



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

Reference

RTS/ESI-0019411-1-TS

Keywords

e-commerce, electronic signature, extended
validation certificat, 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

<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.....	7
3 Definitions, abbreviations and notation.....	8
3.1 Definitions.....	8
3.2 Abbreviations	10
3.3 Notation.....	11
4 General concepts	11
4.1 General policy requirements concepts.....	11
4.2 Certificate policy and certification practice statement	11
4.2.1 Overview	11
4.2.2 Purpose	11
4.2.3 Level of specificity	12
4.2.4 Approach	12
4.2.5 Certificate Policy	12
4.3 Other Trust Service Providers statements	13
4.4 Certification services.....	13
5 General provisions on Certification Practice Statement and Certificate Policies.....	14
5.1 General requirements	14
5.2 Certification Practice Statement requirements	15
5.3 Certificate Policy name and identification	15
5.4 PKI participants.....	16
5.4.1 Certification Authority.....	16
5.4.2 Subscriber and subject	16
5.4.3 Others.....	17
5.5 Certificate usage	17
6 Trust Service Providers practice.....	17
6.1 Publication and repository responsibilities.....	17
6.2 Identification and authentication	18
6.2.1 Naming	18
6.2.2 Initial identity validation.....	18
6.2.3 Identification and authentication for Re-key requests	20
6.2.4 Identification and authentication for revocation requests	20
6.3 Certificate Life-Cycle operational requirements	21
6.3.1 Certificate application.....	21
6.3.2 Certificate application processing.....	22
6.3.3 Certificate issuance	22
6.3.4 Certificate acceptance	23
6.3.5 Key pair and certificate usage.....	24
6.3.6 Certificate renewal	25
6.3.7 Certificate Re-key.....	26
6.3.8 Certificate modification	26
6.3.9 Certificate revocation and suspension.....	26
6.3.10 Certificate status services.....	27
6.3.11 End of subscription	27
6.3.12 Key escrow and recovery.....	27
6.4 Facility, management, and operational controls	27
6.4.1 General.....	27

6.4.2	Physical security controls	28
6.4.3	Procedural controls	28
6.4.4	Personnel controls.....	28
6.4.5	Audit logging procedures.....	29
6.4.6	Records archival	29
6.4.7	Key changeover	29
6.4.8	Compromise and disaster recovery	30
6.4.9	Certification Authority or Registration Authority termination	30
6.5	Technical security controls	31
6.5.1	Key pair generation and installation	31
6.5.2	Private key protection and cryptographic module engineering controls	32
6.5.3	Other aspects of key pair management	33
6.5.4	Activation data	34
6.5.5	Computer security controls	34
6.5.6	Life cycle security controls	34
6.5.7	Network security controls	35
6.5.8	Timestamping	35
6.6	Certificate, CRL, and OCSP profiles.....	35
6.6.1	Certificate profile	35
6.6.2	CRL profile	35
6.6.3	OCSP profile.....	35
6.7	Compliance audit and other assessment	35
6.8	Other business and legal matters	35
6.8.1	Fees	35
6.8.2	Financial responsibility	36
6.8.3	Confidentiality of business information.....	36
6.8.4	Privacy of personal information.....	36
6.8.5	Intellectual property rights	36
6.8.6	Representations and warranties.....	36
6.8.7	Disclaimers of warranties	36
6.8.8	Limitations of liability	36
6.8.9	Indemnities	36
6.8.10	Term and termination.....	37
6.8.11	Individual notices and communications with participants	37
6.8.12	Amendments	37
6.8.13	Dispute resolution procedures.....	37
6.8.14	Governing law	37
6.8.15	Compliance with applicable law	37
6.8.16	Miscellaneous provisions.....	37
6.9	Other provisions	37
6.9.1	Organizational.....	37
6.9.2	Additional testing.....	37
6.9.3	Disabilities	38
6.9.4	Terms and conditions.....	38
7	Framework for the definition of other certificate policies.....	38
7.1	Certificate policy management.....	38
7.2	Additional requirements	38
Annex A (informative):	Model PKI disclosure statement.....	39
A.1	Introduction	39
A.2	The PDS structure	40
A.3	The PDS format.....	40
Annex B (informative):	Revisions made compared to TS 102 042.....	41
Annex C (informative):	Conformity assessment check list.....	42
Annex D (informative):	Bibliography.....	43
History		44