Draft ETSI EN 319 411-1 V1.4.0 (2023-07)

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

Reference
REN/ESI-0019411-1v141

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

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";

NOTE: Part 3 of this multi-part deliverable has been withdrawn.

ETSI TR 119 411-4: "Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2";

ETSI TR 119 411-5: "Guidelines for the coexistence of web browser and EU trust controls".

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

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

Modal verbs terminology

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

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

Introduction

Electronic commerce, in its broadest sense, is a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator and protect the confidentiality of electronic exchanges. This is commonly achieved by using cryptographic mechanisms which are supported by a Trust Service Provider (TSP) issuing certificates, commonly called a Certification Authority (CA).

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

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.14] and those from CA/Browser Forum, BRG [6].

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 [9] 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 [6].

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 security, cybersecurity and privacy protection - 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: "Guidelines for The Issuance and Management of Extended Validation Certificates".

[5] CA/Browser Forum (V1.8.6): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[6] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

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

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

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

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

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

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

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

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

[15] ETSI TS 119 461: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[16] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".

2.2 Informative references

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

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

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

[i.1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.2] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

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

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

[i.5] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

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

[i.7] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".

[i.8] ISO/IEC 7498-2/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 419261: "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] Void.

[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 419221-2: "Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).

[i.17] TS 419221-3: "Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services", (produced by CEN).

[i.18] TS 419221-4: "Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup", (produced by CEN).

[i.19] EN 419221-5: "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 notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [9] 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 [7].

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 [9].

NOTE 3: See ISO/IEC 9594-8/Recommendation ITU-T X.509 [7].

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 [7].

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 [7].

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 [7].

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 [9].

Coordinated Universal Time (UTC): As indicated in ETSI EN 319 401 [9].

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 [9], 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: 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 [8].

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 [7].

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:

AIA	Authority Information Access
BRG	Baseline Requirements Guidelines
CA	Certification Authority
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
DV	Domain Validated
DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
eID	Electronic IDentity
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
OV	Organizational Validated
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
RA	Registration Authority
REQ	Requirement
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 Notations

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

e) [WEB] tagged requirements are applicable to CPs for web-authentication certificates building on the present document. These requirements are common to web-authentication certificates for general purpose. They relate to common topics and refer to requirements in BRG [5]. Incorporating [WEB] requirements in a policy for SSL/TLS certificates built on the present document does not necessarily require following the full and latest version of BRG [6], but requires following the selected requirements from version of BRG as stated in the normative reference [5].

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 a deleted requirement is left and completed with "Void".
- The requirement identifier for a modified requirement is 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 [9], 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 [9]. 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 [9]. According to ETSI EN 319 401 [9], 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 [9], 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. standardization organizations 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.

Three reference 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).

The following four CPs for SSL/TLS certificates based on the reference CPs and offering the level of assurance required by CAB Forum documents [4] and [6]:

NOTE: The intent of the present document is to include requirements so that a TSP that asserts the ETSI DVCP, OVCP, IVCP or EVCP policy OIDs in the IETF RFC 5280 [8] certificatePolicies extension of SSL/TLS certificates, also adheres to the corresponding CAB Forum policies for DV, OV, IV Certificates as defined in [6] or EV certificates as defined in EVCG [4]. Following one of the below CPs requires to follow the full and latest version of BRG [6] or EVCG [4]. As a consequence, for compliance with BRG/EVCG the TSP is required to augment the policy requirements defined in the present document with any additional requirements specific to the identified BRG [6] or EVCG [4] policy. It is recognized that further updates of BRG/EVCG may occur after the publication of the present document. In case of conflict between any requirement in the current version of the present document, be it a [LCP], [OVCP], [IVCP]or [DVCP] or a [NCP] or [EVCP] labelled requirement, the latest version of BRG [6] or EVCG [4] takes precedence. In case of conflicting requirements between latest version of CA/Browser Forum policies for SSL/TLS Certificates and the present document, it is requested that this is brought to the attention of ETSI TC ESI and the CAB Forum. ETSI TC ESI will endeavour to monitor revisions to the BRG/EVCG and reference the latest version within the revision cycle of the present document.

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 [6] 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 [6].

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 [6] 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 [6].

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 [6] 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 [6].

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.