apply.

5.2 Certification Practice Statement requirements

The general requirements specified in ETSI EN 319 401 [8], clause 6.1 shall apply. In addition the following particular requirements apply:

NOTE 1: A TSP can document practices relating to specific CP requirements separate from the main CPS document.

a) The TSP CPS should be structured in accordance with IETF RFC 3647 [i.3].

b) The CPS shall include the complete CA hierarchy, including root and subordinate CA's.

c) The CPS shall include the signature algorithms and parameters employed.

d) The TSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis.

NOTE 2: The TSP is not obliged to disclose any aspects containing sensitive information.

e) [PTC]: Clause 2.2 of BRG [5] and clause 8.3 of EVCG [4] shall apply.

f) [PTC]: Clause 2 of the BRG [5] and clause 8.2.1 of EVCG [4] shall apply.

g) The TSPs CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP.

5.3 Certificate Policy name and identification

As described in IETF RFC 3647 [i.3], clause 3.3, certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. 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 cryptographic 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)
```

d) EVCP: Extended Validation Certificate Policy

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

e) DVCP: Domain Validation Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) dvcp (6)
```

f) OVCP: Organizational Validation Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ovcp (7)
```

If any changes are made to a CP as described in clause 4.2.5 which affects the applicability then the policy identifier should be changed.

5.4 PKI participants

5.4.1 Certification Authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the CA. The CA has overall responsibility for the provision of the certification services identified in clause 4.4. The CA is identified in the certificate as the issuer and its private key is used to sign certificates.

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

EXAMPLE: A CA can sub-contract all the component services, including the certificate generation service (sometimes also called CA with the second meaning of CA as per definition above). However, the key used to sign the certificates is identified as belonging to the CA, and the CA maintains overall responsibility for meeting the requirements defined in the present document.

A CA is a type of Trust Service Provider (TSP), as defined in the Regulation (EU) No 910/2014 [i.14], 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.

A TSP may include a hierarchy of CAs. Where a TSP includes a hierarchy of subordinate CAs up to a root CA the TSP is responsible for ensuring the subordinate-CAs comply with the applicable policy requirements. If the TSPs Trust Anchor is signed by a Root CA outside the scope of the TSP policies then the Root CA requirements apply to the TSP's Trust Anchor.

5.4.2 Subscriber and subject

In the framework of the present policies, the subject can be:

a) a natural person;

b) a natural person identified in association with a legal person;

c) a legal person (that can be an Organization or a unit or a department identified in association with an Organization); or

d) a device or system operated by or on behalf of a natural or legal person.

When a subscriber is the subject it will be held directly responsible if its obligations are not correctly fulfilled.

When the subscriber is acting on behalf of one or more distinct subjects to whom it is linked (e.g. the subscriber is a company requiring certificates for its employees to allow them to participate in electronic business on behalf of the company), responsibilities of the subscriber and of the subject are addressed in clause 6.3.4 item e).

The link between the subscriber and the subject is one of the following:

a) To request a certificate for natural person the subscriber is:

   i) the natural person itself;

   ii) a natural person mandated to represent the subject; or

NOTE: The local legal dispositions can address the handover of responsibility to a third person.

   iii) any entity with which the natural person is associated (such as the company employing the natural person or a non-profit legal person the natural person is member of).

b) To request a certificate for legal person the subscriber is:

   i) any entity as allowed under the relevant legal system to represent the legal person; or

   ii) a legal representative of a legal person subscribing for its subsidiaries or units or departments.

c) To request a certificate for a device or system operated by or on behalf of a natural or legal person the subscriber is:

   i) the natural or legal person operating the device or system;

   ii) any entity as allowed under the relevant legal system to represent the legal person; or

   iii) a legal representative of a legal person subscribing for its subsidiaries or units or departments.

5.4.3 Others

Other participants, not covered by the present document, may be identified by the TSP.

5.5 Certificate usage

The policies NCP, NCP+ and LCP place no constraints on the user community and applicability of the certificate. The applicability of other certificates is as described below.

The specific purpose of EV Certificates is described in EVCG [4], clause 2.

The purpose of PTC is described in BRG [5], clause 1.4.1.

Certificates issued under EVCG [4] or BRG [5] are for publicly trusted certificates used to identify web servers accessed via the TLS or SSL protocol as per IETF RFC 5246 [i.11].

6 Trust Service Providers practice

6.1 Publication and repository responsibilities

The TSP shall make certificates available 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. If the subject is a device or system, the consent of the natural or legal person responsible for the operating of the device or system needs to be obtained, instead of the subject.

c) The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).

d) The applicable terms and conditions shall be readily identifiable for a given certificate.

e) [CONDITIONAL]:

   i) [LCP]: the information identified in b) and c) above shall be available as specified in the TSP's CPS.

   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 TSP, the TSP 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 CPS.

f) [CONDITIONAL] If the TSP is not issuing publicly-trusted certificates, the information identified in c) above should be publicly and internationally available.

g) [CONDITIONAL] If the TSP is issuing publicly-trusted certificates, the information identified in c) above shall be publicly and internationally available.

