



**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**

ReferenceREN/ESI-0019411-2

Keywordse-commerce, electronic signature, security,
trust services

ETSI650 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

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions, abbreviations and notations	8
3.1 Definitions	8
3.2 Abbreviations	8
3.3 Notation.....	8
4 General concepts	9
4.1 General policy requirements concepts.....	9
4.2 Certificate policy and certification practice statement	9
4.2.1 Overview	9
4.2.2 Purpose	9
4.2.3 Level of specificity	9
4.2.4 Approach	9
4.2.5 Certificate policy	9
4.3 Other TSP statements	10
4.4 Certification services	10
5 General provisions on Certification Practice Statement and Certificate Policies.....	10
5.1 General requirements	10
5.2 Certification Practice Statement Requirements	11
5.3 Certificate Policy name and identification	11
5.4 PKI Participants.....	12
5.4.1 Certification authority	12
5.4.2 Subscriber and subject	12
5.4.3 Others.....	12
5.5 Certificate Usage	12
5.5.1 QCP-n	12
5.5.2 QCP-l	12
5.5.3 QCP-n-qscd.....	12
5.5.4 QCP-l-qscd	12
5.5.5 QCP-w	12
6 Trust Service Providers practice.....	13
6.1 Publication and Repository Responsibilities	13
6.2 Identification and Authentication	13
6.2.1 Naming	13
6.2.2 Initial Identity Validation.....	13
6.2.3 Identification and authentication for Re-key requests	13
6.2.4 Identification and authentication for revocation requests	13
6.3 Certificate Life-Cycle Operational Requirements	14
6.3.1 Certificate Application.....	14
6.3.2 Certificate application processing	14
6.3.3 Certificate issuance	14
6.3.4 Certificate acceptance	14
6.3.5 Key Pair and Certificate Usage.....	14
6.3.6 Certificate Renewal.....	14
6.3.7 Certificate Re-key	14
6.3.8 Certificate Modification.....	15
6.3.9 Certificate Revocation and Suspension.....	15

6.3.10	Certificate Status Services	15
6.3.11	End of Subscription	15
6.3.12	Key Escrow and Recovery	15
6.4	Facility, Management, and Operational Controls	15
6.4.1	General	15
6.4.2	Physical Security Controls	15
6.4.3	Procedural Controls	15
6.4.4	Personnel Controls	15
6.4.5	Audit Logging Procedures	16
6.4.6	Records Archival	16
6.4.7	Key Changeover	16
6.4.8	Compromise and Disaster Recovery	16
6.4.9	CA or RA Termination	16
6.5	Technical Security Controls	16
6.5.1	Key Pair Generation and Installation	16
6.5.2	Private Key Protection and Cryptographic Module Engineering Controls	17
6.5.3	Other Aspects of Key Pair Management	17
6.5.4	Activation Data	17
6.5.5	Computer Security Controls	17
6.5.6	Life Cycle Security Controls	17
6.5.7	Network Security Controls	17
6.5.8	Time-stamping	17
6.6	Certificate, CRL, and OCSP Profiles	17
6.6.1	Certificate Profile	17
6.6.2	CRL Profile	18
6.6.3	OCSP Profile	18
6.7	Compliance Audit and Other Assessment	18
6.8	Other Business and Legal Matters	19
6.8.1	Fees	19
6.8.2	Financial Responsibility	19
6.8.3	Confidentiality of Business Information	19
6.8.4	Privacy of Personal Information	19
6.8.5	Intellectual Property Rights	19
6.8.6	Representations and Warranties	19
6.8.7	Disclaimers of Warranties	19
6.8.8	Limitations of Liability	19
6.8.9	Indemnities	19
6.8.10	Term and Termination	19
6.8.11	Individual notices and communications with participants	19
6.8.12	Amendments	19
6.8.13	Dispute Resolution Procedures	20
6.8.14	Governing Law	20
6.8.15	Compliance with Applicable Law	20
6.8.16	Miscellaneous Provisions	20
6.9	Other Provisions	20
6.9.1	Organizational	20
6.9.2	Additional testing	20
6.9.3	Disabilities	20
6.9.4	Terms and conditions	20
7	Framework for the definition of other certificate policies built on the present document	20
7.1	Certificate policy management	20
7.2	Additional requirements	21
Annex A (informative):	Regulation and EU qualified certificate policy mapping	22
Annex B (informative):	Conformity Assessment Check list	26
Annex C (informative):	Revisions made since ETSI EN 319 411-2 version 1.1.1 (2013-01)	27
History		28

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 final draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the 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] "Policy requirements for certification authorities issuing qualified certificates".

