

ETSI TS 119 142-2 V1.0.1 (2015-07)



ETSI TS 119 142-2 V1.0.1 (2015-07) - Preview only Copy via ILNAS e-Shop

Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles

ReferenceRTS/ESI-0019142-2-TS

Keywordselectronic signature, PAdES, 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/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 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 and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	9
4 Profile for CMS digital signatures in PDF	9
4.1 Features	9
4.2 Requirements of Profile for CMS Signatures in PDF	9
4.2.1 Requirements on PDF signatures.....	9
4.2.2 Requirements on PDF signature handlers.....	10
4.2.3 Requirements on signature validation.....	10
4.2.4 Requirements on Time Stamping.....	10
4.2.4.1 Requirements on electronic time-stamp creation	10
4.2.4.2 Requirements on electronic time-stamp validation	11
4.2.5 Requirements on revocation checking	11
4.2.6 Requirements on Seed Values	11
4.2.7 Requirements on encryption	11
5 Extended PAdES signature profiles	11
5.1 Features	11
5.2 General Requirements	11
5.2.1 Requirements from Part 1	11
5.2.2 Notation of Requirements.....	11
5.3 PAdES-E-BES Level.....	12
5.4 PAdES-E-EPES Level.....	14
5.5 PAdES-E-LTV Level	14
6 Profiles for XAdES Signatures signing XML content in PDF	14
6.1 Features	14
6.2 Profiles for XAdES signatures of signed XML documents embedded in PDF containers.....	14
6.2.1 Overview	14
6.2.2 Profile for Basic XAdES signatures of XML documents embedded in PDF containers	16
6.2.2.1 Features	16
6.2.2.2 General syntax and requirements	17
6.2.2.3 Requirements for applications generating signed XML document to be embedded.....	17
6.2.2.4 Mandatory operations.....	18
6.2.2.4.1 Protecting the signing certificate	18
6.2.2.5 Requirements on XAdES optional properties	18
6.2.2.6 Serial Signatures	18
6.2.2.7 Parallel Signatures.....	18
6.2.2.8 PAdES Signatures	19
6.2.3 Profile for long-term XAdES signatures of signed XML documents embedded in PDF containers	19
6.2.3.1 Features	19
6.2.3.2 Augmentation mechanism.....	19
6.2.3.3 Optional properties.....	19
6.2.3.4 Validation Process.....	19
6.3 Profiles for XAdES signatures on XFA Forms	19
6.3.1 Overview	19
6.3.2 Profile for Basic XAdES signatures on XFA forms	22

6.3.2.1	Features	22
6.3.2.2	General syntax and requirements	22
6.3.2.3	Mandatory operations.....	23
6.3.2.3.1	Protecting the signing certificate	23
6.3.2.4	Requirements on XAdES optional properties	23
6.3.2.5	Serial Signatures	24
6.3.2.6	Parallel Signatures.....	25
6.3.3	Profile for long-term validation XAdES signatures on XFA forms.....	25
6.3.3.1	Overview	25
6.3.3.2	Features	25
6.3.3.3	General Requirements.....	25
6.3.4	Extensions Dictionary.....	25

Annex A (informative): General Features.....26

A.1	PDF signatures	26
A.2	PDF Signature types.....	27
A.3	PDF Signature Handlers.....	27
A.4	PDF serial signatures.....	27
A.5	PDF signature Validation and Time-stamping	28
A.6	ISO 19005-1: 2005 (PDF/A-1).....	28
A.7	ISO 19005-2: 2008 (PDF/A-2).....	29
A.8	Seed Values and Signature Policies	29
	History	30