eduGAIN Policy Framework

SAML Profile

Version	Date	Description of Change	Person
0.1	2017-07-06	Draft version	N Harris
0.2	2017-07-13	Restructuring, references, layout harmonization	L Hämmerle
0.3	2017-11-08	Incorporating feedback from first consultation	N Harris
0.4	2018-02-13	Incorporating feedback from the second consultation	N Harris
0.5	2018-04-03	Fixes to xml namespace and grammar fixes	N Harris and P Schober

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 SAML 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

Definition	Description
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 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 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 Operational Team (OT)	eduGAIN Operational Team, as defined in section 2.3 of the eduGAIN Constitution [eduGAIN-CONST].
eduGAIN Policy Declaration	The agreement signed by Federations on joining eduGAIN.
eduGAIN Policy Framework	A set of documents which includes this document (SAML Profile), the eduGAIN Constitution and the eduGAIN Policy Declaration, which is signed by Member Federations.
eduGAIN Steering Group (eSG)	The 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 an end user is 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 an organisation that 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.
Interfederation	Sharing of federation metadata to allow a user from one federation to access a service which is registered in another federation.
Metadata Distribution Service (MDS)	The eduGAIN Metadata Service (MDS) aggregates eduGAIN upstream SAML2 metadata of eduGAIN Members. 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.
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].
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 known errata [SAMLMetaErrata].
SAML	

Metadata Consumer	An entity or organisation that downloads, processes and uses SAML V2.0 Metadata.
SAML Metadata Producers	An organisation that produces and publishes SAML V2.0 Metadata. An XML document describing SAML Entities.
SAML V2.0	Version 2.0 of the Security Assertion Markup Language specification.
Security Assertion Markup Language (SAML)	The Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorisation data between parties, in particular, between an Identity Provider and a Service Provider.
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.
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].

1.3 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 [RFC2119].

The XML elements (e.g. `<Element>`) and attributes (e.g. `attribute`) in this document use the following XML Namespace prefixes and respective namespaces:

Prefix	XML Namespace	Comment

(none or) `md`	`urn:oasis:names:tc:SAML:2.0:metadata`	The SAML V2.0 metadata namespace defined in Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLMeta].
`mdrpi`	`urn:oasis:names:tc:SAML:metadata:rpi`	The SAML V2.0 metadata namespace defined in SAML V2.0 Metadata Extensions for Registration and Publication Information [MDRPI].
`mdui`	`urn:oasis:names:tc:SAML:metadata:ui`	The SAML V2.0 metadata namespace defined in SAML V2.0 Metadata Extensions for Login and Discovery User Interface [MDUI].
`shibmd`	`urn:mace:shibboleth:metadata:1.0`	The SAML V2.0 metadata namespace defined in ShibMetaExt V1.0 [ShibMD].

2. Metadata Registration

SAML Metadata Producers MUST publish a SAML Metadata Registration Practice Statement in English in order for their SAML Metadata to be aggregated and published by eduGAIN. 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 SAML Metadata Registration Practice Statement Template [REFEDS-MRPS] or ensure that that content described in the template is fully covered within published statements.

SAML Metadata Producers MUST NOT register any Identity or Attribute Providers with scopes (i.e., `<shibmd:Scope>` elements as defined in [ShibMD]) without checking the validity and purpose of the claim. SAML Metadata Producers MAY publish entities that represent multiple scopes.

3. SAML Metadata Production

SAML Metadata Producers MUST adhere to the following requirements when producing SAML Metadata for aggregation in eduGAIN. Support for these requirements is fully described

in the eduGAIN Metadata Aggregation Practice Statement [eduGAIN-MAPS].