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):	12 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) N° 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) 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 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) N° 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) 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 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 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 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) N° 910/2014 [i.1].

NOTE: See ETSI EN 319 403 [i.6] 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 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".

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

- [i.3] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.
- [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] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5, CA/Browser Forum.

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], the Regulation (EU) N° 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-I	Policy for EU qualified certificate issued to a legal person
QCP-I-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 applicable to the services offered under the applicable certificate policy. Such requirements are indicated by clauses marked by the applicable certificate policy indicator: "[QCP-I]", "[QCP-n]", "[QCP-I-qscd]", "[QCP-n-qscd]" and/or "[QCP-w]".

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:

- a) A policy for EU qualified certificates issued to natural persons (QCP-n) offering the level of quality defined in Regulation (EU) N° 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) N° 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) N° 910/2014 [i.1].
- b) A policy for EU qualified certificates issued to legal persons (QCP-l) offering the level of quality defined in Regulation (EU) N° 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) N° 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) N° 910/2014 [i.1].

- c) A policy (QCP-n-qscd) for EU qualified certificates issued to natural persons offering the level of quality defined in Regulation (EU) N° 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) N° 910/2014 [i.1], including those specific to the QSCD provision.
- d) A policy (QCP-l-qscd) for EU qualified certificates issued to legal persons offering the level of quality defined in Regulation (EU) N° 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) N° 910/2014 [i.1], including those specific to the QSCD provision.
- e) A policy for EU qualified website certificates (QCP-w) offering the level of quality defined in Regulation (EU) N° 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) N° 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) N° 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.

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

- a) [QCP-n] and [QCP-l] [CONDITIONAL]:
 - i) If the TSP's terms and conditions does 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.

- ii) If the TSP's terms and conditions requires 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.
- b) [QCP-w] [CONDITIONAL]:
 - i) If the certificate is issued to a legal person, all requirements defined for EVCP in ETSI EN 319 411-1 [2], shall apply.
 - ii) If the certificate is issued to a natural person, all requirements defined for NCP in ETSI EN 319 411-1 [2], shall apply.
- c) [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.
- d) [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.

5.2 Certification Practice Statement Requirements

The requirements identified in ETSI EN 319 411-1 [2], clause 5.2 shall apply.

5.3 Certificate Policy name and identification

As described in IETF RFC 3647 [i.4], clause 3.3, certificates include a certificate policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.

The identifiers for the EU qualified certificate policies specified in the present document are:

- a) **QCP-n:** certificate policy for EU qualified certificates issued to natural persons;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-natural (0)
```

- b) **QCP-l:** certificate policy for EU qualified certificates issued to legal persons;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-legal (1)
```

- c) **QCP-n-qscd:** certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-natural-qscd (2)
```

- d) **QCP-l-qscd:** certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-legal-qscd (3)
```

