safeID Metadata Registration Practice Statement

Document	safeID Metadata Registration Practice Statement
Version	1.1
Publication date	2019-11-27
Status	FINAL
License	Creative Commons BY 3.0

License

This document draws on work carried out by the UK Access Management Federation, the ACOnet Identity Federation and the eduID Luxembourg with gratitude.

Table of Contents

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 RFC2119, see https://www.ietf.org/rfc/rfc2119.txt.

The following definitions are used in this document:

Federation	Identity Federation. An association of organizations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Member	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing.
Federation Operator	An organization operating the central components of the Federation, providing Infrastructure for Authentication and Authorization to Federation Members.
Federation Policy	A document describing the obligations, rights and expectations of the Federation Members and the Federation Operator.
Entity	A discrete component that a member wishes to register and describe in metadata. This is typically an Identity Provider or a Service Provider.
Registry	System used by the Federation Operator to register entity metadata. This may be via a self-service tool or via other manual process.
Registered Representatives	Individuals authorized to act on behalf of the member. These may take on different roles with different rights attached to them.

2 Introduction and Applicability

This document describes the metadata registration practice statement of the Federation Operator with effect from the publication date shown on the cover sheet. All new entity registrations performed on or after that data SHALL be processed as described here until the document is superseded.

This document SHALL be published on the Federation website at: https://www.safeid.sk/doc/policy. Updates to the documentation SHALL be accurately reflected in entity metadata.

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

3 Member Eligibility and Ownership

Members of the Federation are eligible to make use of the Federation Operator’s registry to register entities. Registration requests from other sources SHALL NOT be accpted.

The procedure for becoming a member of the Federation is documented at http://www.safeid.sk/doc/join.

The membership procedure verifies that the prospective member has legal capacity, and requires that

all members 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. The checks are conducted with a number of official databases (e.g. Statistical Register of Organizations, Business Register maintained by the Department of Justice and various Registers of Legal Entities maintained by the Department of Interior, where applicable).

The membership process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organization in dealing with the Federation Operator. Verification is achieved by personal contact between the Federation Operator and the organization, exceptionally via email or phone.

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.

4 Entity Management

Once a member has joined the Federation any number of entities MAY be added, modified or removed by the organization.

The process by which a Federation member can register an entity is described at http://www.safeid.sk/doc/join.

4.1 Entity Change Requests

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

Communication of addition, change or removal happens via e-mail.

4.2 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 the interfederation agreements;
- Improve interoperability;
- Add value to the metadata.

Registered Representatives of the affected entity can observe changes by inspection of the published federation metadata. For technology profiles which do not lead to public disclosure of metadata, the Federation Operator SHALL inform the Registered Representatives for the entity.

5 Metadata for SAML WebSSO Technology Profile

SAML 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://safeid.sk"
registrationInstant="2016-11-29T13:39:41Z">
<mdrpi:RegistrationPolicy xml:lang="en">
http://safeid.sk/doc/mrps-01.pdf</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5.1 SAML Entity Validation

The member's canonical name is disclosed in the entity's <md:OrganizationName> element [SAML-Metadata-OS].

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

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

- A members canonical name matches registrant information shown in DNS;
- A member 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 basis. Permission SHALL NOT be regarded as including permission for the use of sub-domains.

5.2 SAML Entity Identifier Format

Registered entityID attribute values MUST be an absolute URI using http, https or urn schemes.

https-scheme URIs are RECOMMENDED to all members.

http-scheme and https-scheme URIs used for entityID values MUST contain a host part whose value is a DNS domain which the member has a right to use (as defined above).

5.3 SAML Scope Element 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 can be used, but all DNS domains covered by the expression MUST be included in checks by the Federation Operator for the member'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, e.g. `(fool bar)\.example\.com$`.

5.4 SAML Metadata Validation

On entity registration, the Federation Operator SHALL carry out entity validation checks and re-evaluate periodically as long as the entity stays registered. These checks include:

- Ensuring all required information is present in metadata;
- Ensuring metadata is correctly formatted;
- Ensuring URLs specified in the metadata are technically reachable;
- Ensuring protocol endpoints are protected with TLS / SSL certificates:
    1. TLS / SSL certificates on user-facing protocol endpoints are trusted by selected HTTP User Agents (or Operating Systems' Trust Stores);

2. TLS / SSL certificates on non-user-facing protocol endpoints match the entity's trust fabric keys published in SAML metadata (if applicable).

6 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 Extension for Registration and Publication Information Version 1.0. 03 April 2012. 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]	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.