ETSI TS 119 132-3 V1.1.1 (2021-01)

Electronic Signatures and Infrastructures (ESI);
XAdES digital signatures;
Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES

Reference
DTS/ESI-000121

Keywords
electronic signature, profile, security, XAdES, XML

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

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
Introduction 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definition of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Abbreviations 7
4 General requirements 7
4.1 XML Namespaces 7
4.2 Electronic time-stamps in evidence-records 7
4.3 Placement of validation data of time-stamp tokens 8
5 The `xadesen:SealingEvidenceRecords` qualifying property 8
5.1 Semantics 8
5.1.1 Data time-stamped by time-stamp tokens 8
5.1.2 Incorporation of validation data during the life cycle of evidence records 9
5.2 Syntax 10
5.2.1 Introduction 10
5.2.2 Requirements for incorporating the first time-stamp token in the initial ArchiveTimestamp within an evidence-record 10
5.2.2.1 General requirements 10
5.2.2.2 Contribution of unsigned qualifying properties directly incorporated 12
5.2.2.3 Contribution of unsigned qualifying properties indirectly incorporated 12
6 XAdES signature level including ERS 12
6.1 Overview 12
6.2 General requirements 12
6.3 XAdES-E-ERS 12
7 Legacy XAdES baseline signatures 15
Annex A (normative): XML Schema file 16
A.1 XML Schema file location for namespace http://uri.etsi.org/19132/v1.1.1# 16
History 17

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 3 of a multi-part deliverable covering XAdES digital signatures. Full details of the entire series can be found in ETSI EN 319 132-1 [1].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Evidence Record Syntax (ERS) allows to cover different data objects with a single time-stamp, and subsequently augment the lifetime of the Evidence Record (ER) by adding validation data to the previous time-stamp and adding new time-stamps. The aim of the present document is to provide clear indications on how to bind an evidence record to a XAdES signature which is covered by the evidence record.

NOTE: ETSI EN 319 162-1 [i.3] and ETSI EN 319 162-2 [i.4] specify the use of evidence records in ASiC. ETSI TS 119 122-3 [i.5] specifies the use of evidence records in CAdES.

1 Scope

The present document specifies the semantics and the syntax for a new unsigned XAdES qualifying property able to contain evidence records.

The present document specifies the rules that govern the incorporation of evidence records within a XAdES signature or a legacy XAdES signature.

NOTE: The present specification allows to incorporate Evidence Records in two different formats, namely: the XML format for ERS specified in IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)" [5], and the ASN.1 format for ERS specified in IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)" [8].

The present document also specifies a new level for XAdES signatures, incorporating one or more than one of the aforementioned qualifying properties. The signatures specified in the present document are not baseline XAdES signatures.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[2] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[3] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[4] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[5] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[6] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

[7] W3C Recommendation (11 April 2013): "XML Signature Syntax and Processing Version 1.1".

[8] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.2] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.3] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.4] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.5] ETSI TS 119 122-3: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.1], ETSI EN 319 132-1 [1] and the following apply:

ArchiveTimeStamp: either a XMLERS ArchiveTimeStamp or an ERS ArchiveTimeStamp

ArchiveTimeStampChain: either `ers:ArchiveTimeStampChain`, as specified in IETF RFC 6283 [5] or an instance of `ArchiveTimeStampChain` type, as specified in IETF RFC 4998 [8]

ArchiveTimeStampSequence: either `ers:ArchiveTimeStampSequence`, as specified in IETF RFC 6283 [5] or an instance of `ArchiveTimeStampChain` type, as specified in IETF RFC 4998 [8]

ERS ArchiveTimeStamp: instance of `ArchiveTimeStampType` type, as specified in IETF RFC 4998 [8]

ERS evidence-record: Evidence record as specified in IETF RFC 4998 [8].

