

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40



**\* MREN Identity Federation (eduID)\***

Federation Operator Practice: Metadata Registration Practice Statement

Authors	Aleksandra Radulović, prof. dr. Božo Krstajić
Publication Date	
Version	0.3

41  
42  
43  
44  
45  
46

**License**



47  
48  
49  
50

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.

51 **Table of Contents**  
52  
53 1. Definitions and Terminology..... 3  
54  
55 2. Introduction and Applicability..... 4  
56  
57 3. Member Eligibility and Ownership..... 5  
58  
59 4. Metadata Format..... 6  
60  
61 5. Entity Eligibility and Validation ..... 7  
62  
63 6. Entity Management..... 8  
64  
65 7. References ..... 9

66 **1. Definitions and Terminology**

67

68 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",  
69 "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be  
70 interpreted as described in RFC 2119 [RFC2119].

71

72 The following definitions are used in this document:

73

74

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 authorized to act on behalf of the member. These may take on different roles with different rights attached to them.

75

76 **2. Introduction and Applicability**

77

78

79 This document describes the metadata registration practices of the MREN Identity Federation  
80 with effect from the publication date shown on the cover sheet. All new entity registrations  
81 performed on or after that date SHALL be processed as described here until the document is  
82 superseded.

83

84 This document SHALL be published on the Federation website at:

85 *<<http://www.mren.ac.me/eduGAIN.php>>*. Updates to the documentation SHALL be  
86 accurately reflected in entity metadata.

87

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

91 **3. Member Eligibility and Ownership**

92

93

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

97

98 The procedure for becoming a member of the MREN Identity Federation is documented at:  
99 <<http://www.mren.ac.me/eduGAIN.php>>.

100

101 The membership process verifies that the prospective member has legal capacity, and  
102 requires that all members enter into a contractual relationship with the MREN Identity  
103 Federation by agreeing to the MREN Identity Federation Policy. The Operator makes checks  
104 based on the legal name provided. The checks are conducted with a number of official  
105 databases.

106

107 The membership process also identifies and verifies Registered Representatives, who are  
108 permitted to act on behalf of the organization in dealings with the MREN Identity Federation.

109

110 The process also establishes a canonical name for the Federation member. The canonical  
111 name of a member MAY change during the membership period, for example as a result of  
112 corporate name changes or mergers. The member's canonical name is disclosed in the  
113 entity's <OrganizationName> element.

114 **4. Metadata Format**

115

116

117 Metadata for all entities registered by the MREN Identity Federation SHALL make use of the  
118 [SAML-Metadata-RPI-V1.0] metadata extension to indicate that the MREN Identity Federation  
119 is the registrar for the entity and to detail the version of the MRPS statement that applies to  
120 the entity. The following is a non-normative example:

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

121

122 **5. Entity Eligibility and Validation**

123

124

125 **5.1 Entity Registration**

126

127 The process by which a MREN Identity Federation member can register an entity is described  
128 at <http://www.mren.ac.me/eduGAIN.php>.

129

130 The MREN Identity Federation verifies the member's right to use particular domain names in  
131 relation to entityID attributes.

132

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

134

- 135 • A member's canonical name matches registrant information shown in DNS.
- 136 • A member MAY be granted the right to make use of a specific domain name through  
137 a permission letter from the domain owner on a per-entity basis. Permission SHALL  
138 NOT be regarded as including permission for the use of sub-domains.

139

140 **5.2 EntityID Format**

141

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

144

145 https-scheme URIs are RECOMMENDED to all members.

146

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

149

150 **5.3 Entity Validation**

151

152 The MREN Identity Federation SHALL verify the entityID attributes of metadata of the  
153 institution before being registered on the MREN Identity Federation.

154 **6. Entity Management**

155

156 Once a member has joined the MREN Identity Federation any number of entities MAY be  
157 added by the organization.

158

159 **6.1 Entity Change Requests**

160

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

163

164 Communication of change happens via *e-mail*.

165

166 **6.2 Unsolicited Entity Changes**

167

168 The MREN Identity Federation may amend or modify the Federation metadata at any time in  
169 order to:

170

- 171 • Ensure the security and integrity of the metadata;
- 172 • Comply with interfederation agreements;
- 173 • Improve interoperability;
- 174 • Add value to the metadata.

175

176 Changes will be communicated to Entity owners.



177 **7. References**  
178

- [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>.
- [MREN Identity Federation (eduID) Policy] MREN Identity Federation (eduID) Policy <http://www.mren.ac.me/documents/Identity...>

179