

XML Advanced Electronic Signatures (XAdES)

What is XAdES?

The XML Advanced Electronic Signatures (XAdES) standard is an extension of the IETF XMLDSIG specification. The XAdES specification is designed to conform to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. XAdES aims to address the problems of non-repudiation and long term validation of XML digital signatures.

Unlike transactional signatures used by protocols such as SOAP, digital signatures applied to documents often have archival requirements that extend past the lifetime of the signing entity and the revocation information that is current at the time of signing. Under these circumstances, more information must be saved within the signature. By providing a schema for secure timestamps, countersignatures and embedded revocation data, XAdES provides a richer set of features that can be used to create more detailed non-repudiation information for XML signatures that are applied to documents.

By allowing for the archival and long term validation, signatures that conform to the XAdES specification are compliant with Directive 1999/93/EC. Enabling applications for XAdES signatures will help assure regulatory compliance when operating within the European Union.

Contents

XAdES and XMLDSIG	3
Anatomy of a XAdES Signature	4
Signed Properties	4
Signed Signature Properties	4
Signed Data Object Properties	4
Unsigned Properties	5
Unsigned Signature Properties	5
Unsigned Data Object Properties	5
XAdES Signature Forms	6
Summary of XAdES Forms	6
XAdES	7
XAdES with Timestamp (XAdES-T)	8
XAdES with Complete Validation Data (XAdES-C)	9
XAdES with Extended Validation Data (XAdES-X)	10
XAdES with Extended Long Term Validation Data (XAdES-X-L)	11
XAdES with Archiving Validation Data (XAdES-A)	12
Toolkit Support	13
References	14
For More Information	14
About Gemini Security Solutions	14

XAdES and XMLDSIG

XAdES is, at its core, a set of XML schema definitions that define an object to be inserted into the `<ds:Object>` node of an XMLDSIG signature. This makes XAdES interoperable with existing XMLDSIG toolkits in some respects, as a XAdES signature can be validated simply as an XMLDSIG signature. However, doing so does not maximize the usefulness of the XAdES format, because a generic XMLDSIG module will not be able to interpret the embedded information in the XAdES extensions, such as secure timestamps or revocation information.

An XMLDSIG signature has the following basic structure¹:

```
<ds:Signature ID?>
  <ds:SignedInfo/>
  <ds:SignatureValue/>
  <ds:KeyInfo/>(optional)
  <ds:Object/>(optional, multiple values allowed)
</ds:Signature>
```

The `<ds:Object>` node is where the qualifying signature properties are inserted to create a XAdES signature. XAdES specifies the following additions to the XMLDSIG schema:

```
<ds:Signature ID?>
  <ds:SignedInfo/>
  <ds:SignatureValue/>
  <ds:KeyInfo/>(optional)
  <ds:Object>
    <QualifyingProperties>
      <SignedProperties>
        <SignedSignatureProperties/>
        <SignedDataObjectProperties/>
      </SignedProperties>
      <UnsignedProperties>
        <UnsignedSignatureProperties/>
      </UnsignedProperties>
    </QualifyingProperties>
  </ds:Object>
</ds:Signature>
```

Each XAdES form specifies attribute nodes that appear within the `<SignedSignatureProperties>`, `<SignedDataObjectProperties>`, and `<UnsignedSignatureProperties>` objects in the XML schema. The XML nodes nested inside of the `<SignedProperties>` node are referenced in the XMLDSIG signature, so this data must be created before the signature is generated. The nodes subordinate to `<UnsignedProperties>` are

¹ For the full schema defined by XMLDSIG, see <http://www.w3.org/TR/xmlsig-core/#sec-CoreSyntax>

not covered by the signature, and therefore may be generated after the signature is created; they may even be added by the relying party without the signer's involvement.

Anatomy of a XAdES Signature

There are six extended forms of XMLDSIG signatures that comprise the XAdES standard. Each form provides a differing level of long term validation capability beyond what standard XMLDSIG offers. XAdES provides for signatures that contain signed and unsigned attributes and, in some forms, cryptographic timestamps and embedded revocation information.

Signed Properties

A XAdES signature contains two groups of signer properties that are treated as signed data by the digital signature. These categories are described below. The first group, called the Signed Signature Properties, qualifies the signature by describing the signature itself. The Signed Data Object Properties qualify the signature by describing the signed data objects after the XML transformation has been applied.