ERS initial ArchiveTimeStamp: first instance of `ArchiveTimeStamp` type of the first instance of `ArchiveTimeStampChain` type within the instance of `ArchiveTimeStampSequence` type, as specified in IETF RFC 4998 [8]

evidence-record: either an ERS evidence-record or a XMLERS evidence-record

evidence-record property: unsigned qualifying property which contains one or more evidence-records as defined in the present document

evidence record renewal: either time-stamp renewal or hash-tree renewal within an evidence record

HashTree: either an instance of `ers:HashTree` type as specified in IETF RFC 6283 [5], or an instance of `ParcialHashtree` type as specified in IETF RFC 4998 [8]

initial ArchiveTimeStamp: either a XMLERS initial ArchiveTimeStamp or an ERS initial ArchiveTimeStamp

time-stamp token: instance of type TimeStampToken as specified in IETF RFC 3161 [4] and updated by IETF RFC 5816 [6]

validation data: data that is used to validate a digital signature

XMLERS ArchiveTimeStamp: instance of `ers:ArchiveTimeStampType`, as specified in IETF RFC 6283 [5]

XMLERS evidence-record: Evidence record as specified in IETF RFC 6283 [5].

XMLERS initial ArchiveTimeStamp: first `ers:ArchiveTimeStamp` element of the first `ers:ArchiveTimeStampChain` element within the `ers:ArchiveTimeStampSequence` element within an instance of `ers:EvidenceRecordType` type, as specified in IETF RFC 6283 [5]

NOTE: Within the XAdES signatures specified in the present document time-stamp tokens may appear either within some of the qualifying properties specified in ETSI EN 319 132-1 [1], or within some XMLERS ArchiveTimeStamp, or within some ERS ArchiveTimeStamp.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.1] and the following apply:

ER	Evidence Record
ERS	Evidence Record Syntax
TSA	Time Stamp Authority
XML	eXtensible Markup Language
XMLERS	XML Evidence Record Syntax

4 General requirements

4.1 XML Namespaces

The present document uses the URI namespaces listed below:

- http://www.w3.org/2001/XMLSchema
- urn:ietf:params:xml:ns:ers

In addition to that, it defines a new namespace for including the new unsigned qualifying property specified in the present document, namely:

- http://uri.etsi.org/19132/v1.1.1#

Table 1 shows the mapping between namespaces' URIs and the prefixes used throughout the present document.

Table 1: Namespaces with constant prefixes

XML Namespace URI	Prefix
http://www.w3.org/2001/XMLSchema	`xsd`
http://uri.etsi.org/19132/v1.1.1#	`xadesen`
urn:ietf:params:xml:ns:ers	`ers`

ETSI has generated a XML Schema file for the present specification, namely "XAdES1913203v111-202101.xsd", using the XML Schema syntax and structures specified in annex A for details on its location.

Below follows a copy of the `xsd:schema` element of the aforementioned XML Schema file "XAdES1913203v111-202101.xsd".

```
<xsd:schema elementFormDefault="qualified" targetNamespace="http://uri.etsi.org/19132/v1.1.1#"
xmlns="http://uri.etsi.org/19132/v1.1.1#" xmlns:ers="urn:ietf:params:xml:ns:ers"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

4.2 Electronic time-stamps in evidence-records

All the electronic time-stamps present within the evidence-records incorporated to the XAdES signatures specified in the present document shall be instances of `TimeStampToken` type as specified in IETF RFC 3161 [4] and updated by IETF RFC 5816 [6].

4.3 Placement of validation data of time-stamp tokens

When including validation data required for verifying a time-stamp token that is encapsulated within an ArchiveTimeStamp, one of the following methods shall be used:

1) adding the information in the `SignedData` of the instance of the `TimeStampToken` type specified in IETF RFC 3161 [4] and updated by IETF RFC 5816 [6] itself; or

2) if the time-stamp token is present within an XML Evidence Record as specified in IETF RFC 6283 [5], then the validation data may be added within `ers:CryptographicInformation` children of the `ers:CryptographicInformationList` element (specified in IETF RFC 6283 [5], clause 3.1.3) that shares the same `ers:ArchiveTimeStamp` element as the `ers:TimeStamp` element that encapsulates the time-stamp token.

Method 1) should be used.

NOTE: According to IETF RFC 6283 [5], clause 2.1, `ers:CryptographicInformationList` element "is protected by successive Time-Stamps in the sequence of the Archive Time-Stamps".

If the XAdES signature contains any of the XAdES signed or unsigned qualifying properties that encapsulate a time-stamp token (i.e. `xades:AllDataObjectsTimeStamp`, `xades:IndividualDataObjectsTimeStamp`, `xades:SignatureTimeStamp`, `xades:SigAndRefsTimeStamp`, `xadesv141:SigAndRefsTimeStampV2`, `xades:RefsOnlyTimeStamp`, `xades:`, `xadesv141:RefsOnlyTimeStampV2`, `xades:ArchiveTimeStamp`, or `xadesv141:ArchiveTimeStamp`) then before adding any unsigned qualifying property encapsulating an evidence-record, the validation material for the corresponding time-stamp tokens that are not already present within the XAdES signature or within the time-stamp tokens themselves shall be incorporated using the corresponding `xadesv141:TimeStampValidationData` elements as specified in ETSI EN 319 132-1 [1] and ETSI TS 101 903 [3].

5 The `xadesen:SealingEvidenceRecords` qualifying property

5.1 Semantics

5.1.1 Data time-stamped by time-stamp tokens

The present document specifies one qualifying property that allows to incorporate into the XAdES signature one or more evidence records: `xadesen:SealingEvidenceRecords`.

The `xadesen:SealingEvidenceRecords` qualifying property shall be an unsigned qualifying property.

The `xadesen:SealingEvidenceRecords` unsigned qualifying property shall contain either a sequence of instances of `ers:EvidenceRecordType` type specified in IETF RFC 6283 [5] or a sequence of instances of `EvidenceRecord` type specified in IETF RFC 4998 [8].

This qualifying property may be incorporated only in XAdES signatures using either direct or indirect incorporation of qualifying properties, as specified in clause 4.4 of ETSI EN 319 132-1 [1].

The evidence records present within the same `xadesen:SealingEvidenceRecords` qualifying property shall act as parallel evidence records (from different TSAs or using different hash algorithms), protecting the same parts of the signature, except the other evidence records present within the same `xadesen:SealingEvidenceRecords` qualifying property.