6.2 Identification and authentication

6.2.1 Naming

NOTE: Requirements for naming in certificates are as specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7] and the appropriate part of ETSI EN 319 412 [2], [9] and [10]. See clause 6.6.1 of the present document.

6.2.2 Initial identity validation

The TSP shall verify the identity of the subscriber and subject and shall check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

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

In particular:

Registration

a) The TSP 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 (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

   - [PTC]: The verification methods shall follow those specified in clause 11 of the EVCG [4] and clause 3.2 of BRG [5].

b) [CONDITIONAL] [NCP]: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

NOTE 2: An example of the required indirect evidence of identity is one or more registration documents electronically signed by a person trusted to have checked the persons' identity in line with the requirements of this clause. Some other examples can be found in Annexes B and C of the EVCG [4].

c) [CONDITIONAL]: If the subject is a natural person (i.e. physical personal as opposed to legal person), evidence shall be provided of:

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

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

      The place of birth should be given in accordance to national or other applicable conventions for registering births.

d) [CONDITIONAL] [NCP]: If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence of the identity, in particular the ones listed in e), shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

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

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

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

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

4) any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity identified in association with the legal person, consistent with the national or other applicable identification practices;

5) affiliation of the natural person to the legal person consistent with national or other applicable identification practices;

6) [CONDITIONAL]: when applicable, the association between the legal person and any organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices; and

7) approval by the legal person and the natural person that the subject attributes also identify such organization.

f) [CONDITIONAL] [NCP]: If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence of the identity, in particular the ones listed in g), shall be checked against a duly mandated subscriber either directly, by physical presence of a person allowed to represent the legal person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

g) [CONDITIONAL]: If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided:

1) of full name of the organizational entity (private organization, government entity, business entity or non-commercial entity) consistent with the national or other applicable identification practices:

- [PTC]: BRG [5], clause 3.2.2, shall apply.
- [EVCP]: EVCG [4], clause 11.2, shall apply.

2) [CONDITIONAL]: when applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.

h) [CONDITIONAL] [NCP]: If the subject is a device or system operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person, evidence of the identity, in particular the ones listed in i), shall be checked against a duly mandated subscriber either directly, by physical presence of a person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

i) [CONDITIONAL]: If the subject is a device or system operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided of:

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

2) full name of the organizational entity:

- [PTC]: clause 3.2.2 of BRG [5] shall apply.
- [EVCP]: EVCG [4], clause 11.2.1, shall apply.

3) any relevant existing registration information (e.g. company registration) of the legal person or other organizational entity identified in association with the legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices;

4) a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the organizational entity from others with the same name; and

5) [CONDITIONAL]: when applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.

j) [CONDITIONAL] [NCP]: If the subject is a device or system operated by a natural person, evidence of the identity, in particular the ones listed in k), shall be checked against either directly, by physical presence of the natural person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

k) [CONDITIONAL]: If the subject is a device or system operated by a natural person, evidence shall be provided of:

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

2) a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the natural person from others with the same name;

3) [PTC]: clause 3.2.3 of BRG [5] shall apply.

l) The TSP 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.

m) [CONDITIONAL] If an entity other than the subject is subscribing to the TSP services (i.e. the subscriber and subject are separate entities - see clause 5.4.2) 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), in particular:

1) full name (including surname and given names consistent with the national or other applicable identification practices) of the subscriber;

2) when the subscriber represents a natural person (not associated with a legal person) an agreement to this representation; or

3) when the subscriber represents a legal person (either for requesting a certificate for that legal person or to request a certificate for a natural person identified in association with the legal person), an agreement that the subscriber is allowed to represent the legal person and is entitled to request certificates for that legal person or its members are required. In particular, if the subscriber is not a natural person, it shall be represented by a natural person whose authorization to represent the subscriber shall be proved.

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

o) The TSP shall provide evidence of how they meet applicable data protection legislation within their registration process.

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

q) To avoid any conflicts of interests, the subscriber and TSP organization entity shall be separate entities. The only exception is the organization running all or part of the RA tasks subscribing a certificate for itself or persons identified in association with it (as a subject), and for which the exception is stated in the TSP's policies.

6.2.3 Identification and authentication for Re-key requests

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized. This includes re-key following revocation or prior to expiration, or update due to change to the subject's attributes.

In particular:

Registration

a) i) The TSP shall check the existence and validity of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid.

ii) [EVCP]: Clauses 9.4 and 11.3 of EVCG [4] shall apply.

iii) [OVCP] and [DVCP]: Clauses 6.3.2 and 3.3.1 of BRG [5] shall apply.

b) If any of the TSP terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with clause 6.3.4, items a), b), c) and d).

c) Requirements of clause 6.2.2 shall apply.

NOTE: Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

6.2.4 Identification and authentication for revocation requests

The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

In particular:

Revocation management

a) The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

i) Who can submit requests for revocation or reports of events which may indicate the need to revoke a certificate.

ii) How they can be submitted.

iii) Any requirements for subsequent confirmation of requests for revocation or reports of events which may indicate the need to revoke a certificate.

EXAMPLE 1: Confirmation can be required from the subscriber if a compromise is reported by a third party.

iv) Whether and for what reasons certificates can be suspended or revoked.

- [PTC]: Clause 4.9 of the BRG [5] shall apply.

v) The mechanism used for distributing revocation status information.

vi) The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties. This shall be at most 24 hours.

NOTE: If the revocation or suspension request cannot be confirmed within 24 hours then the status need not be changed.

vii) The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties. This shall be at most 60 minutes.

With regard to vii), if the revocation request requires revocation in advance (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time according to the TSP policies.

With regard to vi) and vii), a TSP may give faster process times for certain revocation reasons.

viii) The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours.

b) Requests for revocation and reports of events relating to revocation shall be processed on receipt.

EXAMPLE 2: 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.

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

6.3 Certificate Life-Cycle operational requirements

6.3.1 Certificate application

NOTE: See also clause 6.2.2 regarding identity validation.

In particular:

Registration

a) [CONDITIONAL] if the subject's key pair is not generated by the CA, the certificate request process shall check that the subject has possession or control of the private key associated with the public key presented for certification.

b) [EVCP]: For a dual control procedure in the validation process EVCG [4], clause 14.1.3, shall apply.

6.3.2 Certificate application processing

Application for certificates shall be from a trusted registration service.

NOTE: General requirements on the security of the TSP including human resources, operational security, and networks and privacy as specified in clauses 6.4.4, 6.5.6, 6.5.7 and 6.8.4 apply to external registration authorities.

In particular:

a) [CONDITIONAL] when external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

6.3.3 Certificate issuance

The CA shall issue certificates securely to maintain their authenticity. The requirements for the use of the certificate profiles should be linked to a CP.

In particular:

Certificate generation

a) See clause 6.6.1 for certificate profiles.

b) The CA shall take measures against forgery of certificates, and in cases where the CA generates the subjects' key pair, 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 rekey, including the provision of any subject-generated public key.

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

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

   ii) [LCP] and [NCP] the private key shall be securely passed to the registered subject; or to the TSP managing the subject's private key; and

iii) [NCP+] the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of the TSP managing the key on behalf of the subject, the TSP shall ensure that the subject has sole control (or if the subject is a legal person "control") over its signing key.

e) Over the life time of the CA a distinguished name which has been used in a certificate by it shall never be re-assigned to another entity.

f) [CONDITIONAL] if a certificate is issued to a natural person identified as being as associated with the legal person, then the subject attributes identifying the organization in the certificate should represent the legal person or sub-entity of that legal person and the subject identifier in the certificate shall be the natural person.

g) Use of the policy identifier:

- [NCP]: The CP identifier shall be:

  i) as specified in clause 5.3 item a); and/or

  ii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

- [NCP+] The CP identifier shall be:

  i) as specified in clause 5.3 item b); and/or

  ii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

- [LCP] The CP identifier shall be:

  i) as specified in clause 5.3 item c); and/or

  ii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

- [EVCP] The CP identifier shall be:

  i) as specified in clause 5.3, item d);

  ii) as specified in EVCG [4], clause 9.3.5; and/or

  iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

- [DVCP] The CP identifier shall be:

  i) as specified in clause 5.3, item e);

  ii) as specified in BRG [5], clause 7.1.6.1; and/or

  iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

- [OVCP] The CP identifier shall be:

  i) as specified in clause 5.3 item f);

  ii) as specified in BRG [5], clause 7.1.6.1; and/or

  iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

6.3.4 Certificate acceptance

The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate. See clause 6.9.4.

In particular:

Registration

a) Before entering into a contractual relationship with a subscriber, the TSP shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 6.9.4.

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) i) The TSP shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form;

ii) The terms and conditions may be transmitted electronically;

iii) The terms and conditions may use the model PKI disclosure statement given in annex A.

d) The TSP shall record the signed agreement with the subscriber (see clause 6.4.5 c)).

e) [CONDITIONAL]: Where the subscriber and subject are two separate entities and the subject is a natural person, the signed agreement shall be in 2 parts:

1) The first part shall be signed by the subscriber and shall include:

i) agreement to the subscriber's obligations (see clause 6.9.4) and the general terms and conditions as identified in clause 6.1;

ii) if required by the TSP, agreement by the subscriber to use a secure cryptographic device;

iii) consent to the keeping of a record by the TSP 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 clauses 6.4.5 and 6.4.6), 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 TSP 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;

vi) obligations applicable to subjects (see clause 6.9.4);

vii) [PTC]: clause 9.6.3 of BRG [5] shall apply;

viii) [EVCG]: EVCG [4] clause 11.8 shall apply.

2) The second part shall be signed by the subject and shall include:

i) the agreement by the subject;

ii) obligations applicable to subjects (see clause 6.9.4);

iii) if required by the TSP, agreement by the subject to use a secure cryptographic device;

iv) consent to the keeping of a record by the TSP 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 clauses 6.4.5 and 6.4.6), 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 TSP terminating its services.

f) [CONDITIONAL]: Where the subject and subscriber are the same entity the agreement shall be in one or two parts and shall include the part 1 and part 2 items listed above.

NOTE 1: The subscriber can agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct can be carried out subsequent to other aspects of the agreement.

g) This agreement may be in electronic form.

