XML Digital Signatures Working Group
INTERNET-DRAFT
draft-ietf-xmldsig-requirements-00.txt
Expires December 23, 1999

J. Reagle,
W3C/MIT

XML-Signature Requirements

IETF Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This document is a production of the joint IETF/W3C XML Signature Working Group.

http://www.w3.org/Signature

The latest version of this draft series may be found at:

http://www.w3.org/TR/1999/xmldsig-requirements

XML-Signature Requirements
W3C Working Draft 1999-June-23

This version:
http://www.w3.org/TR/1999/xmldsig-requirements-990623 {ASCII}
http://www.ietf.org/internet-drafts/draft-ietf-xmldsig-requirements-00.txt

Latest version:
http://www.w3.org/TR/1999/xmldsig-requirements

Previous version:

http://www.w3.org/Signatures/Drafts/xml-dsig-requirements-990601

Editor(s):
Joseph Reagle Jr. <reagle@w3.org>

W3C Status of this Document

This is the first Public Working Draft of the IETF/W3C XML-Digital Signature Working Group Requirements document. Its content is based on the Charter [Charter], XML-Signature Workshop [WS], Brown's IETF draft [Brown] and mailing list discussion. This draft will be published prior to the June 25 IETF deadline for consideration at the IETF in Oslo as an IETF-draft and W3C Working Draft. The first draft of a Working Group consensus version should be produced by July.

This document does not necessarily represent the working group's consensus on a finished document; it also includes contrary positions (or alternative wordings) in order to elicit review and discussion. Positions which are potentially in conflict are specified as a list of lettered points. For example:

1 Extensibility
- a. Position
- b. Alternative/Contrary Position

Please send comments to the editor <reagle@w3.org> and cc: the list <w3c-ietf-xmldsig@w3.org>. 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 W3C Drafts as other than "work in progress".A list of current W3C working drafts can be found at http://www.w3.org/TR. Publication as a Working Draft does not imply endorsement by the W3C membership.

Abstract

This document lists the design principles, scope, and requirements for the XML Digital Signature specification. It includes requirements as they relate to the signature syntax, data model, format, cryptographic porcessing, and external requirements and coordination.

Table of Contents

---

1 Introduction

The XML 1.0 Recommendation [XML] describes the syntax of a class of data objects called XML documents. The mission of this working group is to develop an XML compliant syntax used for representing signatures on Web resources and portions of protocol messages (anything that can be referenced by a URI) and procedures for computing and verifying such signatures. Signatures will provide data integrity, authentication, and/or non-repudiatability

2 Design Principles and Scope

1 The XML-Signature specification will describe how to a digitally sign a Web resource in general, and an XML document in particular. [Charter] The specification will not specify methods of providing confidentiality though the Working Group may report on the feasibility of such work in a future or rechartered activity. [List(Bugbee)]
2 The meaning of the signature is very simple: The XML signature syntax associates the cryptographic signature value with Web resources using XML markup.
    1 The WG is not chartered to specify trust semantics, but syntax and processing rules necessary for communicating signature validity (authenticity, integrity and non-repudiation). [Charter(Requirement1)]
    2 The XML signature syntax must be highly extensible such that it can support arbitrary application/trust semantics and assertion capabilities -- that can also be signed. For example, potential trust applications include sophisticated

timestamps, endorsement, and threshold signature schemes. At the Chairs' discretion and in order to test the extensibility the syntax, the WG may produce non-standard-track proposals defining common semantics relevant to signed assertions about

Web resources and their relationships in a schema definition (XML/RDF) or link type definition (XLink). [Charter(Requirement1&4), List(Bugbee, Solo)]

3 Validity and Identity

A. Only enough information necessary to check the validity of the cryptographic signature need be provided. [Reagle]

B. Each signature shall be associated with information to identify the signer and/or the cryptographic information required to validate the signature. [List(Solo)]

3 An XML-Signature can apply to a part or totality of an XML document. [Charter, Brown]

4 More than one signature may exist over any resource.[Charter, Brown]

5 A key use of XML Signatures will be detached Web signatures. In conjunction with XML facilities (including packaging) signatures may be embedded within or encapsulate XML or encoded content. [Charter]

6 The Signature syntax specification will not specify methods of serialization or canonicalization. XML content is normalized by specifying an appropriate content C14N (canonicalization) algorithm [DOMHASH, C14N]; applications are expected to normalize application specific semantics prior to handing data to a XML-Signature application. [Charter]

7 An XML-Signature application must be able to use and understand

1 XML-namespaces [XML-namespaces] within its own signature syntax. Applications may optionally choose C14N algorithms which do or do not process namespaces within XML content.

2 XLink [Xlink]. Applications will use XLink locators within the signature manifest to reference signed resources. Signature applications will not embed or expand XLink references in the signed content, though applications may optionally choose C14N algorithms which provide this feature.

