

ETSI TS 102 853 V1.2.1 (2014-12)



Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies

Reference

RTS/ESI-0002853v121

Keywords

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>

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:

http://portal.etsi.org/chaicor/ETSI_support.asp

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 2014.

All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. 3GPPTM and LTETM 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	6
Foreword.....	6
Modal verbs terminology.....	6
Introduction	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	8
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	10
4 Introduction to signature validation	11
4.1 Status indication of the signature validation process.....	11
4.2 Validation Constraints	15
4.3 X.509 certificate meta-data	16
4.4 Trust Management.....	16
4.5 The concept of revocation freshness	16
5 Basic Building Blocks.....	17
5.1 Identification of the Signer's Certificate (ISC).....	18
5.1.1 Description.....	18
5.1.2 Inputs	18
5.1.3 Outputs.....	18
5.1.4 Processing.....	19
5.1.4.1 XAdES processing	19
5.1.4.2 CAdES processing	19
5.1.4.3 PAdES processing.....	20
5.2 Validation Context Initialization (VCI).....	20
5.2.1 Description.....	20
5.2.2 Inputs	20
5.2.3 Outputs.....	20
5.2.4 Processing.....	20
5.2.4.1 Processing commitment type indication.....	21
5.2.4.1.1 XAdES Processing	21
5.2.4.2 Processing Signature Policy Identifier	21
5.3 X.509 Certificate Validation (XCV)	22
5.3.1 Description.....	22
5.3.2 Inputs	22
5.3.3 Outputs.....	22
5.3.4 Processing.....	22
5.4 Cryptographic Verification (CV)	23
5.4.1 Description.....	23
5.4.2 Inputs	23
5.4.3 Outputs.....	24
5.4.4 Processing.....	24
5.5 Signature Acceptance Validation (SAV).....	24
5.5.1 Description.....	24
5.5.2 Inputs	24
5.5.3 Outputs.....	25
5.5.4 Processing.....	25
5.5.4.1 Processing AdES properties/attributes	26
5.5.4.2 Processing signing certificate reference constraint	26
5.5.4.3 Processing claimed signing time	26

5.5.4.4	Processing signed data object format	26
5.5.4.5	Processing indication of production place of the signature	26
5.5.4.6	Processing Time-stamps on signed data objects	27
5.5.4.7	Processing Countersignatures	27
5.5.4.8	Processing signer attributes/roles	27
6	Basic Validation Process	27
6.1	Description	27
6.2	Inputs	28
6.3	Outputs	28
6.4	Processing	28
7	Validation Process for Time-Stamps	29
7.1	Description	29
7.2	Inputs	30
7.3	Outputs	30
7.4	Processing	30
8	Validation Process for AdES-T	30
8.1	Description	30
8.2	Inputs	30
8.3	Outputs	31
8.4	Processing	31
8.4.1	Message Imprint Verification of the signature-timestamp for XAdES	32
8.4.2	Message Imprint Verification of the signature-time-stamp for CAdES/PAdES	32
9	Validation of LTV forms	32
9.1	The concept of Proof Of Existence (POE)	33
9.2	Additional Building blocks	33
9.2.1	Past certificate validation	33
9.2.1.1	Description	33
9.2.1.2	Input	34
9.2.1.3	Output	34
9.2.1.4	Processing	34
9.2.2	Control-time sliding process	34
9.2.2.1	Description	34
9.2.2.2	Input	35
9.2.2.3	Output	35
9.2.2.4	Processing	35
9.2.3	POE extraction	36
9.2.3.1	Description	36
9.2.3.2	Input	36
9.2.3.3	Output	36
9.2.3.4	Processing	37
9.2.3.4.1	Extraction from a time-stamp on the signature	37
9.2.3.4.2	Extraction from a time-stamp on certificates and revocation references	37
9.2.3.4.3	Extraction from a time-stamp on the signature and certificates and revocation references	37
9.2.3.4.4	Extraction from an archive-time-stamp	37
9.2.3.4.5	Extraction from a long-term-validation attribute	37
9.2.3.4.6	Extraction from a PDF document time-stamp	38
9.2.4	Past signature validation process	38
9.2.4.1	Description	38
9.2.4.2	Input	38
9.2.4.3	Output	38
9.2.4.4	Processing	39
9.3	Long Term Validation Process	39
9.3.1	Description	39
9.3.2	Input	40
9.3.3	Output	40
9.3.4	Processing	40
Annex A (informative):	Validation Constraints	43
A.1	X.509 Certificate path validation constraints	43