Workgroup: Network Working Group
Internet-Draft: draft-young-md-query-saml-18
Published: 6 January 2023
Intended Status: Informational
Expires: 10 July 2023
A I.A. Young, Ed.
uIndependent
t
h
o
r
s
:

SAML Profile for the Metadata Query Protocol

Abstract

This document profiles the Metadata Query Protocol for use with SAML metadata.

This document is a product of the Research and Education Federations (REFEDS) Working Group process.

Editorial Note (To be removed by RFC Editor before publication)

Discussion of this draft takes place on the MDX mailing list (mdx@lists.iay.org.uk), which is accessed from [MDX.list].

XML versions, latest edits and the issues list for this document are available from [md-query].

The changes in this draft are summarized in Appendix A.19.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 10 July 2023.

Table of Contents

1. Introduction

This document profiles the Metadata Query Protocol [I-D.young-md-query] for use with SAML metadata [SAML2Meta].

The Research and Education Federations group ([REFEDS]) is the voice that articulates the mutual needs of research and education identity federations worldwide. It aims to represent the requirements of research and education in the ever-growing space of access and identity management.

From time to time REFEDS will wish to publish a document in the Internet RFC series. Such documents will be published as part of the RFC Independent Submission Stream [RFC4844]; however the REFEDS working group sign-off process will have been followed for these documents, as described in the REFEDS Participant's Agreement [REFEDS.agreement].

This document is a product of the REFEDS Working Group process.

1.1. Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document makes use of the Augmented BNF metalanguage defined in [STD68].

2. Request Profile

2.1. Content Type

Requests compliant with this profile MUST include the following HTTP header to indicate that the metadata returned should be SAML metadata (see Appendix A of [SAML2Meta]):

```
Accept: application/samlmetadata+xml
```

2.2. Identifiers

2.2.1. Unique Identifier

Each entity known to the responder MUST be associated with the unique identifier of the entity, corresponding to the entityID attribute of the entity's EntityDescriptor element in SAML metadata.

2.2.2. Transformed Identifier

SAML 2.0 [SAML2Core] includes profiles based on the transfer of an "artifact" containing the unique identifier of a SAML entity transformed by means of the SHA-1 [RFC3174] hash algorithm (see [SAML2Bind] sections 3.6 and 3.6.4).

In order to support use cases in which clients may be in possession of only such a transformed representation of a SAML entity's unique identifier without any way to establish the original entity identifier, a responder compliant with this profile MUST associate each entity with an identifier matching the sha1id production in the following ABNF grammar, and treat such an identifier as equivalent to the corresponding untransformed identifier:

```
SHA1     = %x73 %x68 %x61 %x31 ; lower case "sha1"
DIGIT    = %x30-39
HEXDIGIT = DIGIT | %x61-66 ; lower case a-f
sha1id   = "{" SHA1 "}" sha1hex
sha1hex  = 40*HEXDIGIT
```

In the above, the sha1hex component encodes the 20-octet (160-bit) binary SHA-1 hash value as a sequence of 40 lower case hexadecimal digits.

For example, the identifier

```
http://example.org/service
```

transformed by means of SHA-1 hashing would become

```
{sha1}11d72e8cf351eb6c75c721e838f469677ab41bdb
```

Responder implementations MAY detect malformed SHA-1 transformed identifiers (for example where the string of characters following the "}" contains characters other than hexadecimal digits, or is other than exactly 40 characters in length) and return an HTTP status code of 400 ("bad request"). Alternatively, implementations MAY process these as normal identifiers and return an HTTP status code of 404 ("not found") if appropriate.

2.2.3. Additional Identifiers

Entities MAY also be associated with any number of additional responder-defined identifiers naming arbitrary groups of entities.

3. Response Profile

3.1. Response Cardinality

A request may return information for any number of entities, including none. Responses compliant with this profile MUST use the appropriate representation described below depending on the number of EntityDescriptor elements returned.