Signed Signature Properties

The signed signature properties qualify the XMLDSIG signature by specifying details about the signer. The properties that are supported in this collection are:

- The signature time (Non-authoritative. May come from signer's computer. Required)
- The certificate identifier used to create the signature (Required)
 - Hash of the certificate
 - Serial Number of the Issuing CA's Certificate
- The signature policy identifier (Required)
- The location where the signature was created (Optional)
- The role of the signer (Optional)

Signed Data Object Properties

The Signed Data Object Properties qualify the signature by specifying details about the data that was signed. The properties that are supported in this collection are:

- The format of the data objects covered by the signature, such as the MIME type or encoding type
- The type of commitment that is conveyed by the digital signature, such as a proof of origin or proof of receipt of the signed data
- A timestamp that covers all of the signed data, except for the signed properties of the signature (Optional)
- An arbitrary number of timestamps that cover specific portions of the signed data (Optional)

Unsigned Properties

The XAdES specification also provides for a number of unsigned attributes which may accompany a signature. Like the signed properties, these are broken into two groups, one group qualifying the signature by providing details about the signature itself, the other qualifying the signature by providing details about the signed data.

Unsigned Signature Properties

The Unsigned Signature Properties qualify the signature by specifying details about the signature itself. This collection houses all of the additional properties that the various forms of XAdES add to the base specification. The properties that may be included as unsigned attributes are:

- An arbitrary number of countersignatures that are applied to the signature. Countersignatures may be applied in serial or parallel. (Optional)
- An arbitrary number of cryptographic timestamps that cover the digital signature. This property is not used in the XAdES form, but is required for XAdES-T and all forms based on XAdES-T.
- The complete collection of certificate identifiers for the certificate chain used to create the signature. This property is not used in the XAdES or XAdES-T forms. It is required by XAdES-C and all forms based on XAdES-C.
- The complete collection of revocation information identifiers used to validate the signature. This property is not used in the XAdES or XAdES-T forms. It is required by XAdES-C and all forms based on XAdES-C
- A timestamp that covers the digital signature, the full collection of certificate identifiers, and the full collection of revocation identifiers

OR

A timestamp that covers the full collection of certificate identifiers and the full collection of revocation identifiers. This property is not used in the XAdES, XAdES-T, or XAdES-C forms. It is required by XAdES-X and all forms based on XAdES-X.

- The collection of certificate and revocation files used to build and validate the signer's certificate path. This property is only allowed for the XAdES-X-L and XAdES-A forms.
- An arbitrary number of timestamp countersignatures that cover the entire XAdES-X-L form of the signature. This attribute is used to enable long term validation of signatures. It is only allowed in the XAdES-A form.

Unsigned Data Object Properties

Unsigned Data Object Properties qualify the signature by specifying details about the signed data. Currently, the XAdES specification does not provide any specific properties in this area. However, the standard does allow an arbitrary-length collection of XML **AnyType** objects, which can be used to this end.

XAdES Signature Forms

There are several forms of XAdES signatures. These forms act as a sequence, with each form adding an additional set of attributes to the unsigned properties collection from the previous one. The simplest form is XAdES, which does not provide for timestamps on the signature, nor does it allow for embedded revocation information. The most complicated form is XAdES-A, which allows for timestamps, embedded revocation information, and a collection of countersignature timestamps to preserve the integrity of the signature over an indefinite period.

Summary of XAdES Forms

The following table shows the capabilities added by each layer of information in the XAdES schema.

	Provides Digital Signature	Allows Cryptographic Timestamp	Includes Revocation References	Includes Full Revocation Data	Allows Secure Timestamp Counter-signature
XAdES	Yes	No	No	No	No
XAdES-T	Yes	Yes	No	No	No
XAdES-C	Yes	Yes	Yes	No	No
XAdES-X	Yes	Yes	Yes	No	No
XAdES-X-L	Yes	Yes	Yes	Yes	No
XAdES-A	Yes	Yes	Yes	Yes	Yes

