Draft ETSI EN 319 411-1 V1.0.0 (2015-06)

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

Reference

DEN/ESI-0019411-1

Keywords

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

ETSI

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

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

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

Important notice

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

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This 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 on policy requirements for Trust Service Providers issuing certificate as identified below:

Part 1: "General requirements";

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

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

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

Modal verbs terminology

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

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

Introduction

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

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

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.15] 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 specified in the present document and specifying any additional requirements in a manner similar to ETSI EN 319 411-2 [i.5], which builds on the present document requirements so as to benefit from the use of generally accepted global best practices.

1 Scope

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

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

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

The present document is applicable to:

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

The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE: See ETSI EN 319 403 [i.2] for guidance on assessment of TSP processes and services. The present document references ETSI EN 319 401 [8] for general policy requirements common to all classes of TSP services.

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

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

2 References

2.1 Normative references

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

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

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

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

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

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

[3] ISO/IEC 19790:2006: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[i.14] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.15] 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.16] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.17] CEN EN 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup".

[i.18] CEN EN 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services".

[i.19] CEN EN 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup".

[i.20] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services".

3 Definitions, abbreviations and notation

3.1 Definitions

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

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

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

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

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

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

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

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

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

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

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

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

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

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

NOTE 1: A CA can be:

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

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

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

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

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

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

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

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

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

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

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

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

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

EV certificate: See Extended Validation certificate.

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

high security zone: physical location where a CA's private key or cryptographic hardware is located

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

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

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

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

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

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

revocation officer: person responsible for operating certificate status changes

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, …).

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

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 can be a CA that 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: The certification authority that provides a trust point for a trust service addressed by the present document is considered to be a trust anchor.

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

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

3.2 Abbreviations

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

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB Forum	CA/Browser Forum
CARL	Certification Authority Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider

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

DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
LCP	Lightweight Certificate Policy
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy
PDS	Policy Disclosure Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTC	Publicly-Trusted Certificate

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

QCP	Qualified Certificate Policy
RA	Registration Authority
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol

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

TSP	Trust Service Provider
UTC	Coordinated Universal Time

3.3 Notation

The requirements identified in the present document include:

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

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

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

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

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

4 General concepts

4.1 General policy requirements concepts

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

4.2 Certificate policy and certification practice statement

4.2.1 Overview

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

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

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

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

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

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

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

4.2.2 Purpose

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