12 July 2017

eduGAIN Policy Framework

SAML Profile

Document Revision History

Version	Date	Description of Change	Person
0.1	06-07-2017	Draft version	N Harris
0.2	13-07-2017	Restructuring, references, layout harmonization	L Hämmerle

eduGAIN Policy Framework

SAML Profile

Contents

1 Introduction

1.1 Overview

This document defines the rules for eduGAIN Participant Federations that support the use of SAML within their federations. When supporting SAML entities and publishing these entities to the eduGAIN Metadata Service (MDS) Participant Federations become SAML Metadata Producers.

SAML Metadata Producers are listed on the eduGAIN website [eduGAIN-FEDS] and submit their metadata to the eduGAIN Metadata Service (MDS) for aggregation.

The role that the eduGAIN Operational Team takes in supporting this profile is described in the eduGAIN Operational Practice statement [eduGAIN-OP] and the eduGAIN Metadata Aggregation Practice Statement [eduGAIN-MAPS].

For entities within Federations, eduGAIN supports a series of Best Current Practice documents that are supported by the eduGAIN Steering Committee and published on the eduGAIN website

[eduGAIN-BCP]. SAML Metadata Producers SHOULD support all the Best Current Practice published by eduGAIN within their Federations.

1.2 Terms

AAI	Authentication and authorisation infrastructure.
eduGAIN	eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) via its Member Federations by offering a policy framework, consolidated metadata and shared governance for the eduGAIN service.
eduGAIN Policy Declaration	The agreement signed by Federations on joining eduGAIN.
eduGAIN Operational Practice Statement	A document which covers any issues relevant to ensure the integrity and availability of tools centrally operated by eduGAIN to support Technology Profiles.
eduGAIN Steering Group (eSG)	eduGAIN Steering Group is a body that consists of Member Federations' representatives and has an oversight role in the eduGAIN service, as defined in section 2.2 of the eduGAIN Constitution [eduGAIN-CONST]
Entity	Entity means an AAI endpoint. For example, an Entity can be an Identity Provider, a Service Provider or an Attribute Provider. In this document, an Entity refers to an entity's metadata that a Participant Federation has exchanged through eduGAIN.
Federation	Identity federation. An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions. Federations are typically represented in eduGAIN by a Federation Operator.
Federation Operator	Organisation providing or commissioning the infrastructure for Authentication and Authorisation to the members of its Federation.
Home Organisation	The organisation with which the end users are affiliated. It is responsible for managing end users' identity data (attributes) and authenticating them. The Home Organisation is responsible for setting up and operating one or more Identity Providers, either by itself or via an outsourced service. In this document, a Home Organisation refers to a home organisation who is a member of a Federation.
Identity Provider	A server acting in an Identity Provider role. The system that issues assertions on behalf of end users of a Home Organisation who use them to access services of Service Providers.
Interfederation	Sharing of federation metadata to allow a user from one federation to access a service which is registered in another federation.

eduGAIN Member Federation	A Federation which has met the joining requirements for eduGAIN as defined in section 3.2 of the eduGAIN Constitution [eduGAIN-CONST]
eduGAIN Operational Team (OT)	eduGAIN Operational Team, as defined in section 2.3 of the eduGAIN Constitution [eduGAIN-CONST]
Participant Federation	A Member Federation that is actively participating in eduGAIN having met the requirements defined in section 3.3 of the eduGAIN Constitution [eduGAIN-CONST]
eduGAIN Policy Framework	A set of documents which includes this document (SAML Profil), the eduGAIN Constitution and the eduGAIN Policy Declaration, which is signed by Member Federations.
Service Provider	An organisation that is responsible for offering the end user the service s/he is going to use via a federated login.
Technology Profile	This document is a Technology Profile for SAML. Technology Profiles in general describe how given technologies are implemented within the eduGAIN framework. Each Technology Profile is made up of one or more documents which describe and define rules for specific trust brokers, including metadata production and aggregation and use of protocols. Each Technology Profile is associated with an operational team responsible for the management of core trust broker infrastructure.
Security Assertion Markup Language (SAML)	The Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an Identity Provider and a Service Provider.
SAML V2.0	Version 2.0 of the Security Markup Language specification
SAML Metadata Producers	An organisations that produces and publishes SAML V2.0 Metadata.
SAML Metadata Consumer	An entity or organisation that downloads processes and uses SAML V2.0 Metadata.
SAML Metadata	An XML document describing SAML Entities, both in technical as well as non-technical terms. Valid SAML Metadata MUST meet the requirements defined in the SAML Metadata Specification [SAMLMeta] including [SAMLMetaErrata].
Metadata Distribution Service (MDS)	The eduGAIN Metadata Service (MDS) aggregates eduGAIN upstream SAML2 metadata of the eduGAIN Member. It verifies and validates it before it is signed and republished [eduGAIN-MDS].
Metadata Registration Practice Statement (MRPS)	Document that describes the rules and procedures used for registering Entities which get exposed to eduGAIN. Every eduGAIN Member Federation must publish an MRPS.

1.3 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 Metadata Registration

SAML Metadata Producers MUST publish a Metadata Registration Practice Statement and a link to an English version of this statement MUST be provided to the eduGAIN Operational Team for publication on the eduGAIN website. This document SHALL describe rules and procedures used for registering entities which get exposed to interfederation, including eligibility. It is RECOMMENDED that SAML Metadata Producers use the Metadata Registration Practice Statement Template [REFEDS-MDRPS] or ensure that that contents described in the template are fully covered within published statements.

SAML Metadata Producers MAY publish entities that represent multiple scopes. When doing so, SAML Metadata Producers MUST ensure that IdPs use the `shibmd:Scope` element with `regexp="false"`. SAML Metadata Producers MUST NOT register any IdPs with scopes without checking the validity and purpose of the claim.

Comment [1]: There are few legitimate uses of regexp scopes that even UKf accepts. IMO it's a SHOULD. One should have no worries about the entity being silently discarded somewhere if it violates a SHOULD.

Comment [2]: Actually the Scope element is only a subset of the issue of using internet domain names in metadata. Domain names are significant (in terms of security):
* entityIDs
* endpoint URLs
* scopes
I'd suggest to include a more generic section about using domain names in metadata, and include the special requirement of Scope's not being a regexp here.

3 Metadata Production

SAML Metadata Producers MUST adhere to the following requirements when producing metadata. Support for these requirements is fully described in the eduGAIN Metadata Aggregation Practice Statement [eduGAIN-MAPS].

This profile supports the SAML V2.0 Metadata Interoperability Profile [SAMLMetaIoP]. Whatever is specified as a MUST in the SAML V2.0 Metadata Interoperability Profile should also be considered as REQUIRED within this eduGAIN Metadata Profile.

The references defined in this section use the following namespaces:

- `urn:oasis:names:tc:SAML:2.0:assertion` - The SAML V2.0 Assertion namespace defined in the SAML V2.0 Core specification [SAMLCore].
- `urn:oasis:names:tc:SAML:2.0:metadata` - The SAML V2.0 metadata namespace defined in theSAML V2.0 Metadata specification [SAMLMeta].
- `urn:oasis:names:tc:SAML:metadata:rpi` - The namespace defined in the SAML V2.0 Metadata Extensions for Registration and Publication Information [MDRPI].
- `urn:oasis:names:tc:SAML:metadata:ui` - The namespace defined in SAML V2.0 Metadata Extensions for Login and Discovery User Interface [MDUI].

The metadata root element MUST contain:

- `A validUntil attribute` with a value not earlier then 120 hours (5 days) and not later than 2304 hours (28 days) after the `creationInstant`.
- `<mdrpi:PublicationInfo>` with `publisher` and `creationInstant`.

Each <md:EntityDescriptor> element MUST contain:

- <mdrpi:RegistrationInfo>.
- registrationAuthority with a value that has been registered with the eduGAIN Operational Team.
- <md:Organization> with values in English other values in the service's native languages for the elements where appropriate.
- <md:OrganizationName>.
- <md:OrganizationURL>.
- <md:ContactPerson> with contactType="technical" and/or contactType="support".
- entityID prefixes that start with either urn:, https://, or http:// only.

The <md:EntityDescriptor> SHOULD contain:

- registrationInstant.
- <mdrpi:RegistrationPolicy>.
- <md:OrganizationDisplayName>.

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.
- <mdui:Description> with a value in English.

Where the service supports other languages, these elements SHOULD be supported for those languages.

