

ILNAS

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

**ILNAS-EN 319 411-1 V1.1.1
(2016-02)**

**Electronic Signatures and
Infrastructures (ESI); Policy and
security requirements for Trust Service
Providers issuing certificates; Part 1:**

02/2016



National Foreword

This European Standard EN 319 411-1 V1.1.1 (2016-02) was adopted as Luxembourgish Standard ILNAS-EN 319 411-1 V1.1.1 (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!

ETSI EN 319 411-1 V1.1.1 (2016-02)



ILNAS-EN 319 411-1 V1.1.1 (2016-02) - Preview only Copy via ILNAS e-Shop

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements



Reference

DEN/ESI-0019411-1

Keywords

e-commerce, electronic signature, extended validation certificate, public key, security, trust services

ETSI

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

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

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

Important notice

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

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.....	8
3 Definitions, abbreviations and notation.....	9
3.1 Definitions	9
3.2 Abbreviations	11
3.3 Notation.....	12
4 General concepts	12
4.1 General policy requirements concepts.....	12
4.2 Certificate policy and certification practice statement	12
4.2.1 Overview	12
4.2.2 Purpose	13
4.2.3 Level of specificity	13
4.2.4 Approach	13
4.2.5 Certificate Policy	13
4.3 Other Trust Service Providers statements	14
4.4 Certification services.....	14
5 General provisions on Certification Practice Statement and Certificate Policies.....	15
5.1 General requirements	15
5.2 Certification Practice Statement requirements	16
5.3 Certificate Policy name and identification	16
5.4 PKI participants.....	17
5.4.1 Certification Authority.....	17
5.4.2 Subscriber and subject	17
5.4.3 Others.....	18
5.5 Certificate usage	18
6 Trust Service Providers practice.....	18
6.1 Publication and repository responsibilities.....	18
6.2 Identification and authentication	19
6.2.1 Naming	19
6.2.2 Initial identity validation.....	19
6.2.3 Identification and authentication for Re-key requests	21
6.2.4 Identification and authentication for revocation requests	22
6.3 Certificate Life-Cycle operational requirements	23
6.3.1 Certificate application.....	23
6.3.2 Certificate application processing.....	23
6.3.3 Certificate issuance	23
6.3.4 Certificate acceptance	25
6.3.5 Key pair and certificate usage.....	26
6.3.6 Certificate renewal.....	27
6.3.7 Certificate Re-key.....	27
6.3.8 Certificate modification	27
6.3.9 Certificate revocation and suspension.....	28
6.3.10 Certificate status services.....	28
6.3.11 End of subscription	29
6.3.12 Key escrow and recovery.....	29
6.4 Facility, management, and operational controls	29
6.4.1 General.....	29

6.4.2	Physical security controls	29
6.4.3	Procedural controls	30
6.4.4	Personnel controls.....	30
6.4.5	Audit logging procedures.....	30
6.4.6	Records archival	31
6.4.7	Key changeover	31
6.4.8	Compromise and disaster recovery	31
6.4.9	Certification Authority or Registration Authority termination	32
6.5	Technical security controls.....	33
6.5.1	Key pair generation and installation	33
6.5.2	Private key protection and cryptographic module engineering controls	34
6.5.3	Other aspects of key pair management	35
6.5.4	Activation data.....	35
6.5.5	Computer security controls	36
6.5.6	Life cycle security controls.....	36
6.5.7	Network security controls.....	37
6.5.8	Timestamping	37
6.6	Certificate, CRL, and OCSP profiles.....	37
6.6.1	Certificate profile	37
6.6.2	CRL profile	37
6.6.3	OCSP profile.....	37
6.7	Compliance audit and other assessment	37
6.8	Other business and legal matters	37
6.8.1	Fees	37
6.8.2	Financial responsibility	37
6.8.3	Confidentiality of business information.....	38
6.8.4	Privacy of personal information.....	38
6.8.5	Intellectual property rights	38
6.8.6	Representations and warranties.....	38
6.8.7	Disclaimers of warranties	38
6.8.8	Limitations of liability	38
6.8.9	Indemnities	38
6.8.10	Term and termination.....	38
6.8.11	Individual notices and communications with participants	39
6.8.12	Amendments	39
6.8.13	Dispute resolution procedures.....	39
6.8.14	Governing law	39
6.8.15	Compliance with applicable law	39
6.8.16	Miscellaneous provisions.....	39
6.9	Other provisions	39
6.9.1	Organizational.....	39
6.9.2	Additional testing.....	39
6.9.3	Disabilities	39
6.9.4	Terms and conditions.....	40
7	Framework for the definition of other certificate policies.....	40
7.1	Certificate policy management.....	40
7.2	Additional requirements	40
Annex A (informative): Model PKI disclosure statement.....		41
A.1	Introduction	41
A.2	The PDS structure	41
A.3	The PDS format.....	42
Annex B (informative): Revisions made since previous versions.....		43
Annex C (informative): Conformity assessment checklist.....		44
Annex D (informative): Bibliography		45
History		46