Network Working Group I. Young, Ed.
Internet-Draft Independent
Intended status: Informational December 29, 2013
Expires: July 2, 2014

SAML Profile for the Metadata Query Protocol
draft-young-md-query-saml-00

Abstract

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

Status of This Memo

This Internet-Draft will expire on July 2, 2014.

Copyright Notice

Table of Contents

1. Introduction

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

1.1. Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [BCP14].

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

Each identifier in a request may be either:

- The unique identifier of an entity, corresponding to the "entityID" attribute of the entity's "EntityDescriptor" element in SAML metadata, or

- The responder-defined identifier of an arbitrary group of entities.

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 accept an extended identifier matching the "sha1id" production in the following ABNF grammar as 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
```

Malformed SHA-1 transformed extended 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, MUST result in an HTTP status code of 400 ("bad request").

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.

- SHOULD 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 a 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.

Because the SHA-1 cryptographic hash is not being used within this profile in the context of a digital signature, it is not believed to introduce a security concern over and above that which already exists in SAML due to the possibility of a post-hash collision between entities whose "entityID" attributes hash to the same value.

Implementations may guard against this possibility 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

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[I-D.young-md-query] Young, I., Ed., "Metadata Query Protocol", draft-young-md-query-01 (work in progress), December 2013.

[RFC3174] Eastlake, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

[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.

[STD68] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

7.2. Informative References

[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>.

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

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

Initial version.

Author's Address

Ian A. Young (editor)
Independent

EMail: ian@iay.org.uk