

1 **eduGAIN Policy Framework**  
2 **Metadata Profile**  
3 **(REQUIRED)**  
4  
5

Version date	Editor	Change
29.4.2011	Mikael Linden	Approved by NREN PC 21.3.2011.

## 6 Introduction

7 The eduGAIN metadata profile defines rules for SAML metadata producers (acting in the role of a registrar or  
8 aggregator) and metadata consumers participating in the eduGAIN interederation service.

9 Adopting this profile lays the ground for scalable SAML interoperability.

10 This profile is based on [SAMLMetalOP]. Whatever is specified in the SAML V2.0 Metadata Interoperability  
11 Profile is also valid within this eduGAIN Metadata Profile.

## 12 1 Requirements Notation

13 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",  
14 "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in  
15 [RFC2119].

## 16 2 References to SAML 2.0 specification

17 saml2 urn:oasis:names:tc:SAML:2.0:assertion

18 The SAML 2.0 Assertion namespace defined in the SAML 2.0 Core specification [SAMLCore].

19 md urn:oasis:names:tc:SAML:2.0:metadata

20 The SAML V2.0 metadata namespace defined in the SAML V2.0 Metadata specification [SAMLMeta].

21 ds <http://www.w3.org/2000/09/xmldsig#>

22 The XML Signature namespace [XMLSig].

23 `mdrpi urn:oasis:names:tc:SAML:metadata:rpi`

24 The namespace defined in the SAML V2.0 Metadata Extensions for Registration and Publication  
25 Information [MDRPI].

26 `mdui urn:oasis:names:tc:SAML:metadata:ui`

27 The namespace defined in SAML V2.0 Metadata Extensions for Login and Discovery User Interface  
28 [MDUI].

## 29 3 Additional eduGAIN Metadata Producer 30 Requirements

31 Any metadata file which makes use of parts of metadata published by eduGAIN MUST include either a  
32 reference with a URL to the eduGAIN Metadata Terms of Use [ToU] or the entire ToU text. It MUST be placed  
33 at the top of the metadata file formatted as an XML comment.

34 Example:

```
35 <!--  
36 Use of this metadata is subject to the Terms of Use at  
37 http://www.edugain.org/policy/metadata-tou\_1\_0.txt  
38 -->
```

39  
40 The metadata root element MUST contain

- 41 • `<mdrpi:PublicationInfo>`, it MUST contain
  - 42 ○ publisher
  - 43 ○ `<mdrpi:UsagePolicy>` with a link to the eduGAIN Metadata Terms of Use [ToU]
  - 44 it SHOULD contain one of the attributes
  - 45 ○ `creationInstant` or `publicationID`

46  
47 Each `<md:EntityDescriptor>` element MUST contain

- 48 • `<md:ContactPerson>` with `contactType="technical"`, it MUST contain
  - 49 ○ `<md:EmailAddress>` which SHOULD be a role address and not a personal address.

- 50 • <mdrpi:RegistrationInfo>, it MUST contain
- 51 ○ registrationAuthority
- 52 it SHOULD contain
- 53 ○ registrationInstant
- 54 ○ <mdrpi:RegistrationPolicy>
- 55 it SHOULD contain the element:
- 56 • <md:Organization> with values in English for the elements
- 57 ○ <md:OrganizationName>
- 58 ○ <md:OrganizationDisplayName>
- 59 ○ <md:OrganizationURL>
- 60 and with values in the service's native languages for the elements
- 61 ○ <md:OrganizationName>
- 62 ○ <md:OrganizationDisplayName>
- 63 ○ <md:OrganizationURL>
- 64
- 65 If the <md:EntityDescriptor> contains one of these elements:
- 66 • <md:IDPSSODescriptor>
- 67 • <md:AttributeAuthorityDescriptor>
- 68 • <md:SPSSODescriptor>
- 69 each one of them SHOULD contain the elements:
- 70 • <mdui:DisplayName> with a value in English
- 71 • <mdui:DisplayName> with a value in the languages that the service supports, other than English
- 72 • <mdui:Description> with a value in English
- 73 • <mdui:Description> with a value in the languages that the service supports, other than English
- 74
- 75 Each <md:SPSSODescriptor> element MAY contain:
- 76 • <md:AttributeConsumingService> that lists all attributes requested by this SP as <md:RequestedAttribute>
- 77 element with isRequired="true" for required attributes and isRequired="false" for just useful attributes.
- 78
- 79 Whenever contents of a metadata file gets aggregated from multiple sources, the <mdrpi:PublicationPath>
- 80 element SHOULD be used where appropriate.
- 81 For signing its metadata, a metadata producer MUST use an RSA private key of at least 2048 bits.

## 82 4 eduGAIN Metadata Conformance

83 A metadata producer conforms to this profile if it conforms to:

- 84 • SAML V2.0 Metadata Interoperability Profile [SAMLMetaloP]
- 85 • Additional eduGAIN Metadata Producer Requirements

86 A metadata consumer conforms to this profile if it conforms to:

- 87 • SAML V2.0 Metadata Interoperability Profile [SAMLMetaloP]

## 88 References

89	<b>[SAMLMetaloP]</b>	OASIS SAML V2.0 Metadata Interoperability Profile Version 1.0, currently in Committee Specification 01, 4 August 2009 <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf</a>
90		
91		
92	<b>[SAMLCore]</b>	OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. March 2005 <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf</a>
93		
94		
95	<b>[SAMLMeta]</b>	OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. March 2005 <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf</a>
96		
97		
98	<b>[SAMLErr]</b>	SAML V2.0 Approved Errata. December 2009 <a href="http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf">http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf</a>
99		
100	<b>[ToU]</b>	eduGAIN Metadata Terms of Use. November 2010 <a href="http://www.edugain.org/policy/metadata-tou_1_0.txt">http://www.edugain.org/policy/metadata-tou_1_0.txt</a>
101		
102	<b>[XMLSig]</b>	D. Eastlake et al. XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008 <a href="http://www.w3.org/TR/xmlsig-core/">http://www.w3.org/TR/xmlsig-core/</a>
103		
104		
105	<b>[MDRPI]</b>	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0, Working Draft 02, 17 December 2010. <a href="http://wiki.oasis-open.org/security/SAML2MetadataDRI">http://wiki.oasis-open.org/security/SAML2MetadataDRI</a>
106		
107		
108	<b>[MDUI]</b>	SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, Working Draft 06, 16 November 2010, approved as Committee Specification Draft 01 <a href="http://wiki.oasis-open.org/security/SAML2MetadataUI">http://wiki.oasis-open.org/security/SAML2MetadataUI</a>
109		
110		
111	<b>[RFC2119]</b>	S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, March 1997. <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
112		
113		