XML Signature Properties

W3C Working Draft 26 February 2009

This version:
http://www.w3.org/TR/2009/WD-xmldsig-properties-20090226/
Latest version:
http://www.w3.org/TR/xmldsig-properties/
Editor:
Frederick Hirsch, Nokia

Abstract

This document outlines proposed standard XML Signature Properties syntax and processing rules and an associated namespace for these properties. The intent is these can be composed with any version of XML Signature using the XML SignatureProperties element.

Status of this Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publications and the latest revision of this technical report can be found in the W3C technical reports index at http://www.w3.org/TR/.

This is a First Public Working Draft of "XML Signature Properties."

The properties specified in this document are believed to be broadly useful, but are primarily motivated by use of XML Signature for code signing, and by relevant work in the W3C Web Applications Working Group. This specification is intended to provide building blocks for profiles of XML Signature; specifying detailed processing for individual properties is left to these profiles.

This document was developed by the XML Security Working Group. The Working Group expects to advance this Working Draft to Recommendation Status.

Please send comments about this document to public-xmlsec-comments@w3.org (with

public archive).

Publication as a Working Draft does not imply endorsement by the W3C Membership. This is a draft document and may be updated, replaced or obsoleted by other documents at any time. It is inappropriate to cite this document as other than work in progress.

This document was produced by a group operating under the 5 February 2004 W3C Patent Policy. W3C maintains a public list of any patent disclosures made in connection with the deliverables of the group; that page also includes instructions for disclosing a patent. An individual who has actual knowledge of a patent which the individual believes contains Essential Claim(s) must disclose the information in accordance with section 6 of the W3C Patent Policy.

Table of Contents

---

1 Introduction

The SignatureProperties element defined by XML Signature [XMLDSIG2nd] offers a means to associate property values with an XML Signature. This document defines specific properties that may be used by various applications of XML Signature, without requiring those applications to define such properties on a per case basis. This document defines how these properties are to be specified and processed when used but does not require their use - specifications that reference this document may or may not require their use.

The changes proposed in this document would not be a breaking change to XML Signature, but warrant a new namespace for the properties themselves so that they can be used in various versions of XML Signature.

2 Versions, Namespaces and Identifiers

No provision is made for an explicit version number in this syntax. If a future version is needed, it will use a different namespace. The XML namespace [XML-ns] URI that MUST be used by implementations of this (dated) specification is:

```
    xmlns dsp="http://www.w3.org/2009/xmldsig-properties#"
```

This namespace is also used as the prefix for identifiers defined by this specification. While applications MUST support XML and XML namespaces, the use of internal entities [XML] or our `dsp` XML namespace prefix and defaulting/scoping conventions are OPTIONAL; we use these facilities to provide compact and readable examples.

This specification uses Uniform Resource Identifiers [URI] to identify resources, algorithms, and semantics. The URI in the namespace declaration above is also used as a prefix for URIs under the control of this specification.

This document does not change the namespace URI associated with XML Signature itself.

3 Normative Material and Compliance

3.1 Normative Material

All material in this document is Normative except for examples and sections marked as non-normative.

3.2 Compliance

Use of any or all of these Signature Properties in an XML Signature is OPTIONAL and nothing precludes the use of additional properties defined elsewhere.

[Definition: A **Common Signature Property** is a property defined in this specification and identified by the namespace defined in this document.]

4 Usage scenarios and Requirements

This section is non-normative.

4.1 Mobile Code Signing Scenario

A developer (author) produces code that is delivered to users by a distributor (mobile operator). The code package contains an XML Signature and this should be validated upon code installation to provide integrity for the package. The signature delivered with

the package from the distributor may change upon later installations for various reasons, such as the inclusion of more timely revocation information, so signatures should have an expiration. One goal is not to depend an X509 certificate expiration for this functionality, since that certificate may have a longer lifetime.

This case can introduce requirements for an expiration of a signature as well as identifying the role of a signer (developer or distributor), as well as a possible profile of the general signature standard for that specific use case (such as restricting algorithms etc).

4.2 Mobile Code Signing Requirements

There are specific requirements associated with this use case:

1. Specify any additional constraints on the use of XML Signature, referencing an appropriate profile by URI. This might limit algorithms, for example.

2. Define an expiration with a signature, enabling a validator to determine that the signature should no longer validate after a given time.

3. State the role of the signature creator, e.g. author, distributor etc.

5 Signature Properties

This section includes schema definitions and processing rules for Common Signature Properties.

This section defines a number of signature properties that are expected to be commonly used in profiles. For each property, an intended processing model is suggested. However, the details of processing each of these properties will depend upon individual application scenarios, and MUST be specified in any profile that makes use of the properties defined in this document.

5.1 Profile Property

The Profile Property specifies a URI to be associated with the Signature instance to identify a Profile specification that details how the XML Signature is to be used. This profile may restrict the choice of algorithms, for example, as well as requiring certain Common Signature Properties and/or other properties in the signature.

