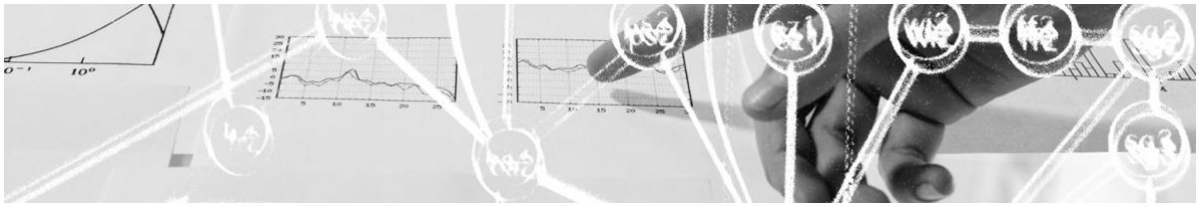
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

SWITCHaai Federation

Metadata Registration Practice Statement (MRPS)



SWITCHaai Federation Operator

Document Type:	Documentation
Version:	V2.0
Created:	23.08.18
Last changes:	26.09.18
Classification:	Public

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Content

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

1 Definitions and Terminology

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 [RFC2119].

The following definitions are used in this document:

Federation Identity Federation	An association of organisations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator	SWITCH is the organisation providing the governance, the coordination as well as the operation of central components of the Authentication and Authorisation Infrastructure to the SWITCHaai Participants.
SWITCHaai Participant	A SWITCHaai participating organisation (a legal entity) is called a SWITCHaai Participant and is legally bound to the Federation Policy.
Federation Policy	The document describing the obligations, rights and expectations of the SWITCHaai Participant and SWITCH as the Federation Operator. It is published as chapter 5 of the *SWITCH edu-ID Service Description* [SWITCH edu-ID]
Entity	A discrete component that a member wishes to register and describe in metadata. This is typically an Identity Provider (IdP) or Service Provider (SP).
AAI Resource Registry	The self-service system provided by the Federation Operator where SWITCHaai Participants can register their Entities and which generates the appropriate metadata.
Registered Representatives	Individuals authorised to act on behalf of the SWITCHaai Participant. These may take on different roles with different rights attached to them.
Resource Registration Authority Administrator (RRA Admin)	Each SWITCHaai Participant eligible to operate an IdP appoints its Resource Registration Authority Administrators who take the responsibility to review and approve the SP entities associated to the SWITCHaai Participant.
SP Administrator	The executing person at a SWITCHaai Participant that operates an SP.

2 Introduction and Applicability

This document describes the metadata registration practices of SWITCH as Federation Operator for all entities published to eduGAIN by the SWITCHaai Federation with effect from the publication date shown on the cover sheet. All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.

This document SHALL be published on the Federation website at:
https://www.switch.ch/aai/switchaai-mrps-v2.0.pdf.

Updates to the documentation SHALL be accurately reflected in entity metadata.

An entity that does not include a reference to a registration policy MUST be assumed to have been registered under an historic, undocumented registration practice regime. Requests to re-evaluate a given entity against a current MRPS MAY be made to the Federation helpdesk.

3 Member Eligibility and Ownership

All SWITCHaai Participants have accepted the SWITCHaai Federation Policy that is published as chapter 5 of the SWITCH edu-ID Service Description [SWITCH edu-ID]. Its chapter 5.2.1 Target Audience specifies the kind of organisations eligible to become SWITCHaai Participants.

The procedure to join the SWITCHaai Federation is documented at:
https://www.switch.ch/aai/join/

The on-boarding process for SWITCHaai Participants verifies that the prospective participant has legal capacity, and requires that all participants enter into a contractual relationship with SWITCH as the SWITCHaai Federation Operator.

The Federation Operator makes checks based on the legal name provided. The checks are conducted with official databases like:

- Zefix: Central Business Name Index
- Collections of federal and cantonal law (for public institutions)

Associations not registered in a Swiss registry of commerce need to present a list of its board of directors together with its bylaws, both documents signed by members of the board.

The on-boarding process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organisation in dealings with the Federation Operator. Verification is achieved by direct contact, or confirmation of prior relationship with the organisation, or consulting the organisation's on-line staff directory.

