eduGAIN Policy Framework Metadata Profile (REQUIRED)

Version date	Editor	Change
15.9.2010	TL	Changes based on the Call for Comments

Introduction

The eduGAIN metadata profile defines rules for SAML metadata producers (acting in the role of a registrar or aggregator) and metadata consumers participating in the eduGAIN interfederation service.

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 'SAML 2.0 Core specification' [SAMLCore]

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

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

`ds`   `http://www.w3.org/2000/09/xmldsig#`

The XML Signature namespace [XMLSig]

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

The namespace defined in 'SAML Metadata Document and Registration Information Extension' [MDAttribs]

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

The namespace defined in 'SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0' [MDUI]

3 Additional eduGAIN Metadata Producer Requirements

The metadata root element

MUST contain

- <dri:DocumentInfo> element with
  - <dri:CreationInstant> or <dri:SerialNumber>
  - <dri:UsagePolicy>

Each <md:EntityDescriptor> element

MUST contain the elements

- <md:ContactPerson> with contactType "technical" with the element
- <md:EmailAddress> which SHOULD be a role address and not a personal address.
- <dri:RegistrationInfo> with the elements
  - <dri:RegistrationAuthority>
  - <dri:RegistrationInstant>
  - <dri:RegistrationPolicy>
- <dri:DocumentInfo> (unless the list of contained <dri:Publisher> elements would be empty) with the element
  - <dri:Publishers> with a list of <dri:Publisher> elements.

SHOULD contain the elements

- <md:Organization> with values in English for the elements
  - <md:OrganizationName>
  - <md:OrganizationDisplayName>
  - <md:OrganizationURL>
- <md:Organization> with values in the service's native languages for its elements
  - <md:OrganizationName>
  - <md:OrganizationDisplayName>
  - <md:OrganizationURL>

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

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

each one of them

SHOULD contain the elements

- <mdui:DisplayName> with a value in English
- <mdui:DisplayName> with a value in the languages the service supports, other than English
- <mdui:Description> with a value in English
- <mdui:Description> with a value in the languages the service supports, other than English

Each <md:SPSSODescriptor> element

MAY contain an element

- <md:AttributeConsumingService> that lists all attributes requested by this SP as <md:RequestedAttribute> element with isRequired="true" for required attributes and isRequired="false" for just useful attributes.

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

A metadata consumer conforms to this profile if it conforms to

- SAML V2.0 Metadata Interoperability Profile [SAMLMetaIoP]

References

[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

[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

[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

[SAMLErr] SAML V2.0 Approved Errata. December 2009. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf

[XMLSig] D. Eastlake et al. XML-Signature Syntax and Processing. World Wide Web Consortium Recommendation. February 2002. http://www.w3.org/TR/xmldsig-core/

[MDAttribs] SAML Metadata Document and Registration Information Extension, currently in Draft 02, 29 March 2010. https://spaces.internet2.edu/download/attachments/9731/saml_md_dri_02.odt

[MDUI] SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, currently in Working Draft 02, 7 September 2010. http://www.oasis-open.org/committees/download.php/39243/draft-sstc-saml-metadata-ui-02.pdf

[RFC2119] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, March 1997. http://www.ietf.org/rfc/rfc2119.txt

Changelog

The Changelog is primarily a reference for the eduGAIN-Policy group, it can be removed from the document to be submitted.

0.7 - 20100915

- added reference to SAML 2 Approved Errata
- mdui: namespace reference adapted to OASIS working draft version.
- Dropped specific value requirements for validUntil and cacheDuration this should be covered in specific profiles like WebSSO.
- Replaced the MUST requirements for English descriptive values with SHOULD
- Dropped the SHOULD requirement for admin contact and MUST requirement for support contacts. Upgraded tech contact from SHOULD to MUST with a SHOULD for a role based address.
- Dropped all NameIDFormat and embedded key length requirements. They should go into specific profiles like WebSSO.
- Dropped the requirements for published metadata registration and aggregation practice statements. This should go into the eduGAIN Metadata Aggregation Practice Statement as requirements to Participating Fedeartions.
- Dropped chapter 'Further Reading'.
- Dropped chapter ‘To Do’.
- Dropped the addendum 'eduGAIN *pre-pilot limited* metadata profile'.

0.6 - 20100623

- To Do chapter added
- Correct references and use of XML name spaces for the elements
- Relaxed requirements for <md:ContactPerson> elements. Dropped MUST for GivenName and SurName and OPTIONAL for TelephoneNumber only EmailAddress remains as MUST.
- <dri:DocumentInfo> is only a MUST if the list of contained <dri:Publisher> elements is not empty.
- Added a MUST for <md:NameIDFormat> transient for IdP endpoints.
- Added a SHOULD for <md:NameIDFormat> persistent for IdP endpoints.
- Added that each RSA public key SHOULD be embedded within a <ds:X509Certificate>
- Reference to the eduGAIN Data Protection Profile [eduGAINDPP] moved from the SPSSODescriptor, to a requirement for Metadata Registrars within the 'metadata registration practice statement'.
- Slightly changed semantics for <md:ContactPerson> contactType values to align it better with [saml2int].

0.5 - 20100525

- dropped this reference since we no longer make use of Entity Attributes: 'SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, Committee Specification 01, 4 August 2009' http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html
- New section 'Further Reading' with reference to [saml2int]
- New reference to eduGAIN Data Protection Profile [eduGAINDPP]
- validUntil has no longer a pre-defined range of 1 to 5 days. The max validity has influence on revocation. It is up to the aggregation practice statement to define the validity period an aggregator accepts from publishers.
- no validUntil in each EntityDescriptor, require it only at the root level.
- refer to 'RSA public key' instead of 'embedded X.509 certificate'
- SPSSODescriptor SHOULD (instead MUST) contain an RSA key. We do not want to be more limiting than [saml2int].
- Support for scoping is not part of this profile. The metadata aggregation practice statement should state how an aggregator deals with scopes.
- SPSSODescriptor element MAY (instead of SHOULD) contain an AttributeConsumingService listing attribute requirements.
- For SAML 2 endpoints, RequestedAttributes MUST use urn:oid format, otherwise the urn format should be used.
- New MUST requirement for signing metadata with 2048 bits RSA key

0.4 - 20100305

- validUntil requirement detailed
- cacheDuration requirement added
- Open question on scoping requirements added
- Interpretation of ContactPerson types added
- RequestedAttribute NameFormat URI required
- SPSSODescriptor needs only an embedded certificate if at least one endpoint is not SSL/TLS protected
- a new version of [MDAttribs] came out. It replaces Metadata Document Processors with DocumentInfo element. It specifies also the RegistrationInfo element
- DocumentInfo in the root element as SHOULD for pre-pilot, MUST later on.
- do not require ServiceName and ServiceDescription for SPSSODescriptors, but use the DisplayName and Description elements from [MDUI]
- for the pre-pilot: RegistrationAuthority SHOULD not MUST