- e) **QCP-w:** certificate policy for EU qualified website authentication certificates;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-web (4)
```

Including one of the policy identifiers defined above in a EU qualified certificate indicates that the certificate is issued and managed according to the present document for that policy. The policy identifier can be used by relying parties in determining the certificate's suitability and trustworthiness in the framework of Regulation (EU) N° 910/2014 [i.1].

NOTE: See clause 4.2.5 for a general description of the above policies.

5.4 PKI Participants

5.4.1 Certification authority

The concepts described in ETSI EN 319 411-1 [2], clause 5.4.1 apply.

NOTE: Regulation (EU) No 910/2014 addresses liability of trust service providers. In particular, the TSP identified as the qualified TSP issuing EU qualified certificates in the trusted list of qualified services, maintains overall responsibility for meeting liability for the issuing of certificates as required in Regulation (EU) N° 910/2014 [i.1].

5.4.2 Subscriber and subject

ETSI EN 319 411-1 [2], clause 5.4.2 applies.

5.4.3 Others

ETSI EN 319 411-1 [2], clause 5.4.3 applies.

5.5 Certificate Usage

5.5.1 QCP-n

Certificates issued under these requirements are aimed to support the advanced electronic signatures based on a qualified certificate defined in articles 26 and 27 of the Regulation (EU) N° 910/2014 [i.1].

5.5.2 QCP-l

Certificates issued under these requirements are aimed to support the advanced electronic seals based on a qualified certificate defined in articles 36 and 37 of the Regulation (EU) N° 910/2014 [i.1].

5.5.3 QCP-n-qscd

Certificates issued under these requirements are aimed to support qualified electronic signatures such as defined in article 3 (12) of the Regulation (EU) N° 910/2014 [i.1].

5.5.4 QCP-l-qscd

Certificates issued under these requirements are aimed to support qualified electronic seals such as defined in article 3 (27) of the Regulation (EU) N° 910/2014 [i.1].

5.5.5 QCP-w

Certificates issued under these requirements are aimed to support website authentication based on a qualified certificate defined in articles 3 (38) and 45 of the Regulation (EU) N° 910/2014 [i.1].

Certificates issued under these requirements endorse the requirement of EV Certificates whose purpose is specified in clause 5.5 of ETSI EN 319 411-1 [2]. In addition, EU qualified certificates issued under this policy may be used to provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website as specified in Regulation (EU) N° 910/2014 [i.1].

6 Trust Service Providers practice

6.1 Publication and Repository Responsibilities

The requirements specified in ETSI EN 319 411-1 [2], clause 6.1 shall apply.

6.2 Identification and Authentication

6.2.1 Naming

The requirements specified in ETSI EN 319 411-1 [2], clause 6.2.1 shall apply.

See also clause 6.6.1 of the present document.

6.2.2 Initial Identity Validation

The requirements identified in ETSI EN 319 411-1 [2], clause 6.2.2 shall apply.

In addition the following particular requirements apply.

Registration

- a) [QCP-n] and [QCP-n-qscd] the identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:
 - i) by the physical presence of the natural person; or
 - ii) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence.

NOTE 1: The proof of equivalence can be done according to the Regulation (EU) N° 910/2014 [i.1].

NOTE 2: The proof of equivalence needs to consider the impersonation risks inherent to remote applications. In particular, an uninterrupted chain of subsequent remote registrations can increase such risks, because the person can never be actually seen for years, and/or because the traceability with the initial face to face is weakened.

- b) [QCP-l] and [QCP-l-qscd] the identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:
 - i) by the physical presence of an authorized representative of the legal person; or
 - ii) using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which the TSP can prove the equivalence.

NOTE 3: See notes 1 and 2 above.

- c) [QCP-w] [CONDITIONAL]:
 - i) if the subscriber is a natural person the identity of the subscriber and her/his link with the domain name to be certified and, if applicable, any specific attributes of the person shall be verified as per item a) above);
 - ii) if the subscriber is a legal person the identity of the subscriber and its link with the domain name to be certified and, if applicable, any specific attributes of the person shall be verified as per item b) above).

6.2.3 Identification and authentication for Re-key requests

The requirements identified in ETSI EN 319 411-1 [2], clause 6.2.3 shall apply.

6.2.4 Identification and authentication for revocation requests