The first time-stamp token in the initial ArchiveTimeStamp within each evidence record within a certain `xadesen:SealingEvidenceRecords` qualifying property shall be generated as specified in clause 5.2.2 of the present document.

After the initial ArchiveTimeStamp in the first ArchiveTimeStampChain, each evidence record may follow its own path, and both, time-stamp token renewal or hash-tree renewal may occur. Both time-stamp token renewal and hash-tree renewal shall be performed as specified in IETF RFC 6283 [5] and IETF RFC 4998 [8].

NOTE: Clauses 4.2.1 and 4.2.2 of IETF RFC 6283 [5] and clause 5 of IETF RFC 4998 [8] specify how the time-stamp renewal and hash-tree renewal are performed.

Once a `xadesen:SealingEvidenceRecords` element with one or more evidence records is incorporated into the XAdES signature as an unsigned qualifying property, the only changes that may be applied to the XAdES signature are:

- the (time-stamp or hash-tree) renewal of the evidence records present within the same `xadesen:SealingEvidenceRecords` qualifying property itself;
- the incorporation of a new evidence record within the same `xadesen:SealingEvidenceRecords` qualifying property;, and
- the incorporation of a new `xadesen:SealingEvidenceRecords` unsigned qualifying property.

Incorporation of new `xadesen:SealingEvidenceRecords` unsigned qualifying properties allows for evidence records that seal evidence records that are present in previously incorporated `xadesen:SealingEvidenceRecords` unsigned qualifying properties (serial evidence records).

5.1.2 Incorporation of validation data during the life cycle of evidence records

Before incorporating the `xadesen:SealingEvidenceRecords` unsigned qualifying property with its first evidence record, any validation data, not already present within the signature, which is required for validating any signed component present in the signature, shall be incorporated into the XAdES signature as specified in ETSI EN 319 132-1 [1].

EXAMPLE: Examples of this validation material are certificates, CRLs, OCSP responses or other material as required to validate, for instance, the signature itself, any present counter-signature, any present time-stamp token, certificate, OCSP response, attribute certificates, signed assertions, etc.

In the case that the validation data contains a Delta CRL, then the whole set of CRLs shall be included to provide a complete revocation list.

NOTE 1: Validation data already present for example in the time-stamp token need not be included again.

Before incorporating a new time-stamp token within an evidence record, i.e. during a time-stamp renewal or a hash-tree renewal, the validation data missing to validate the latest time-stamp token within the aforementioned evidence record, shall be incorporated using one of the two methods specified in clause 4.3.

NOTE 2: The incorporation of a new time-stamp token within an Evidence Record only requires the incorporation of the validation data of the latest time-stamp token present within that Evidence Record. All the rest of material had been incorporated before.

If a XAdES signature incorporates one or more `xadesen:SealingEvidenceRecords` unsigned qualifying properties, before incorporating a new `xadesen:SealingEvidenceRecords` unsigned qualifying property, the validation data required for validating the last time-stamp tokens of all the evidence records encapsulated within the last `xadesen:SealingEvidenceRecords` unsigned qualifying property already present into the XAdES signature, shall be incorporated using one of the two methods specified in clause 4.3.

5.2 Syntax

5.2.1 Introduction

The `xadesen:SealingEvidenceRecords` unsigned qualifying property shall be defined as in XML Schema file "XAdES1913203v111-202101.xsd", whose location is detailed in clause A.1, and is copied below for information.