Figure 1 - XAdES Form Summary

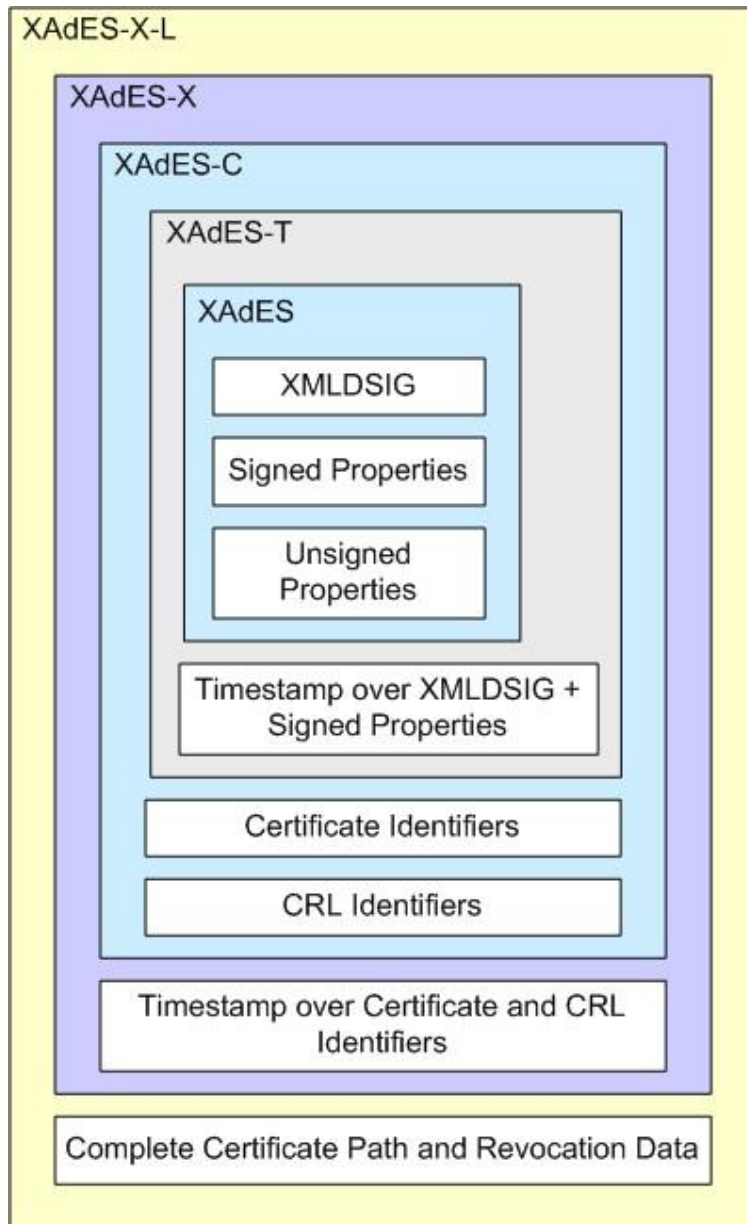


Figure 2 - XAdES Form Hierarchy

XAdES

The XAdES form is the most basic form of a XAdES compliant signature. This form provides no secure timestamp capability and provides no mechanism for embedding revocation information. The XAdES form specifies the following information:

- Signed Signature Properties
 - Signing Time (non-authoritative: may be from signer's computer)
 - Signature Certificate
 - Signature Policy Identifier
 - Signature Production Place (optional)
 - Signer Role (optional)
- Signed Data Properties
 - Data Object Format *
 - Commitment Type Indication *
 - All Data Objects Time Stamp *
 - Individual Data Objects Time Stamp *
- Unsigned Signature Properties
 - Counter Signature *

[Fields marked with a * may contain any number of entries, including zero. Fields marked as (optional) may contain zero or one entry. Fields marked with a + must contain at least one entry. All unqualified items must have one entry.]

XAdES with Timestamp (XAdES-T)

XAdES-T builds on XAdES by adding the ability to affix a secure timestamp to the signature as an unsigned attribute. Because this value is not covered by the XMLDSIG digital signature, the timestamp does not have to be obtained during the signing event; it may also be applied *by the relying party* after the receipt of the signature. This strengthens the non-repudiation value of the signature, even if the timestamp was not obtained by the signer.

The XAdES-T form builds on the XAdES form by adding the **Signature Timestamp** attribute to the Unsigned Signature Properties collection:

- *Signed Signature Properties*
 - *Signing Time (non-authoritative: may be from signer's computer)*
 - *Signature Certificate*
 - *Signature Policy Identifier*
 - *Signature Production Place (optional)*
 - *Signer Role (optional)*
- *Signed Data Properties*
 - *Data Object Format **
 - *Commitment Type Indication **
 - *All Data Objects Time Stamp **
 - *Individual Data Objects Time Stamp **
- *Unsigned Signature Properties*
 - *Counter Signature **
 - **Signature Timestamp+**

[Fields marked with a * may contain any number of entries, including zero. Fields marked as (optional) may contain zero or one entry. Fields marked with a + must contain at least one entry. All unqualified items must have one entry.]