h) The records identified above shall be retained for the period of time as indicated to the subscriber (see item c) above).

NOTE 2: See also clause 6.4.6 regarding retention of information.

6.3.5 Key pair and certificate usage

The subscriber's obligations (see clause 6.3.4) shall include items a) to j) below.

If the subject and subscriber are separate entities and the subject is a natural person, the subject's obligations shall include at least items b) c) e) f) h) i) and j) (as listed below):

a) accurate and complete information is submitted to the TSP 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 and the subject if the subject is a natural or legal person (see clause 6.9.4);

c) unauthorized use of the subject's private key is avoided;

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

   i) subject keys should be generated using an algorithm as specified in ETSI TS 119 312 [i.10] for the uses of the certified key as identified in the CP; and

   ii) a key length and algorithm should be as specified in ETSI TS 119 312 [i.10] for the uses of the certified key as identified in the CP during the validity time of the certificate.

NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

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

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

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 cryptographic device;

h) notify the TSP 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, potentially compromised;

   ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; 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, except for key decipherment;

j) in the case of being informed that the subject's certificate has been revoked, or the issuing CA has been compromised, ensure that the private key is not used by the subject.

NOTE 2: In the case of being informed that the subject's certificate has been compromised, the subject certificate is revoked, see clauses 6.2.4 and 6.3.9.

The notice to relying parties (see clause 6.9.4) shall recommend the relying party to:

k) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 6.9.4);

NOTE 3: See clauses 6.2.4, 6.3.9 and 6.3.10 for requirements on certificate revocation and suspension.

l) 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 6.9.4; and

m) take any other precautions prescribed in agreements or elsewhere:

i) Depending on CA's practices related to the problem reporting and response capability:

1) [EVCP]: refer to clause 11.3 of EVCG [4].

2) [OVCP] and [DVCP]: refer to clause 4.9.3 of BRG [5].

6.3.6 Certificate renewal

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized.

EXAMPLE: The subscriber can, if the TSP offers this service, request a certificate renewal where relevant attributes presented in the certificate have not changed or when the certificate lifetime is nearing expiry.

In particular:

Registration

a) i) The TSP 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.

ii) [EVCP]: Clauses 9.4 and 11.3 of EVCG [4] shall apply.

iii) [OVCP] and [DVCP]: Clauses 6.3.2 and 3.3.1 of BRG [5] shall apply.

b) If any of the TSP terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with clause 6.3.4, items a), b), c) and d).

c) Requirements h) to l) of clause 6.2.2 shall apply.

NOTE 1: Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

Certificate generation

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 nor that the certificate has been revoked due to any other security breach.

NOTE 2: See also clause 6.3.8.

6.3.7 Certificate Re-key

NOTE: See clause 6.2.3.

6.3.8 Certificate modification

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized. This includes certificate update due to change to the subject's attributes.

EXAMPLE: The subscriber can, if the TSP offers this service, request a certificate re-key where relevant attributes presented in the certificate have changed.

In particular:

Registration

a) If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information shall be verified, recorded, agreed to by the subscriber in accordance with clause 6.2.2.

6.3.9 Certificate revocation and suspension

The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

In particular:

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

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

c) [CONDITIONAL]: Where Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours; and:

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

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

   iii) the CRL shall be signed by the CA or an entity designated by the TSP.

NOTE: See clause 6.6.2 regarding CRL profile requirements.

d) [OVCP] and [DVCP]: The TSP shall operate and maintain its certificate status information. Clause 4.10.2 of BRG [5] shall apply.

e) [EVCP]: TSP shall comply with EVCG [4], clause 13.

f) [CONDITIONAL]: Where CARL is used a new CARL shall be generated at least once a year with a nextUpdate of at most 1 year after the issuing date. In any case, a new CARL shall be generated once a CA certificate has been revoked.

g) In the case of any cross-certificates issued by the CA, the CARL should be issued at least every 31 days.

6.3.10 Certificate status services

The TSP shall provide services for checking the status of the certificates.

In particular:

Revocation status

a) 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 TSP, the TSP 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 CPS.

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

c) Revocation status information shall include information on the status of certificates at least until the certificate expires.

d) OCSP shall be supported.

NOTE 1: See clause 6.6.3 for profile requirements of OCSP.

e) CRL should be supported.

NOTE 2: See clause 6.6.2 for profile requirements of CRL.

f) [CONDITIONAL]: If a TSP 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, and the information provided by all services shall be consistent over time taking into account different delays in updating the status information for all the methods.

g) The revocation status information shall be publicly and internationally available.

6.3.11 End of subscription

No policy requirement.

6.3.12 Key escrow and recovery

a) The security of any duplicated subject's private keys shall be at the same level as for the original subject's private keys.

b) The number of any duplicated subject's private keys shall not exceed the minimum needed to ensure continuity of the service.

c) [CONDITIONAL]: If the subject's private key is to be used for digital signatures, 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), and results in its use not being under the sole control of the signer or owner.

NOTE: This does not preclude the TSP generating and managing the key on behalf of the user provided that the key is kept under the sole control of the user.

d) [CONDITIONAL]: If the subject's private key is to be used for authentication, then the CA should not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow), and results in its use not being under the sole control of the signer or owner.

