SIFULAN™ Malaysian Access Federation

Metadata Registration Practice Statement

Authors	Muhammad Farhan Sjaugi and Suhaimi Napis
Last Modified	26 July, 2018
Version	1.2

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 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.
[SIFULAN™ 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.
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 member. These may take on different roles with different rights attached to them.

2. Introduction and Applicability

This document describes the metadata registration practices of the Federation Operator SIFULAN™ 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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://sifulan.my/federation-metadata/. Updates to the documentation SHALL be accurately reflected in entity metadata.

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 accepted.

The procedure for becoming a member of the Federation is documented at: https://sifulan.my/how-to-join-sifulan-federation/ .

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.

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 requiring the prospective member to complete the SIFULAN™ Service Application Form, which states the organisation's billing and technical contacts. The completed SIFULAN™ Service Application Form is to be signed by the organisation's representative, with the organisation's stamp.

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 , and the technical contact in the `<md:ContactPerson>` 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:

```
<md:Extensions
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi">
  <mdrpi:RegistrationInfo
   registrationAuthority="https://sifulan.my"/>
  <mdrpi:RegistrationPolicy> https://sifulan.my/sifulan-mrps-v1-
2/</mdrpi:RegistrationPolicy>
</md:Extensions>
```

5. Entity Eligibility and Validation

5.1 Entity Registration

The process by which a Federation member can register an entity is described at http://infohub.sifulan.my/display/SIFULAN .

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.
- Any other acceptable methods that can prove the right to use a domain name by the member.

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.

The use of `urn`-scheme URIs for `entityID` values is NOT RECOMMENDED but MAY be permitted in exceptional circumstances. When permitted, such values MUST be part of a properly delegated registry under the `urn:mace` namespace, as described in [RFC3613]. The registrant MUST also demonstrate that the `urn:mace` URI value in question has been issued for their use.

5.3 Entity Validation

On entity registration, the Federation Operator SHALL carry out entity validations 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.

SIFULAN™'s convention is that scopes are named by DNS domain names, expressed in lower case. Entity owners registering metadata containing `<shibmd:Scope>` elements MUST demonstrate that each domain used is either owned by them, or that specific permission has been given to them to use the domain for the purpose of registering the entity. When establishing the right of a registrant to use a domain name in a `<shibmd:Scope>` element, the registrar MAY rely on a permission letter from an existing SIFULAN™ federation member. Permission letters from non-members SHALL NOT be accepted for this purpose.

6. Entity Management

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

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 inter-federation 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.
[SIFULAN™ Federation Policy]	https://sifulan.my/federation-policy/
[SIFULAN™ SAML Web Single Sign-On Technology Profile]	https://sifulan.my/saml-web-single-sign-on-technology-profile/