The requirements identified in ETSI EN 319 411-1 [2], clause 6.2.4 shall apply.

6.3 Certificate Life-Cycle Operational Requirements

6.3.1 Certificate Application

NOTE: See also clause 6.2.2 regarding identity validation.

The requirements identified in ETSI EN 319 411-1 [2], clause 6.3.1 shall apply.

6.3.2 Certificate application processing

The requirements identified in ETSI EN 319 411-1 [2], clause 6.3.2 shall apply.

6.3.3 Certificate issuance

The requirements identified in ETSI EN 319 411-1 [2], clause 6.3.3 shall apply.

6.3.4 Certificate acceptance

The requirements identified in ETSI EN 319 411-1 [2], clause 6.3.4 shall apply. In addition:

- a) [CONDITIONAL]: if the subscriber agreement is in electronic form, it should be signed with an Advanced Electronic Signature or an Advanced Electronic Seal as specified by Regulation (EU) N° 910/2014 [i.1].

6.3.5 Key Pair and Certificate Usage

The general obligations specified in ETSI EN 319 411-1 [2], clause 6.3.5 shall apply.

In addition:

- a) [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]: if the TSP manages the QSCD for the subject:
 - i) the private key shall not be used for signing except within a QSCD.
 - ii) [QCP-n-qscd]: the subject's private key shall be used under the subject's sole control.
 - iii) [QCP-l-qscd]: the subject's private key shall be used under the subject's control.
 - iv) [QCP-n-qscd]: the subject's key pair should be used only for electronic signatures.
 - v) [QCP-l-qscd]: the subject's key pair should be used only for electronic seals.
- b) The subscriber's obligations (see clause 6.3.4) (or respectively the obligations on the TSP managing the key on behalf of the subject) shall require that:
 - i) [QCP-n] and [QCP-n-qscd]: the subject's private key is maintained (or respectively is used) under the subject's sole control.
 - ii) [QCP-l] and [QCP-l-qscd]: the subject's private key is used under the subject's control.
 - iii) [QCP-n-qscd] and [QCP-l-qscd]: digital signatures are only created by a QSCD device.
- c) The subscriber's obligations (see clause 6.3.4) or the obligations on the TSP managing the key on behalf of the subject should recommend that:
 - i) [QCP-n] and [QCP-n-qscd]: the subject's key pair is used only for electronic signatures.
 - ii) [QCP-l] and [QCP-l-qscd]: the subject's key pair is used only for electronic seals.

6.3.6 Certificate Renewal

The requirements identified in ETSI EN 319 411-1 [2], clause 6.3.6 shall apply.

6.3.7 Certificate Re-key

NOTE: See clause 6.2.3.

6.3.8 Certificate Modification

The requirements identified in ETSI EN 319 411-1 [2], clause 6.3.8 shall apply.

6.3.9 Certificate Revocation and Suspension

The requirements specified in ETSI EN 319 411-1 [2], clause 6.3.9 shall apply.

6.3.10 Certificate Status Services

The requirements specified in ETSI EN 319 411-1 [2], clause 6.3.10 shall apply.

In addition the following particular requirements apply:

NOTE 1: Regulation (EU) No 910/2014 [i.1] requires this service to be provided free of charge.

Revocation status

- a) Revocation status information shall be made available beyond the validity period of the certificate.

NOTE 2: The obligation from ETSI EN 319 411-1 [2] to support OCSP is not applicable after the certificate expiry.

- b) The TSP shall document precisely in its practices statements and in its terms and conditions how requirement a) is met, including TSP termination (see clause 6.4.9).

NOTE 3: There are plans for further standardization activities for handling revocation status beyond the validity period of the certificate.

6.3.11 End of Subscription

No policy requirement.

6.3.12 Key Escrow and Recovery

The requirements specified in ETSI EN 319 411-1 [2], clause 6.3.12 shall apply.

6.4 Facility, Management, and Operational Controls

6.4.1 General

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.1 shall apply.

6.4.2 Physical Security Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.2 shall apply.

6.4.3 Procedural Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.3 shall apply.

6.4.4 Personnel Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.4 shall apply.

6.4.5 Audit Logging Procedures

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.5 shall apply.

In addition, for the recording of information concerning EU qualified certificates, the following particular requirements apply.

Subject device provision

- a) [QCP-n-qscd] and [QCP-l-qscd]: the TSP shall log all events relating to the preparation of QSCDs.

General

- b) The TSP shall record all relevant information concerning data issued and received and shall log all events relating to the EU qualified certificate registration, generation, dissemination, and when applicable, revocation management and device preparation.