3.1.1. No Entity Descriptors Returned

A response which returns no EntityDescriptor elements MUST be represented by an HTTP status code of 404 ("not found").

3.1.2. One Entity Descriptor Returned

A response which returns a single EntityDescriptor element MUST use that element as its document element. The responder MUST NOT make use of a EntitiesDescriptor element in this situation (see [SAML2Meta] section 2.3).

Such a response MUST include the following HTTP header to indicate that the metadata returned is SAML metadata:

```
Content-Type: application/samlmetadata+xml
```

3.1.3. More Than One Entity Descriptor Returned

A response which returns more than one EntityDescriptor element MUST consist of a document element which is an EntitiesDescriptor element, containing the returned EntityDescriptor elements as children. Responses MUST NOT contain nested EntitiesDescriptor elements.

Such a response MUST include the following HTTP header to indicate that the metadata returned is SAML metadata:

```
Content-Type: application/samlmetadata+xml
```

4. Security Considerations

4.1. Integrity

As SAML metadata contains information necessary for the secure operation of interacting services it is strongly RECOMMENDED that a mechanism for integrity checking is provided to clients.

It is RECOMMENDED that the integrity checking mechanism provided by a responder is a digital signature embedded in the returned metadata document, as defined by [SAML2Meta] section 3.

Such digital signatures:

* SHOULD use an RSA keypair whose modulus is no less than 2048 bits in length.
* MUST NOT use the SHA-1 cryptographic hash algorithm as a digest algorithm.
* MUST NOT use the MD5 cryptographic hash algorithm as a digest algorithm.
* SHOULD otherwise follow current cryptographic best practices in algorithm selection.

4.2. Use of SHA-1 in Transformed Identifiers

This profile mandates the availability of an identifier synonym mechanism based on the SHA-1 cryptographic hash algorithm. Although SHA-1 is now regarded as weak enough to exclude it from use in new cryptographic systems, its use in this profile is necessary for full support of the SAML 2.0 standard.

The use of SHA-1 in section 3.6.4 of [SAML2Bind], and its resulting use in this protocol, would be vulnerable to an attack in which metadata was introduced into a system by an attacker capable of creating an entity identifier with the same SHA-1 hash as that of an existing entity's identifier.

Such an identifier is known as a *second preimage* of the original, and SHA-1's resistance to discovery of it is referred to as SHA-1's *second-preimage resistance*.

As demonstrated by the the [SHAttered] and [Shambles] attacks, the SHA-1 algorithm is known to have weak collision resistance. However, at the time of writing no attacks are known on SHA-1's second-preimage resistance; a result in this area would be required to provide the basis of an attack based on duplicating the SHA-1 hash of an existing identifier. As a result, the use of SHA-1 in SAML and in this protocol is not believed to introduce a security concern.

Implementations may guard against the possibility of a future practical attack on the second-preimage resistance of SHA-1 by treating two entities whose entityID values have the same SHA-1 equivalent as an indicator of malicious intent on the part of the owner of one of the entities.

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgements

The editor would like to acknowledge the following individuals for their contributions to this document:

*Scott Cantor (The Ohio State University)

*Leif Johansson (SUNET)

*Joe St Sauver (University of Oregon)

*Tom Scavo (Internet2)

7. References

7.1. Normative References

[I-D.young-md-query] Young, I.A., Ed., "Metadata Query Protocol", Work in Progress, Internet-Draft, draft-young-md-query-18, January 2023, <https://datatracker.ietf.org/doc/html/draft-young-md-query-18>.

[RFC2119] Bradner, S. and RFC Publisher, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3174] Eastlake 3rd, D., Jones, P., and RFC Publisher, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, DOI 10.17487/RFC3174, September 2001, <https://www.rfc-editor.org/info/rfc3174>.

