ETSI TR 119 411-4 V1.3.1 (2025-09)

TECHNICAL REPORT

Electronic Signatures and Trust 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

Reference
RTR/ESI-0019411-4v131

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 Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

The present document is part 4 of a multi-part deliverable covering policy requirements for Trust Service Providers issuing certificates. Full details of the entire series can be found in part 1 [i.2].

Modal verbs terminology

In the present document "**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 measures in order to minimize the operational and financial threats and risks associated with public key cryptographic systems.

ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3] are 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 1183/2024 [i.4] and those from CA/Browser Forum in BRG [i.6] and EVCG [i.5].

The present document provides a check-list for self-assessment or independent conformity assessment of TSPs issuing certificates according to ETSI EN 319 411-1 [i.2] and/or issuing EU qualified certificates according to ETSI EN 319 411-2 [i.3]. It also aims to facilitate the preparatory activities the trust service provider undertakes.

1 Scope

The present document is a checklist of the policy requirements specific to TSP issuing certificates (as expressed in ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3]) including the generic requirements which are independent of the type of service (as expressed in ETSI EN 319 401 [i.1]).

The checklist identifies each requirement associated with each certificate policy, as specified in ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3], and also relates where relevant the requirement to a particular TSP component service. Additional fields are provided to allow TSPs to indicate claimed compliance to a particular requirement and for assessors to indicate the results of an assessment for each requirement. This checklist can be used by the TSP itself to prepare for an assessment of its practices against the referenced documents (i.e. serve as a basis for a self-declaration) and/or by the assessor when conducting the assessment.

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 319 403-1 [i.7] for guidance on assessment of TSP's processes and services.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI EN 319 401 (V3.1.1): "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.2] ETSI EN 319 411-1 (V1.5.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.3] ETSI EN 319 411-2 (V2.6.1): "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.4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.5] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

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

[i.7] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [i.1], ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [i.1], ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3] apply.

4 Checklist of the policy requirements applicable to TSP issuing certificates

The present document includes a checklist of the policy requirements specific to TSP issuing certificates as expressed in ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3]. The checklist is contained in the spreadsheets file tr_11941104v010301p0.zip which accompanies the present document.

In the case of conflict between the requirements listed in these sheets and those specified in the referenced documents ETSI EN 319 401 [i.1], ETSI EN 319 411-1 [i.2] and ETSI EN 319 411-2 [i.3], the referenced documents take precedence.

History

Document history		
V1.1.1	May 2018	Publication
V1.2.1	June 2024	Publication
V1.3.1	September 2025	Publication