ETSI EN 319 411-1 V1.3.1 (2021-05)

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

Reference
REN/ESI-0019411-1v131

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

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

ETSI EN 319 411-1: "General requirements";

ETSI EN 319 411-2: "Requirements for trust service providers issuing EU qualified certificates";

ETSI TR 119 411-4: "Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2 [i.5]".

NOTE: Part 3 of this multi-part deliverable has been withdrawn.

The present document is derived from the requirements specified in ETSI TS 102 042 [i.6].

National transposition dates	
Date of adoption of this EN:	12 May 2021
Date of latest announcement of this EN (doa):	31 August 2021
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	28 February 2022
Date of withdrawal of any conflicting National Standard (dow):	28 February 2022

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 (TSPs) 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 several reference certificate policies, defined in clauses 4 and 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 for electronic 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's processes and services. The present document references ETSI EN 319 401 [8] for general policy requirements common to all classes of TSP's services.

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 https://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 (V1.6.7): "Guidelines for The Issuance and Management of Extended Validation Certificates".

[5] CA/Browser Forum (V1.7.1): "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

[6] ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: 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".

[13] ETSI TS 119 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

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/Recommendation ITU-T X.800: "Data communications network - Open systems interconnection - Security, structure and applications: Security architecture for open systems interconnection for CCITT applications".

[i.9] TS 419 261: "Security requirements for trustworthy systems managing certificates and time stamps", (produced by CEN).

[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] TS 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).

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

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

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

[i.20] ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2".

[i.21] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.22] ETSI TS 119 511:"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

3 Definition of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the terms 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 have been revoked 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 have been revoked 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 name: the label assigned to a node in the Domain Name System

NOTE: See BRG [5].

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

Individual Validation Certificate (IVC): certificate that includes validated individual identity information for the subject

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: permanent termination of the certificate's validity before the expiry date indicated in the certificate

revocation officer: person responsible for operating certificate status changes ISO/IEC 7498-2/Recommendation ITU-T X.800 [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

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice statement

NOTE: Validity period as defined by IETF RFC 5280 [7].

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 (ETSI TS 119 612 [i.12]) or a list of trusted CA certificates distributed by an application software provider.

3.2 Symbols

Void.

3.3 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.

DIS	DIssemination Services
DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
IVC	Individual Validation Certificate
IVCP	Individual 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
OVR	General Requirement
PDF/A	Portable Document Format/Archive
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, IVC and OVC as per CAB Forum documents [4] and [5].

RA	Registration Authority
SDP	Subject Device Provisioning
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

3.4 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 that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) 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]", "[IVCP]" and "[DVCP]";

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

Each requirement is identified as follows:

<3 letters service component> - < the clause number> - <2 digit number - incremental>.

The service components are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **GEN:** Certificate Generation Services
- **REG:** Registration Services
- **REV:** Revocation Services
- **DIS:** Dissemination Services
- **SDP:** Subject Device Provisioning
- **CSS:** Certificate Status Service

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for deleted requirements are left and completed with "Void".
- The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

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 Certification Services applicable documentation

4.2.1 Certification Practice Statement

In general, the Certificate Policy (CP) (see clause 4.2.2), referenced by a policy identifier in a certificate, states "what is to be adhered to", while a Certification Practice Statement (CPS) states "how it is adhered to", i.e. the processes the TSP will use in creating and maintaining the certificate. The TSP issuing certificates develops, implements, enforces, and updates a **Certification Practice Statement (CPS)** which is a trust service practice statement such as defined in ETSI EN 319 401 [8]. See clause 5.2.

The CPS describes ***how*** the TSP operates its service and is owned by the TSP: it is tailored to the organizational structure, operating procedures, facilities, and computing environment of the TSP. The CPS defines how the TSP meets the technical, organizational and procedural requirements identified in a Certificate Policy (CP) (see clause 4.2.2). For example, where the CP requires secure management of the private key(s), the CPS can describe the dual-control, secure storage practices, and so on, relying on operational procedures that in turn can provide the details with locations, access lists and access procedures.

NOTE: The operational procedures mentioned above can be in low-level documents providing the specific details necessary to complete the practices identified in the CPS. This documentation is generally regarded as internal, e.g. defining specific tasks and responsibilities within the organization. Such documentation can be used in the daily operation of the TSP and reviewed by those doing a process review, but due to its internal nature it is considered private and proprietary and therefore beyond the scope of the present document. The published CPS can thus be limited to the information useful for subscribers/subject and relying parties, and be completed by (confidential) elements that do not have to be disclosed.

The target audience of the practice statements can be the auditors, the subscribers, the subjects and the relying parties.

The present document provides requirements identified as necessary to support state-of-the-art certification services built on best practices.

4.2.2 Certificate Policy

A **Certificate policy (CP)** describes ***what*** the certificate is in terms of quality (requirements to be adhered to), profile, applicability, etc. It can contain diverse information beyond the scope of the present document to indicate the applicability of the service (e.g. the detailed description of the certificate profile). A CP is a specific type of trust service policy as defined in ETSI EN 319 401 [8]. According to ETSI EN 319 401 [8], it is mandatory for a TSP to identify the trust service policies it supports. Such policy is defined independently of the specific details of the specific operating environment of a TSP and is not necessarily part of the TSP's documentation; practice statement and general terms and conditions are sufficient.

Following ETSI EN 319 401 [8], a CP can apply to several TSPs supporting a user community that abide by the common set of rules specified in that CP. A CP can be defined, for example: by the TSP, by a third party (e.g. standardisation organisations such as ETSI), by national government or international organizations, by the customers (subscribers) of the TSP or by the users of certification services. The CPS is defined by the TSP.

When the TSP does not issue its own CP, it is expected that the TSP provides minimal information about the certification service it offers in its documentation (CPS or terms and conditions (see clause 4.2.3), including the indication that it complies with all rules valid for a given referred CP, in the case of the present document as specified in clause 5 or clause 7. The present document does not put constraints on the form of the CPs; a CP can be a stand-alone document or be provided as part of the practice statements and/or the general terms and conditions.

The target audience of the CP can be the subscribers, the subjects and the relying parties.

NOTE: Subscribers and relying parties can consult the CPS and/or terms and conditions of the issuing TSP to obtain details how the CP is implemented by the TSP. These documents can refer to each other.

For certification services, the identification of the CP is communicated through the documentation provided to the subscribers and relying parties and in addition, 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.

TSP conforming to the present document's normative requirements may use OIDs defined in the present document in its documentation and in the certificates it issues. The present document defines seven 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).

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].

7) An Individual Validation Certificate Policy (IVCP) for TLS/SSL certificates offering the level of assurance required by CAB Forum for IVC. 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 individual validation certificates. It includes, except where explicitly indicated, all the Lightweight Certificate Policy (LCP) requirements, plus additional provisions suited to support IVC issuance and management as specified in BRG [5].

The above CPs can be used as they are without amendments but can also be used as a basis for creating more elaborate policies; clause 7 specifies a framework for other CPs which enhance or further constrain the above policies.

4.2.3 Terms and conditions and PKI disclosure statement

A TSP is required to issue terms and conditions (see clause 6.9.4). This can be as part of the CPS or the CP if issued by the TSP. Alternatively, this can be a standalone document. The terms and conditions are specific to a TSP. The target audience of the terms and conditions can be the subscribers, the subjects and the relying parties.

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

NOTE: The presence of some elements is mandatory in the terms and conditions as requested in the present document, however the present document places no restriction on the form of terms and conditions; it can be a standalone document for a public audience, or it can be split over subscriber's agreement(s) and information to relying parties. The form and content of the terms and conditions can also depend on national regulations.

4.3 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, or control over, 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:

  - a service which generates the subject's key pair and distributes the private key to the subject (this includes "soft" keys i.e. keys protected by software environment);
  - 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 TSP's services.

Figure 1 illustrates the interrelationship between the services.

