Draft ETSI EN 319 411-2 V2.5.0 (2023-07)

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-0019411-2v251

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://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 prevailing version of an ETSI
deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of
experience to understand and interpret its content in accordance with generally accepted engineering or
other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not
limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property
rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages
for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use
of or inability to use the software.

Copyright Notification

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 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] and [i.7].

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.

NOTE: See ETSI EN 319 403 [i.6] for guidance on assessment of TSP's processes and services. The present document references ETSI EN 319 411-1 [2] for general requirements on TSP issuing certificates.

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 - Part 8: The Directory: 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 of 23 July 2014 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".

NOTE: The version is as referenced in ETSI EN 319 411-1 [2].

[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".

NOTE: The version is as referenced in ETSI EN 319 411-1 [2].

[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".

[i.10]   ETSI TR 119 411-4: "Electronic Signatures and 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".

[i.11]   Commission implementing decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of 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.

[i.12]   ETSI TS 119 615: "Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists".

[i.13]   ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

3   Definition of terms, symbols, abbreviations and notations

3.1   Terms

For the purposes of the present document, the terms 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 (QSCD): As specified in Regulation (EU) No 910/2014 [i.1].

3.2   Symbols

Void.

3.3 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
QEVCP-w Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG [i.7]

NOTE: Previous versions of the present document used the abbreviation QCP-w.

QNCP-w Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person based on the BRG [i.3]
QNCP-w-gen Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person, applicable for general purpose certificate for qualified website authentication
QSCD Qualified electronic Signature/Seal Creation Device

3.4 Notations

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]", "[QEVCP-w]", "[QNCP-w]" and/or "[QNCP-w-gen]".

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 a deleted requirement is left and completed with "Void".

- The requirement identifier for a modified requirement is 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 a number of 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 policy requirements specified in ETSI EN 319 411-1 [2]:

- Requirements of the Normalized Certificate Policy (NCP).

- Requirements of the enhanced Normalized Certificate Policy (NCP+).

- Requirements of the Extended Validation Certificate Policy (EVCP).

- Requirements of the Organizational Validation Certificate Policy (OVCP), the Individual Validation Certificate Policy (IVCP) and the Domain Validation Certificate Policy (DVCP).

- Requirements common to web-authentication certificates for general purpose tagged [WEB].

NOTE: Some relying parties (e.g. vendors of Internet browser software) may also require conformance to the entirety of CA/Browser Forum Baseline Requirements or Extended Validation Guidelines or other policy requirements.

The 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 for EU qualified certificates issued to natural persons (QCP-n-qscd) 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 for EU qualified certificates issued to legal persons (QCP-l-qscd) 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 (QEVCP-w) that conforms to the latest version of EVCG [i.7], offering at a minimum the "Extended Validated" level of assurance as defined by the CA/Browser Forum, and the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates used in support of websites authentication:

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

6) A policy for EU qualified website certificates (QNCP-w) that conforms to the latest version of BRG [i.3], offering at a minimum the "Organization Validated" or "Individual Validated" level of assurance as defined by the CA/Browser Forum and the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates used in support of websites authentication:

   - The requirements for QNCP-w include all the NCP requirements for certificates issued to natural or legal persons, plus either the IVCP or the OCVP requirements, plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) No 910/2014 [i.1].

7) A policy for EU qualified website certificates (QNCP-w-gen) offering the level of quality defined in Regulation (EU) No 910/2014 [i.1] for EU qualified certificates used in support of websites authentication for general purpose certificate for qualified website authentication:

- The requirements for QNCP-w-gen include all the NCP requirements for certificates issued to natural or legal persons, plus selected requirements from BRG [i.3] tagged as [WEB] in ETSI EN 319 411-1 [2], 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.

OVR-5.1-01: The general requirements specified in ETSI EN 319 411-1 [2], clause 5.1 shall apply.

In addition the following particular requirements apply:

OVR-5.1-02 [QCP-n] and [QCP-l] [CHOICE]:

- If the TSP's terms and conditions do not require a secure cryptographic device, all requirements defined for NCP in ETSI EN 319 411-1 [2] shall apply. Where a requirement for NCP is specified differently for natural person or legal person respectively, such requirement shall apply for QCP-n or QCP-l accordingly.

- If the TSP's terms and conditions require a secure cryptographic device all requirements defined for NCP+ in ETSI EN 319 411-1 [2] shall apply. Where a requirement for NCP+ is specified differently for natural person or legal person respectively, such requirement shall apply for QCP-n or QCP-l accordingly.

OVR-5.1-03 [QEVCP-w]: All requirements defined for [EVCP] in ETSI EN 319 411-1 [2] shall apply.

NOTE 1: This implies compliance with the latest version of EVCG [i.7].

OVR-5.1-04 [QCP-n-qscd]: All requirements defined for [QCP-n], including all requirements defined for NCP+ in ETSI EN 319 411-1 [2], shall apply. Where a requirement for NCP+ is specified differently for natural person or legal person respectively, the requirement for natural person shall apply for QCP-n-qscd.

OVR-5.1-05 [QCP-l-qscd]: All requirements defined for [QCP-l], including all requirements defined for NCP+ in ETSI EN 319 411-1 [2], shall apply. Where a requirement for NCP+ is specified differently for natural person or legal person respectively, the requirement for legal person shall apply for QCP-l-qscd.

OVR-5.1-06 [QNCP-w], [QNCP-w-gen]: All requirements defined for NCP in ETSI EN 319 411-1 [2] shall apply.

OVR-5.1-07 [QNCP-w-gen]: All requirements tagged as [WEB] in ETSI EN 319 411-1 [2] shall apply.