ETSI TS 119 411-2 V2.0.7 (2015-07)

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

Reference
RTS/ESI-0019411-2-TS

Keywords
e-commerce, electronic signature, 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

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 Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

The present document is derived from the requirements specified in ETSI TS 101 456 [i.2] "Policy requirements for certification authorities issuing qualified certificates".

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

The Regulation (EU) N° 910/2014 [i.1] establishes a legal framework for electronic signature and electronic seal and for website authentication services. It addresses for example the ability to electronically sign data in the same way they are signed using a hand-written signature. These concepts can be commonly achieved by using cryptographic mechanisms. Electronic signatures and seals implemented by this way are digital signatures. Cryptographic mechanisms are generally supported by a trust service provider (TSP) issuing public key certificates, commonly called a certification authority (CA).

By providing general policy and security requirements for trust service providers issuing certificates, the part 1 of the series ETSI TS 119 411 [2], is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, requirements from Regulation (EU) No 910/2014 [i.1] and from CA Browser Forum [i.4].

The present document incorporates the general policy and security requirements as specified in ETSI TS 119 411-1 [2] and adds further requirements in order to meet the specific requirements of Regulation (EU) N° 910/2014 for TSPs issuing EU qualified certificates for electronic signatures and/or EU qualified certificates for electronic seals and/or EU qualified certificates for web site authentication in accordance with but not limited to Articles 19, 24, 28, 38 and 45 of Regulation (EU) N° 910/2014 [i.1].

Bodies wishing to establish policy requirements for TSPs issuing certificates in a regulatory context other than the EU can build their specifications on the general policy requirements specified in ETSI TS 119 411-1 [2] to benefit from global best practices, and specify any additional requirements in a manner similar to the present document.

1 Scope

The present document specifies policy and security requirements for the issuance, maintenance and life-cycle management of EU qualified certificates as defined in Regulation (EU) N° 910/2014 [i.1]. These policy and security requirements support reference certificate policies for the issuance, maintenance and life-cycle management of EU qualified certificates issued to natural persons (including natural persons associated with a legal person), to legal persons and to web sites, respectively.

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. The present document however provides in annex B a check list of the policy requirements specific to TSP issuing EU qualified certificates (as expressed in the present document) as well as all the requirements incorporated by reference to ETSI TS 119 411-1 [2] and ETSI TS 119 401 [1], that can be used by the TSP to prepare an assessment of its practices against the present document and/or by the assessor when conducting the assessment for confirming that a TSP meets the requirements for issuing qualified certificates under Regulation (EU) N° 910/2014 [i.1].

NOTE: See ETSI TS 119 403 [i.7] for guidance on assessment of TSP processes and services.

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] ETSI TS 119 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ETSI TS 119 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5, CA/Browser Forum.

[4] ETSI TS 119 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

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] Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.