```
<!-- targetNamespace="http://uri.etsi.org/19132/v1.1.1#"-->

<xsd:element name="SealingEvidenceRecords" type="EvidenceRecordsType"/>

<xsd:complexType name="EvidenceRecordsType">
    <xsd:choice>
        <xsd:sequence minOccurs="1" maxOccurs="unbounded">
            <xsd:element ref="ers:EvidenceRecord"/>
        </xsd:sequence>
        <xsd:sequence minOccurs="1" maxOccurs="unbounded">
            <xsd:element name="ASN1EvidenceRecord" type="xsd:base64Binary"/>
        </xsd:sequence>
    </xsd:choice>
</xsd:complexType>
```

The `xadesen:SealingEvidenceRecords` unsigned qualifying property shall contain either:

- one or more `ers:EvidenceRecord` element specified within IETF RFC 6283 [5]; or
- one or more instances of `EvidenceRecord` type specified in IETF RFC 4998 [8].

All the `xadesen:SealingEvidenceRecords` unsigned qualifying properties present in one XAdES signature shall have the same type of evidence-record, either `ers:EvidenceRecord` or `ASN1EvidenceRecord`.

5.2.2 Requirements for incorporating the first time-stamp token in the initial ArchiveTimestamp within an evidence-record

5.2.2.1 General requirements

The initial time-stamp token encapsulated within the first ArchiveTimeStamp of any of the evidence-records enclosed within the `xadesen:SealingEvidenceRecords` unsigned qualifying property, shall incorporate a HashTree, whose first child shall contain the digest value of the group of data objects listed below, concatenated in the order specified in IETF RFC 6283 [5] if the `xadesen:SealingEvidenceRecords` unsigned qualifying property contains XMLERS evidence-records, or in IETF RFC 4998 [8] if the `xadesen:SealingEvidenceRecords` unsigned qualifying property contains ERS evidence-records:

1) The data objects resulting of processing each `ds:Reference` element within `ds:SignedInfo` as specified below:

   - Process the `ds:Reference` element according to the reference processing model of XMLDSIG [7], clause 4.4.3.2.
   - If the result is a XML node set, canonicalize using the canonicalization algorithm present in `ds:CanonicalizationMethod` element.

NOTE 1: The XAdES qualifying signed properties are part of this set of data objects.

2) The data objects resulting of taking the XMLDSIG elements listed below, and canonicalizing each one using the canonicalization algorithm present in `ds:CanonicalizationMethod` element:

   - The `ds:SignedInfo` element.
   - The `ds:SignatureValue` element.
   - The `ds:KeyInfo` element, if present.

3) The data objects resulting of taking all the unsigned qualifying properties incorporated into the XAdES signature except the `xadesen:SealingEvidenceRecords` element under construction, and canonicalizing each one as specified in clause 4.5 of ETSI EN 319 132-1 [1].

While generating these data objects, requirements a), b), c), and d) of step 4) in clause 5.5.2.2 of ETSI EN 319 132-1 [1] shall apply:

4) As many `xadesv141:TimeStampValidationData` qualifying properties will be added as required for incorporating the validation data, not already present in the XAdES signature, that are required for validating all the time-stamp tokens incorporated (within signed or unsigned qualifying properties) into the XAdES qualifying properties different than `xadesen:SealingEvidenceRecords`. Each `xadesv141:TimeStampValidationData` shall be generated following the specifications of ETSI EN 319 132-1 [1]. For every `xadesv141:TimeStampValidationData` qualifying property incorporated, the corresponding data object resulting of canonicalizing this qualifying property as specified in clause 4.5 of ETSI EN 319 132-1 [1] will be generated and added to the group of data objects to be time-stamped.

5) All the `ds:Object` elements except the one containing `QualifyingProperties` element, as specified in step 5) of clause 5.5.2.2 of ETSI EN 319 132-1 [1].

6) The objects derived from the presence of signed `ds:Manifest` elements. These objects shall be generated as it is specified below:

   a) For each `ds:Reference` child element of each signed `ds:Manifest` element retrieve the data object referenced by its `URI` attribute.

   b) If the retrieved data object is not a XML node set, or it is a XML node set different than a `ds:Manifest` element, process it as specified by the reference processing model of XMLDSIG [7], clause 4.4.3.2. The resulting data object shall be added to the group of data objects to be digested.

   c) If the retrieved data object is a `ds:Manifest` element, apply the steps 6) a) to 6) c) recursively for generating the objects to be added to the group of data objects to be digested.

