



**Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Trust Service Providers issuing certificates;
Part 2: Requirements for trust service providers issuing
EU qualified certificates**

Reference

RTS/ESI-0019411-2-TS

Keywords

e-commerce, electronic signature, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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

6.3.10	Certificate Status Services	13
6.3.11	End of Subscription	13
6.3.12	Key Escrow and Recovery	14
6.4	Facility, Management, and Operational Controls	14
6.4.1	General	14
6.4.2	Physical Security Controls	14
6.4.3	Procedural Controls	14
6.4.4	Personnel Controls	14
6.4.5	Audit Logging Procedures	14
6.4.6	Records Archival	14
6.4.7	Key Changeover	14
6.4.8	Compromise and Disaster Recovery	15
6.4.9	CA or RA Termination	15
6.5	Technical Security Controls	15
6.5.1	Key Pair Generation and Installation	15
6.5.2	Private Key Protection and Cryptographic Module Engineering Controls	15
6.5.3	Other Aspects of Key Pair Management	16
6.5.4	Activation Data	16
6.5.5	Computer Security Controls	16
6.5.6	Life Cycle Security Controls	16
6.5.7	Network Security Controls	16
6.5.8	Time-stamping	16
6.6	Certificate, CRL, and OCSP Profiles	16
6.6.1	Certificate Profile	16
6.6.2	CRL Profile	17
6.6.3	OCSP Profile	17
6.7	Compliance Audit and Other Assessment	17
6.8	Other Business and Legal Matters	17
6.8.1	Fees	17
6.8.2	Financial Responsibility	17
6.8.3	Confidentiality of Business Information	17
6.8.4	Privacy of Personal Information	17
6.8.5	Intellectual Property Rights	17
6.8.6	Representations and Warranties	17
6.8.7	Disclaimers of Warranties	18
6.8.8	Limitations of Liability	18
6.8.9	Indemnities	18
6.8.10	Term and Termination	18
6.8.11	Individual notices and communications with participants	18
6.8.12	Amendments	18
6.8.13	Dispute Resolution Procedures	18
6.8.14	Governing Law	18
6.8.15	Compliance with Applicable Law	18
6.8.16	Miscellaneous Provisions	18
6.9	Other Provisions	18
6.9.1	Organizational	18
6.9.2	Additional testing	18
6.9.3	Disabilities	19
6.9.4	Terms and conditions	19
7	Framework for the definition of other certificate policies built on the present document	19
7.1	Certificate policy management	19
7.2	Additional requirements	19
Annex A (informative):	Regulation and EU qualified certificate policy mapping	20
Annex B (informative):	Conformity Assessment Check list	24
Annex C (informative):	Revisions made since version 1.1.1 (2013-01)	25
History		26

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

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

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

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

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

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

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

1 Scope

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

The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors. The present document however provides in annex B a check list of the policy requirements specific to TSP issuing EU qualified certificates (as expressed in the present document) as well as all the requirements incorporated by reference to ETSI TS 119 411-1 [2] and ETSI TS 119 401 [1], that can be used by the TSP to prepare an assessment of its practices against the present document and/or by the assessor when conducting the assessment for confirming that a TSP meets the requirements for issuing qualified certificates under Regulation (EU) N° 910/2014 [i.1].

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

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

- [1] ETSI TS 119 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [2] ETSI TS 119 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".
- [3] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5, CA/Browser Forum.
- [4] ETSI TS 119 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.