e) [CONDITIONAL]: If the subject's private key is to be used for decryption, then the CA may back it up.

f) [CONDITIONAL]: If the CA requires a subject private key used for decryption to be escrowed by the CA or a designated entity, then this private key shall not have other key usages.

g) [CONDITIONAL]: If a copy of the subject's key is kept by the CA for escrow then the CA shall keep secret the private key and only make it available to appropriately authorized persons.

6.4 Facility, management, and operational controls

6.4.1 General

The requirements identified in ETSI EN 319 401 [8], clauses 5, 6.3 and 7.3, shall apply.

6.4.2 Physical security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.6, shall apply. In addition the following particular requirements apply:

Certificate generation and revocation management

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

b) Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.

c) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation 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 TSP's physical and environmental security policy for systems concerned with certificate generation 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.

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

f) Other functions relating to TSP operations may be supported within the same secured area provided that the access is limited to authorized personnel.

g) Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.

6.4.3 Procedural controls

The requirements identified in ETSI EN 319 401 [8], clause 7.4, items b), c), d) and e) shall apply.

In addition the following particular requirements apply:

NOTE: With regards general to requirement "*Sensitive data shall be protected*" [8], Sensitive data includes registration information.

Certificate generation

a) Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

- [PTC]: BRG [5], clause 4.3 shall apply.

6.4.4 Personnel controls

The requirements identified in ETSI EN 319 401 [8], clause 7.2 shall apply:

a) In addition to the trusted roles identified in ETSI EN 319 401 [8], 7.2 item i), the trusted roles, of the registration and revocation officers responsibilities as defined in CEN TS 419 261 [i.9] shall be supported.

b) [PTC]: the role of validation specialist shall be included as specified in BRG [5] and EVCG [4].

6.4.5 Audit logging procedures

The requirements identified in ETSI EN 319 401 [8], clause 7.10, shall apply. In addition the following particular requirements apply:

NOTE: ETSI TS 101 533-1 [i.13] suggests provisions on how to preserve digital data objects.

a) All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

Registration

b) All events related to registration including requests for certificate re-key or renewal shall be logged.

c) All registration information including the following shall be 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 identity card or passport) of identification documents, if applicable;

iii) storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 6.3.4, item d));

iv) any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 6.3.4, item d);

v) identity of entity accepting the application;

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

vii) name of receiving TSP and/or submitting Registration Authority, if applicable.

d) The TSP shall maintain the privacy of subject information.

Certificate generation

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

f) The TSP shall log all events relating to the life-cycle of certificates.

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

Revocation management

h) The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

6.4.6 Records archival

The following particular requirements apply:

NOTE: ETSI TS 101 533-1 [i.13] suggests provisions on how to preserve digital data objects.

a) The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

i) log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA (see clause 6.4.5, item g));

ii) documentation as identified in clause 6.3.4.

6.4.7 Key changeover

No policy requirement.

6.4.8 Compromise and disaster recovery

The requirements identified in ETSI EN 319 401 [8], clauses 7.9 and 7.11, shall apply. In addition the following particular requirements apply:

TSP systems data backup and recovery

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

b) In line with ISO/IEC 27002 [i.7], clause 12.3: 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.

c) Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.

d) [CONDITIONAL]: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

CA key compromise

e) The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster and the planned processes shall be in place.

NOTE: It is suggested that the plan include a requirement that all subject keys are revoked.

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

g) In the case of compromise the TSP shall as a minimum:

i) inform the following of the compromise: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs. 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; and

iii) revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA.

Algorithm compromise

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

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

ii) schedule a revocation of any affected certificate.

6.4.9 Certification Authority or Registration Authority termination

The requirements identified in ETSI EN 319 401 [8], clause 7.12, shall apply. In addition the following particular requirements apply:

a) Regarding the requirement of bullet b) iii) of clause 7.12 of ETSI EN 319 401 [8], this shall apply to registration information (see clauses 6.2.2, 6.3.1 and 6.3.4), revocation status information (see clause 6.3.10) and event log archives (see clauses 6.4.5 and 6.4.6) for their respective period of time as indicated to the subscriber and relying party (see clause 6.8.10).

b) Regarding the requirement d) of clause 7.12 of ETSI EN 319 401 [8], this shall also include the handling of the revocation status for unexpired certificates that have been issued.

c) When another cross certified TSP stops all operations, including handling revocation (see clause 6.4.9 b), all cross certificates to that TSP shall be revoked.

NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [8], clause 7.12 d) i), include cross certified TSP.

6.5 Technical security controls

6.5.1 Key pair generation and installation

The requirements identified in ETSI EN 319 401 [8], clause 7.5, shall apply.

In addition the following particular requirements apply:

Certificate generation

The CA shall generate keys securely and the private key shall be secret.

a) CA key pair generation and the subsequent certification of the public key, shall be undertaken in a physically secured environment (see clause 6.4.2) by personnel in trusted roles (see clause 6.4.4) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

b) CA key pair generation should be performed using an algorithm as specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

c) The selected key length and algorithm for CA signing key should be one which is specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

NOTE 2: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

d) Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate for signing subject key pairs and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate shall also be generated and distributed in accordance with this policy.