XAdES with Complete Validation Data (XAdES-C)

The XAdES-C form extends the XAdES-T form further by providing a capability for embedding certificate revocation *references* into the signature as unsigned attributes. It is important to note that these additions do not contain the complete data structures; they contain unique ways to identify which certificates and revocation lists should be used to validate the signature certificate. In the case of a certificate, the identifier is the combination of the certificate serial number and a hash of the issuer's distinguished name. For a Certificate Revocation List (CRL), it is a hash of the complete CRL file. This information is useful only if there is a trusted repository for historical revocation information that can be accessed by the relying party.

Similarly to the timestamp field added by XAdES-T, these references can be embedded by either the signer or the relying party, as they are not signed attributes and therefore are not covered by the XMLDSIG signature nor the timestamp signature. Additionally, this allows these references to be removed in the case where a relying party supports only the XAdES or XAdES-T formats.

The XAdES-C form builds on the XAdES-T form by adding the **Complete Certificate Refs and Complete Revocation Refs** attributes to the Unsigned Signature Properties collection:

- *Signed Signature Properties*
 - *Signing Time (non-authoritative: may be from signer's computer)*
 - *Signature Certificate*
 - *Signature Policy Identifier*
 - *Signature Production Place (optional)*
 - *Signer Role (optional)*
- *Signed Data Properties*
 - *Data Object Format **
 - *Commitment Type Indication **
 - *All Data Objects Time Stamp **
 - *Individual Data Objects Time Stamp **
- *Unsigned Signature Properties*
 - *Counter Signature **
 - *Signature Timestamp+*
 - **Complete Certificate Refs**
 - **Complete Revocation Refs**

[Fields marked with a * may contain any number of entries, including zero. Fields marked as (optional) may contain zero or one entry. Fields marked with a + must contain at least one entry. All unqualified items must have one entry.]

XAdES with Extended Validation Data (XAdES-X)

The XAdES-X signature form extends the XAdES-C form by providing an attribute to hold a secure timestamp that covers the revocation and certificate references. This is intended to preserve the integrity of the certificate and revocation item identifiers in the case of a key compromise of any of the CA certificates in the certificate path. This is useful because the revocation references are not signed attributes.

As an example, imagine a digital signature that references a CRL that is issued by a compromised CA key. The revocation reference that indicates the uncompromised CRL that should be used to validate the path can be removed from the XAdES-C form and replaced with the identifier of a CRL created with the compromised key, and the signature would still validate because the CRL Reference is not covered by the XMLDSIG. By applying a timestamp to the certificate and revocation references, their integrity is assured as long as the timestamp authority's key is valid.

The XAdES-X form extends the XAdES-C form by adding the **Refs Only Time Stamp** and **Sig and Refs Time Stamp** elements to the collection of unsigned attributes. Only one of these attributes is applied to an individual signature. The **Refs Only Time Stamp** covers only the certificate and revocation references from the XAdES-C form, while the **Sig and Refs Time Stamp** element covers the digital signature as well.

Covering the signature in addition to the certificate and revocation references avoids a possible replay attack by binding the revocation references to the specific signature.

- *Signed Signature Properties*
 - *Signing Time (non-authoritative: may be from signer's computer)*
 - *Signature Certificate*
 - *Signature Policy Identifier*
 - *Signature Production Place (optional)*
 - *Signer Role (optional)*
- *Signed Data Properties*
 - *Data Object Format **
 - *Commitment Type Indication **
 - *All Data Objects Time Stamp **
 - *Individual Data Objects Time Stamp **
- *Unsigned Signature Properties*
 - *Counter Signature **
 - *Signature Timestamp+*
 - *Complete Certificate Refs*
 - *Complete Revocation Refs*
 - **Refs Only Time Stamp - or – Sig and Refs Time Stamp**

[Fields marked with a * may contain any number of entries, including zero. Fields marked as (optional) may contain zero or one entry. Fields marked with a + must contain at least one entry. All unqualified items must have one entry.]

XAdES with Extended Long Term Validation Data (XAdES-X-L)

The XAdES-X-L signature form extends the XAdES-X form by providing a capability for embedding complete revocation information into the signature. This signature form still contains the certificate and revocation references covered by XAdES-X, but it also embeds the certificates and revocation structures in their entirety. This allows a relying party to perform long term validation of the signature without requiring access to a trusted repository of revocation information.

