
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/>]

Copyright © 2014 OASIS Open, Inc. All Rights Reserved.

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

Copyright © OASIS® Open 2012. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at <http://www.oasis-open.org/who/intellectualproperty.php>.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical

Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS [<http://www.oasis-open.org>], the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

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	3
Related Publications	3
Terminology	3

Key words	3
Glossary of Terms	3
Usage	4
Key Material Representations	4
Signature Metadata	4
Signature Algorithm	4
Signature Processing Rules	4
Canonical Representation	4
Graph Signatures	5
Message Signatures	5
Algorithms	5
Security Considerations	5
Normative References	5
A. Examples	5
Graph Signature Examples	5
Message Signature Examples	5

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