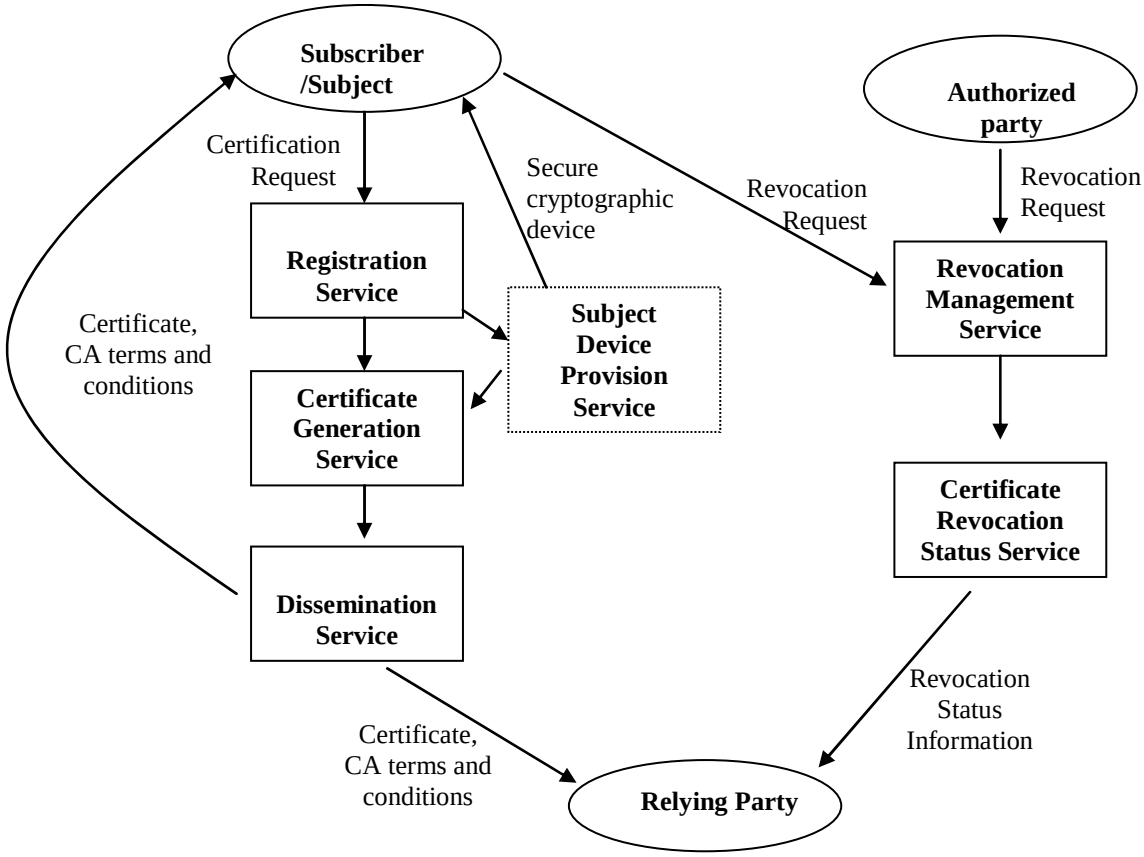

Figure 1: Illustration of subdivision of certification services used in the present document

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

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 documentation.

The present document includes the provision of services for registration, certificate generation, dissemination, revocation management and revocation status (see clause 4.3).

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

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a 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.

OVR-5.1-01: Void.

OVR-5.1-01A [NCP+, EVCP]**:** Unless otherwise specified, all requirements specified for [NCP] shall apply.

OVR-5.1-02: Void.

OVR-5.1-02A [DVCP, IVCP, OVCP]**:** Unless otherwise specified, all requirements specified for [LCP] shall apply.

OVR-5.1-03: The TSP's CP should specify the requirements for the use of certificate profiles.

5.2 Certification Practice Statement requirements

OVR-5.2-01: 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.

OVR-5.2-02: The TSP's CPS should be structured in accordance with IETF RFC 3647 [i.3].

OVR-5.2-03: Void.

OVR-5.1-03A: The CP(s) identified by the TSP's documentation should specify the requirements on certificate profiles to be used.

OVR-5.2-04: The TSP's CPS shall include the signature algorithms and parameters employed.

OVR-5.2-05: 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.

OVR-5.2-06 [PTC]**:** The requirement preceding clause 2.1 in clause 2 of the BRG [5] shall apply.

OVR-5.2-07 [PTC]**:** Clause 2.2 of BRG [5] shall apply.

OVR-5.2-08 [EVCP]**:** Clause 8.3 of EVCG [4] shall apply.

OVR-5.2-09 [EVCP]**:** Clause 8.2.1 of EVCG [4] shall apply.

OVR-5.2-10: The TSP's CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP.

OVR-5.2-11: If the TSP applies size limits on any subject naming attributes which are longer than the limits stated in IETF RFC 5280 [7] then the applied size limits should be stated in the TSP's published certification practice statement or terms and conditions.

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)
```

g) IVCP: Individual Validation Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ivcp (8)
```

OVR-5.3-01: If any changes are made to a CP as described in clause 4.2.2 which affects the applicability then the policy identifier should be changed.

5.4 PKI participants

5.4.1 Certification Authority

A CA is commonly understood to be 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. However, in the present document the term is used more to reference the technical component of the TSP concerned with certificate issuance.

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

OVR-5.4.1-01: The TSP may make use of other parties to provide parts of the certification service.

NOTE: However, the TSP always maintains overall responsibility and ensures that the policy requirements identified in the present document are met (ETSI EN 319 401 [8], requirements REQ-6.3-05 and REQ-6.3-06).

EXAMPLE: A TSP can sub-contract all the component services, including the certificate generation service (referred to as the CA in the present document). However, the key used to sign the certificates is identified as belonging to the CA, and the TSP maintains overall responsibility for meeting the requirements defined in the present document.

OVR-5.4.1-02: A TSP may include a hierarchy of CAs.

OVR-5.4.1-03 [CONDITIONAL]**:** Where a TSP includes a hierarchy of subordinate CAs up to a root CA, the TSP shall be responsible for ensuring the subordinate-CAs comply with the applicable policy requirements.

5.4.2 Subscriber and subject

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

- a natural person;
- a natural person identified in association with a legal person;

- a legal person (that can be an Organization or a unit or a department identified in association with an Organization); or
- 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, REG-6.3.4-09 to REG-6.3.4-17.

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

- To request a certificate for natural person the subscriber is:
  - the natural person itself;
  - a natural person mandated to represent the subject; or

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

  - 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).
- To request a certificate for legal person the subscriber is:
  - any entity as allowed under the relevant legal system to represent the legal person; or
  - a legal representative of a legal person subscribing for its subsidiaries or units or departments.
- To request a certificate for a device or system operated by or on behalf of a natural or legal person the subscriber is:
  - the natural or legal person operating the device or system;
  - any entity as allowed under the relevant legal system to represent the legal person; or
  - a legal representative of a legal person subscribing for its subsidiaries or units or departments.

5.4.3 Others

OVR-5.4.3-01: 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

DIS-6.1-01: Void.

DIS-6.1-01A: The TSP shall make certificates available to subscribers and subjects.

DIS-6.1-01B: The TSP may make certificates available to relying parties only if subject's consent has been obtained.

DIS-6.1-01C [CONDITIONAL]**:** If the subject is a device or system, the consent for **DIS -6-1-01B** shall be obtained from the natural or legal person responsible for operating the device or system, instead of the subject.

DIS-6.1-02: Void.

DIS-6.1-02A: The complete and accurate certificate shall be available for use by the subscriber or subject or, if needed, TSP managing the private key on behalf of the user.

NOTE: The certificate does not need to be available for use immediately upon generation.

DIS-6.1-03: Void.

DIS-6.1-04: The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).

DIS-6.1-05: The applicable terms and conditions shall be readily identifiable for a given certificate.

DIS-6.1-06: Void.

DIS-6.1-06A [LCP]**:** The information identified in **DIS-6.1-01A** , **DIS-6.1-01B** and **DIS-6.1-04** above shall be available as specified in the TSP's CPS.

DIS-6.1-07: Void.

DIS-6.1-07A [NCP]**:** The information identified in **DIS-6.1-01A** , **DIS-6.1-01B** and **DIS-6.1-04** 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.

DIS-6.1-08: The information identified in **DIS-6.1-04** above should be publicly and internationally available.

DIS-6.1-09 [CONDITIONAL]**:** If the TSP is issuing publicly-trusted certificates, the information identified in **DIS-6.1-04** 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

REG-6.2.2-01: 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.

NOTE 2: Identity validation is part of at least one of processes: certificate application, certificate issuance, subject device provisioning.

In particular:

- **REG-6.2.2-02:** Void.
- **REG-6.2.2-02A:** The TSP shall collect and validate 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.

NOTE 3: Submitted evidence may be in the form of either paper or electronic documentation.

- **REG-6.2.2-02B:** Verification of the subject's identity shall be at time of registration by appropriate means.

NOTE 4: The collection of evidence may include the copy of personal data, such as ID or passport. National regulations vary as to whether it is necessary or not to archive this information as such over long term. See **REG-6.2.2-18**.

