eduGAIN Policy Framework Metadata Profile

Version date	Editor	Change
13.11.2012	tl	First draft addressing comments as collected by eduGAIN-policy. Comment MET-12 on attribute scopes still needs to be addressed
4.12.2012	tl	Second draft with many changes and still a number of open points!
18.1.2013	tl	Third draft dropped the ToU references. Still a few points open.
25.1.2013	tl	Fourth draft includes the comments from Ian. Scopes to be covered in the attribute profile.
15.2.2013	tl	Final Draft. Dropping the downstream metadata. That should all go into the MDS Aggregation Practice Statement [MAPS].

Introduction

The eduGAIN metadata profile defines rules for SAML metadata producers that plan to submit their metadata to the eduGAIN Metadata Service (MDS) for aggregation. A metadata producer can act in the role of a registrar and/or aggregator.

Adopting this profile lays the ground for scalable SAML interoperability.

This profile is based on [SAMLMetaIoP]. Whatever is specified in the SAML V2.0 Metadata Interoperability Profile is also valid within this eduGAIN Metadata Profile.

1 Requirements Notation

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 [RFC2119].

2 References to SAML 2.0 specification

`saml2` `urn:oasis:names:tc:SAML:2.0:assertion`

The SAML 2.0 Assertion namespace defined in the SAML 2.0 Core specification [SAMLCore].

`md` `urn:oasis:names:tc:SAML:2.0:metadata`

The SAML V2.0 metadata namespace defined in the SAML V2.0 Metadata specification [SAMLMeta].

`mdrpi` `urn:oasis:names:tc:SAML:metadata:rpi`

The namespace defined in the SAML V2.0 Metadata Extensions for Registration and Publication Information [MDRPI].

`mdui` `urn:oasis:names:tc:SAML:metadata:ui`

The namespace defined in SAML V2.0 Metadata Extensions for Login and Discovery User Interface [MDUI].

3 Additional eduGAIN Metadata Producer Requirements

The metadata root element MUST contain

- validUntil attribute with a value not later than 28 days after the signature timestamp

it SHOULD contain

- <mdrpi:PublicationInfo>, it MUST contain
  - publisher

  it SHOULD contain one of the attributes
  - creationInstant or publicationID

If the metadata root element contains

- cacheDuration attribute, its value SHOULD be between one hour and six hours.
  The MDS takes it as an advice on how long to cache it. The MDS Aggregation Practice Statement [MAPS] will describe the details.

Note on validUntil: setting validUntil to an instant very close to the signing timestamp (i.e., using a very short validity "window") can cause interoperability problems in cases where a consumer does not refresh metadata very often, or where a consumer cannot reach the producer due to transient system or network failures.

Note on validUntil: [SAML Core] RECOMMENDS in 2.3.1 and 2.3.2 that only the root element of a metadata instance contains a validUntil attribute.

Each <md:EntityDescriptor> element MUST contain

- <mdrpi:RegistrationInfo>, it MUST contain
  - registrationAuthority with a value that has been registered with the eduGAIN OT

  it SHOULD contain
  - registrationInstant
  - <mdrpi:RegistrationPolicy>

it SHOULD contain

- <md:Organization> with values in English and as appropriate also values in the service's native languages for the elements
  - <md:OrganizationName>
  - <md:OrganizationDisplayName>
  - <md:OrganizationURL>
- <md:ContactPerson> with contactType="technical" and/or contactType="support".
  If present, <md:EmailAddress> SHOULD not be a personal address but a role address to get in contact with the entity's responsible persons.

If the <md:EntityDescriptor> contains one of these elements:

- <md:IDPSSODescriptor>
- <md:SPSSODescriptor>

each one of them SHOULD contain the elements:

- <mdui:DisplayName> with a value in English and as appropriate also values in the languages supported by the service
- <mdui:Description> with a value in English and as appropriate also values in the languages supported by the service

NOTE on <md:RequestedAttribute>: Whenever a Service Provider needs attributes it should list them as <md:RequestedAttribute> in the <md:AttributeConsumingService> of its <md:SPSSODescriptor> element to increase the chance that Identity Providers really release them.

If a metadata producer aggregates metadata from multiple sources, the <mdrpi:PublicationPath> element SHOULD be used where appropriate.

For signing its metadata, a metadata producer MUST use an RSA private key of at least 2048 bits.

4 eduGAIN Metadata Conformance

A metadata producer conforms to this profile if it conforms to:

- SAML V2.0 Metadata Interoperability Profile [SAMLMetaIoP]
- Additional eduGAIN Metadata Producer Requirements in chapter 3 above

References

[MAPS]	Metadata Service Aggregation Practice Statement to be written by eduGAIN OT
[MDRPI]	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0, Committee Specification 01, 03 April 2012. http://wiki.oasis-open.org/security/SAML2MetadataDRI
[MDUI]	SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, Committee Specification 01, 03 April 2012. http://wiki.oasis-open.org/security/SAML2MetadataUI
[RFC2119]	S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, March 1997. http://www.ietf.org/rfc/rfc2119.txt
[SAMLCore]	OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[SAMLErr]	SAML V2.0 Approved Errata 05. 01 May 2012 http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf
[SAMLMeta]	OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
[SAMLMetaIoP]	OASIS SAML V2.0 Metadata Interoperability Profile Version 1.0, currently in Committee Specification 01, 4 August 2009 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf