XML Digital Signatures Working Group J. Reagle,
INTERNET-DRAFT W3C/MIT
draft-ietf-xmldsig-requirements-03.txt
Expires August 01, 2000

XML Signature Requirements

Copyright Notice

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.

W3C Status of this document

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

http://www.w3.org/Signature

The comparable html draft of this version may be found at

http://www.w3.org/TR/2000/xmldsig-requirements-20000104/

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

http://www.w3.org/TR/xmldsig-core

This Working Draft of XML Signature Requirements is a very stable result of this Working Draft that has been advanced through W3C Last Call and has been published as an IETF Informational RFC. The only changes from the previous version were those necessary to comply with

RFC Editor publication requirements, including the addition of a security considerations section.

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

Patent disclosures relevant to this specification may be found on the WG's patent disclosure page.

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 processing, 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 a XML syntax used for representing signatures on digital content and procedures for computing and verifying such signatures. Signatures will provide data integrity, authentication, and/or non-repudiatability.

This document lists the design principles, scope, and requirements over three things: (1) the scope of work available to the WG, (2) the XML signature specification, and (3) applications that implement the specification. It includes requirements as they relate to the signature syntax, data model, format, cryptographic processing, and external requirements and coordination. Those things that are required are designated as "must," those things that are optional are designated by "may," those things that are optional but recommended are designated as "should."

2. Design Principles and Scope

1. The specification must describe how to sign digital content, and XML content in particular. The XML syntax used to represent a signature (over any content) is described as an XML Signature. [Charter]
2. XML Signatures are generated from a hash over the canonical form of a signature manifest. (In this document we use the term manifest to mean a collection of references to the objects being signed. The specifications may use the terms manifest, package or other terms differently from this document while still meeting this requirement.) The manifest must support references to Web resources, the hash of the resource content (or its canonicalized form), and (optionally) the resource content type. [Brown, List(Solo)] Web resources are defined as any digital content that can be addressed using the syntax of XLink locator [XLink]).
3. The meaning of a signature is simple: The XML Signature syntax associates the content of resources listed in a manifest with a key via a strong one-way transformation.
    1. The XML Signature syntax must be extensible such that it can support arbitrary application/trust semantics and assertion capabilities -- that can also be signed. [Charter(Requirement1&4), List(Bugbee, Solo)]
    2. 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)] At the Chairs' discretion and in order to test the extensibility of the syntax, the WG may produce non-critical-path proposals defining common semantics (e.g., manifest, package, timestamps, endorsement, etc.) relevant to signed assertions about Web resources in a schema definition [XML, RDF] or link type definition [XLink].

   Comment: A more formal definition of a signed resource is below. The notation is "definition(inputs):constraints" where definition evaluates as true for the given inputs and specified constraints.
   signed-resource(URI-of-resource, content, key, signature): (there was some protocol message at a specific time such that "GET(URI-of-resource) = content") AND (sign-doc(content, key, sig))
   sign-doc(content, key, signature): signature is the value of a strong one-way transformation over content and key that yields content integrity/validity and/or key non-repudiability
4. The specification must not specify methods of confidentiality though the Working Group may report on the feasibility of such work in a future or rechartered activity. [List(Bugbee)]
5. The specification must only require the provision of key information essential to checking the validity of the cryptographic signature. For instance, identity and key recovery

information might be of interest to particular applications, but they are not within the class of required information defined in this specification. [List(Reagle)]

6. The specification must define or reference at least one method of canonicalizing and hashing the signature syntax (i.e., the

manifest and signature blocks). [Oslo] The specification must not specify methods of canonicalizing resource content [Charter], though it may specify security requirements over such methods. [Oslo] Such content is normalized by specifying an appropriate content C14N (canonicalization) algorithm [DOMHASH, XML-C14N]. Applications are expected to normalize application specific semantics prior to handing data to a XML Signature application or specify the necessary transformations for this process within the signature. [Charter]