- **REG-6.2.2-03** [PTC]**:** The verification methods shall follow those specified in clause 3.2 of BRG [5].
- **REG-6.2.2-04** [EVCP]**:** The verification methods shall follow those specified in clause 11 of the EVCG [4].

When the subject is a natural person (i.e. physical person as opposed to legal person):

- **REG-6.2.2-05** [NCP] [CONDITIONAL]**:** 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 5: 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].

- **REG-6.2.2-06** [CONDITIONAL]**:** If the subject is a natural person (i.e. physical person as opposed to legal person), evidence shall be provided of:

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

  b) 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.

- **REG-6.2.2-07** [CONDITIONAL]**:** If the subject is a natural person (i.e. physical person as opposed to legal person), the place of birth should be given in accordance to national or other applicable conventions for registering births.

When the subject is a natural person who is identified in association with a legal person (e.g. the subscriber):

- **REG-6.2.2-08** [NCP] [CONDITIONAL]**:** 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 **REG-6.2.2-09**, 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.

- **REG-6.2.2-09** [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:

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

  b) 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;

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

d) 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;

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

f) [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

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

When the subject is a legal person, or other organizational entity identified in association with a legal person:

- **REG-6.2.2-10** [NCP] except [EVCP] [CONDITIONAL]**:** 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 **REG-6.2.2-12**, 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.

- **REG-6.2.2-11:** Void.

- **REG-6.2.2-12** [CONDITIONAL]**:** If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided of:

  a) 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.

  b) [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.

When 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:

- **REG-6.2.2-13** [NCP] except [EVCP] [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 of the identity, in particular the ones listed in **REG-6.2.2-15**, 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.

- **REG-6.2.2-14:** Void.

- **REG-6.2.2-14A** [EVCP] [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 of the identity, in particular the ones listed in **REG-6.2.2-15** , 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 with the exception of the verification of assumed name.

- **REG-6.2.2-14B** [EVCP] [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, the verification of the distinguished name shall follow the verification methods of the EVCG [4] as required by **REG-6.2.2-04**.

- **REG-6.2.2-15:** Void.

- **REG-6.2.2-15A** except [DVCP] [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:

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

  b) full name of the organizational entity;

  c) 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;

  d) 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

  e) [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.

When the subject is a device or system operated by a natural person:

- **REG-6.2.2-16** [NCP] [CONDITIONAL]**:** If the subject is a device or system operated by a natural person, evidence of the identity, in particular the ones listed in **REG-6.2.2-17**, shall be checked against a natural person either directly, by physical presence of the natural person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.
- **REG-6.2.2-17:** Void.
- **REG-6.2.2-17A** except [DVCP] [CONDITIONAL]**:** If the subject is a device or system operated by a natural person, evidence shall be provided of:

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

  b) 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.

- **REG-6.2.2-18:** 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.

NOTE 6: In order to comply with REG-6.4.6-03 and REG-6.4.6-04 below, the TSP does not need to archive all data collected during the registration over long term, and can limit the record to a reference to the documentation used at that time.

EXAMPLE 1: If a passport was used for the verification of the identity, the passport number can be recorded.

When an entity other than the subject is subscribing to the TSP's services (i.e. the subscriber and subject are separate entities - see clause 5.4.2):

- **REG-6.2.2-19** [CONDITIONAL]**:** If an entity other than the subject is subscribing to the TSP's services (i.e. the subscriber and subject are separate entities - see clause 5.4.2), 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:

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

  b) [CHOICE]:

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

- 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.

- **REG-6.2.2-20** [CONDITIONAL]**:** If an entity other than the subject is subscribing to the TSP's services (i.e. the subscriber and subject are separate entities - see clause 5.4.2) and 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.

- **REG-6.2.2-21:** The subscriber shall provide a physical address, or other attributes, which describe how the subscriber shall be contacted.

- **REG-6.2.2-22:** The TSP shall provide evidence of how they meet applicable data protection legislation within their registration process.

- **REG-6.2.2-23:** 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.

- **REG-6.2.2-24:** Void.

REG-6.2.2-24A: To avoid any conflicts of interests, the subscriber and TSP organization entity shall be separate entities. The only exceptions are:

A third party organization running all or part of the RA tasks in order to subscribe to certificates for subjects identified in association with it.

EXAMPLE 2: An organization HR department that prepares certificate requests for the employees to which a certificate need to be issued.

- Certificates that a TSP issues for itself (as a legal person) or natural persons belonging to it (as a subject).

REG-6.2.2-25: Certificates that a TSP issues for itself or persons belonging to it (as a subject) shall be requested, validated and handled according to the TSP's defined processes for the selected type of certificates.

6.2.3 Identification and authentication for Re-key requests

REG-6.2.3-01: 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:

- **REG-6.2.3-02:** 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.

- **REG-6.2.3-03** [EVCP]**:** Clauses 11.14.2 and 11.14.3 of EVCG [4] shall apply.

- **REG-6.2.3-04** [EVCP]**:** Clause 9.4 of EVCG [4], specifying the maximum validity period, shall apply.

- **REG-6.2.3-05:** Void.

- **REG-6.2.3-06** [OVCP], [IVCP] and [DVCP]**:** Validation information obtained by the TSP may be reused if compatible with clause 4.2.1 of BRG [5].

- **REG-6.2.3-07** [OVCP], [IVCP] and [DVCP]**:** Clause 6.3.2 of BRG [5], specifying the maximum validity period, shall apply.

- **REG-6.2.3-08:** If any of the TSP's terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements **REG-6.3.4-02**, **REG-6.3.4-03, OVR-6.3.4-04** to **OVR-6.3.4-06, REG-6.3.4-07** and **REG-6.3.4-08**.

- **REG-6.2.3-09:** 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

NOTE 1: See also clause 6.3.9.

REV-6.2.4-01: The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

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

b) How they can be submitted.

c) 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.

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

e) The mechanism used for distributing revocation status information.

f) 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.

g) 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.

REV-6.2.4-02 [PTC]**:** Clause 4.9 of the BRG [5] shall apply.

REV-6.2.4-03: Void.

REV-6.2.4-03A: The maximum delay between receipt of a certificate revocation or suspension request and the actual change of the certificate status information being available to all relying parties shall be at most 24 hours.

REV-6.2.4-03B [CONDITIONAL]**:** If the revocation or suspension request cannot be confirmed within 24 hours then the status need not be changed.

REV-6.2.4-03C [CONDITIONAL]**:** If a TSP supports both CRL and on-line certificate status service to provide revocation status and delays in updating the status information for all the methods exist or are possible, the maximum delay of 24 hours shall apply to both methods.

REV-6.2.4-04: Void.

REV-6.2.4-05: Void.

REV-6.2.4-05A [CONDITIONAL]**:** If the revocation request requires revocation at a future date (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the time at which receipt of the request has occurred.

REV-6.2.4-06: Void.

REV-6.2.4-06A: A TSP may give faster process times than the time required in **REV-6.2.4-03A** for certain revocation reasons.

REV-6.2.4-07: The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours.

REV-6.2.4-08: 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.

REV-6.2.4-09: Requests for revocation and reports of events relating to revocation shall be authenticated, checked to be from an authorized source.

NOTE 2: 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.

REG-6.3.1-01 [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.

REG-6.3.1-02 [EVCP]**:** For a dual control procedure in the validation process EVCG [4], clause 14.1.3, shall apply.

6.3.2 Certificate application processing

REG-6.3.2-01: 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:

- **REG-6.3.2-02** [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

See clause 6.6.1 for certificate profiles.

GEN-6.3.3-01: The CA shall issue certificates securely to maintain their authenticity.

In particular:

- **GEN-6.3.3-02:** The CA shall take measures against forgery of certificates.
- **GEN-6.3.3-02A** [NCP]**:** The CA should introduce randomness in certificate's serial number.
- **GEN-6.3.3-03** [CONDITONAL]**:** In cases where the CA generates the subjects' key pair, the CA shall guarantee confidentiality during the process of generating such data.
- **GEN-6.3.3-04:** 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.
- **GEN-6.3.3-05:** The TSP should not issue certificates whose lifetime exceeds that of the CA's signing certificate.
- **GEN-6.3.3-06** [CONDITIONAL]**:** If the TSP does issue certificates whose lifetime exceeds the lifetime of the CA's signing certificate, the TSP shall ensure that the certificate status (see clause 6.3.10) can still be verified by relying parties after expiry of the CA certificate.

  When the CA generated the subject's key pair:

  - **GEN-6.3.3-07** [CONDITIONAL]**:** If the CA generated the subject's key pair, the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA;

- **SDP-6.3.3-08** [LCP] and [NCP] [CONDITIONAL]**:** If the CA generated the subject's key pair, the private key shall be securely passed to the registered subject; or to the TSP managing the subject's private key; and
- **SDP 6.3.3-09:** Void.
- **SDP-6.3.3-09A** [NCP+][CONDITIONAL]**:** If the TSP generated the subject's key pair, the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of a third party TSP managing the key on behalf of the subject, to that third party TSP.

GEN-6.3.3-10: Re-assignment of distinguish name [CHOICE]:

- [All policies except DVCP]: Over the life time of the CA a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject.
- [DVCP] Over the life time of the CA a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject unless the subscriber has provided evidence of rightful ownership of the name.

GEN-6.3.3-11 [CONDITIONAL]**:** If a certificate is issued to a natural person identified in association 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.

GEN-6.3.3-12: The CP identifier shall be [CHOICE]:

- [NCP]:
  - as specified in clause 5.3 item a); and/or
  - 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+]:
  - as specified in clause 5.3 item b); and/or
  - 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]:
  - as specified in clause 5.3 item c); and/or
  - 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]:
  - as specified in clause 5.3, item d);
  - as specified in EVCG [4], clause 9.3.2; and/or
  - 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]:
  - as specified in clause 5.3, item e);
  - as specified in BRG [5], clause 1.2 or 7.1.6.1; and/or
  - 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]:
  - as specified in clause 5.3 item f);
  - as specified in BRG [5], clause 1.2 or 7.1.6.1; and/or
  - 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.
- [IVCP]:
  - as specified in clause 5.3 item g);
  - as specified in BRG [5], clause 1.2 or 7.1.6.1; and/or
  - 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

OVR-6.3.4-01: The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate. See clause 6.9.4.

In particular:

- **REG-6.3.4-02:** 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.
- **REG-6.3.4-03** [CONDITIONAL]**:** If the subject is a person (i.e. not a device), and not the same as the subscriber, the subject shall be informed of his/her obligations.

  Communication of the terms and conditions:
  - **OVR-6.3.4-04:** 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 before the agreement.
  - **OVR-6.3.4-05:** The terms and conditions may be transmitted electronically.
  - **OVR-6.3.4-06:** The terms and conditions may use the model PKI disclosure statement given in annex A.
- **REG-6.3.4-07:** The TSP shall record the agreement with the subscriber and if the subscriber and subject are two separate entities and the subject is a natural or legal person, with the subject.
- **REG-6.3.4-08:** The agreement in requirement **REG-6.3.4-07** shall involve explicit acceptance of the terms and conditions by a wilful act which can be later supported by evidence.

  Where the subscriber and subject are two separate entities and the subject is a natural or legal person:
  - **REG-6.3.4-09** [CONDITIONAL]**:** If the subscriber and subject are two separate entities and the subject is a natural or legal person, the agreement shall be in 2 parts.
  - **REG-6.3.4-10:** Void.
  - **REG-6.3.4-10A** [CONDITIONAL]**:** If the subscriber and subject are two separate entities and the subject is a natural or legal person, the first part of the agreement shall be ratified by the subscriber by means of a traceable action (e.g. ticking a box or signing) and shall include:
    a) agreement to the subscriber's obligations (see clause 6.9.4);
    b) if the TSP's practices require use of a secure cryptographic device, agreement by the subscriber to use a secure cryptographic device;

c) 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;

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

e) confirmation that the information to be held in the certificate is correct;

NOTE 1: This can be achieved by reference (e.g. reference to the CP for the fields of the certificate that are fixed by the CP).

f) obligations applicable to subjects (see clause 6.9.4).

- **REG-6.3.4-11:** Void.

- **REG-6.3.4-11A** [CONDITIONAL]**:** Where the subscriber and subject are two separate entities and the subject is a natural or legal person, the second part of the agreement shall be ratified by the subject by means of a traceable action (e.g. ticking a box or signing) and shall include:

a) the agreement by the subject on the obligations applicable to subjects (see clause 6.9.4);

b) if the TSP's practices require use of a secure cryptographic device, agreement by the subject to use a secure cryptographic device;

c) 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.

NOTE 2: If the subscriber is the official representative of the legal person that is the subject, or the official representative of the subscriber and the subject is the same, part 1 (see REG-6.3.4-10) and part 2 (see REG-6.3.4-11) items listed above can be ratified together.

Where the subject and subscriber are the same entity or the subject is a device:

- **REG-6.3.4-12** [CONDITIONAL]**:** If the subject and subscriber are the same entity or the subject is a device, the agreement shall be in one or two parts.

- **REG-6.3.4-13** [CONDITIONAL]**:** If the subject and subscriber are the same entity or the subject is a device, the agreement shall include the part 1 (see **REG-6.3.4-10)** and part 2 (see **REG-6.3.4-11)** items listed above.

NOTE 3: 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.

- **REG-6.3.4-14** [PTC]**:** Clause 9.6.3 of BRG [5] shall apply to the first part of the agreement (see **REG-6.3.4-10**).

- **REG-6.3.4-15** [EVCP]**:** Clause 11.8 of EVCG [4] shall apply to the first part of the agreement (see **REG-6.3.4-10**).

- **REG-6.3.4-16:** The agreement may be in electronic form.

- **REG-6.3.4-17:** The records identified above shall be retained for the period of time as indicated to the subscriber (as part of the terms and conditions).

NOTE 4: See also clause 6.4.6 regarding retention of information.

6.3.5 Key pair and certificate usage

OVR-6.3.5-01: The subscriber's obligations (see clause 6.3.4) shall include:

a) an obligation to provide the TSP with accurate and complete information in accordance with the requirements of the present document, particularly with regards to registration;

b) an obligation for the key pair to be only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person;

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

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

   i) an obligation or recommendation to generate the subject keys 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) an obligation or recommendation to use key length and algorithm 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 certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 [9]:

   i) when the subject is a natural person: an obligation for the subject's private key to be maintained under the subject's sole control;

   ii) when the subject is a legal person: an obligation for the subject's private key to be maintained under the subject's control;

f) [NCP+] an obligation to 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: an obligation to generate the subject's keys within the secure cryptographic device;

h) an obligation to 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;

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

i) an obligation, following compromise of the subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment; and

j) an obligation, in the case of being informed that the subject's certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the subject.

NOTE 2: See clause 6.3.9 for details on revocation management and on reasons for revocation.

OVR-6.3.5-02 [CONDITIONAL]**:** If the subject and subscriber are separate entities and the subject is a natural or legal person, the subject's obligations shall comply with **OVR-6.3.5-01 for** points b), c), e), f), h), i) and j).

OVR-6.3.5-03: The notice to relying parties (see clause 6.9.4) shall recommend the relying party to:

a) 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.

b) take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied as required in clause 6.9.4; and

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

NOTE 4: Depending on CA's practices related to problem reporting and revocation requests (e.g. see clause 4.9.3 of BRG [5]) this can include instructions regarding reporting potential problems.

- **OVR-6.3.5-04** [NCP][CONDITIONAL]**:** If the TSP manages the private key on behalf of the subject and the certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 [9], the TSP shall ensure that the subject has sole control (or if the subject is a legal person, "control") over its private key.

- **OVR-6.3.5-05** [NCP][CONDITIONAL]**:** If a third party TSP manages the private key on behalf of the subject and the certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 [9], the TSP shall confirm that the TSP managing the key ensures that the subject has sole control (or if the subject is a legal person, "control") over its private key.

- **OVR-6.3.5-06:** Conformance to ETSI TS 119 431-1 [i.21], should be used to demonstrate that the TSP managing the key on behalf of the subject meets the requirements for ensuring (sole) control as required in **OVR-6.3.5-04** or **OVR-6.3.5-05**.

6.3.6 Certificate renewal

NOTE 1: Certificate renewal refers to the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate (see IETF RFC 3647 [i.3]).

REG-6.3.6-01: Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized.

In particular:

- **REG-6.3.6-02:** 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.

- **REG-6.3.6-03** [EVCP]**:** Clauses 11.14.2 and 11.14.3 of EVCG [4] shall apply.

- **REG-6.3.6-04** [EVCP]**:** Clause 9.4 of EVCG [4], specifying the maximum validity period, shall apply.

- **REG-6.3.6-05:** Void.

- **REG-6.3.6-06** [OVCP], [IVCP] and [DVCP]**:** Validation information obtained by the TSP may be reused if compatible with clause 4.2.1 of BRG [5].

- **REG-6.3.6-07** [OVCP], [IVCP] and [DVCP]**:** Clause 6.3.2 of BRG [5], specifying the maximum validity period, shall apply.

