XDI Signatures V1.0

Edited by Peter Davis and Dan Blum

$Id: oasis-specification-0.6-wd04.xml,v 1.2 2012/06/14 01:57:23 admin Exp $

Standards Track Work Product

http://docs.oasis-open.org/templates/DocBook/spec-1.0/oasis-specification-1.0-wd01.html

http://docs.oasis-open.org/templates/DocBook/spec-1.0/oasis-specification-1.0-wd01.pdf

http://docs.oasis-open.org/templates/DocBook/spec-1.0/oasis-specification-1.0-wd01.xml

http://docs.oasis-open.org/templates/DocBook/spec-0.0/oasis-specification-0.0.html

http://docs.oasis-open.org/templates/DocBook/spec-0.0/oasis-specification-0.0.pdf

http://docs.oasis-open.org/templates/DocBook/spec-0.0/oasis-specification-0.0.xml

http://docs.oasis-open.org/templates/DocBook/oasis-specification/oasis-specification.html

http://docs.oasis-open.org/templates/DocBook/oasis-specification/oasis-specification.pdf

http://docs.oasis-open.org/templates/DocBook/oasis-specification/oasis-specification.xml

OASIS XRI Data Interchange (XDI) TC [https://www.oasis-open.org/apps/org/workgroup/xdi/]

Additional artifacts

This Working Draft 01 is part of a broader suite of specifications collectively referred to as XDI 1.0. The following specifications constitute the complete suite:

- XDI Core [XDICore]
- XDI Messaging [XDIMsg]
- XDI Discovery [XDIDisc]
- XDI Policy [XDIPolicy]
- XDI Security Mechanisms [XDISec]
- XDI Privacy [XDIPriv]
- XDI Dictionary [XDIDictionary]
- XDI Signature [XDISig]

Notices

25 July 2013

Abstract

This Working Draft 01 specifies security requirements and mechanisms suitable to authenticate, integrity protect and provide confidentiality of information in a graph as a set of conformance profiles. In addition, it defines a template for the creation of additional profiles.

Table of Contents

Introduction

Related Publications

This Working Draft 01 is part of a broader suite of specifications collectively referred to as XDI 1.0. The following specifications constitute the complete suite:

- XDI Core [XDICore]
- XDI Messaging [XDIMsg]
- XDI Discovery [XDIDisc]
- XDI Policy [XDIPolicy]
- XDI Security Mechanisms [XDISec]
- XDI Privacy [XDIPriv]
- XDI Dictionary [XDIDictionary]
- XDI Signature [XDISig]

Terminology

Key words

The key words *MUST*, *MUST NOT*, *REQUIRED*, *SHALL*, *SHALL NOT*, *SHOULD*, *SHOULD NOT*, *RECOMMENDED*, *MAY*, and *OPTIONAL* are to be interpreted as described in [RFC 2119].

Glossary of Terms

XDI	XRI Data Interchange
Normalized Graph	the canonical form of the graph, necessary to ensure successful signature validation.
Signature Block	a collection of XDI statements describing metadata about the signature sufficient to ensure successful validation, and the signature itself.

Usage

XDI requests and responses SHOULD be signed, to ensure message integrity and authenticity. [XDISec] defines other mechanisms to achieve integrity and authenticity. This specification defines signatures that require SHA-256 [SHA] or greater hashing, and allows for HMAC [RFC2104], RSA [RFC3447] and ECDSA ??? algorithms. In the future, additional hashing and encryption algorithms may be added.

Signatures over sub-graphs are established in a manner such that the signature may be included in the graph. The signature covers the entire XDI subgraph rooted in that context node at that point in time. In some cases, the signature was made with a key not rooted in the graph from which the signature was obtained.

Recipients of signed XDI messages SHOULD validate all signatures present in the response graph.

Key Material Representations

TBD

Signature Metadata

To construct the *Signature Block*, the following statements MUST be added to the *Normalized Graph*:

Signature Algorithm

The Algorithm *Signature Block* statement identifies the cryptographic algorithm used to secure the signature.

Example 1. Signature Algorithm

```
(=markus=peterd/+friend)<$sig>/$is#/$sha$256$rsa
```

Signature Processing Rules

Canonical Representation

Signing XDI messages involves first normalizing to the XdiFlatSerialization as defined in [XDICore], and afterwards, incorporation of a *Signature Block* in a manner not disruptive to validators.

XdiFlatSerialization is the only serialization format used for signature creation and validation. Implementations that choose to transfer XDI messages in another serialization format MUST serialize the message in XdiFlatSerialization prior to attempting validation.

Canonicalization Process

The following steps MUST be performed in this order to produce the *Normalized Graph*. These requirements apply to message senders as well as message recipients.

1. Ensure the sub-graph is UTF-8 encoded and formatted as defined in XDI Flat Serialization defined in [XDICore].

2. All unquoted white space and new lines MUST be removed (TODO: better clarify white space. should this go into XdiFlatSerialization?)

3. All JSON [RFC 4627] keys in the unsigned graph MUST be sorted in UTF-8 [RFC3629] byte-order.

Graph Signatures

Message Signatures

Algorithms

Security Considerations

Normative References

[RFC 2119] Key words for use in RFCs to Indicate Requirement Levels, March 1997. S. Bradner. IETF (Internet Engineering Task Force) RFC 2119, *http://www.ietf.org/rfc/rfc2119.txt*

[RFC 4627] The application/json Media Type for JavaScript Object Notation (JSON), July 2006. D. Crockford. IETF (Internet Engineering Task Force) RFC 4627, *http://www.ietf.org/rfc/rfc4627.txt*

[XDICore] XDI Core version , June 2014 Drummond Reed . OASIS *XDICore*

[XDIMsg] XDI Messaging version , June 2014 Drummond Reed . OASIS *XDIMsg*

[XDIDisc] XDI Discovery version , June 2014 Drummond Reed . OASIS *XDIDisc*

[XDIPolicy] XDI Policy version , June 2014 Drummond Reed . OASIS *XDIPolicy*

[XDISec] XDI Security Mechanisms version , June 2014 Peter Davis . OASIS *XDISec*

[XDIPriv] XDI Privacy version , June 2014 Peter Davis . OASIS *XDIPriv*

[XDIDictionary] XDI Dictionary version , June 2014 Drummond Reed . OASIS *XDIDictionary*

[XDISig] XDI Signatures version , June 2014 Peter Davis . OASIS *XDISig*

[RFC3629] UTF-8, a transformation format of ISO 10646 November 2003 F. Yergeau IETF

[RFC2104] HMAC: Keyed-Hashing for Message Authentication February 1997 H. Krawczyk M. Bellare R. Canetti IETF

[RFC3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 February 2003 J. Jonsson B. Kaliski IETF

[SHA] Secure Hash Standard NIST FIPS PUB 180-4 March 2012 F. Yergeau National Institute of Standards and Technology, U.S. Department of Commerce

A. Examples

Graph Signature Examples

Message Signature Examples