The SAML 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>`.
- `mdrpi: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:OrganizationDisplayName>`.
- `<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:

- `<mdrpi:RegistrationPolicy>`.
- If the `<md:EntityDescriptor>` contains `<md:IDPSSODescriptor>` it SHOULD contain an `<mdui:DisplayName>` element and `<mdui:Logo>` element.
- If the `<md:EntityDescriptor>` contains `<md:SPSSODescriptor>` it SHOULD contain an `<mdui:DisplayName>` element, `<mdui:Logo>` element and an `<mdui:Description>` element with a value in English. Where the service supports other languages, these values SHOULD be supported for those languages.
- If an `<mdui:Logo>` element is present, the logo MUST be expressed as a Data URI (embedded logo) or an https URL. URLs used for this element MUST be publicly accessible.

4. SAML Metadata Signing

The eduGAIN Metadata Distribution Service conforms to the rules for Metadata Consumer and Metadata Producers as stated in SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP]. Further information is available in the eduGAIN Metadata Aggregation Practice Statement [eduGAIN-MAPS].

In order to assure SAML Metadata integrity, each federation aggregate produced for

aggregation in eduGAIN MUST be signed as specified in Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLMeta].

SAML Metadata Producers MUST ensure that their SAML Metadata signature meets the following requirements:

- Public keys used for signing are at least 2048 bits in length. At least 3072 bits is RECOMMENDED for new deployments.
- EC public keys are at least 256 bits in length.
- The signature is made using an explicit ID reference, not an empty reference.
- The signature reference refers to the document element.
- The signature's digest algorithm is at least as strong as SHA-256, and does not use MD5 or SHA-1.
- The signature's signature method is RSA with an associated digest at least as strong as SHA-256 and does not use MD5 or SHA-1.
- The signature's transforms contain only these permissible values:
  - Enveloped signature.
  - Exclusive canonicalisation with or without comments.

5. SAML Metadata Publication

The eduGAIN Downstream SAML Metadata contains all entities published in eduGAIN, and all entity information provided to eduGAIN will be made publicly available. It is generated and published by the eduGAIN Metadata Distribution Service (MDS). Federations MUST provide their members with trustworthy SAML Metadata about eduGAIN Entities, signed with their own signing key and MUST NOT recommend direct consumption of SAML 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 SAML Metadata from their Federation Operator with minimal administrative involvement.

6. Participant Federation Requirements

To be accepted as a SAML Metadata Producer within eduGAIN, Participant Federations MUST:

- Produce a SAML Metadata export set that complies with the requirements detailed in this document.
- Register a URL to the SAML Metadata export set with the eduGAIN OT.
- Register and validate a signing certificate for the SAML Metadata export set with the eduGAIN OT.
- Register a `mdrpi:registrationAuthority` with the eduGAIN OT.

7. Adherence

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

eduGAIN supports a series of Best Current Practice (BCP) documents. All such documents are approved by the eduGAIN Steering Group before being published on the eduGAIN website. SAML Metadata Producers SHOULD support eduGAIN BCP. Entity adherence to best current practice is 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].

8. References

- [eduGAIN-BCP] eduGAIN Best Current Practice: https://technical.edugain.org/documents
- [eduGAIN-CONST] eduGAIN Constitution: http://edugain.org/policy
- [eduGAIN-DOC] eduGAIN Policy and Technical Documents: http://edugain.org/policy
- [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-MDS] eduGAIN Metadata Distribution Service: http://mds.edugain.org
- [eduGAIN-OP] eduGAIN Operational Practice Statement: https://technical.edugain.org/documents
- [eduGAIN-VAL] eduGAIN Metadata Validator: https://validator.edugain.org/
- [MDRPI] SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0: http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/saml-metadata-rpi-v1.0.pdf
- [MDUI] SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.pdf
- [REFEDS-MRPS] REFEDS Metadata Registration Practice Statement Template: https://github.com/REFEDS/MRPS
- [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
- [SAMLCore] Assertions and Protocols for the OASIS Security Assertion Markup Language

(SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- [SAMLMeta] Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: 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 1.0: http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-cs-01.pdf
- [ShibMD] ShibMetaExt V1.0: https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0