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

f) The TSP shall have a documented procedure for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users. This procedure shall indicate, at least, the following:

   i) Roles participating in the ceremony (internal and external from the organization);

   ii) Functions to be performed by every role and in which phases;

   iii) Responsibilities during and after the ceremony; and

   iv) Requirements of evidence to be collected of the ceremony.

g) The TSP shall produce a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report shall be signed:

   i) For root CA: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) and a trustworthy person independent of the TSP management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

   ii) For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.

   iii) [PTC]: clause 6.1.1.1 of the BRG [5] shall apply.

Certificate generation and dissemination

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

NOTE 3: For example, CA public keys can be distributed in self-signed certificates, 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.

Certificate generation / subject device provision

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

i) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the uses identified in the CP during the validity time of the certificate.

j) CA-generated subject keys should be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [i.10] for the purposes stated in the CP during the validity time of the certificate.

NOTE 4: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

k) CA-generated subject keys shall be generated and stored securely whilst held by the TSP.

Subject device provision

l) The subject's private key shall be delivered to the subject's device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised. If the TSP or any of its designated RAs become aware that a subject's private key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the TSP shall revoke all certificates that include the public key corresponding to the communicated private key;

m) The CA shall delete all copies of a subject private key after delivery of the private key to the subject, except for conditions as described in clause 6.3.12.

n) [NCP+]: The TSP shall secure the issuance of a secure cryptographic device to the subject. In particular:

   i) Secure cryptographic device preparation shall be done securely.

   ii) Secure cryptographic device shall be securely stored and distributed.

6.5.2 Private key protection and cryptographic module engineering controls

Certificate generation

In addition to requirements in clause 6.5.1 the following particular requirements apply:

a) CA key pair generation shall be carried out within a secure cryptographic device which:

   i) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national or internationally recognized evaluation criteria for IT security. 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; or

NOTE 1: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408 [1], are currently under development within CEN as CEN TS 419 221-2 [i.16], CEN TS 419 221-3 [i.17], CEN TS 419 221-4 [i.18], or CEN EN 419 221-5 [i.19].

   ii) meets the requirements identified in ISO/IEC 19790 [3] or FIPS PUB 140-2 [12] level 3.

   The secure cryptographic device should be as per i).

NOTE 2: With the general availability of devices which meet ISO/IEC 15408 [1], it is expected that ISO/IEC 19790 [3] or FIPS 140-2 [12] level 3 will no longer be acceptable.

NOTE 3: This applies also to key generation even if carried out in a separate system.

b) The CA private signing key shall be held and used within a secure cryptographic device as indicated in a) above.

c) [CONDITIONAL]: When outside the secure cryptographic device (see item b) above) the CA private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

d) 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 6.4.2). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

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

f) [CONDITIONAL]: Where the CA private signing keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.

g) The secure cryptographic device shall not be tampered with during shipment.

h) The secure cryptographic device shall not be tampered with while stored.

i) The secure cryptographic device shall be functioning correctly.

j) The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

NOTE 4: This destruction does not necessarily affect all copies of the private key. Only the physical instance of the key stored in the secure cryptographic device under consideration will be destroyed.

6.5.3 Other aspects of key pair management

The TSP shall use appropriately the CA private signing keys and shall not use them beyond the end of their life cycle.

In particular:

Certificate generation

a) CA signing key(s) used for generating certificates as defined in clause 6.3.3, 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.

c) The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in clause 6.5.1, item c).

d) All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

e) [CONDITIONAL]: If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 [6] and aligned with point c).

6.5.4 Activation data

The following particular requirements apply:

Certificate generation

a) The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees.

Subject device provision

[CONDITIONAL]: In particular, if the TSP issues a secure cryptographic device:

b) Secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

c) Where the secure cryptographic device (e.g. smartcard) has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure cryptographic device.

NOTE: Separation can be achieved by ensuring distribution of activation data and delivery of secure user device at different times, or via a different channel.

6.5.5 Computer security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.4, items a) and f), shall apply.

NOTE: Requirements for the trustworthy systems can be ensured using, for example, systems conforming to CEN TS 419 261 [i.9] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [1].

In addition the following particular requirements apply:

Certificate generation

a) Local network components (e.g. routers) shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by the TSP.

b) The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

Dissemination

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

Certificate Revocation status

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

Certificate generation and revocation management

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

EXAMPLE: This can use an intrusion detection system, access control monitoring and alarm facilities.

6.5.6 Life cycle security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.7 shall apply for all service components. In addition the following particular requirements apply:

System planning

a) [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.

b) [PTC]: clause 5 of the BRG [5] shall apply.

Certificate generation and revocation management

c) See clause 6.5.5, item e).

6.5.7 Network security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.8 shall apply.

In addition the following particular requirements apply:

a) The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

b) The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

c) The TSP shall grant access to secure zones and high security zones to only trusted roles.

d) The Root CA system shall be in a high security zone.

6.5.8 Timestamping

NOTE: Not in the scope of the present document. See ETSI EN 319 421 [i.15] for policy requirements for TSPs issuing time-stamps.

