Preface to the Template Document

Federation Operator Practice (FOP):
Metadata Registration Practice Statement

Purpose

This document is aimed to help emerging and existing Identity Federations build a series of statements to describe their Federation Operator Practice (FOP).

The FOP is designed to help parties understand the technical processes a Federation undertakes to create the Federation trust framework. It is designed to be a companion document to the Identity Federation Policy document and as such should work in a similar way.

As with the Federation policy, sections of the FOP may point or link to other documents or parts of the Federation website to demonstrate compliance or practice rather than include these processes directly in the FOP document.

One way of looking at the documents is that policy deals with WHO can be in a Federation and WHAT they can do, whereas the FOP deals with HOW the Federation ensures these rules are kept.

This template is intended to address the processes undertaken by SAML-based Identity Federations.

Overview

The FOP is formed of five practice statements made by the Federation Operator. It is recommended that all Identity Federations publish the first three statements. The second two may depend on the maturity of your Federation or the focus given to these elements within your Federation set-up.

- Metadata Registration Practice Statement;
- Metadata Publication Practice Statement;
- Key Management Practice Statement;
- Assurance Practice Statement;
- Monitoring Practice Statement.

This template reflects the recommendations for the Metadata Registration Practice Statement (MRPS). Please note that these statements can easily be published as one document or as individual references, depending on the preference of your federation.

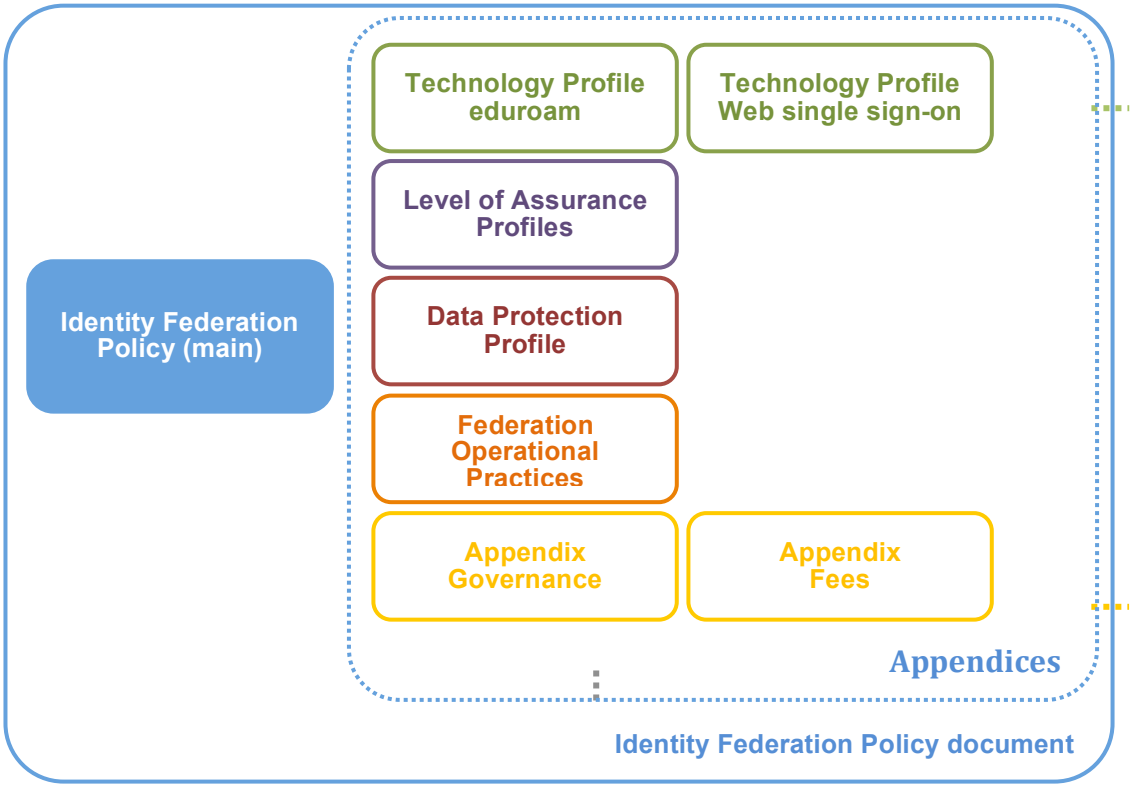
FOP Audience

The FOP when published will be of use and interest to:

- Other Federations wishing to interfederate with your Federation;
- Auditors;
- Members wishing to join your Federation and wanting a deeper understanding of the trust framework.