Because these attributes are unsigned, they can be added to the signature by either the signer or the relying party. Key compromise of any of the certificate authorities is detected in the same way as XAdES-X – by examining the timestamp applied to the certificate and revocation references.

XAdES-X-L extends XAdES-X by adding the **Certificate Values** and **Revocation Values** attributes to the unsigned signature properties.

- *Signed Signature Properties*
 - *Signing Time (non-authoritative: may be from signer's computer)*
 - *Signature Certificate*
 - *Signature Policy Identifier*
 - *Signature Production Place (optional)*
 - *Signer Role (optional)*
- *Signed Data Properties*
 - *Data Object Format **
 - *Commitment Type Indication **
 - *All Data Objects Time Stamp **
 - *Individual Data Objects Time Stamp **
- *Unsigned Signature Properties*
 - *Counter Signature **
 - *Signature Timestamp+*
 - *Complete Certificate Refs*
 - *Complete Revocation Refs*
 - *Refs Only Time Stamp - or – Sig and Refs Time Stamp*
 - **Certificate Values**
 - **Revocation Values**

[Fields marked with a * may contain any number of entries, including zero. Fields marked as (optional) may contain zero or one entry. Fields marked with a + must contain at least one entry. All unqualified items must have one entry.]

XAdES with Archiving Validation Data (XAdES-A)

The most complex XAdES signature form is XAdES-A, which provides for a countersignature to a XAdES-X-L signature. XAdES-A simply adds the **Archive Time Stamp** attribute to the unsigned properties collection, which allows any number of secure timestamp countersignatures to be applied to the signature without invalidating it. This protects against the inevitable weakening of cryptographic algorithms and key lengths used to create the signature by iteratively assuring the integrity of the signature with timestamps created with current key technology.

- *Signed Signature Properties*
 - *Signing Time (non-authoritative: may be from signer's computer)*
 - *Signature Certificate*
 - *Signature Policy Identifier*
 - *Signature Production Place (optional)*
 - *Signer Role (optional)*
- *Signed Data Properties*
 - *Data Object Format **
 - *Commitment Type Indication **
 - *All Data Objects Time Stamp **
 - *Individual Data Objects Time Stamp **
- *Unsigned Signature Properties*
 - *Counter Signature **
 - *Signature Timestamp+*
 - *Complete Certificate Refs*
 - *Complete Revocation Refs*
 - *Refs Only Time Stamp - or – Sig and Refs Time Stamp*
 - *Certificate Values*
 - *Revocation Values*
 - **Archive Time Stamp +**

[Fields marked with a * may contain any number of entries, including zero. Fields marked as (optional) may contain zero or one entry. Fields marked with a + must contain at least one entry. All unqualified items must have one entry.]

Toolkit Support

Currently there are no major development platforms that support XAdES natively. Third party toolkits are available from the following vendors:

- OpenXAdES (<http://openxades.org/>) [C, Java]
- IAIK (http://jce.iaik.tugraz.at/sic/products/xml_security/xades) [Java]
- Microsoft's Government Document Format AIP (<http://www.codeplex.com/gdf>) [C#, Polish language only]

References

- Bartel et al. **XML-Signature Syntax and Processing**. [Online] February, 2002. URL <http://www.w3.org/TR/xmlsig-core/#sec-Acknowledgements>
- Cruellas et al. **XML Advanced Electronic Signatures (XAdES)**. [Online] February, 2003. URL <http://www.w3.org/TR/XAdES/>

For More Information

If you have any questions about the contents of this document, or are interested in learning more about public key infrastructure (PKI), XML digital signatures, or long term signature validation, please contact:

Peter Hesse (pmhesse@geminisecurity.com)

Walter Turnes (wturnes@geminisecurity.com)

Gemini Security Solutions, Inc.

4451 Brookfield Corporate Dr. Suite 200

Chantilly, VA 20151

703-378-5808

<http://geminisecurity.com>

About Gemini Security Solutions

Gemini Security Solutions, Inc. provides impartial information security consulting services that ensure the confidentiality, integrity, and availability of critical business information and resources. Our value is centered on our ability to deliver the right expertise and the right experience, at the right time.

Founded in 2001, and with decades of experience, our certified team of experts assists organizations to assess and deliver security solutions in compliance with business strategy, policy and regulatory requirements. Our services include risk analysis and management, regulatory compliance, identity access and management, operations security, and security software development.

Gemini Security Solutions is focused on providing big business experience with a small business approach. Working with you every step of the way, Gemini Security Solutions enables secure business operations with vigor, agility and a commitment to excellence.