- c) The information shall be maintained as necessary to meet legal requirements beyond the termination of the TSP (see clause 6.4.9).
- d) The TSP shall document how this information is accessible.
- e) The TSP shall document precisely the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan.

NOTE: Regulation (EU) No 910/2014 [i.1] article 24.2 (h) requires a qualified TSP to "*record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically*".

6.4.6 Records Archival

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.6 shall apply.

6.4.7 Key Changeover

No policy requirement.

6.4.8 Compromise and Disaster Recovery

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.8 shall apply.

6.4.9 CA or RA Termination

The requirements identified in ETSI EN 319 411-1 [2], clause 6.4.9 shall apply.

6.5 Technical Security Controls

6.5.1 Key Pair Generation and Installation

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.1 shall apply.

In addition:

Subject device provision

- a) [QCP-n-qscd] and [QCP-l-qscd]: whether the device is prepared by the TSP or not, the TSP shall verify that the device is certified as a QSCD.

NOTE 1: Regulation (EU) N° 910/2014 [i.1] requires the QSCD to be certified as meeting the requirements of annex II through a certificate following the rules expressed in sections 4 and 5 of this Regulation.

NOTE 2: Further standards may be issued in this area.

- b) [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]:
 - i) if the device is managed by a third party TSP on behalf of the subject which is not the TSP issuing the certificate itself, the TSP issuing the certificate shall verify that this third party TSP is meeting the appropriate requirements in terms of qualification;
 - ii) the certificate request process shall ensure that the public key to be certified is from a key pair generated by a QSCD;
 - iii) if the subject's key pair is generated by a TSP and imported into the QSCD used for signature/seal creation, the environmental assumptions and security objectives for the certified device (QSCD used for key generation and QSCD used for signature/seal creation) shall be met by the TSP. If the subject's private key is moved between devices potential vulnerabilities to key compromise shall be determined and adequate mechanisms implemented to mitigate any vulnerabilities.
- c) [QCP-n-qscd] and [QCP-l-qscd]: the TSP shall monitor QSCD certification status until the end of the validity period of the certificate and shall take appropriate measures in case of modification of this status. Such measures shall be documented in the TSP's CPS.

6.5.2 Private Key Protection and Cryptographic Module Engineering Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.2 shall apply.

6.5.3 Other Aspects of Key Pair Management

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.3 shall apply.

6.5.4 Activation Data

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.4 shall apply.

6.5.5 Computer Security Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.5 shall apply.

6.5.6 Life Cycle Security Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.6 shall apply.

6.5.7 Network Security Controls

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.7 shall apply.

6.5.8 Time-stamping

The requirements identified in ETSI EN 319 411-1 [2], clause 6.5.8 shall apply.

6.6 Certificate, CRL, and OCSP Profiles

6.6.1 Certificate Profile

The requirements identified in ETSI EN 319 411-1 [2], clause 6.6.1 shall apply.

In addition the following particular requirements apply.

Certificate generation

- a) The certificate shall include all appropriate qcStatements as defined in ETSI EN 319 412-5 [3].
- b) [QCP-n-qscd] and [QCP-l-qscd]: the certificate shall include the qcStatement for QSCD (esi4-qcStatement-4) defined in ETSI EN 319 412-5 [3].

- c) The qcStatement for QSCD (esi4-qcStatement-4) shall not be included in certificates that are not issued according to [QCP-n-qscd] or [QCP-l-qscd] requirements.
- d) [QCP-n] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 a); and/or
 - ii) an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- e) [QCP-l] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 b); and/or
 - ii) a OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- f) [QCP-n-qscd] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 c); and/or
 - ii) a OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- g) [QCP-l-qscd] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 d); and/or
 - ii) a OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- h) [QCP-w] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 e); and/or
 - ii) a OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- i) [QCP-w] [CONDITIONAL]: if the certificate is issued to a legal person the policy identifier as specified in EVCG [i.7] may be included in addition to the identifier(s) required in h).