7. XML Signature applications must be conformant with the specifications as follows:
    1. XML-namespaces [XML-namespaces] within its own signature syntax. Applications may choose C14N algorithms which do or do not process namespaces within XML content. For instance, some C14N algorithms may opt to remove all namespace declarations, others may rewrite namespace declarations to provide for context independent declarations within every element.
    2. XLink [Xlink] within its own signature syntax. For any resource identification beyond simple URIs (without fragment IDs) or fragmentIDs, applications must use XLink locators to reference signed resources. Signature applications must not embed or expand XLink references in signed content, though applications may choose C14N algorithms which provide this feature.
    3. XML-Pointers [XPointer] within its own signature syntax. If applications reference/select parts of XML documents, they must use XML-Pointer within an XLink locator. [WS-list(1)]

   The WG may specify security requirements that constrain the operation of these dependencies to ensure consistent and secure signature generation and operation. [Oslo]
8. XML Signatures must be developed as part of the broader Web design philosophy of decentralization, URIs, Web data, modularity/layering/extensibility, and assertions as statements about statements. [Berners-Lee, WebData] In this context, existing cryptographic provider (and infrastructure) primitives should be taken advantage of. [List(Solo)]

3. Requirements

3.1 Signature Data Model and Syntax

1. XML Signature data structures must be based on the RDF data model [RDF] but need not use the RDF serialization syntax. [Charter]
2. XML Signatures apply to any resource addressable by a locator -- 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, Brown, List(Vincent), WS, XFDL]

3. XML Signatures must be able to apply to a part or totality of a XML document. [Charter, Brown]
   Comment: A related requirement under consideration is requiring

the specification to support the ability to indicate those portions of a document one signs via exclusion of those portions one does not wish to sign. This feature allows one to create signatures that have document closure [List(Boyer(1)], retain ancestor information, and retain element order of non-continuous regions that must be signed. We are considering implementing this requirement via (1) a special <dsig:exclude> element, (2) an exclude list accompanying the resource locator, or (3) the XML-Fragment or XPointer specifications -- or a requested change to those specifications if the functionality is not available. See List(Boyer(1,2)) for further discussion of this issue.

4. Multiple XML Signatures must be able to exist over the static content of a Web resource given varied keys, content transormations, and algorithm specifications (signature, hash, canonicalization, etc.). [Charter, Brown]
5. XML Signatures are first class objects themselves and consequently must be able to be referenced and signed. [Berners-Lee]
6. The specification must permit the use of varied digital signature and message authentication codes, such as symmetric and asymmetric authentication schemes as well as dynamic agreement of keying material. [Brown] Resource or algorithm identifier are a first class objects, and must be addressable by a URI. [Berners-Lee]
7. XML Signatures must be able to apply to the original version of an included/encoded resource. [WS-list (Brown/Himes)]

3.2 Format

1. An XML Signature must be an XML element (as defined by production 39 of the XML1.0 specification. [XML])
2. When XML signatures are placed within a document the operation must preserve (1) the document's root element tag as root and (2) the root's descendancy tree except for the addition of signature element(s) in places permitted by the document's content model. For example, an XML form, when signed, should still be recognizable as a XML form to its application after it has been signed. [WS-summary]
3. XML Signature must 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. An important use of XML Signatures will be detached Web signatures. However, signatures may be embedded within or encapsulate XML or encoded content. [Charter] This WG must specify a simple method of packaging and encapsulation if no W3C Recommendation is available.

3.3 Cryptography and Processing

1. The specification must permit arbitrary cryptographic signature and message authentication algorithms, symmetric and asymmetric authentication schemes, and key agreement methods. [Brown]
2. The specification must specify at least one mandatory to implement

signature canonicalization, content canonicalization, hash, and signature algorithm.

3. In the event of redundant attributes within the XML Signature syntax and relevant cryptographic blobs, XML Signature applications prefer the XML Signature semantics.
   Comment: Another possibility is that an error should be generated, however it isn't where a conflict will be flagged between the various function and application layers regardless.
4. The signature design and specification text must not permit implementers to erroneously build weak implementations susceptible to common security weaknesses (such as as downgrade or algorithm substitution attacks).

3.4 Coordination

1. The XML Signature specification should meet the requirements of the following applications:
   1. Internet Open Trading Protocol v1.0 [IOTP]
   2. Financial Services Mark Up Language v2.0 [Charter]
   3. At least one forms application [XFA, XFDL]
2. To ensure that all requirements within this document are adequately addressed, the XML Signature specification must be reviewed by a designated member of the following communities:
   1. XML Syntax Working Group: canonicalization dependencies. [Charter]
   2. XML Linking Working Group: signature referants. [Charter]
   3. XML Schema Working Group: signature schema design. [Charter]
   4. Metadata Coordination Group: data model design. [Charter]
   5. W3C Internationalization Interest Group: [AC Review]
   6. XML Package Working Group: signed content in/over packages.
   7. XML Fragment Working Group: signing portions of XML content.