[RFC8174] Leiba, B. and RFC Publisher, "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SAML2Bind] Cantor, S., Hirsch, F., Kemp, J., Philpott, R., and E. Maler, "Bindings for the Security Assertion Markup

Language (SAML) V2.0", OASIS Standard saml-bindings-2.0-os, March 2005.

[SAML2Meta] Cantor, S., Moreh, J., Philpott, R., and E. Maler, "Metadata for the Security Assertion Markup Language (SAML) V2.0", OASIS Standard saml-metadata-2.0-os, March 2005, <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.

[STD68] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

7.2. Informative References

[md-query] Young, I.A., Ed., "md-query Project", <https://github.com/iay/md-query>.

[MDX.list] Young, I.A., Ed., "MDX Mailing List", <http://lists.iay.org.uk/listinfo.cgi/mdx-iay.org.uk>.

[REFEDS] Research and Education Federations, "REFEDS Home Page", <http://www.refeds.org/>.

[REFEDS.agreement] Research and Education Federations, "REFEDS Participant's Agreement", <https://refeds.org/about/about_agreement.html>.

[RFC4844] Daigle, L., Ed., IAB, and RFC Publisher, "The RFC Series and RFC Editor", RFC 4844, DOI 10.17487/RFC4844, July 2007, <https://www.rfc-editor.org/info/rfc4844>.

[SAML2Core] Cantor, S., Kemp, J., Philpott, R., and E. Maler, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard saml-core-2.0-os, March 2005, <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.

[Shambles] "SHA-1 is a Shambles", January 2020, <https://shambles.github.io>.

[SHAttered] "SHAttered", February 2017, <https://shattered.io>.

Appendix A. Change Log (to be removed by RFC Editor before publication)

A.1. draft-young-md-query-saml-00

Initial version.

A.2. Since draft-young-md-query-saml-00

Added REFEDS RFC stream boilerplate.

A.3. Since draft-young-md-query-saml-01

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

Rework Section 2.2 to make the role of transformed identifiers clearer. This changes the semantics slightly (malformed transformed identifiers may now result in a 404 return rather than 400) but this gives implementers more latitude in the way that they handle the feature.

A.4. Since draft-young-md-query-saml-02

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.5. Since draft-young-md-query-saml-03

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

Added an Editorial Note to help direct readers back to the discussion.

A.6. Since draft-young-md-query-saml-04

Fix reference to the Metadata Query Protocol [I-D.young-md-query].

A.7. Since draft-young-md-query-saml-05

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.8. Since draft-young-md-query-saml-06

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.9. Since draft-young-md-query-saml-07

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.10. Since draft-young-md-query-saml-08

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

Modernise normative language to include [RFC8174].

Improved references to RFCs.

A.11. Since draft-young-md-query-saml-09

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.12. Since draft-young-md-query-saml-10

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

Replace citations in the abstract with straight textual mentions, as required by the ID-NITS checklist.

A.13. Since draft-young-md-query-saml-11

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

Strengthen Section 4.1 so that SHA-1 now MUST NOT be used in the context of digital signatures. This brings the section in line with

current best practice recommendations, particularly in light of the [SHAttered] and [Shambles] attacks.

Revised Section 4.2 on the use of SHA-1 in transformed identifiers to:

- Make clear that this is a SAML-level issue, not one introduced by the query protocol.
- Reference the attacks demonstrating SHA-1's weak collision resistance.
- Identify second-preimage resistance as the potential source of the attack we'd be concerned about for the query protocol.
- Note that SHA-1's second-preimage resistance is at present uncompromised.

A.14. Since draft-young-md-query-saml-12

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.15. Since draft-young-md-query-saml-13

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.16. Since draft-young-md-query-saml-14

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.17. Since draft-young-md-query-saml-15

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.18. Since draft-young-md-query-saml-16

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

A.19. Since draft-young-md-query-saml-17

Bump reference to the Metadata Query Protocol [I-D.young-md-query].

Author's Address

Ian A. Young (editor)
Independent

Email: ian@iay.org.uk