- j) [QCP-w] [CONDITIONAL]: if the certificate is issued to a natural person the policy identifier for NCP as specified in ETSI EN 319 411-1 [2] may be included in addition to the identifier(s) required in h).
- k) [CONDITIONAL] if the certificate contains only an OID allocated by the TSP, the referred certificate policy shall be built according to clause 7. In particular it shall clearly identify which of the certificate policy defined in the present document it adopts as the basis.

NOTE: The rationales for writing a certificate policy are provided in clause 4.

6.6.2 CRL Profile

The requirements identified in ETSI EN 319 411-1 [2], clause 6.6.2 shall apply.

6.6.3 OCSP Profile

The requirements identified in ETSI EN 319 411-1 [2], clause 6.6.3 shall apply.

6.7 Compliance Audit and Other Assessment

The requirements identified in ETSI EN 319 411-1 [2], clause 6.7 shall apply.

6.8 Other Business and Legal Matters

6.8.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP services.

6.8.2 Financial Responsibility

The requirements identified in ETSI EN 319 411-1 [2], clause 6.8.2 shall apply.

6.8.3 Confidentiality of Business Information

No policy requirement.

6.8.4 Privacy of Personal Information

The requirements identified in ETSI EN 319 411-1 [2], clause 6.8.4 shall apply.

6.8.5 Intellectual Property Rights

No policy requirement.

6.8.6 Representations and Warranties

The general obligations specified in ETSI EN 319 411-1 [2], clause 6.8.6 shall apply. In addition:

- a) [QCP-n] and [QCP-l] [CONDITIONAL]:
 - i) If the TSP's terms and conditions do not require a secure cryptographic device, all obligations specified for NCP in ETSI EN 319 411-1 [2] shall apply.
 - ii) If the TSP's terms and conditions requires a secure cryptographic device, all obligations specified for NCP+ in ETSI EN 319 411-1 [2] shall apply.
- b) [QCP-n-qscd] and [QCP-l-qscd]: all obligations specified for NCP+ in ETSI EN 319 411-1 [2] shall apply.
- c) [QCP-w]: all obligations specified for EVCP in ETSI EN 319 411-1 [2] shall apply.

6.8.7 Disclaimers of Warranties

See clause 6.8.6.

See also clause A.2 in ETSI EN 319 411-1 [2] for additional information.

6.8.8 Limitations of Liability

The requirements identified in ETSI EN 319 411-1 [2], clause 6.8.8 shall apply.

6.8.9 Indemnities

No policy requirement.

6.8.10 Term and Termination

No policy requirement.

6.8.11 Individual notices and communications with participants

No policy requirement.

6.8.12 Amendments

No policy requirement.

6.8.13 Dispute Resolution Procedures

The requirements identified in ETSI EN 319 411-1 [2], clause 6.8.13 shall apply.

6.8.14 Governing Law

Not in the scope of the present document.

6.8.15 Compliance with Applicable Law

The requirements identified in ETSI EN 319 411-1 [2], clause 6.8.15 shall apply.

6.8.16 Miscellaneous Provisions

No policy requirement.

6.9 Other Provisions

6.9.1 Organizational

The requirements identified in ETSI EN 319 411-1 [2], clause 6.9.1 shall apply.

6.9.2 Additional testing

The requirements identified in ETSI EN 319 411-1 [2], clause 6.9.2 shall apply.

6.9.3 Disabilities

The requirements identified in ETSI EN 319 411-1 [2], clause 6.9.3 shall apply.

6.9.4 Terms and conditions

The requirements specified in ETSI EN 319 411-1 [2], clause 6.9.4 shall apply.

In addition the following particular requirements apply:

- a) the certificate policy shall include a clear statement indicating that the policy is for EU qualified certificates and whether the policy requires use of a QSCD;
- b) a PKI disclosure statement shall be supported;
- c) the PKI disclosure statement should be structured according to annex A in ETSI EN 319 411-1 [2].

NOTE: This PKI disclosure statement can assist a TSP to respond to regulatory requirements and concerns, particularly those related to consumer deployment and the requirements of EU Regulation N° 910/2014 [i.1], article 24 2.

7 Framework for the definition of other certificate policies built on the present document

7.1 Certificate policy management

The requirements identified in ETSI EN 319 411-1 [2], clause 7.1 shall apply.

In addition the following particular requirements apply:

- a) The certificate policy shall incorporate, or further constrain, all the requirements identified in clauses 5 and 6 of the present document, as appropriate to the usage, building on the requirements of the appropriate certificate policy as defined in the present document.

NOTE: Clause 4.4 provides the rationales for writing a certificate policy.

7.2 Additional requirements

The requirements identified in ETSI EN 319 411-1 [2], clause 7.2 shall apply.

Annex A (informative): Regulation and EU qualified certificate policy mapping