Typically, readers are going to want to understand the actual processes undertaken by a Federation to ensure that their entity registration processes are effective and robust. Other Federations reading the document may wish to understand if your processes are equivalent to those that they carry out.

Document Suite



The content and purpose of these documents are:

Identity Federation Policy (main)

Covers core and very static topics that are not likely to be changed. This is the document that was developed and is presented in the reminder.

Technology Profile (eduroam, Web single sign-on, Moonshot, provisioning service) (appendix)

Contains technical description of specific Technology Profile and defines requirements and obligations for Federation Operator and Member who implements that Technology Profile. Since those documents are very technology oriented, they will vary between federations depending on architecture and technical requirements that a federation set for a specific service. However, in further development of Identity Federation Policy template document, it is planned to at minimum provide some guidelines for writing certain Technology Profiles.

Level of Assurance Profiles (appendix)

Deals with Identity Management practices which are used by Home Organizations and allows a Service Provider to determine with which degree of certainty individual is truly presented by a digital identity he is using. This document is not yet developed and it is planned to follow the work of stakeholder community in this area and when there are clear directions how this document should look, to create it under the further development of Identity Federation Policy template document.

Data Protection Profile (appendix)
Deals with data protection issues and considers Home Organizations and especially Service Providers in cases when they are processing personal data. This document is not yet developed and it is planned to develop it in further development of Identity Federation Policy template document.

Federation Operational Practices (appendix)

Defines operational practices that Federation Operator is undertaking. In this moment it is recognized by the existing federations that there is a need for such a document that would describe issues like how the federation operator ensures the integrity and availability of its services, systems and configuration data, such as the top-level RADIUS servers (for eduroam service), SAML 2.0 metadata files and their signing keys (for WebSSO service) and adequate and skilled staff for operations work. Since there is not yet a common understanding of what issues this document should address, it is planned to follow the work of stakeholder community in this area and when there are clear directions how this document should look, to create it under the further development of Identity Federation Policy template document.

Instruction for Using this Document

This document is written according to the current best practice in operation of Identity Federations and the experience of Authors and Contributors to the document. As these practices may change over time, this document can also be updated and it is expected that it will in certain degree keep evolving. It was intended to write a general-purpose document that can be easily reused, but you should carefully read this document and adapt it to local circumstances and needs .All organisations should seek local technical advice before implementing a process based on this template.

This document is structured by sections, and each section looks like this:

x.x Name of the Section

Description of the section. This is to be used be the person writing the document for better understanding of what the purpose of the section is, which issues it covers and which circumstances should be taken into consideration when adapting the example wording for the actual policy. This isn't part of the actual policy that will be generation from the template and should be deleted.

Example wording:

Suggested wording for the section. This wording should be easily reused and adapted for the actual document. Placeholders for Federation names are in the form *xxx.* Comments are written in the form *comment: xxx* and they should be deleted from the final document.

Whilst this document makes use of page breaks and spacing for ease of use, it is expected that most MRPS documents will be reasonably short and concise in length. Each of the proposed sections will be no more than a few paragraphs when taken out of the template context.

Acknowledgements

This templates draws heavily on work carried by the UK Access Management Federation and ACOnet in the development of their Metadata Registration Practice Statements.

Disclaimer

Please note that the FOP template document is only a recommendation and therefore you are using this template document at your own risk. While using this template document you should take into account the legal framework of your country.

For all of the information in this template document, Authors make no warranties, expressed or implied, and accepts no responsibility in relation to the use of this document.