6.6 Certificate, CRL, and OCSP profiles

6.6.1 Certificate profile

The certificates shall meet the requirements, specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

The certificate shall be issued according to the relevant certificate profile as identified below:

i) [LCP, NCP and NCP+] for issuance of certificates to natural persons (excluding for web site certificates): ETSI EN 319 412-2 [9].

ii) [LCP, NCP and NCP+] for issuance of certificates to legal persons (excluding for web site certificates): ETSI EN 319 412-3 [10].

iii) [PTC] for issuance of certificates for web sites or devices: ETSI EN 319 412-4 [2].

6.6.2 CRL profile

The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

6.6.3 OCSP profile

The OCSP shall be as defined in IETF RFC 6960 [11].

6.7 Compliance audit and other assessment

NOTE: See ETSI EN 319 403 [i.2].

6.8 Other business and legal matters

6.8.1 Fees

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

6.8.2 Financial responsibility

The requirements identified in ETSI EN 319 401 [8], clause 7.1.1, item c) shall apply.

6.8.3 Confidentiality of business information

No policy requirement.

6.8.4 Privacy of personal information

The requirements identified in ETSI EN 319 401 [8], clause 7.13, item c) shall apply. In addition the following particular requirements apply:

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

b) Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clauses 6.4.5 and 6.4.6).

NOTE: Data protection issues specific to these policy requirements are addressed in:

i) registration (see clause 6.2.2);

ii) confidentiality of records (clauses 6.3.2, item a) and 6.4.5, item d));

iii) protecting access to personal information;

iv) user consent (see clause 6.3.4, item d)).

6.8.5 Intellectual property rights

No policy requirement.

6.8.6 Representations and warranties

The requirements identified in ETSI EN 319 401 [8] clause 6.3, item b and clause 6.4 of the present document shall apply. TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP functionality is undertaken by outsourcers.

In addition the following particular requirements apply:

a) The TSP shall provide all its certification services consistent with its CPS.

b) [PTC]: the TSP shall comply with BRG [5], clause 9.6.

6.8.7 Disclaimers of warranties

See clause 6.8.6.

NOTE: See also clause A.2 for additional information.

6.8.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.9.4.

NOTE: For TSP operating in EU, see article 13 of the Regulation (EU) No 910/2014 [i.14] and ETSI EN 319 401 [8], clause 7.12, item d).

6.8.9 Indemnities

No policy requirement.

6.8.10 Term and termination

No policy requirement.

6.8.11 Individual notices and communications with participants

No policy requirement.

6.8.12 Amendments

No policy requirement.

6.8.13 Dispute resolution procedures

The requirements identified in ETSI EN 319 401 [8], clauses 6.2, item i) and 7.1.1, item e) shall apply.

NOTE: See clause A.2 for additional information.

6.8.14 Governing law

Not in the scope of the present document.

6.8.15 Compliance with applicable law

The requirements identified in ETSI EN 319 401 [8], clause 7.13, item a) shall apply.

6.8.16 Miscellaneous provisions

No policy requirement.

6.9 Other provisions

6.9.1 Organizational

The requirements identified in ETSI EN 319 401 [8], clause 7.1 shall apply. In addition the following particular requirements apply:

Certificate generation and revocation management

a) The parts of the TSP 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.

NOTE: The TSP may need to take into account privacy requirements.

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

6.9.2 Additional testing

a) The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

EXAMPLE: Publishing PKCS#12 certificates in its web site.

b) Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).

c) [PTC]: BRG [5], clause 2.2 shall apply.

d) For cross certificates, clause 3.2.6 of BRG [5] shall apply.

6.9.3 Disabilities

The requirements identified in ETSI EN 319 401 [8], clause 7.13, item b) shall apply.

6.9.4 Terms and conditions

The requirements identified in ETSI EN 319 401 [8], clause 6.2 shall apply.

In addition the following particular requirements apply:

a) The terms and conditions shall include a notice as specified in clause 6.3.4.

b) [PTC]: Clause 9.8 of BRG [5] shall apply with the exception indicated in EVCG [5], clause 18.

7 Framework for the definition of other certificate policies

7.1 Certificate policy management

The authority issuing a CP other than the ones defined in clause 5 shall demonstrate that the CP is effective.

In particular, when the TSP issues other CPs:

a) The CP 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 CP.

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

d) CPs should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP.

e) A defined review process should exist to ensure that the CP is supported by the CA's CPS.

f) The TSP should make available the CPs supported by the TSP to its user community.

NOTE: The TSP'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 CPs supported by the TSP should be made available to subscribers and relying parties.

h) The CP shall incorporate, or further constrain, all the requirements identified in clauses 5 and 6 where they are without a specific marking relating CP as specified in clause 5.3.

i) The CP shall specify the Recommendation ITU-T X.509 [6] certificate profile requirements.

j) [CONDITIONAL]: Certificate profiles as defined by ETSI EN 319 412 part 2 to 4 [2], [9] and [10] should be used where appropriate.

k) A unique object identifier shall be obtained for the CP of the form required in Recommendation ITU-T X.509 [6].

