



**Electronic Signatures and Infrastructures (ESI);
CADES digital signatures;
Part 1: Building blocks and CADES baseline signatures**

Reference

RTS/ESI-0019122-1-TS

KeywordsASN.1, CAdES, electronic signature, profile,
security**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.

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	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 and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations	9
4 General syntax.....	9
4.1 General requirements	9
4.2 The data content type.....	9
4.3 The signed-data content type.....	9
4.4 The SignedData type	9
4.5 The EncapsulatedContentInfo type	10
4.6 The SignerInfo type	10
4.7 ASN.1 Encoding.....	10
4.7.1 DER	10
4.7.2 BER	10
4.8 Other standard data structures	10
4.8.1 Time-stamp token format.....	10
4.8.2 Additional types.....	10
4.9 Attributes.....	11
5 Attribute semantics and syntax.....	11
5.1 CMS defined basic signed attributes	11
5.1.1 The content-type attribute	11
5.1.2 The message-digest attribute	11
5.2 Basic attributes for CADES signatures	12
5.2.1 The signing-time attribute	12
5.2.2 Signing certificate reference attributes	12
5.2.2.1 General requirements	12
5.2.2.2 ESS signing-certificate attribute	12
5.2.2.3 ESS signing-certificate-v2 attribute	13
5.2.3 The commitment-type-indication attribute.....	13
5.2.4 Attributes for identifying the signed data type.....	14
5.2.4.1 The content-hints attribute	14
5.2.4.2 The mime-type attribute.....	14
5.2.5 The signer-location attribute	15
5.2.6 Incorporating attributes of the signer	15
5.2.6.1 The signer-attributes-v2 attribute	15
5.2.6.2 claimed-SAML-assertion	17
5.2.7 The countersignature attribute.....	17
5.2.8 The content-time-stamp attribute.....	18
5.2.9 The signature-policy-identifier attribute and the SigPolicyQualifierInfo type.....	18
5.2.9.1 The signature-policy-identifier attribute.....	18
5.2.9.2 The SigPolicyQualifierInfo type	19
5.2.10 The signature-policy-store attribute	21
5.2.11 The content-reference attribute	21
5.2.12 The content-identifier attribute.....	22
5.3 The signature-time-stamp attribute.....	22

5.4	Attributes for validation data values	23
5.4.1	Introduction	23
5.4.2	OCSP responses	23
5.4.2.1	OCSP response types	23
5.4.2.2	OCSP responses within RevocationInfoChoices	23
5.4.3	CRLs	23
5.5	Archive validation data	23
5.5.1	Introduction	23
5.5.2	The <code>ats-hash-index-v2</code> attribute	23
5.5.3	The <code>archive-time-stamp-v3</code> attribute	25
6	CAdES baseline signatures	27
6.1	Signature levels	27
6.2	General requirements	28
6.2.1	Algorithm requirements	28
6.2.2	Notation for requirements	28
6.3	Requirements on components and services	30
6.4	Legacy CAdES baseline signatures	33
Annex A (normative):	Additional Attributes Specification	34
A.1	Attributes for validation data	34
A.1.1	Certificates validation data	34
A.1.1.1	The <code>complete-certificate-references</code> attribute	34
A.1.1.2	The <code>certificate-values</code> attribute	35
A.1.2	Revocation validation data	35
A.1.2.1	The <code>complete-revocation-references</code> attribute	35
A.1.2.2	The <code>revocation-values</code> attribute	37
A.1.3	The <code>attribute-certificate-references</code> attribute	38
A.1.4	The <code>attribute-revocation-references</code> attribute	39
A.1.5	Time-stamps on references to validation data	40
A.1.5.1	The <code>time-stamped-certs-crls-references</code> attribute	40
A.1.5.2	The <code>CAdES-C-timestamp</code> attribute	40
A.2	Deprecated attributes	41
A.2.1	Usage of deprecated attributes	41
A.2.2	The <code>other-signing-certificate</code> attribute	41
A.2.3	The <code>signer-attributes</code> attribute	41
A.2.4	The <code>archive-time-stamp</code> attribute	41
A.2.5	The <code>long-term-validation</code> attribute	41
A.2.6	The <code>ats-hash-index</code> attribute	42
Annex B (informative):	Signature Format Definitions Using X.208 ASN.1 Syntax	43
Annex C (normative):	Signature Format Definitions Using X.680 ASN.1 Syntax	49
Annex D (informative):	Example Structured Contents and MIME	56
D.1	Use of MIME to Encode Data	56
D.1.1	MIME Structure	56
D.1.2	Header Information	56
D.1.3	Content Encoding	57
D.1.4	Multi-Part Content	57
D.2	S/MIME	58
D.2.1	Using S/MIME	58
D.2.2	Using <code>application/pkcs7-mime</code>	58
D.2.3	Using <code>multipart/signed</code> and <code>application/pkcs7-signature</code>	59
D.3	Use of MIME in the signature	59
Annex E (informative):	Change history	61
History		62