The process also establishes a canonical name for the Federation member. The canonical name of a member MAY change during the membership period, for example as a result of corporate name changes or mergers. The member's canonical name is disclosed in the entity's `<md:OrganizationName>` element [SAML-Metadata-OS].

4 Metadata Format

Metadata for all entities registered by the Federation Operator SHALL make use of the [SAML-Metadata-RPI-V1.0] metadata extension to indicate that the Federation Operator is the registrar for the entity and to detail the version of the MRPS statement that applies to the entity.

The following is a non-normative example:

```
<mdrpi:RegistrationInfo
    registrationAuthority=http://rr.aai.switch.ch/
    registrationInstant="2016-11-29T13:39:41Z">
    <mdrpi:RegistrationPolicy xml:lang="en">
        https://www.switch.ch/aai/switchaai-mrps-v1.0.pdf
    </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5 Entity Eligibility and Validation

The SWITCHaai federation is built on a delegation model to manage the entities. Each SWITCHaai Participant eligible to operate an Identity Provider appoints its *Resource Registration Authority Administrators (RRA Admin)* who take the responsibility to review and approve the SP entities associated to the SWITCHaai Participant. SPs can also be operated by third parties to whom the SWITCHaai Participant outsource services.

SWITCH as Federation Operator takes the responsibility for the registration of all IdPs, its own SPs as well as further SPs, e.g. the ones of Federation Partners that offer services to the whole community and not only to a single SWITCHaai Participant.

5.1 Entity Registration

A SWITCHaai Participant has to register its entities in the *AAI Resource Registry:*
https://rr.aai.switch.ch
Registration requests from other sources SHALL NOT be accepted.

The SP administrator registers itself the SP entry within the AAI Resource Registry. The SP administrator picks the SWITCHaai Participant to which the SP should be associated and submits the entry for approval by the RRA Admins of that SWITCHaai Participant.

The RRA Admin SHALL verify the SWITCHaai Participant's right to use particular domain names in relation to entityID attributes.

5.2 EntityID Format

Values of the entityID attribute registered MUST be an absolute URI using the http and https schemes.

https-scheme URIs are RECOMMENDED for all entities.

http-scheme and https-scheme URIs used for entityID values MUST contain a host part whose value is a DNS domain.

5.3 Entity Validation

On entity registration, the RRA Admin, supported by the AAI Resource Registry's built-in checks, SHALL carry out entity validation checks. These checks include:

- Ensuring all required information is present in the metadata;
- Ensuring protocol endpoints are properly protected with TLS / SSL certificates.

The federation manager web application, the AAI Resource Registry, generates the metadata for all the entities based on the data registered and approved. Therefore, it is always in a well-defined and consistent representation.

6 Entity Management

Once a SWITCHaai Participant has joined the Federation any number of SP entities MAY be added, modified or removed by the organisation. The number of entities of a SWITCHaai Federation Partner published to eduGAIN may be limited by subscription plan. Once registered, a SWITCHaai Participant entitled to operate an IdP can modify its IdP entry at any time.

A Registered Representative with the administration right for an entity can invite a further person to gain the same administration right for this entity. Vice versa, each Registered Representative with the administration right for an entity can revoke another person's administration right for this entity.

6.1 Entity Change Requests

Any request for entity addition, change or removal from SWITCHaai Participants needs to be performed within the AAI Resource Registry by their respective Registered Representatives entitled by their administration rights. Each change has to be reviewed and approved by an RRA Admin again before it gets active.

Changes on behalf of SWITCHaai Federation Partners for their own entities can be requested by e-mail to the SWITCHaai Helpdesk. The Federation Operator verifies and processes such requests.

6.2 Unsolicited Entity Changes

SWITCH as Federation Operator may amend or modify the Federation metadata at any time in order to:

- Ensure the security and integrity of the metadata;
- Comply with interfederation agreements;
- Improve interoperability;
- Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

7 References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[SAML-Metadata-RPI-V1.0]	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.
[SAML-Metadata-OS]	OASIS 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.
[SWITCH edu-ID]	SWITCH edu-ID Service Description, Version 1.0.3, 15 February 2018. https://www.switch.ch/edu-id/terms/