7.2 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 6.9.4, of the ways in which the specific policy adds to or further constrains the requirements of the CP as defined in the present document.

Annex A (informative): Model PKI disclosure statement

A.1 Introduction

The proposed model PKI disclosure statement is for use as a supplemental instrument of disclosure and notice by a TSP. A PKI disclosure statement may assist a TSP to respond to regulatory requirements and concerns, particularly those related to consumer deployment. Further, the aim of the model PKI disclosure statement is to foster industry "self-regulation" and build consensus on those elements of a CP and/or CPS that require emphasis and disclosure.

Although CP and CPS 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 CP or CPS.

This annex provides an example of the structure for a PKI disclosure 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 CP/CPS clauses.

Statement types	Statement descriptions	Specific Requirements of certificate policy
TSP contact info:	The name, location and relevant contact information for the CA/PKI (name of responsible person, address, website, info mail, faq, etc.), including clear information on how to contact the TSP to request a revocation.	
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. CP being applied (including OID and short summary).
Reliance limits:	The reliance limits, if any.	Indication that the certificate is only for use with digital signatures or seals. The period of time which registration information and TSP event logs (see clauses 6.4.5 and 6.4.6) 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 6.3.5, item a) to j), including whether the policy requires use of a secure cryptographic 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 6.3.5, item k) to m)).
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 6.8.8).
Applicable agreements, CPS, CP:	Identification and references to applicable agreements, CPS, CP and other relevant documents.	CP being applied.

Statement types	Statement descriptions	Specific Requirements of certificate policy
Privacy policy:	A description of and reference to the applicable privacy policy.	See clause 6.8.4 for issues relating to Data Protection. The period of time during which registration information (see clause 6.3.4, item h)) is retained.
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.
TSP 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 TSP has been certified to be conformant with a CP, and if so through which scheme. The link toward the Trusted List of the country within which the TSP is operated.

A.3 The PDS format

The PDS should be available under PDF/A format as specified in ISO 19005 parts 1 to 3 [i.4].

Annex B (informative): Revisions made since previous versions

Some updates and additional requirements to the present document have been added.

The main clauses of the ETSI TS 102 042 [i.6] are the same but restructured according to the IETF RFC 3647 [i.3] for a better clarification because the present document is only intended for the issuance and management of public key certificates.

The present document is based on the general requirements applicable to TSPs, the ETSI EN 319 401 [8], which is used as the main document.

Main revisions are:

- Harmonization of terminology between the ETSI EN 319 400 series (Trust Service Provider (TSP), Certification Service Provider (CSP), Certification Authority (CA), Subject, Subscriber).
- Clarification of the scope with regard to legal person.
- Addition of requirements relating to Root and subordinate CAs.
- Annexation of a checklist summarizing the conformity criteria in such a way that it can be used by the TSP itself to prepare for an assessment and/or by the assessor when conducting the assessment, for the sake of facility for both the assessor and the TSP to be assessed.
- Update reference to Cryptographic suites to ETSI TS 119 312 [i.10].
- Modification of *Subject* definition.
- Move *Subscriber* definition toward ETSI EN 319 401 [8].
- Clarification of requirements' applicability to Root versus Subordinate CA where relevant.
- In responsibilities, clause 5.4.1.
- Addition of key generation procedure's requirements, clause 6.5.1.
- Clarification of requirements related to Subject and Subscriber.
- Clarification Subject / Subscriber obligation in case of certificate compromise (clause 6.3.5, item a) to j)).
- Clarification with regard to the use of a PDS (clause 6.9.4).
- Addition of a requirement on the maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the revocation status information (clause 6.2.4, item a).
- Introduction of two trusted roles in clause 6.4.4 (Registration Officers and Revocation Officers) in order to align with CEN terminology. Also introducing another role used in CAB Forum documents, validation specialist.
- Precisions in the annex related to the PDS.
- Restructured according to IETF RFC 3647 [i.3].

All revisions done in CAB Forum documents up to date are included in the present document.

Annex C (informative): Conformity assessment checklist

A checklist for the policy requirements specified in the present document as well as the generic requirements which are independent of the TSP (as expressed in ETSI EN 319 401 [8]) is contained in the spreadsheet file (en_31941101v010100v0.zip) which accompanies the present document.

The checklist summarizes the requirements in such a way that it can be used by the TSP itself to prepare for an assessment of its practices against the present document (i.e. serve as a basis for a self-declaration) and/or by the assessor when conducting the assessment, for the sake of facility for both the assessor and the TSP to be assessed.

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the checklist file identified in this annex so that it can be used for its intended purposes and may further publish the completed checklist.

Annex D (informative): Bibliography

- Recommendation ITU-T X.843/ISO/IEC 15945: "Information technology - Security techniques - Specification of TTP services to support the Application of Digital Signatures".
- Recommendation ITU-T X.842/ISO/IEC 14516: "Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services".
- ANSI X9.79: "Public Key Infrastructure - Practices and Policy Framework".

History

Document history				
V1.0.0	June 2015	EN Approval Procedure	AP 20151016:	2015-06-18 to 2015-10-16
V1.0.1	July 2015	Publication as ETSI TS 119 411-1		
V1.1.0	December 2015	Vote	V 20160221:	2015-12-23 to 2016-02-22