4 Metadata Signing

For signing its metadata, SAML Metadata Producers MUST use an RSA private key of at least 2048 bits. The Algorithm for SignatureMethod MUST NOT be SHA1 and MUST be at least as strong as SHA256. SAML Metadata Producers MUST provide the eduGAIN Operational Team with a URL to federation metadata and a signing certificate that ensures metadata is genuine.

5 Metadata Publication

If a SAML Metadata Producer aggregates metadata from multiple sources, the <mdrpi:PublicationPath> element MUST be used where appropriate.

The eduGAIN Downstream metadata contains all entities in eduGAIN. It is generated and published by the eduGAIN Metadata Distribution Service (MDS). Federations MUST republish the eduGAIN

Deleted: <#>cacheDuration attribute, with a value between one hour and six hours.

Deleted: If present, <md:EmailAddress> SHOULD not be a personal address but a role address to get in contact with the entity's responsible persons.

Comment [NH4]: Do we want to maintain any SHOULDs in the document at all?

Comment [5]: This is crossing with SAML2Int but with slightly less requirements. Should we strengthen? From SAML2Int:

Metadata documents provided by a Service Provider MUST include an <md:SPSSODescriptor> element containing all necessary <md:KeyDescriptor> and <md:AssertionConsumerService> elements. The metadata SHOULD also include one or more <md:NameIDFormat> elements indicating which <saml2:NameID> Format values are supported and one or more <md:AttributeConsumingService> elements describing the service(s) offered and their attribute requirements.

Metadata provided by Service Provider SHOULD also contain a descriptive name of the service that the Service Provider represents (not the company) in at least English. It is RECOMMENDED to also provide the name in other languages which is much used in the geographic scope of the deployment. The name should be placed in the <md:ServiceName> in the <md:AttributeConsumingService> container.

metadata as a signed metadata feed to its members and MUST NOT recommend direct consumption of metadata from the MDS or any other sources. Federations MAY filter out certain entities for technical or practical reasons. It is expected that entities will have access to and consume eduGAIN metadata from their home Federation within minimal administrative involvement.

6 Adherence

A SAML Metadata Producer conforms to this profile if it conforms to:

- SAML V2.0 Metadata Interoperability Profile [SAMLMetaIoP].
- Additional eduGAIN Metadata Producer Requirements described in this document.

Adherence to this profile is monitored by the eduGAIN Metadata Validator [eduGAIN-VAL]. SAML Metadata Producers SHOULD use the validator to verify their metadata compliance on a regular basis.

Entity adherence to best current practice is also monitored by the eduGAIN Operational Team via the eduGAIN Entities Database [eduGAIN-ED]. Federation Operators SHOULD monitor the eduGAIN Entities Database on a regular basis.

For more information on how validations and warnings are supported by the eduGAIN Operational Team, please see the eduGAIN Operational Practice Statement [eduGAIN-OPS].

7 References

[eduGAIN-CONST] eduGAIN Constitution: http://edugain.org/policy

[eduGAIN-DOC] eduGAIN Policy and Technical Documents: http://edugain.org/policy

[eduGAIN-OP] eduGAIN Operational Practice Statement: https://technical.edugain.org/documents

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, https://www.ietf.org/rfc/rfc2119.txt

[eduGAIN-BCP] eduGAIN Best Current Practice, https://technical.edugain.org/documents

[eduGAIN-ED] eduGAIN Entities Database, https://technical.edugain.org/entities

[eduGAIN-FEDS] eduGAIN Membership Status webpage, https://technical.edugain.org/status

[eduGAIN-MAPS] eduGAIN Metadata Aggregation Practice Statement, https://technical.edugain.org/documents

[eduGAIN-VAL] eduGAIN Metadata Validator, https://validator.edugain.org/

[SAMLMeta] http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAMLMetaErrata] http://www.oasis-open.org/committees/download.php/35391/sstc-saml-metadata-errata-2.0-wd-04-diff.pdf

[SAMLMetaIoP] SAML V2.0 Metadata Interoperability Profile Version 2.0 https://www.oasis-open.org/committees/download.php/36645/draft-sstc-metadata-iop-2.0-01.pdf

[eduGAIN-MDS] eduGAIN Metadata Distribution Service, http://mds.edugain.org

Comment [LH6]: This document is currently being written by the eduGAIN OT (Tomasz Wolniewicz and co)