

African Catch All Federation

Federation Operator Practice: Metadata Registration Practice Statement

Authors	Mario Reale, Alex Mwotil, Omo Oaiva, Eriko Porto
Publication Date	June 2 2021
Version	1.0

License



This template document is license under Creative Commons CC BY 3.0. You are free to share, re-use and adapt this template as long as attribution is given. This document draws on work carried out by the UK Access Management Federation and the ACONet Identity Federation with gratitude.

27
28

Table of Contents

29	1. Definitions and Terminology	3
30	2. Introduction and Applicability	4
31	3. Member Eligibility and Ownership	5
32	4. Metadata Format	6
33	5. Entity Eligibility and Validation	7
34	6. Entity Management	8
35	7. References	9

36
37
38
39
40
41
42
43
44
45
46
47

1. Definitions and Terminology

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.
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.

48
49
50
51
52
53
54
55
56
57
58
59
60
61
62

2. Introduction and Applicability

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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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: <https://www.eduid.africa/>. 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

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 as an Identity Provider is documented at: <https://www.eduid.africa/identity-providers>.

The procedure for becoming a member of the Federation as a Service Provider is documented at: <https://www.eduid.africa/service-providers>

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 (provide examples).

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 (describe process).

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 [SAML-Metadata-OS].

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:

```
-----  
<mdl:pi:Registrationinfo  
  registrationAuthority="http://Federation.org"  
  registrationInstant="2016-11-29T11:39:41Z">  
  ..:mdrpi:RegistrationPolicy xml:lang="en">  
    http://Federation.org/doc/MRPS20121110</mdrpi:RegistrationPolicy>  
  ..:/mdrpi:Registrationinfo>
```

103 5. Entity Eligibility and Validation

104

105

106

5.1 Entity Registration

107

108

The process by which a Federation member can register an entity is described at <https://www.eduid.africa/>

109

110

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

111

112

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

113

114

115

- 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.

116

117

118

119

5.2 EntityID Format

120

121

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

122

123

124

https-scheme URIs are RECOMMENDED to all members.

125

126

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

127

128

129

5.3 Entity Validation

130

131

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

132

133

134

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

135

136

137

138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162

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 email.

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.

163
164
165
166
167
168

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/v2.0/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
[AFRICAN-CATCH-ALL) Identity Federation Policy	https://www.IAFRICAN-CATCH-ALL/Catch-All-Identity-Federation-Policy-Document-v1.0.docx.pdf

169