

ETSI TS 103 171 V2.1.1 (2012-03)



Technical Specification

**Electronic Signatures and Infrastructures (ESI);
XAdES Baseline Profile**

Reference

RTS/ESI-000103

Keywords

electronic signature, profile, security, XAdES

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

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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 except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2012.
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	4
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	6
3 Definitions and abbreviations.....	6
3.1 Definitions	6
3.2 Abbreviations	7
4 Conformance Levels.....	7
5 General requirements	8
5.1 Algorithm requirements	8
5.2 Compliance requirements.....	8
6 Requirements for B-Level Conformance	9
6.1 Incorporation of XAdES qualifying properties to the signature.....	10
6.2 Profile of elements defined in XML Signature.....	10
6.2.1 Placement of the signing certificate	10
6.2.2 Canonicalization of ds : SignedInfo element	11
6.2.3 Profile of ds : Reference element.....	11
6.2.4 Transforms within ds : Reference element.....	12
6.3 Profile of XAdES elements	12
6.3.1 Profile of xades : SigningCertificate element	12
6.3.2 Profile of xades : SigningTime element.....	13
6.3.3 Profile of xades : DataObjectFormat element.....	13
7 Requirements for T-Level Conformance.....	13
8 Requirements for LT-Level Conformance	14
8.1 Profile of XAdES elements	14
8.1.1 Profile of xades : CertificateValues property.....	14
8.1.2 Profile of xades : RevocationValues property	15
8.1.3 Profile of xades : AttrAuthoritiesCertValues property	15
8.1.4 Profile of xades : AttributeRevocationValues property	15
8.1.5 Validation material for time-stamp tokens.....	15
9 Requirements for LTA-Level Conformance	16
9.1 Transition strategy for ArchiveTimeStamp frameworks	16
History	18