LOGO

*** enter Federation Name ***

Federation Operator Practice: Metadata Registration Practice Statement

Authors	
Publication Date	
Version	

License

Table of Contents

1. Definitions and Terminology

In this section, basic terms that are used in the document are defined. If a specific notation system is used (such as RFC2119), this should also be referenced.

Readers will be looking to ensure that they have an accurate understanding of any terminology used in the document.

Example Wording:

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 Member	An organisation that has joined the Federation by agreeing to be bound by the Federation Policy in writing.
Federation Operator	Organisation providing the infrastructure for Authentication and Authorisation 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 Service Provider.
Registered Representatives	Individuals authorised to act on behalf of the member. These may take on different roles with different rights attached to them.

2. Introduction and Applicability

The introduction should briefly introduce the Metadata Registration Practice Statement and describe the document publication process. It is important to remember that you may wish to change and update your Metadata Registration Practice Statement over time. If these changes are significant, it will mean that you will be publishing metadata that has been processed against different practice statements and as such it is important that is represented both in the documentation and in the metadata (see section 5). Previous editions of the MRPS should continue to be published to support referencing of these changes.

If you provide the document in multiple languages this should be referenced here, indicating which version is normative.

Readers will be looking to understand where you publish documentation, how you reflect changes and how this relates to published metadata.

Example Wording:

This document describes the metadata registration practices of the Federation Operator 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: <*url*>. 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

This section should describe the process by which the Federation establishes member eligibility. HOW members join is probably already documented in the Federation Policy, and this can be referenced here. The MRPS should provide more detail about WHAT the Federation does to manage and restrict membership.

Readers will be looking to understand how organisations become members of your Federation, how you carry out any specific checks on these organisations and whether you permit any exceptions to these processes, such as outsourcing arrangements.

Example Wording:

Members of the Federation Operator are eligible to make use of the Federation Operator's registrar to register entities. Registration requests from other sources SHALL NOT be accepted.

The procedure for becoming a member of the Federation is documented at: <url>.

The membership process 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.

The membership 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

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 <OrganizationName> element.

4. Metadata Format

This section should refer to the way in which registration information is referenced in the entity metadata. For the purposes of this document, use of the SAML V2.0 Metadata Extensions for Registration and Publication Information is assumed.

Example Wording:

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://Federation.org"
registrationInstant="2016-11-29T13:39:41Z">
<mdrpi:RegistrationPolicy xml:lang="en">
http://Federation.org/doc/MRPS20121110</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. Entity Eligibility and Validation

This section describes the processes and checks put in place before an entity is registered. Readers will be looking to understand how you determine a member's right to publish information about a given entity and any checks you make to ensure the entity metadata is well constructed.

Text regarding entityIDs using URIs is included below. Some Federations will also permit URN-based entityIDs. You should describe what you do and do not permit under each schema. Please ensure that any processes described here reflect your current practice and any published documentation currently available for your Federation.

Example Wording:

5.1 Entity Registration

The process by which a Federation member can register an entity is described at <url>.

The Federation Operator SHALL verify the member's right to use particular domain names in relation to entityID attributes.

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

- A member's 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 EntityID Format

Values of the entityID attribute registered MUST be an absolute URI using the 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.

5.3 Entity Validation

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

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

6. Entity Management

This section describes the processes undertaken once an entity has been registered – including processes for change requests, removal and any intervention the Federation Operator may take. If you have a Monitoring Practice Statement, this is likely to be referenced here. The reader will want to understand that any changes made to an entity are completed with the correct permission and for good reasons. Please ensure that any processes described here reflect your current practice and any published documentation currently available for your Federation.

If you have multiple different roles under the Registered Representative category (e.g. management contacts, technical contacts, administrative contacts) the different rights of these roles can be detailed here.

Example Wording:

Once a member has joined the Federation any number of entities MAY be added by the organisation.

6.1 Entity Change Requests

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

Communication of change happens via *(e-mail, Federation registry tool etc.)*

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.

7. References

Remember to include references to documentation within your own Federation, such as your Identity Federation Policy.

[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.