- **REG-6.3.6-08:** If any of the TSP's terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements **REG-6.3.4-02**, **REG-6.3.4-03, OVR-6.3.4-04** to **OVR-6.3.4-06, REG-6.3.4-07 and REG-6.3.4-08** of clause 6.3.4.

- **REG-6.3.6-09:** Requirements **REG-6.2.2-06**, **REG-6.2.2-07**, **REG-6.2.2-09**, **REG-6.2.2-11**, **REG-6.2.2-12**, **REG-6.2.2-14**, **REG-6.2.2-15** and **REG-6.2.2-17** to **REG-6.2.2-21** of clause 6.2.2 shall apply.

NOTE 2: Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

- **GEN-6.3.6-10:** 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.

6.3.7 Certificate Re-key

NOTE: Certificate re-key refers to the issuance of a new certificate that certifies the new public key (see IETF RFC 3647 [i.3]).

REG-6.3.7-01: The requirements of clause 6.2.3 shall apply.

REG-6.3.7-02: 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.

6.3.8 Certificate modification

NOTE: Certificate modification refers to the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key (see IETF RFC 3647 [i.3]).

REG-6.3.8-01: Void.

REG-6.3.8-01A: The requirements of **REG-6.3.6-01** to **REG-6.3.6-09** and **GEN-6.3.6-10** of clause 6.3.6 apply.

In particular:

- **REG-6.3.8-02:** If any certified names or attributes have changed, 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

REV-6.3.9-01: The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests (see also **REV-6.2.4-03**).

REV-6.3.9-02: The TSP shall revoke any non expired certificate:

a) that is no longer compliant with the CP under which it has been issued; or

b) that the TSP is aware of changes which impact the validity of the certificate; or

NOTE 1: It is not implied that the TSP needs to monitor information relating to the content.

c) for which the used cryptography is no longer ensuring the binding between the subject and the public key.

REV-6.3.9-03: The subject, and where applicable the subscriber, of a revoked or suspended certificate, where possible, shall be informed of the change of status of the certificate.

NOTE 2: It may not be possible to inform the subject for example if known to be deceased or otherwise not available to be contacted.

REV-6.3.9-04: Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

Where Certificate Revocation Lists (CRLs) concerning end users' certificates including any variants (e.g. Delta CRLs) are used:

NOTE 3: See clause 6.6.2 regarding CRL profile requirements.

- **CSS-6.3.9-05** [CONDITIONAL]**:** If Certificate Revocation Lists (CRLs) concerning end users certificates are used, including any variants, *either the CRL or the variant* shall be published at least every 24 hours;

- **CSS-6.3.9-06** [CONDITIONAL]**:** If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, every CRL shall state a time for next scheduled CRL issue, unless it is the last CRL issued for those certificates in the scope of the CRL, in which case the nextUpdate field in the CRL defined in IETF RFC 5280 [7], should be set to "99991231235959Z";

NOTE 4: This value, defined in IETF RFC 5280 [7] for certificates that have no well-defined expiration date, is here extended for CRL.

- **CSS-6.3.9-07** [CONDITIONAL]**:** If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, a new CRL may be published before the stated time of the next CRL issue.

CSS-6.3.9-08 [CONDITIONAL]**:** If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, the CRL shall be signed by the CA or an entity designated by the TSP.

CSS-6.3.9-09 [PTC]**:** The TSP shall operate and maintain its certificate status information.

CSS-6.3.9-10 [PTC]**:** Clause 4.10.2 of BRG [5] shall apply.

CSS-6.3.9-11 [EVCP]**:** TSP shall comply with EVCG [4], clause 13.

Where CARL is used:

- **CSS-6.3.9-12** [CONDITIONAL]**:** If 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;

- **CSS-6.3.9-13** [CONDITIONAL]**:** If CARL is used, a new CARL shall be generated once a CA certificate has been revoked.

CSS-6.3.9-14: In the case of any cross-certificates issued by the CA to other TSPs, the CARL should be issued at least every 31 days.

REV-6.3.9-15: A TSP need not to have a revocation management service to address requirements **REV-6.2.4-01, REV-6.2.4-03A, REV-6.2.4-03B, REV-6.2.4-05** to **REV-6.2.4-09, REV-6.3.9-01, REV-6.3.9-02** and **SDP-6.5.1-2** for short-term certificates, as these requirements are not necessarily applicable to short-term certificates.

NOTE 5: Requirements CSS-6.3.10-07 and CSS-6.3.10-08 still apply to TSP issuing short-term certificates. A TSP issuing short-term certificate can provide "good" OCSP responses or empty CRL for the concerned short-term certificate for backward compatibility, however, checking such revocation status services will not provide additional information about the validity of the certificate.

NOTE 6: Possibilities offered by **REV-6.3.9-15** applies only to end user certificates; if a TSP fails to apply the applicable certificate policy, then its CA certificate can be revoked.

REV-6.3.9-16: A TSP issuing short-term certificates shall explicitly describe in the CPS which certificates cannot be revoked through a revocation management service and which certificates cannot be revoked even by the TSP on its own initiative.

NOTE 7: The explanation that certain group of certificates cannot be revoked and their status never changes can be considered as an alternative to **REV-6.2.4-01**.

6.3.10 Certificate status services

CSS-6.3.10-01: The TSP shall provide services for checking the status of the certificates.

In particular:

- **CSS-6.3.10-02:** 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.

- **CSS-6.3.10-03:** The integrity and authenticity of the status information shall be protected.

- **CSS-6.3.10-04:** Revocation status information shall include information on the status of certificates at least until the certificate expires.

NOTE 1: ETSI EN 319 411-2 [i.5] specifies a standard way of providing certificate status information beyond expiry.

Revocation status information methods:

- **CSS-6.3.10-05:** OCSP or CRL shall be supported.
- **CSS-6.3.10-06:** OCSP should be supported.

NOTE 2: The support of OCSP is recommended. It is particularly important where CRLs are susceptible to be big in size, which can be the case for certificates whose validity at the time of use of the private key cannot be assured by the TSP.

- **CSS-6.3.10-07** [PTC]**:** OCSP shall be supported.

NOTE 3: See clause 6.6.3 for profile requirements of OCSP.

NOTE 4: See clause 6.6.2 for profile requirements of CRL.

When a TSP supports multiple methods (CRL and OCSP) to provide revocation status:

- **CSS-6.3.10-08** [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;
- **CSS-6.3.10-09** [CONDITIONAL]**:** If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, 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.

NOTE 5: Consistency over time allows for the difference in delays to be taken into account provided that the status of the certificate is ultimately the same and provided **REV-6.2.4-03C** can be respected. This can be done on the basis of the information provided under **CSS-6.3. 10-9A.**

EXAMPLE: If OCSP can be updated immediately, OCSP and CRL may differ, until the new CRL has been generated.

- **CSS-6.3.10-9A** [CONDITIONAL]**:** If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status and delays in updating the status information for all the methods exist or are possible, the TSP shall document in its CPS the origin of such delays and how to interpret the results in case of differences.

- **CSS-6.3.10-10:** 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

SDP-6.3.12-01: The security of any duplicated subject's private keys shall be at the same level as for the original subject's private keys.

SDP-6.3.12-02: The number of any duplicated subject's private keys shall not exceed the minimum needed to ensure continuity of the service.

SDP-6.3.12-03 [CONDITIONAL]**:** If the certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 [9], 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 (or if the subject is a legal person "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 (or if the subject is a legal person "control") of the user.

SDP-6.3.12-04 [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 control of the signer or owner.

SDP-6.3.12-05 [CONDITIONAL]**:** If the subject's private key is to be used for decryption, then the CA may back it up.

SDP-6.3.12-06 [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.

SDP-6.3.12-07 [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

OVR-6.4.1-01: The requirements identified in ETSI EN 319 401 [8], clauses 5, 6.3 and 7.3, shall apply.

6.4.2 Physical security controls

OVR-6.4.2-01: The requirements identified in ETSI EN 319 401 [8], clause 7.6, shall apply.

In addition the following particular requirements apply:

OVR-6.4.2-02: 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.

OVR-6.4.2-03: 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.

OVR-6.4.2-04: Every entry and exit shall be logged.

OVR-6.4.2-05: 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.

OVR-6.4.2-06: Any parts of the premises shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services.

OVR-6.4.2-07: 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.

OVR-6.4.2-08: 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.

OVR-6.4.2-09: Controls shall be implemented to protect against equipment, information, media and software relating to the TSP's services being taken off-site without authorization.

OVR-6.4.2-10: Other functions relating to TSP's operations may be supported within the same secured area provided that the access is limited to authorized personnel.

