deutsches forschungsnetz

# DFN-AAI Federation

## Metadata Registration Practice Statement

| | |
|---|---|
| **Authors** | Wolfgang Pempe |
| **Last Modified** | 2019-03-31 |
| **Version** | 1.0 |

**Acknowledgements**

This document is based on the REFEDS Metadata Registration Practice Statement template.



## 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:

| Definition | Description |
| --- | --- |
| 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 | Organisation providing the infrastructure for Authentication and Authorisation to Federation Participants. |
| Federation Participant | An organisation that has joined the Federation by agreeing to be bound by the Federation Policy in writing. There are two types of Federation Participants: Home Organisations (entitled to register both Identity and Service Provider entities) and Service Providers (entitled to register Service Provider entities) |
| Federation Policy | A document or set of documents describing the obligations, rights and expectations of the Federation Participants and the Federation Operator. |
| Entity | A discrete component that a Federation Participant wishes to register and describe in metadata. This is typically an Identity Provider (IdP) or Service Provider (SP). |
| Registry | System used by the Federation Operator to register entity metadata. This may be via a self-service tool or via other manual processes. |
| Registered Representatives | Individuals authorised to act on behalf of the Federation Participant. These may take on different roles with different rights attached to them. |

# 2. Introduction and Applicability

This document describes the metadata registration practices of DFN as Federation Operator for all entities published by the DFN-AAI 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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.aai.dfn.de/fileadmin/documents/mrps_dfn-aai_1.0.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. Federation Participant Eligibility and Ownership

Federation Participants are eligible to make use of the Federation Operator's registry ("Metadata Administration Tool") to register entities. Registration requests from other sources SHALL NOT be accepted.

The procedure for becoming a participant of the Federation is documented at: https://doku.tid.dfn.de/en:join.

The application procedure verifies that the prospective Federation Participant has legal capacity, and requires that all Federation Participants enter into a contractual relationship with the Federation Operator by agreeing to the Federation policy. The Operator makes checks based on the legal name provided. As part of the contract, the Federation Participant has to designate at least one contact person who is entitled to appoint and dismiss Registered Representatives. Registered Representatives are permitted to act on behalf of the Federation Participant in dealings with the Federation Operator, namly metadata registration and management.

The process also establishes a canonical name for the Federation Participant. The canonical name MAY change during the membership period, for example as a result of corporate name changes or mergers. The Federation Participants's canonical name is disclosed in the entity's SAML v2.0 `<md:OrganizationName>` element.

# 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="https://www.aai.dfn.de"
    registrationInstant="2016-11-29T13:39:41Z">
    <mdrpi:RegistrationPolicy xml:lang="en">
        https://www.aai.dfn.de/fileadmin/documents/mrps_dfn-aai_1.0.pdf
    </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

# 5. Entity Eligibility and Validation

## 5.1 Entity Registration

The process by which a Federation Participant can register an entity is described at: https://doku.tid.dfn.de/en:registration

The Federation Operator SHALL verify the Federation Participant's right to use particular domain names in relation to entityID attributes and, for Identity Provider entities, any scope elements.

The right to use a domain name SHALL be established in one of the following ways:

- A Federation Participant's canonical name matches registrant information shown in WHOIS.
- A Federation Participant MAY be granted the right to make use of a specific domain name through a permission letter from the domain owner on a per-entity or an overall contractual basis. Permission SHALL NOT be regarded as including permission for the use of sub-domains, unless stated otherwise by the domain owner.

## 5.2 EntityID Format

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

https-scheme URIs are RECOMMENDED to all Federation Participants.

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

## 5.3 Scope Format

For Identity Provider entities, scopes MUST be rooted in the DNS domain name space, expressed in lowercase. Multiple scopes are allowed.

Regular expressions representing multiple scopes MAY be used, but all DNS domains covered by the expression SHALL be included in checks by the Federation Operator for the Federation Participants's right to use those domains. For these checks to be achievable by the Federation Operator, the set of DNS domains covered by the regular expression MUST end with a domain under a public suffix - that is, a literal '.', followed by at least two DNS labels separated by literal '.'s (representing a domain to be validated as "owned" by the entity owner), and ending with a '$' anchor (e.g. `(foo|bar)\.example\.com$`).

### 5.4 Entity Validation

On entity registration, the Federation Operator SHALL carry out entity validation checks. These checks include:

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

## 6. Entity Management

Once a Federation Participant has joined the Federation any number of entities MAY be added, modified or removed by the organisation. Home Organisations SHALL NOT register more than one Identity Provider with the DFN-AAI production environment. Any exceptions must be authorised by the Federation Operator.

### 6.1 Entity Change Requests

Any request for entity addition, change or removal from Federation Participants needs to be communicated from or confirmed by their respective Registered Representatives.

Communication of change happens via the Federation's registry tool. Requests submitted via e-mail to the Federation Operator's helpdesk are only accepted in exceptional cases and require additional verification.

### 6.2 Unsolicited Entity Changes

The 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.

## 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.