NOTE 1: Step 6) c) allows to process chained signed `ds:Manifest` elements so that every data object referenced by one `ds:Manifest` element in the chain, is added to the group of data objects to be digested.

NOTE 2: The procedures for performing the hash tree renewal specified in IETF RFC 4998 [8] and IETF RFC 6283 [5] will imply that every time that a Hash Tree Renewal is performed in an evidence record, every data object referenced by one signed `ds:Manifest` element will be processed as specified in step 6) and therefore added to the group of data objects to be digested.

NOTE 3: The process specified in step 6) implies that the XAdES signatures conformant with the present document do not need to incorporate qualifying properties dealing with renewal of signed `ds:Manifest` elements (`xadesv141:RenewedDigest` for instance).

NOTE 4: Each unsigned qualifying property results in one object. Therefore any `xadesen:SealingEvidenceRecords` qualifying property already present within the XAdES signature, will contribute in the mentioned HashTree and all its children elements will be time-stamped. The new evidence record will become a serial evidence record of the ones that had been previously incorporated.

5.2.2.2 Contribution of unsigned qualifying properties directly incorporated

In non-distributed XAdES signatures, where the direct incorporation of the unsigned qualifying properties is used, the set of unsigned qualifying properties contributing to the message imprint computation input shall be the set formed by all the unsigned qualifying properties present within the sequence in the `xadesen:UnsignedSignatureProperties` element.

5.2.2.3 Contribution of unsigned qualifying properties indirectly incorporated

In distributed XAdES signatures, where the indirect incorporation of the unsigned qualifying properties is used, the set of the unsigned qualifying properties contributing to the message imprint computation input shall be as formed as follows:

1) First add to the set the unsigned qualifying properties that are children of the `xadesen:UnsignedSignatureProperties` element that is descendant of the `ds:Signature` signature root element.

2) After that, for each `xadesen: QualifyingPropertiesReference` child element of the `ds:Object` within the `ds:Signature` XAdES root element, in their order of appearance:

   - Retrieve the `xadesen: QualifyingProperties` element.

   - Add to the set all the unsigned qualifying properties found in the `xadesen:UnsignedSignatureProperties` child element.

NOTE: No process needs to be carried out with signed qualifying properties if present in the retrieved `xadesen: QualifyingProperties` element: they have already been processed as part of the process of the `ds:Reference` elements within `ds:SignedInfo`.

6 XAdES signature level including ERS

6.1 Overview

The present document specifies a new level for XAdES signatures including evidence records.

Each level is created by a combination of attributes defined in ETSI EN 319 132-1 [1] and the present document.

6.2 General requirements

The XAdES signature shall be a signature incorporating signed and unsigned qualifying properties as specified in clauses 4 and 5 of ETSI EN 319 132-1 [1].

The algorithms and key lengths used to generate and augment digital signatures should be as specified in ETSI TS 119 312 [i.2].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.2] can be superseded by national recommendations.

6.3 XAdES-E-ERS

XAdES-E-ERS may be built on all the levels described in ETSI EN 319 132-1 [1] or ETSI EN 319 132-2 [2].

Table 2: Requirements for XAdES-E-ERS

Elements/Qualifying properties/Services	Presence in E-ERS level	Cardinality	Additional notes and requirements	Reference
`xades:SigningTime`	may be present	1	a	ETSI EN 319 132-1 [1], clause 5.2.1
`xades:SigningCertificateV2`	conditioned presence	0 or 1	b, c	ETSI EN 319 132-1 [1], clause 5.2.2
`xades:CommitmentTypeIndication`	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.3
`xades:DataObjectFormat`	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.4
`xades:SignatureProductionPlaceV2`	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.5
`xades:SignerRoleV2`	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.6
`xades:CounterSignature`	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.7.2
`xades:AllDataObjectsTimeStamp`	may be present	≥ 0	1	ETSI EN 319 132-1 [1], clause 5.2.8.1
`xades:IndividualDataObjectsTimeStamp`	may be present	≥ 0	1	ETSI EN 319 132-1 [1], clause 5.2.8.2