The element has no content, but specifies a URI attribute that is required.

Example: Schema Definition

```
<element name="Profile" type="dsp:ProfileType"/>
<complexType name="ProfileType">
 <attribute name="URI" type="anyURI"/>
</complexType>
```

5.1.1 Generation

Upon Signature generation, if this property is used, the URI attribute value MUST be set to a value that can be understood by the relying party.

5.1.2 Validation

Applications are expected to use this property to verify an assertion that a signature is meant to fulfill a specific profile. Validation behavior is application-specific.

Profiles MUST specify what application behavior is expected in case an unknown profile URI is encountered.

Profiles MUST specify whether profile URIs defined by them can coexist with other instances of the profile property element.

5.2 Role Property

The Role Property allows a URI to be associated with the signature to specify an application specific role for the signature, implying application specific processing steps related to the signature.

An example might be to indicate that the signer of code is the author or the distributor of that code.

The element has no content, but specifies a URI attribute that is required.

Example: Schema Definition

```
<element name="Role" type="dsp:RoleType"/>

<complexType name="RoleType">
 <attribute name="URI" type="anyURI"/>
</complexType>
```

5.2.1 Generation

Upon Signature generation, if this property is used, the URI attribute value MUST be set to a value that can be understood by the relying party.

5.2.2 Validation

Applications are expected to use this property to identify a specific role for a signature (e.g., author or distributor signed). An unexpected role URI will frequently be reason for applications to deem a signature invalid. Profiles MUST specify what application behavior is expected in case an unknown role URI is encountered, or when several role properties exist on a single signature.

5.3 Expires Property

The Expires Property is intended to enable use cases where the signature is intended to expire.

Example: Schema Definition

```
<element name="Expires" type="dsp:ExpiresType"/>

<xsd:complexType name="ExpiresType" >
  <xsd:extension base="xsd:dateTime">
  </xsd:extension>
</xsd:complexType>
```

Expiration times MUST be given as *timezoned* values. (See section 3.2.7 of [XML Schema part 2].) This property MUST NOT occur more than once for a given signature.

5.3.1 Generation

Upon Signature generation, if this property is used, the time value is set to a reference time, as defined by the application. The value of the time does not need to be from a trusted timestamp authority. The time value needs only be accurate enough for comparison, as required by the application usage.

5.3.2 Validation

Applications are expected to use this property to identify the expiry date of a signature. Evaluation of this property is with respect to an application defined reference time (possibly wall clock time, possibly a time that is determined otherwise). A property value that is later than the reference time will typically be reason for applications to deem a signature invalid with respect to the reference time.

Profiles MUST specify what reference time should be used when interpreting this property.

An expiry property with an *untimezoned* time value MUST NOT be considered valid. If multiple instances of this property are found on a single signature, then applications MUST NOT deem any of these properties valid.

5.4 ReplayProtect Property

To prevent against inappropriate reuse of the signature after its intended use, a replay nonce may be provided. This is a random value that should not be repeated, allowing the verifier to determine that the signature has already been seen. In order to avoid the need to retain nonce values indefinitely, a timestamp is included, indicating that all signatures before that time should be ignored.

This property may be used in applications where the signature is used to secure a message or other applications where it should not be reused.

Example: Schema Definition

```
<element name="ReplayProtect" type="dsp:ReplayProtectType"/>

<xsd:complexType name="ReplayProtectType" >
  <xsd:sequence>
```

```
      <xsd:element name="timestamp" type="xsd:dateTime"/>
      <xsd:element name="nonce" type="xsd:NonceValueType"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="NonceValueType" >
    <xsd:extension base="xsd:string">
      <xsd:attribute name="EncodingType" type="xsd:anyURI"/>
    </xsd:extension>
  </xsd:complexType>
```

Timestamp values MUST be timezoned.

5.4.1 Generation

Upon Signature generation, if this property is used, the nonce value MUST be set to a previously unused random value and the timestamp MUST be set to a time before which the signature is determined to no longer be valid (and for which nonces need not be maintained).

5.4.2 Validation

If timestamp values are untimezoned, validation fails.

Validation succeeds when the relying party is able to determine that the nonce in the property has not been seen before and the current time is after the timestamp recorded in the ReplayProtect property. Otherwise validation fails.

Behavior of applications when an invalid property is encountered is application-specific.

6 Acknowledgments

Thanks to Mark Priestley, Vodafone, and Marcos Caceres, Opera Software, of the W3C Web Applications Working Group for requirements discussions related to widget signing.

Acknowledgements to XML Security WG members TBD.

7 References

SCHEMA2
XML Schema Part 2: Datatypes Second Edition, Paul V. Biron, Ashok Malhotra. W3C Recommendation, 28 October 2004, http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/.

XMLDSIG
XML-Signature Syntax and Processing, D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. W3C Recommendation, 12 February 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.

XMLDSIG2nd
XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008 http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/