3 XML-Pointers [XPointer]. Applications will reference/select parts of XML documents using XML-Pointer within an XLink locator. [Reagle, WS-list(1)]

8 Implementation/Design Philosophy

A. XML Signatures will be developed as part of the broader Web design philosophy of decentralization, URIs, Web data [WebData], modularity/layering/extensibility, and assertions as statements about statements. [Reagle]

B. The ability to leverage existing cryptographic provider (and infrastructure) primitives is desirable. [List(Solo)]

3 Requirements

Signature Data Model and Syntax

1 The XML-Signature data structures will be predicated on an RDF

data model [RDF] but need not use the RDF serialization syntax. [Charter]

2 XML-Signatures can be applied to any Web resource -- including non-XML content. XML-Signature referents are identified with XML

locators (URIs or fragments) within the manifest that refer to external or internal resources (i.e., network accessible or within the same XML document/package). [Berners-Lee, Reagle, Brown, List(Vincent)]

1 Entries may include explicit content type information. [List(Solo)]

3 XML-Signatures are first class objects themselves and consequently can be referenced and signed. [Berners-Lee, Reagle]

4 Algorithm Identification

A. Whenever possible, any resource or algorithm identifier is a first class object, and addressable by a URI. [Beners-Lee, Reagle]

B. Ability to specify algorithms independently and to reference the algorithms linked to standard algorithm specifications (e.g. OIDs) [List(Solo)]

5 XML-Signatures must be able to apply to the original version of an included/encoded resource. [WS-list (Brown/Himes)]

Format

1 An XML-Signature is XML. [Charter]

2 An XML document of a certain type must still be recognizable as its original type when signed. [WS-summary]

3 XML-Signature will provide a mechanism that facilitates the production of composite documents -- by addition or deletion -- while preserving the signature characteristics (integrity, authentication, and non-repudiatability) of the consituent parts. [Charter, Brown, List(Bugbee)]

4 ?Packaging?

Cryptography

1 The solution shall provide indifferently for digital signature and message authentication codes, considering symmetric and asymmetric authentication schemes as well as dynamic negotiation of keying material. [Brown]

Processing

1 In the event of redundant attributes within the XML Signature syntax and relevant cryptographic blobs, XML Signature applications prefer the XML Signature semantics. [Reagle]

Coordination

The XML Signature specification should meet the requirements of the following applications:

1 Internet Open Trading Protocol v2.0 [Charter]

2 Financial Services Mark Up Language v2.0 [Charter]

To ensure the above requirements are adequately addressed, the XML Signature specification must be reviewed by a designated member of the following communities:

1 XML Syntax Working Group [Charter]
2 XML Linking Working Group [Charter]
3 XML Schema Working Group [Charter]
4 Metadata Coordination Group [Charter]
5 ?W3C Internationalization Interest Group?

4 References

Berners-Lee
Axioms of Web Architecture: URIs.
http://www.w3.org/DesignIssues/Axioms.html

Brown-XML-DSig
Internet Draft. Digital Signatures for XML
http://search.ietf.org/internet-drafts/draft-brown-xml-dsig-00.txt

C14N
XML Canonicalization Requirements.
http://www.w3.org/TR/NOTE-xml-canonical-req

Charter
XML-DSig Charter.
http://www.w3.org/1999/05/XML-DSig-charter-990521.html

DOMHASH
Internet Draft. Digest Values for DOM (DOMHASH)
http://search.ietf.org/internet-drafts/draft-hiroshi-dom-hash-01txt

Infoset-Req
XML Information Set Requirements Note.
http://www.w3.org/TR/NOTE-xml-infoset-req

IOTP-DSig
Internet Draft. Digital Signatures for the Internet Open Trading Protocol
http://www.ietf.org/internet-drafts/draft-ietf-trade-iotp-v1.0-dsig-00.txt

Namespaces
Namespaces in XML Recommendation.
http://www.w3.org/TR/REC-xml-names

Signature List
http://lists.w3.org/Archives/Public/w3c-ietf-xmldsig/

WS (list, summary)
XML-DSig '99: The W3C Signed XML Workshop
http://www.w3.org/DSig/signed-XML99/
http://www.w3.org/DSig/signed-XML99/summary.html

XLink
XML Linking Language
http://www.w3.org/TR/WD-xlink

XML
Extensible Markup Language (XML) Recommendation.
http://www.w3.org/TR/REC-xml

XML-namespaces
Namespaces in XML
http://www.w3.org/TR/REC-xml-names/

XPointer
XML Pointer Language (XPointer)
http://www.w3.org/TR/WD-xptr

WebData
Web Architecture: Describing and Exchanging Data.
http://www.w3.org/1999/04/WebData