`xades:SignaturePolicyIdentifier`	may be present	Built on E-EPES: 1 Not built on E-EPES: 0	2, 3	ETSI EN 319 132-1 [1], clause 5.2.9
`xadesv141:SignaturePolicyStore`	conditioned presence	0 or 1	d	ETSI EN 319 132-1 [1], clause 5.2.10
`xades:SignatureTimeStamp`	shall be present	≥ 1	e, f 1, 4	ETSI EN 319 132-1 [1], clause 5.3
`xades:CertificateValues`	conditioned presence	0 or 1	g, h	ETSI EN 319 132-1 [1], clause 5.4.1
`xades:AttrAuthoritiesCertValues`	conditioned presence	0 or 1	g, i	ETSI EN 319 132-1 [1], clause 5.4.3
`xades:RevocationValues`	conditioned presence	0 or 1	j, k	ETSI EN 319 132-1 [1], clause 5.4.2
`xades:AttributeRevocationValues`	conditioned presence	0 or 1	j, l	ETSI EN 319 132-1 [1], clause 5.4.4
Service: incorporation of validation data for time-stamp tokens	shall be provided	-	m	Clauses 4.3 and 5.1.2 of the present document
SPO: `xadesv141:TimeStampValidationData`	conditioned presence	≥ 0	n	Clause 4.3 of the present document
SPO: certificate and revocation values within the `ers:CryptographicInformationList` element	conditioned presence	≥ 0		Clause 4.3 of the present document
SPO: certificate and revocation values within the `SignedData` field of the time-stamp token	conditioned presence	≥ 0		Clause 4.3 of the present document
`xadesv141:ArchiveTimeStamp`	*	≥ 0	o, p	ETSI EN 319 132-1 [1], clause 5.5.2
`xadesv141:RenewedDigest`	shall not be present	0		ETSI EN 319 132-1 [1], clause 5.5.3
`xadesv141:CompleteCertificateRefsV2`	*	0 or 1	q	ETSI EN 319 132-1 [1], clause A.1.1
`xadesv141:AttributeCertificateRefsV2`	*	0 or 1	q, r	ETSI EN 319 132-1 [1], clause A.1.3
`xades:CompleteRevocationRefs`	*	0 or 1		ETSI EN 319 132-1 [1], clause A.1.2

Elements/Qualifying properties/Services	Presence in E-ERS level	Cardinality	Additional notes and requirements	Reference
xades:AttributeRevocationRefs	*	0 or 1	r	ETSI EN 319 132-1 [1], clause A.1.4
xadesv141:RefsOnlyTimeStampV2	*	≥ 0	1	ETSI EN 319 132-1 [1], clause A.1.5.2
xadesv141:SigAndRefsTimeStampV2	*	≥ 0	1	ETSI EN 319 132-1 [1], clause A.1.5.1
Service: ERS inclusion	shall be provided	≥ 1		Clause 5 of the present document
SPO: xadesen:SealingEvidenceRecords	shall be present	≥ 1		Clause 5 of the present document

Additional requirements:

a) Requirement for `xades:SigningTime`. The generator shall include the claimed UTC time when the signature was generated as content of the `xades:SigningTime` qualifying property.

b) Requirement for `xades:SigningCertificateV2`. The `xades:SigningCertificateV2` qualifying property shall be present if the signing certificate is not present within the `ds:KeyInfo` element, or if the signing certificate is present within the `ds:KeyInfo` element but it is not signed by the signature. Otherwise the `xades:SigningCertificateV2` qualifying property may be absent.

c) Requirement for `xades:SigningCertificateV2`. The references to certificates should not include the `IssuerSerialV2` element.

d) Requirement for `xadesv141:SignaturePolicyStore`. This qualifying property may be incorporated into the XAdES signature only if the `xades:SignaturePolicyIdentifier` is also incorporated and it contains the `SigPolicyHash` element with the digest value of the signature policy document. Otherwise the `xadesv141:SignaturePolicyStore` shall not be incorporated into the XAdES signature.

e) Requirement for `xades:SignatureTimeStamp`. Each `xades:SignatureTimeStamp` element may contain one or more electronic time-stamps issued by different TSAs.

f) Requirement for `xades:SignatureTimeStamp`. The electronic time-stamps encapsulated within the `signature-time-stamp` attributes shall be created before the signing certificate has been revoked or has expired.

g) Requirement for `xades:CertificateValues` and `xades:AttrAuthoritiesCertValues`. Duplication of certificate values within the signature should be avoided.

h) Requirement for incorporation of `xades:CertificateValues`. The incorporation of `xades:CertificateValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4) a) of the algorithms specified for computing the input to the electronic time-stamp's message imprint.

i) Requirement for incorporation of `xades:AttrAuthoritiesCertValues`. The incorporation of `xades:AttrAuthoritiesCertValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4) c) of the algorithms specified for computing the input to the time-stamp token's message imprint.

j) Requirement for `xades:RevocationValues` and `xades:AttributeRevocationValues`. Duplication of revocation values within the signature should be avoided.