Table A.1 identifies how the security controls objectives and other parts of the EU qualified certificate policies (QCP) defined in the present document address the requirements of TSP issuing qualified certificates as defined in articles 19 and 24 and annexes of Regulation (EU) N° 910/2014 [i.1].

This annex should not be taken as definitive statement of conformance to the Regulation (EU) No 910/2014 [i.1]. There are requirements in the Regulation (EU) No 910/2014 [i.1] which are not technical and are then out of scope of the present document, and the present document has not been subject to any legal review.

Table A.1

Regulation 5.1 Data protection	EU qualified certificate policy reference
<i>"5 1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC."</i>	ETSI EN 319 401 [1], clause 7.13 c) and note
Regulation article 13.2 Liability and burden of proof	EU qualified certificate policy reference
<i>"13 2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations."</i>	ETSI EN 319 401 [1], clauses 6.2 f) and g)
Regulation article 15 Accessibility for persons with disabilities	EU qualified certificate policy reference
<i>Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities</i>	ETSI EN 319 401 [1] clause 7.13 b)
Regulation article 19 Security requirements applicable to trust service providers	EU qualified certificate policy reference
<i>"19 1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk."</i>	Clause 6.4 ETSI EN 319 411-1 [2], clause 6.4 ETSI EN 319 401 [1], clauses 5, 6.3 and 7.3 ETSI EN 319 401 [1], clause 7.6 ETSI EN 319 401 [1], clause 7.4 b), c), d) and e) ETSI EN 319 401 [1], clause 7.2 ETSI EN 319 401 [1], clause 7.10 ETSI EN 319 401 [1], clauses 7.9 and 7.11 ETSI EN 319 401 [1], clause 7.12 (termination) Clause 6.5 ETSI EN 319 411-1 [2], clause 6.5 ETSI EN 319 401 [1], clause 7.5 ETSI EN 319 401 [1], clause 7.4 a) & f) ETSI EN 319 401 [1] clause 7.7 ETSI EN 319 401 [1], clause 7.8
<i>In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."</i>	Clause 6.4.8, = ETSI EN 319 411-1 [2], clause 6.4.8 ETSI EN 319 401 [1], clauses 7.9 and 7.11
<i>"19. 2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay."</i>	Clause 6.4.8, = ETSI EN 319 411-1 [2], clause 6.4.8 ETSI EN 319 401 [1], clauses 7.9 and 7.11

Regulation article 24 Requirements for qualified trust service providers	EU qualified certificate policy reference
<p><i>"24.1 verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued. The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:</i></p> <p><i>(a) by the physical presence of the natural person or of an authorised representative of the legal person; or</i></p> <p><i>(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or</i></p> <p><i>(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or</i></p> <p><i>(d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body."</i></p>	<p>Clause 6.2.2 ETSI EN 319 411-1 [2], clause 6.2.2 Clause 6.2.3 = ETSI EN 319 411-1 [2], clause 6.2.3</p>
<p><i>"24. 2 (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards"</i></p>	<p>Clause 6.4.4 = ETSI EN 319 411-1 [2], clause 6.4.4</p>
<p><i>"24.2 (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;"</i></p>	<p>Clause 6.8.2 = ETSI EN 319 411-1 [2], clause 6.8.2 ETSI EN 319 401 [1], clause 7.1.1 c)</p>
<p><i>"24.2 (d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;"</i></p>	<p>ETSI EN 319 411-1 [2], clause 6.1 c), d), e), f) ETSI EN 319 411-1 [2], clause 6.3.4 a), b), c)</p> <p>Clause 6.9.4 = ETSI EN 319 411-1 [2], clause 6.9.4 ETSI EN 319 401 [1] clause 6.2</p>
<p><i>"24.2 (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;"</i></p>	<p>Clause 6.5 ETSI EN 319 411-1 [2], clause 6.5 ETSI EN 319 401 [1], clause 7.5 ETSI EN 319 401 [1], clause 7.4 a) & f), ETSI EN 319 401 [1] clause 7.7 ETSI EN 319 401 [1], clause 7.8</p>

Regulation article 24 Requirements for qualified trust service providers	EU qualified certificate policy reference
<p>"24. 2 (f) use trustworthy systems to store data provided to them, in a verifiable form so that:</p> <p>(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,</p> <p>(ii) only authorised persons can make entries and changes to the stored data,</p> <p>(iii) the data can be checked for authenticity;"</p>	<p>Clause 6.4.3 = ETSI EN 319 411-1 [2], clause 6.4.3</p> <p>Clause 6.4.6 = ETSI EN 319 411-1 [2], clause 6.4.6</p> <p>Clause 6.5 ETSI EN 319 411-1 [2], clause 6.5 ETSI EN 319 401 [1], clause 7.5 ETSI EN 319 401 [1], clause 7.4 a) & f), ETSI EN 319 401 [1] clause 7.7 ETSI EN 319 401 [1], clause 7.8</p>
<p>"24.2 (g) take appropriate measures against forgery and theft of data;"</p>	<p>Clause 6.4 ETSI EN 319 411-1 [2], clause 6.4 ETSI EN 319 401 [1] clauses 5, 6.3 and 7.3 ETSI EN 319 401 [1], clause 7.6 ETSI EN 319 401 [1], clause 7.4 b), c), d) and e) ETSI EN 319 401 [1], clause 7.2 ETSI EN 319 401 [1], clause 7.10 ETSI EN 319 401 [1], clauses 7.9 and 7.11 ETSI EN 319 401 [1], clause 7.12 (termination)</p> <p>Clause 6.5 ETSI EN 319 411-1 [2], clause 6.5 ETSI EN 319 401 [1], clause 7.5 ETSI EN 319 401 [1], clause 7.4 a) & f), ETSI EN 319 401 [1] clause 7.7 ETSI EN 319 401 [1], clause 7.8</p>