   Comment: Members of the WG are very interested in signing and processing XML fragments and packaged components. Boyer asserts that [XML-fragment] does not "identify non-contiguous portions of a document in such a way that the relative positions of the connected components is preserved." Packaging is a capability critical to XML Signature applications, but it is clearly dependent on clear trust/semantic definitions, package application requirements, and even cache-like application requirements. It is not clear how this work will be addressed.

4. Security Considerations

This document lists XML Digital Signature requirements as they relate to the signature syntax, data model, format, cryptographic processing, and external requirements and coordination. In that context much of this document is about security.

5. References

AC Review
Misha Wolf. "The Charter should include the I18N WG in the section on 'Coordination with Other Groups.'"

http://lists.w3.org/Archives/Team/xml-dsig-review/1999May/0007.html

Berners-Lee
Axioms of Web Architecture: URIs.
http://www.w3.org/DesignIssues/Axioms.html
Web Architecture from 50,000 feet
http://www.w3.org/DesignIssues/Architecture.html

Brown-XML-DSig
Internet Draft. Digital Signatures for XML
http://www.w3.org/Signature/Drafts/xmldsig-signature-990618.html

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

DOMHASH
Internet Draft. Digest Values for DOM (DOMHASH)
http://www.ietf.org/internet-drafts/draft-ietf-trade-hiroshi-dom-hash-03.txt

FSML
FSML 1.5 Reference Specification
http://www.echeck.org/library/ref/fsml-v1500a.pdf

Infoset-Req
XML Information Set Requirements Note.
http://www.w3.org/TR/1999/NOTE-xml-infoset-req-19990218.html

IOTP
Internet Open Trading Protocol v1.0
http://www.ietf.org/internet-drafts/draft-ietf-trade-iotp-v1.0-protocol-07.txt

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-05.txt

Oslo
Minutes of the XML Signature WG Sessions at IETF face-to-face meeting in Oslo.

RDF
RDF Schema
http://www.w3.org/TR/1999/PR-rdf-schema-19990303

RDF Model and Syntax
http://www.w3.org/TR/1999/REC-rdf-syntax-19990222

Signature WG List

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

URI
Uniform Resource Identifiers (URI): Generic Syntax
http://www.ietf.org/rfc/rfc2396.txt

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/1999/07/WD-xlink-19990726

XML
Extensible Markup Language (XML) Recommendation.
http://www.w3.org/TR/1998/REC-xml-19980210

XML-C14N
XML Canonicalization Requirements.
http://www.w3.org/TR/1999/NOTE-xml-canonical-req-19990605

XFA
XML Forms Architecture (XFA)
http://www.w3.org/Submission/1999/05/

XFDL
Extensible Forms Description Language (XFDL) 4.0
http://www.w3.org/Submission/1998/16/

XML-Fragment
XML-Fragment Interchange
http://www.w3.org/1999/06/WD-xml-fragment-19990630.html

XML-namespaces
Namespaces in XML
http://www.w3.org/TR/1999/REC-xml-names-19990114

XML-schema
XML Schema Part 1: Structures
http://www.w3.org/1999/05/06-xmlschema-1/
XML Schema Part 2: Datatypes
http://www.w3.org/1999/05/06-xmlschema-2/

XPointer
XML Pointer Language (XPointer)
http://www.w3.org/1999/07/WD-xptr-19990709

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

6. Acknowledgements

This document was produced as a collaborative work item of the XML Signature (xmldsig) Working Group.

7. Author's Address

Joseph M. Reagle Jr., W3C
XML Signature Co-Chiar
Massachusetts Institute of Technology
Laboratory for Computer Science
W3C, NE43-350
545 Technology Square
Cambridge, MA 02139
Phone: 1.617.258.7621
E-Mail: reagle@w3.org
URL: http://www.w3.org/People/Reagle

8. Full Copyright Statements

The terms of use of this document is governed by either the IETF or W3C terms. The reader must comply with either the complete IETF or W3C terms but need not comply with both.

IETF

TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.