JUCC JOINT UNIVERSITIES COMPUTER CENTRE LTD.
大學聯合電腦中心

HONG KONG
ACCESS
FEDERATION

Hong Kong Access Federation (HKAF)

Federation Operator Practice:

Metadata Registration Practice Statement (MRPS)

Version 2.0

Table of Contents

1. Document Control

1.1 Document Status

Document Name	HKAF Metadata Registration Practice Statement
Document Code	HKAF-FOP-MRPS
Author	HKAF Operator Team
Version Number	2.0
Document Status	~~Draft for Internal Review~~ / ~~Release for Consultation~~ / Approved
Date Approved	12-Apr-2019
Date of Next Review	01-May-2021
Superseded Version	1.1

1.2 Document History

Version Number	Revision Date	Summary of Changes	Authored By	Approved By
1.0	07-Jul-2017	Official release	AFWG	JUCC Steering Committee
1.1	11-Oct-2017	Amendments of terms in p.3 & 4	HKAF Operator Team	JUCC Steering Committee
2.0	09-Apr-2019	Alignment with REFEDS template as required by eduGAIN Steering Group	HKAF Operator Team	JUCC Steering Committee

2. 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, see http://tools.ietf.org/html/rfc2119.

The following definitions are used in this document:

Federation	Hong Kong Access 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	Organization 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.
Registry	Federation 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 authorized to act on behalf of the Federation Member. These may take on different roles with different rights attached to them.

3. Introduction and Applicability

This document describes the metadata registration practices of the Federation Operator with effect from the publication date shown in the Document Control section. 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.hkaf.edu.hk/mrps. 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 Operator.

4. Member Eligibility and Ownership

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

The policy and procedure for becoming a Member of the Federation is documented at: https://www.hkaf.edu.hk/eligibility-policy.

The membership application procedure verifies that the prospective member has legal capacity, and requires that each member enters 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 which include but are not limited to:

- Companies Registry - https://www.cr.gov.hk/en/home/index.htm
- Legislative Council - https://www.legco.gov.hk/index.html
- Social Welfare Department - https://www.swd.gov.hk/en/index/
- Education Bureau - https://www.edb.gov.hk/en/index.html
- University Grants Committee - https://www.ugc.edu.hk/eng/ugc/index.html

The membership application process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organization in dealings with the Federation Operator. Verification of information is achieved by direct contact, prior relationship with JUCC or by consulting the organization's online staff directory. The vetted application forms, with recommendation from the Federation Operator, would be eventually submitted to the JUCC Steering Committee for approval.

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

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

6. Entity Eligibility and Validation

6.1 Entity Registration

Respective Registered Representatives of a Member can logon to the HKAF Federation Registry with their institutional accounts to register the entity for the organization. Registration requests from other sources SHALL NOT be accepted.

Full Members are eligible to register Identity Provider (IdP) or Service Provider (SP) entity. Associate Member can only register Service Provider entity.

The Federation Operator SHALL verify the potential 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 legal 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.

Identity Provider Entity

The member SHALL ensure that the entity is fully compliant with the HKAF Federation Policy. The minimal set of items that need to be confirmed are listed below:

- All registered end points are using the secure https protocols.
- The internal SAML certificates are self-signed and long-lived.
- All certificates have embedded a Public-Key that is at least 2048 bits in length.
- The scope is in a domain owned by the organization.
- The Display Name is not in conflict with the identity of the organization.
- All HKAF Core Attributes have been marked as available to the wider federation.

Service Provider Entity

An SP has a number of required attributes for its functioning. The member SHOULD justify the reason for each required attribute for the SP, with the objective of minimizing the set of attributes requested from the IdPs of the end users.

The member SHALL ensure that the entity is fully compliant with the HKAF Federation Policy. The minimal set of items that need to be confirmed are listed below:

- All registered end points are using the secure https protocols.
- The internal SAML certificates are self-signed and long-lived.

- All certificates have embedded a Public-Key that is at least 2048 bits in length.
- The scope is in a domain owned by the organization.
- The Display Name is not in conflict with the identity of the organization.
- The requested attributes are a minimal set required for the SP to function.

6.2 EntityID Format

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

https-scheme URIs are RECOMMENDED to all members.

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

6.3 Scope Format

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

Regular expressions representing multiple scopes SHALL not be used because they are not well supported generally by SAML SPs and some federations do not accept scopes with regular expressions, by default.

6.4 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;
- Ensuring the readiness of the corresponding minimal set of items, that should have been verified by the member during the entity registration process.

The Federation Operator may contact the Respective Registered Representative of the organization to discuss /resolve any issues with the information provided for the entity before approving or rejecting the registration.

7. Entity Management

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

7.1 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 the Federation Registry tool.

7.2 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.

8. References

Federation Policy	HKAF Federation Policy: https://www.hkaf.edu.hk/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.
[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.