k) Requirement for incorporation of `xades:RevocationValues`. The incorporation of `xades:RevocationValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4) b) of the algorithms specified for computing the input to the time-stamp token's message imprint.

l) Requirement for incorporation of `xades:AttributeRevocationValues`. The incorporation of `xades:AttributeRevocationValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4) d) of the algorithms specified for computing the input to the time-stamp token's message imprint.

m) Requirement for service "incorporation of validation data for electronic time-stamps". If the time-stamp token is placed within an evidence-record its validation data shall be incorporated as specified in clause 4.3 of the present document, otherwise, its validation data shall be incorporated as specified in ETSI EN 319 132-1 [1].

n) Requirement for option `xadesv141:TimeStampValidationData` of service "incorporation of validation data for time-stamp-tokens". The validation data, not present elsewhere within the XAdES signature, and required for verifying for electronic time-stamps incorporated within any of the following qualifying properties: `xades:AllDataObjectsTimeStamp`, `xades:IndividualDataObjectsTimeStamp`, `xades:SignatureTimeStamp`, `xades:SigAndRefsTimeStamp`, `xadesv141:SigAndRefsTimeStampV2`, `xades:RefsOnlyTimeStamp`, `xades:`, `xadesv141:RefsOnlyTimeStampV2`, `xades:ArchiveTimeStamp`, or `xadesv141:ArchiveTimeStamp`, shall be included in the corresponding `xadesv141:TimeStampValidationData` qualifying property as specified in ETSI EN 319 132-1 [1].

o) Requirement for `xadesv141:ArchiveTimeStamp`. Each `xadesv141:ArchiveTimeStamp` qualifying may contain more than one electronic time-stamp issued by different TSAs.

p) Requirement for `xadesv141:ArchiveTimeStamp`. Before generating and incorporating a new `xadesv141:ArchiveTimeStamp` qualifying property, all the validation material required for validating the XAdES signature shall be included. This validation material shall include all the certificates and all certificate status information (like CRLs or OCSP responses) required for:

- validating the signing certificate;
- validating the signing certificate of any countersignature incorporated into the signature;
- validating any attribute certificate or signed assertion present in the signature; and
- validating the signing certificate of any previous electronic time-stamp already incorporated into the signature within any XAdES electronic time-stamp container qualifying property (including `xadesv141:ArchiveTimeStamp` qualifying property).

q) Requirement for `xadesv141:CompleteCertificateRefsV2`, and `xadesv141:AttributeCertificateRefsV2`. The references to certificates should not include the `IssuerSerialV2` element.

r) Requirement for `xadesv141:AttributeCertificateRefsV2` and `xades:AttributeRevocationRefs`. The `xadesv141:AttributeCertificateRefsV2` and `xades:AttributeRevocationRefs` qualifying properties may be used when at least an attribute certificate or a signed assertion is incorporated into the XAdES signature. Otherwise, `xadesv141:AttributeCertificateRefsV2` and `xades:AttributeRevocationRefs` attributes shall not be used.

NOTE 1: On `xades:SignatureTimeStamp`, `xades:IndividualDataObjectsTimeStamp`, `xades:AllDataObjectsTimeStamp`, `xadesv141:RefsOnlyTimeStampV2`, `xadesv141:SigAndRefsTimeStampV2`. Several instances of these qualifying properties can be incorporated into the XAdES signature, coming from different TSAs.

NOTE 2: On `xades:SignaturePolicyIdentifier`. The semantics of the signed data objects of XAdES-E-BES, XAdES-E-T, and XAdES-E-A signatures, or their context can implicitly indicate a signature policy.

NOTE 3: On `xades:SignaturePolicyIdentifier`. The signature policy can establish specific requirements for other qualifying properties.

NOTE 4: On `xades:SignatureTimeStamp`. `xades:SignatureTimeStamp` qualifying property provides the initial steps towards providing long-term validity.

7 Legacy XAdES baseline signatures

When an `ers:SealingEvidenceRecords` unsigned qualifying property is incorporated into legacy XAdES extended signatures, this unsigned qualifying property shall comply with the present document.

Annex A (normative): XML Schema file

A.1 XML Schema file location for namespace http://uri.etsi.org/19132/v1.1.1#

The file at https://uri.etsi.org/19132/v1.1.1/XAdES1913203v111-202101.xsd (XAdES1913203v111-202101.xsd) contains the definitions of the qualifying properties defined within the namespace whose URI value is http://uri.etsi.org/19132/v1.1.1#.

History

Document history		
V1.1.1	January 2021	Publication