Draft ETSI EN 319 411-2 V2.2.0 (2017-08)

EUROPEAN STANDARD

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
REN/ESI-0019411-2v221

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

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Essential patents

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 (https://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.

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.

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 2 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 [2].

The present document is derived from the requirements specified in ETSI TS 101 456 [i.2].

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

The Regulation (EU) No 910/2014 [i.1] establishes a legal framework for electronic signature and electronic seal and for website authentication services. 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 EN 319 411-1 [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.3].

The present document incorporates the general policy and security requirements as specified in ETSI EN 319 411-1 [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 website authentication in accordance with but not limited to Articles 19, 24, 28, 38 and 45 of Regulation (EU) No 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 EN 319 411-1 [2] to benefit from global best practices, and specify any additional requirements in a manner similar to the present document.

Conformance to the present document on its own does not imply that the TSP, nor the certificates issued by the TSP, are qualified in accordance with Regulation (EU) No 910/2014 [i.1].

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) No 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 or a website) and to legal persons (including legal persons associated with a website), 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 checklist 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 EN 319 411-1 [2] and ETSI EN 319 401 [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) No 910/2014 [i.1].

NOTE: See ETSI EN 319 403 [i.6] for guidance on assessment of TSP's 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 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] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

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

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) No 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.

[i.2] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.3] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5".

[i.8] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.9] IETF RFC 6960: "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP".

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 [1], ETSI EN 319 411-1 [2], Regulation (EU) No 910/2014 [i.1] and the following apply:

EU Qualified Certificate: qualified certificate as specified in Regulation (EU) No 910/2014 [i.1]

Qualified Electronic Signature/Seal Creation Device: As specified in Regulation (EU) No 910/2014 [i.1].

3.2 Abbreviations

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

QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person
QSCD	Qualified electronic Signature/Seal Creation Device

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any certificate policy. 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 certificate policy. Such requirements are indicated by clauses marked by the applicable certificate policy indicator: "[QCP-l]", "[QCP-n]", "[QCP-l-qscd]", "[QCP-n-qscd]" and/or "[QCP-w]".

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 throughout 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 deleted requirements are left and completed with "VOID".
- The requirement identifier for modified requirement are 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

ETSI EN 319 411-1 [2], clause 4.1 applies.

4.2 Certificate policy and certification practice statement

4.2.1 Overview

The explanations identified in ETSI EN 319 411-1 [2], clause 4.2.1 apply.

4.2.2 Purpose

The explanations identified in ETSI EN 319 411-1 [2], clause 4.2.2 apply.

4.2.3 Level of specificity

The guidelines identified in ETSI EN 319 411-1 [2], clause 4.2.3 apply.

4.2.4 Approach

The guidelines identified in ETSI EN 319 411-1 [2], clause 4.2.4 apply.

4.2.5 Certificate policy

The present document defines five certificate policies and allocates a policy identifier for each of them. These policy identifiers are called "EU qualified certificate policy identifiers"; they are defined in clause 5.3.

The certificate policies are based on the following policies specified in ETSI EN 319 411-1 [2]:

- normalized certificate policy (NCP);
- enhanced normalized certificate policy (NCP+); and
- extended validation certificate policy (EVCP).

The five EU qualified certificate policies are:

1) A policy for EU qualified certificates issued to natural persons (QCP-n) offering the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates:

   - The requirements for QCP-n include all the NCP policy requirements, plus additional requirements suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

   - If the TSP's implementation of this policy requires a secure cryptographic device, the requirements for QCP-n include all the NCP+ requirements, plus the additional requirements suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

2) A policy for EU qualified certificates issued to legal persons (QCP-l) offering the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates:

   - The requirements for QCP-l include all the NCP policy requirements, plus additional requirements suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

   - If the TSP's implementation of this policy requires a secure cryptographic device, the requirements for QCP-n include all the NCP+ requirements, plus the additional requirements suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

3) A policy (QCP-n-qscd) for EU qualified certificates issued to natural persons offering the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates and requiring the use of a Qualified Signature Creation Device (QSCD). Such policy requires that the private key related to the certified public key resides in the QSCD:

   - The requirements for QCP-n-qscd include all the QCP-n requirements (including all the NCP+ requirements), plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1], including those specific to the QSCD provision.

4) A policy (QCP-l-qscd) for EU qualified certificates issued to legal persons offering the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates and requiring the use of a Qualified Seal Creation Device (QSCD). Such policy requires that the private key related to the certified public key resides in the QSCD:

   - The requirements for QCP-l-qscd include all the QCP-l requirements (including all the NCP+ requirements), plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1], including those specific to the QSCD provision.

5) A policy for EU qualified website certificates (QCP-w) offering the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates (requiring or not the use of a secure cryptographic device) used in support of websites authentication:

   - When the certificate is issued to a legal person the requirements for QCP-w include all the EVCP requirements, plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

   - When the certificate is issued to a natural person the requirements for QCP-w include all the NCP requirements, plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

Clause 7 specifies a framework for other certificate policies which enhance or further constrain the above policies.

4.3 Other TSP statements

The guidelines identified in ETSI EN 319 411-1 [2], clause 4.3 apply.

4.4 Certification services

The service of issuing EU qualified certificates is broken down in component services presented in ETSI EN 319 411-1 [2], clause 4.4 for the purposes of classifying requirements.

5 General provisions on Certification Practice Statement and Certificate Policies

5.1 General requirements

The present document is structured broadly in line with IETF RFC 3647 [i.4] to assist TSPs in applying these requirements to their own CP and CPS documentation.