OVR-6.4.2-11: 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

OVR-6.4.3-01: The requirements **REQ-7.4-04** to **REQ-7.4-09** in ETSI EN 319 401 [8], shall apply.

In addition the following particular requirements apply:

GEN-6.4.3-02: 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.

GEN-6.4.3-03 [PTC]**:** BRG [5], clause 4.3 shall apply.

6.4.4 Personnel controls

OVR-6.4.4-01: The requirements identified in ETSI EN 319 401 [8], clause 7.2 shall apply.

OVR-6.4.4-02: In addition to the trusted roles identified in ETSI EN 319 401 [8], (7.2-15), the trusted roles of the registration and revocation officers with responsibilities as defined in CEN TS 419 261 [i.9] should be supported.

OVR-6.4.4-03 [PTC]**:** The role of validation specialist shall be included as specified in BRG [5].

6.4.5 Audit logging procedures

OVR-6.4.5-01: The requirements identified in ETSI EN 319 401 [8], clause 7.10, shall apply.

NOTE: ETSI TS 119 511 [i.22] suggests provisions on how to preserve digital data objects.

In addition the following particular requirements apply:

OVR-6.4.5-02: 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.

REG-6.4.5-03: All events related to registration including requests for certificate re-key or renewal shall be logged.

REG-6.4.5-04: All registration information including the following shall be recorded:

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

b) record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;

c) storage location of copies of applications and identification documents, including the subscriber agreement (see requirement **REG-6.3.4-07**);

d) any specific choices in the subscriber agreement (e.g. consent to publication of certificate, see requirement **REG-6.3.4-07**);

e) identity of entity accepting the application;

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

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

OVR-6.4.5-04A: The TSP shall document how the information recorded as per **REG-6.4.5-04** is accessible.

REG-6.4.5-05: The TSP shall maintain the privacy of subject information.

GEN-6.4.5-06: The TSP shall log all events relating to the life-cycle of CA keys.

GEN-6.4.5-07: Void.

OVR-6.4.5-07A: The TSP shall log all events relating to the life-cycle of certificates as requested by **REG-6.4.5-03**, **GEN-6.4.5-08**, **REV-6.4.5-09**, **SDP-6.4.5-10** as well as all events relating to certificates generation and dissemination.

GEN-6.4.5-08: 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.

REV-6.4.5-09: The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

SDP-6.4.5-10 [NCP+]**:** The TSP shall log all events relating to the preparation of the subject's device.

OVR-6.4.5-11: The TSP shall document precisely the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan.

6.4.6 Records archival

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

OVR-6.4.6-01: The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

a) 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 requirement **GEN-6.4.5-08**);

b) documentation as identified in clause 6.3.4.

6.4.7 Key changeover

No policy requirement.

6.4.8 Compromise and disaster recovery

OVR-6.4.8-01: 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:

- **OVR-6.4.8-02:** TSP's 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.
- **OVR-6.4.8-03:** In line with ISO/IEC 27002 [i.7], clause 12.3: Back-up copies of essential information and software should be taken regularly.
- **OVR-6.4.8-04:** Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
- **OVR-6.4.8-05:** Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.
- **OVR-6.4.8-06:** Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.
- **OVR-6.4.8-07** [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:

- **OVR-6.4.8-08:** 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.
- **OVR-6.4.8-09:** The processes planned as per requirement **OVR-6.4.8-08** shall be in place.

NOTE: It is suggested that the plan includes a requirement that all subject certificates are revoked. This is not necessarily applicable to short term certificates.

- **OVR-6.4.8-10:** Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster.
- In the case of compromise as a minimum:
  - **OVR-6.4.8-11:** The TSP shall 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;
  - **OVR-6.4.8-12:** The TSP shall make the information in **OVR-6.4.8-11** available to other relying parties;

- **OVR-6.4.8-13:** The TSP shall indicate that certificates and revocation status information issued using this CA key may no longer be valid; and
- **OVR-6.4.8-14:** Void.
- **OVR-6.4.8-14A:** The TSP shall revoke any CA certificate it has issued when the TSP is informed of the compromise of such a CA (including when the compromised CA is part of the TSP or is managed by another TSP).

Algorithm compromise:

- **OVR-6.4.8-15:** 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 inform all subscribers and relying parties with whom the TSP has agreement or other form of established relations. In addition, the TSP shall make this information available to other relying parties.
- **OVR-6.4.8-16:** 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 schedule a revocation of any affected certificate.

6.4.9 Certification Authority or Registration Authority termination

OVR-6.4.9-01: The requirements identified in ETSI EN 319 401 [8], clause 7.12, shall apply.

In addition the following particular requirements apply:

OVR-6.4.9-02: Requirement **REQ-7.12-06** of ETSI EN 319 401 [8], shall apply to the following information for their respective period of time as indicated to the subscriber and relying party (see in particular **REG-6.3.4-17** and **CSS-6.3.10-02**):

a) registration information (see clauses 6.2.2, 6.3.1 and 6.3.4);

b) revocation status information (see clause 6.3.10);

c) event log archives (see clauses 6.4.5 and 6.4.6).

OVR-6.4.9-03: Requirement **REQ-7.12-10** of ETSI EN 319 401 [8], shall also include the handling of the revocation status for unexpired certificates that have been issued.

OVR-6.4.9-04: When another cross certified TSP stops all operations, including handling revocation (see OVR-6.4.9-03), all cross certificates to that TSP shall be revoked.

NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [8], **REQ-7.12-10** include cross certified TSP.

6.5 Technical security controls

6.5.1 Key pair generation and installation

OVR-6.5.1-01: The requirements identified in ETSI EN 319 401 [8], clause 7.5, shall apply.

In addition the following particular requirements apply:

GEN-6.5.1-02: The TSP shall generate CA keys, including keys used by revocation and registration services, securely and the private key shall be secret.

In particular:

- **GEN-6.5.1-03:** The 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).
- **GEN-6.5.1-04:** The CA key pair used for signing certificates shall be created under, at least, dual control.

- **GEN-6.5.1-05:** The number of personnel authorized to carry out CA key pair generation shall be kept to a minimum and be consistent with the TSP's practices.

- **GEN-6.5.1-06:** 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.

- **GEN-6.5.1-07:** 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.

GEN-6.5.1-08: Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, 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.

GEN-6.5.1-09: Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, the new CA certificate shall also be generated and distributed in accordance with the present document.

GEN-6.5.1-10: The operations described in **GEN-6.5.1-08** and **GEN-6.5.1-09** 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.

GEN-6.5.1-11: The TSP shall have a documented procedure for conducting CA key pair generation for certificate signing keys for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users.

GEN-6.5.1-12: The procedure of **GEN-6.5.1-11** shall indicate, at least, the following:

a) roles participating in the ceremony (internal and external from the organization);

b) functions to be performed by every role and in which phases;

c) responsibilities during and after the ceremony; and

d) requirements of evidence to be collected of the ceremony.

GEN-6.5.1-13: The TSP shall produce a report proving that the ceremony, as in **GEN-6.5.1-11** above, was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured.

GEN-6.5.1-14: This report shall be signed [CHOICE]**:**

- 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's management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

- 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.

GEN-6.5.1-15 [PTC]**:** Clause 6.1.1.1 of the BRG [5] shall apply.

DIS-6.5.1-16: 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.

When the CA generates the subject's keys:

- **SDP-6.5.1-17** [CONDITIONAL]**:** If the CA generates the subject's keys, 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.

- **SDP-6.5.1-18** [CONDITIONAL]**:** If the CA generates the subject's keys, 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.

- **SDP-6.5.1-19** [CONDITIONAL]**:** If the CA generates the subject's keys , CA-generated subject keys shall be generated and stored securely whilst held by the TSP.

- **SDP-6.5.1-20** [CONDITIONAL]**:** If the CA generates the subject's keys, 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.

- **SDP-6.5.1-21** [CONDITIONAL]**:** If the CA generates the subject's keys and 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.

- **SDP-6.5.1-22** [CONDITIONAL]**:** If the CA generates the subject's keys, 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.

- **SDP-6.5.1-23** [NCP+] [CONDITIONAL]**:** If the CA generates the subject's keys, the TSP shall secure the issuance of a secure cryptographic device to the subject.

  In particular:

  - **SDP-6.5.1-24** [CONDITIONAL]**:** If the CA generates the subject's keys, secure cryptographic device preparation shall be done securely.

  - **SDP-6.5.1-25** [CONDITIONAL]**:** If the CA generates the subject's keys, secure cryptographic device shall be securely stored and distributed.