<p>"24.2 (h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;"</p>	<p>ETSI EN 319 411-1 [2], clause 6.2.2 g) ETSI EN 319 411-1 [2], clause 6.3.4 e) ETSI EN 319 411-1 [2], clause 6.3.8 a) ETSI EN 319 411-1 [2], clause 6.4.5 c)</p> <p>Clause 6.4.6 = ETSI EN 319 411-1 [2], clause 6.4.6 Clause 6.4.9 = ETSI EN 319 411-1 [2], clause 6.4.9 ETSI EN 319 401 [1], clause 7.12</p>
<p>"24.2 (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body"</p>	<p>Clause 6.4.9 = ETSI EN 319 411-1 [2], clause 6.4.9 ETSI EN 319 401 [1], clause 7.12</p>
<p>"24.2 (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC"</p>	<p>Clause 6.8.4 = ETSI EN 319 411-1 [2], clause 6.8.4 ETSI EN 319 401 [1], clause 7.13 c)</p>
<p>"24.2 (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database."</p>	<p>Clause 6.1 = ETSI EN 319 411-1 [2], clause 6.1</p>
<p>"24.3 If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication."</p>	<p>Clause 6.2.4 = ETSI EN 319 411-1 [2], clause 6.2.4</p>
<p>"24.4 With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient."</p>	<p>Clause 6.3.10 ETSI EN 319 411-1 [2], clause 6.3.10</p> <p>"free of charge" is out of scope</p>

Regulation Art 28 (38) Qualified certificates for electronic signatures (Qualified certificates for electronic seal)	EU qualified certificate policy reference
28, (38) 3. <i>Qualified certificates for electronic signatures (seals) may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures (seals).</i>	ETSI EN 319 411-1 [2] clause 6.6.1 i) and ii)
"28, (38) 4. <i>If a qualified certificate for electronic signatures (seal) has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.</i> "	ETSI EN 319 411-1 [2] clause 6.3.9 b)
28, (38) 5. <i>Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic signatures (seals):</i> (a) <i>if a qualified certificate for electronic signature (seal) has been temporarily suspended that certificate shall lose its validity for the period of suspension;</i> (b) <i>the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.</i>	The present document places no restrictions on use of suspension
Regulation Articles 28 1, 38 1 and 45 1; conformity to Annexes I, III and IV specifying requirement for qualified certificates	EU qualified certificate policy reference
Annex I and III (a) to (i), Annex IV (a) to (j),	Clause 6.6.1 a) ETSI EN 319 411-1 [2], clause 6.6.1
Annex I and III (j)	Clause 6.6.1 b)
Regulation requirement on other TSP than TSP issuing certificates but to be verified by TSP issuing EU qualified certificates	EU qualified certificate policy reference
Article 30 certification of qualified electronic signature creation devices	Clause 6.5.1 a)
"Annex II 3: <i>Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.</i> "	Clause 6.5.2 a) iii)
"Annex II 4 <i>qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:</i> (a) <i>the security of the duplicated datasets must be at the same level as for the original datasets;</i> (b) <i>the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.</i> "	Clause 6.3.5 b) ii) Clause 6.3.12 = ETSI EN 319 411-1 [2], clause 6.3.12 ETSI EN 319 411-1 [2], clause 7.1 i)

Annex B (informative): Conformity Assessment Check list

A check list for the policy requirements specified in the present document as well as the generic requirements which are independent of the TSP (as expressed in ETSI EN 319 401 [1]) and independent of the type of certificate issued (as expressed in ETSI EN 319 411-1 [2]) is contained in the spreadsheet file (en_31941102v020100v0.zip) which accompanies the present document.

The checklist summarizes the conformity criteria in such a way that it can be used by the TSP itself to prepare for an assessment of its practices against the present document (i.e. serve as a basis for a self-declaration) and/or by the assessor when conducting the assessment, for the sake of facility for both the assessor and the TSP to be assessed.

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the check list file identified in this annex so that it can be used for its intended purposes and may further publish the completed check list.

Annex C (informative): Revisions made since ETSI EN 319 411-2 version 1.1.1 (2013-01)

It is a major revision. It is completely revised to consider the Regulation and builds on part 1 [2].

History

Document history		
V1.1.1	January 2013	Publication
V2.0.6	June 2015	EN Approval Procedure AP 20151016: 2015-06-18 to 2015-10-16
V2.0.7	July 2015	Publication as ETSI TS 119 411-2
V2.1.0	December 2015	Vote V 20160221: 2015-12-23 to 2016-02-22