

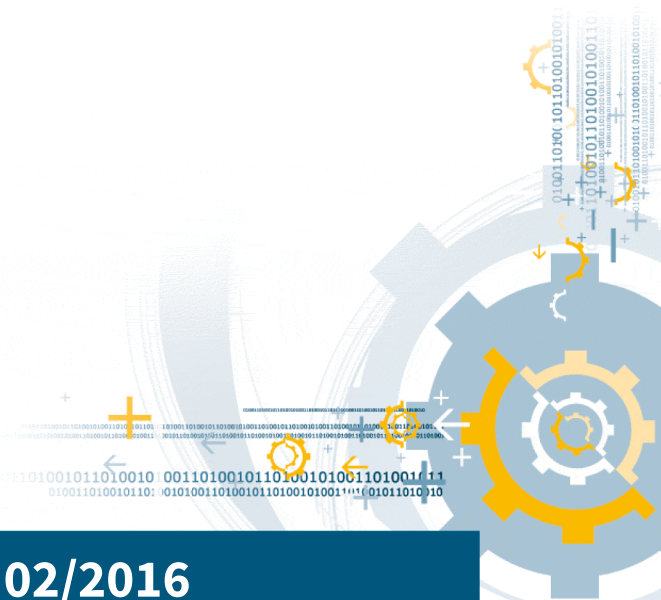


Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 319 411-2 V2.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2:

02/2016



National Foreword

This European Standard EN 319 411-2 V2.1.1 (2016-02) was adopted as Luxembourgish Standard ILNAS-EN 319 411-2 V2.1.1 (2016-02).

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

THIS PUBLICATION IS COPYRIGHT PROTECTED

Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!



**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-0019411-2

Keywordse-commerce, electronic signature, security, trust
services**ETSI**650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

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

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

<https://portal.etsi.org/People/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 2016.

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 notation.....	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