6.5.2 Private key protection and cryptographic module engineering controls

OVR-6.5.2-01: TSP's key pair generation, including keys used by revocation and registration services, shall be carried out within a secure cryptographic device which is a trustworthy system which:

a) 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 provided this is 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's 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].

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

OVR -6.5.2-02: The secure cryptographic device shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

OVR -6.5.2-03: The above secure cryptographic device should be assured as per **OVR-6.5.2-01**-a), above.

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.

GEN-6.5.2-04: The CA private signing key shall be held and used within a secure cryptographic device meeting the requirements of **OVR-6.5.2-01** and **OVR-6.5.2-02** above.

GEN-6.5.2-05 [CONDITIONAL]**:** When outside the secure cryptographic device (see **GEN-6.5.2-04** 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.

GEN-6.5.2-06: 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).

GEN-6.5.2-07: The number of personnel authorized to carry out the CA private signing key back up, storage and recovery shall be kept to a minimum and be consistent with the CA's practices.

GEN-6.5.2-08: Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

GEN-6.5.2-09 [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.

OVR -6.5.2-10: The secure cryptographic device shall not be tampered with during shipment.

OVR -6.5.2-11: The secure cryptographic device shall not be tampered with while stored.

OVR -6.5.2-12: The secure cryptographic device shall be functioning correctly.

GEN-6.5.2-13: 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

OVR-6.5.3-01: The TSP shall use appropriately the CA private signing keys.

In particular:

- **OVR-6.5.3-02:** The TSP shall not use the CA private signing keys beyond the end of their life cycle.
- **GEN-6.5.3-03:** 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.
- **GEN-6.5.3-04:** The certificate signing keys shall only be used within physically secure premises.
- **GEN-6.5.3-05:** 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 requirement **GEN-6.5.1-07**.
- **GEN-6.5.3-06:** All copies of the CA private signing keys shall be destroyed at the end of their life cycle.
- **GEN-6.5.3-07** [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 **GEN-6.5.3-05**.

6.5.4 Activation data

GEN-6.5.4-01: 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.

If the TSP issues a secure cryptographic device:

- **SDP-6.5.4-02** [CONDITIONAL]**:** If the TSP issues a secure cryptographic device, secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

- **SDP-6.5.4-03** [CONDITIONAL]**:** If the TSP issues a secure cryptographic device, and where the personalized 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 cryptographic device at different times, or via a different channel.

6.5.5 Computer security controls

OVR-6.5.5-01: The requirements **REQ-7.4-01, REQ-7.4-02**, **REQ-7.4-03** and **REQ-7.4-10** in ETSI EN 319 401 [8] shall apply.

NOTE 1: 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].

NOTE 2: With regards general to requirement **REQ-7.4-10** *"Sensitive data shall be protected"* in ETSI EN 319 401 [8], Sensitive data includes registration information.

In addition the following particular requirements apply:

GEN-6.5.5-02: Local network components (e.g. routers) shall be kept in a physically and logically secure environment.

GEN-6.5.5-03: Local network components (e.g. routers) configurations shall be periodically checked for compliance with the requirements specified by the TSP.

GEN-6.5.5-04: The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

DIS-6.5.5-05: Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

CSS-6.5.5-06: Revocation status application shall enforce access control on attempts to modify revocation status information.

OVR-6.5.5-07: 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

OVR-6.5.6-01: 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:

OVR-6.5.6-02 [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.

OVR-6.5.6-03 [PTC]**:** Clause 5 of the BRG [5] shall apply.

6.5.7 Network security controls

OVR-6.5.7-01: The requirements identified in ETSI EN 319 401 [8], clause 7.8 shall apply.

In addition the following particular requirements apply:

OVR-6.5.7-02: 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.

OVR-6.5.7-03: 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.

OVR-6.5.7-04: The TSP shall grant access to secure zones and high security zones to only trusted roles.

OVR-6.5.7-05: 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

GEN-6.6.1-01: The certificates shall meet the requirements specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

GEN-6.6.1-02: The certificate shall be issued according to the relevant certificate profile [CHOICE]:

- [LCP, NCP and NCP+] for issuance of certificates to natural persons (excluding for web site certificates): ETSI EN 319 412-2 [9].
- [LCP, NCP and NCP+] for issuance of certificates to legal persons (excluding for web site certificates): ETSI EN 319 412-3 [10].
- [PTC] for issuance of certificates for web sites or devices: ETSI EN 319 412-4 [2].

GEN-6.6.1-03: A TSP issuing short-term certificate should use the validity assured extension `ext-etsi-valassured-ST-certs` defined in ETSI TS 119 412-1 [13] within the short-term certificates which cannot be revoked.

GEN-6.6.1-04: The TSP issuing short-term certificates should not use the validity assured extension ext-etsi-valassured-ST-certs defined in ETSI TS 119 412-1 [13] in short-term certificates which can be revoked.

GEN-6.6.1-05: The TSP shall not use the validity assured extension ext-etsi-valassured-ST-certs defined in ETSI TS 119 412-1 [13] in certificates which are not short-term certificates.

6.6.2 CRL profile

OVR-6.6.2-01: 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

OVR-6.6.3-01: The OCSP shall be as defined in IETF RFC 6960 [11].

NOTE 1: A TSP can decide to use the id-pkix-ocsp-nocheck extension in the certificate profile of a delegated OCSP responder as described in clause 4.2.2.2.1 (Revocation Checking of an Authorized Responder) of IETF RFC 6960 [11]. In that case, no revocation status information is required for determining the status of the corresponding responder certificate which may be considered as useful for various reasons. However, a TSP who decides to do so takes the following additional risks into account in its risk assessment:

- As stipulated in IETF RFC 6960 [11], an OCSP responder key compromise is, in this case, as severe as a compromise of the corresponding issuing CA key. To this reason, the TSP carefully considers OCSP responder key management and particularly considers reducing responder certificate lifetime to a reasonable duration.

- Third party applications like SVAs that rely on the TSP's certificate status information services may not be able to handle this non-critical extension. Consequently they can end up with operational issues when no fall back scenario like complementary provisioning of a CRL is implemented for revealing the responder status, or can end up in invalidating the signature.

  This can be documented within the CPS/CP.

OVR-6.6.3-02: If the OCSP responder receives a request for status of a certificate that has not been issued then the responder shall not respond with a "good" status as per clause 2.2 of IETF RFC 6960 [11].

NOTE 2: When both OCSP and CRL are provided, the TSP needs to configure OCSP answers for non-issued certificates in a way which is appropriate to meet the consistency requirement **CSS-6.3.10-09**. In particular, if the responder sends a "revoked" response, the non-issued reason needs to be identifiable (knowing that non-issued certificates do not appear in a CRL).

OVR-6.6.3-03: The CA should monitor such requests concerning non-issued certificates on the responder as part of its security response procedures to check if this is an indication of an attack.

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's services.

6.8.2 Financial responsibility

OVR-6.8.2-01: The requirement **REQ-7.1.1-04** identified in ETSI EN 319 401 [8], shall apply.

6.8.3 Confidentiality of business information

No policy requirement.

6.8.4 Privacy of personal information

OVR-6.8.4-01: The requirement **REQ 7.13-05** identified in ETSI EN 319 401 [8], shall apply.

In addition the following particular requirements apply:

OVR-6.8.4-02: The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP's system components.

OVR-6.8.4-03: 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:

a) registration (see clause 6.2.2);

b) confidentiality of records (see requirements **REG-6.3.2-02** and **REG-6.4.5-05**);

c) protecting access to personal information (**OVR-6.8.4-02);**

d) user consent (see requirement **REG-6.3.4-07** and **REG-6.3.4-08**).

6.8.5 Intellectual property rights

No policy requirement.

6.8.6 Representations and warranties

OVR-6.8.6-01: Void.

NOTE 1: TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP's functionality is undertaken by outsourcers.

NOTE 2: The requirements **OVR-6.4.1-01** and **OVR-6.9.1-01** of the present document, referencing **REQ-6.3-05**, **REQ-6.3-06**, and **REQ-7.1.1-07 to 10** identified in ETSI EN 319 401 [8], apply also to the relationship between the TSP and trust service component providers, when part of the TSP operations are provided by separate trust service component providers.

In addition the following particular requirements apply:

- **OVR-6.8.6-02:** The TSP shall provide all its certification services consistent with its CPS.
- **OVR-6.8.6-03** [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].

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

OVR-6.8.13-01: The item h) of requirement **REQ-6.2-02** identified in ETSI EN 319 401 [8], and the requirement **REQ-7.1.1-06** identified in ETSI EN 319 401 [8], 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

OVR-6.8.15-01: The requirements **REQ-7.13-01 and REQ-7.13-02** identified in ETSI EN 319 401 [8], shall apply.

