ETSI EN 319 411-1 V1.5.1 (2025-04)

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

Reference
REN/ESI-0019411-1v151

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Trust 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";

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 TS 119 411-5: "Implementation of qualified certificates for website authentication as in amended regulation 910/2014";

ETSI TS 119 411-6: "Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates".

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:	24 March 2025
Date of latest announcement of this EN (doa):	30 June 2025
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 December 2025
Date of withdrawal of any conflicting National Standard (dow):	31 December 2025

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 in the ETSI docbox.

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 Trust 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".