6.8.16 Miscellaneous provisions

No policy requirement.

6.9 Other provisions

6.9.1 Organizational

OVR-6.9.1-01: The requirements identified in ETSI EN 319 401 [8], clause 7.1 shall apply.

In addition the following particular requirements apply:

OVR-6.9.1-02: 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:

- **OVR-6.9.1-03:** The senior executive, senior staff and staff in trusted roles, of the TSP concerned with certificate generation and revocation management 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.

OVR-6.9.1-04: 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

OVR-6.9.2-01: The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

OVR-6.9.2-02: Void.

OVR-6.9.2-02A: Any certificates issued for test purposes should clearly indicate that they are for testing purposes (e.g. by the subject name).

OVR-6.9.2-03 [PTC]**:** BRG [5], clause 2.2 shall apply.

OVR-6.9.2-04 [PTC]**:** For cross certificates, clause 3.2.6 of BRG [5] shall apply.

6.9.3 Disabilities

OVR-6.9.3-01: The requirements **REQ-7.13-03** and **REQ-7.13-04** identified in ETSI EN 319 401 [8], shall apply.

6.9.4 Terms and conditions

OVR-6.9.4-01: The requirements identified in ETSI EN 319 401 [8], clause 6.2 shall apply.

In addition the following particular requirements apply:

OVR-6.9.4-02: The terms and conditions shall include at minimum the following elements:

a) the indication of what constitutes certificate acceptance, as specified in **OVR-6.3.4-01**;

b) the period of time for which the records are retained according to **OVR-6.3.4-17**;

c) the subscriber's obligations as specified in **OVR-6.3.5-01**;

d) where applicable, the subject's obligations as specified in **OVR-6.3.5-02**;

e) the notice to relying parties as specified in **OVR-6.3.5-03**;

f) the ways in which a specific policy adds to or further constrains the requirements of the CP as defined in the present document, see **OVR-7.2-01**.

OVR-6.9.4-03 [PTC]**:** The TSP may limit its responsibilities as indicated in clause 9.8 of BRG [5].

OVR-6.9.4-04 [EVCP]**:** The TSP may limit its responsibilities as indicated in clause 9.8 of BRG [5] within the restrictions indicated in EVCG [4], clause 18.

7 Framework for the definition of other certificate policies

7.1 Certificate policy management

OVR-7.1-01: 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:

- **OVR-7.1-02:** 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.
- **OVR-7.1-03:** There shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the CP.
- **OVR-7.1-04:** 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.
- **OVR-7.1-05:** CPs should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP.
- **OVR-7.1-06:** A defined review process should exist to ensure that the CP is supported by the CA's CPS.
- **OVR-7.1-07:** 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 rely on those certificates.

- **OVR-7.1-08:** Revisions to CPs supported by the TSP should be made available to subscribers and relying parties.
- **OVR-7.1-09:** 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.
- **OVR-7.1-10:** The CP shall specify the Recommendation ITU-T X.509 [6] certificate profile requirements.
- **OVR-7.1-11:** Certificate profiles as defined by ETSI EN 319 412 part 2 to 4 [2], [9] and [10] should be used where appropriate.

- **OVR-7.1-12:** 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

OVR-7.2-01: 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 electronic signatures or seals. The period of time which registration information and TSP's 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, **OVR-6.3.5-02** items 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, **OVR-6.3.5-03** items a) to c)).
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, **REG-6.3.4-17**) 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): 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 ETSI TR 119 411-4 [i.20].

The checklist provides all requirements identifiers 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.

Annex C (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".

Annex D (informative): Change history

Date	Version	Information about changes
February 2016	1.1.1	Publication
June 2017	1.2.0	Below is a non-exhaustive list of the changes carried out since V1.1.1. • All requirements numbered as per clause 3.4. • Requirement numbering; all requirements are identified by a unique number. • New versions of the CA/B Forum documents are considered (EVCG V.1.6.1 for ECVP], and BRG v1.4.2 for PTC). • Several editorial changes and clarifications. • Adaptation of definitions for CRL and CARL. • New definitions for revocation and domain name. • Clarification on the concepts CA and TSP (and consistent application thorough the document). • Addition of a CP, the IVCP, for certificates that includes validated individual identity information for the subject. • Clarification on subject device provisioning service to cover the fact that it includes "soft keys" management. • Clarification that Identity validation is part of at least one of processes: certificate application, certificate issuance, subject device provisioning. • Clarification of requirement mentioning "issuing certificates considering the expiry date of the CA certificate" with "issuing certificates whose lifetime exceeds that of the CA's signing certificate" and further specifications. • Clarification of requirement on DN re-assignment. • Clarification of requirements with regard to the subscriber agreement that does not need to be "signed" anymore but "ratified". • Clarification of requirements with regard to the "confirmation that the information in the certificate is correct" by "the information to be held in the certificate is correct" and allowing to do this by reference (to the CP e.g.). • Alleviation of obligation to notify the subject in case of revocation (e.g. this may be impossible if the subject is dead). • Definition of a value for the CRL nextUpdate field when the CRL is the last one issued for a certain scope. • Mandatory support of CRL or OCSP. OCPS remains recommended, and is mandatory for certain CPs, but not strictly mandatory for all CPs. • Trusted Role identified in CEN TS 419 261 should be supported (not mandatory anymore). • Extension of some requirements on the CA (certificate signing) keys, to keys used by revocation and registration services. • Additional requirements on OCSP profile; if the OCSP responder receives a request for status of a certificate that has not been issued, then the responder is mandated not to respond with a "good" status and the TSP should monitor such requests. • Requirement to have subject legal person to ratify a second part of the subscriber agreement. • Additional requirement for trustworthy device (HSM) to be operated in its evaluated configuration as described in the CC guidance documentation or an equivalent configuration. • Clarification of the minimal elements to be part of the general terms and conditions (clause 6.4.9). • Deletion of text "*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.*" because the definition of Root-CA is sufficiently clear to this regard. • Removal of references to physical presence of the subscriber in clause 6.3.6 (renewal).

Date	Version	Information about changes
January 2018	1.2.1	Following ENAP public enquiry, the following changes were made. On https://docbox.etsi.org/esi/Open/Compared_deliverables, one will be able to see what changes have taken place between the previous published version (v1.1.1) and this version. REV-6.2.4-05: replaced "in advance" by "at a future date" and correction of wrong reference. Harmonisation of the use of "electronic signature", "electronic seal" and "digital signature" and reference to the certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 to generalize electronic signatures or seal to usage beyond the eIDAS Regulation (mainly impacting OVR-6.3.5-01 and SDP-6.3.12-03). Reworking of OVR-6.3.5-01 as the requirement was requiring the subscriber's obligations to literally include items a) to j) expressed below, i.e. a copy paste of the text of the standard and adaptation of OVR-6.3.5-02 accordingly. Addition of REV-6.3.9-02 to require revocation under certain circumstances. Annex B modified to point to ETSI TR 119 411-4 will contain the checklist.
April 2018	1.2.2	Publication
September 2020	1.2.3	CR#1 Reshuffling clause 4.2 to align with other ETSI/ESI policy documents CR#2 Revocation processing and delays CR#3 Short term certificates CR#4 Clarify and correct DIS 6.1-01, 02 and 03 CR#5 Clarify OCSP / CRL "consistency" CR#6 "secure user device" versus alternative terms CR#8 Introduce random data in the tbsCertificate CR#9 Corrections to the note under OVR-6.4.3-01 CR#10 Proof of possession or control CR#11 Separate trust service components CR#12 Meaning of ratifying CR#13 Management of private key by TSP CR#14 "Key" revocation CR#15 Importing from ETSI EN 319 411-2 CR#16 Applicability of LCP/NCP requirements to DV etc CR#17 Have references to CABF non-specific CR#18 TSP-RA-Subscriber segregation CR#19 CA Revocation CR#20 Evidence collection and records archival @ registration CR#21 SSL certificate subject cannot be legal person CR#22 DVCP and CABF BR requirements re-alignement CR#23 Test certificates CR#24 General clean up CR#25 IETF RFC 5280 subject name size limits CR#26 Correct and clarify certificate modification, rekey and renew CR#27 Clarify CRL update every 24h.

History

Document history		
V1.0.1	July 2015	Publication as ETSI TS 119 411-1 (withdrawn)
V1.1.1	February 2016	Publication
V1.2.2	April 2018	Publication
V1.3.0	February 2021	EN Approval Procedure AP 20210512: 2021-02-11 to 2021-05-12
V1.3.1	May 2021	Publication