Best Current Practice

Version 2020-04-22

This document specifies recommendations for upstream metadata produced by eduGAIN participants. Failure to comply with these recommendations will result in a warning produced by the eduGAIN metadata validator using the eduGAIN SAML profile v2.

The recommendations are organised as a set of rules which may be easily verified by the eduGAIN metadata validator.

The rules marked red are actually specification errors and should be upgraded to validator errors (to be discussed within the eduGAIN SG)

The significance column is meant for possible future use, i.e. grouping problems in order to solve the most important first. Proposed significance range is from 1 (least significant) to 5 (most significant). If found useful, this classification should be subject to a future discussion in the eduGAIN SG.

	Condition	Level	Significance	Reason
1	Signing certificate expired	1-global	1	Currently implemented as a validator warning. To be confirmed by the SG.
2	md:EmailAddress in md:ContactPerson element should start with mailto: prefix	2-entity	4	This violates line 495 of https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf and should be considered an error!
3	SIRTFI attribute present and security ContactPerson definition found but contact type not http://refeds.org/metadata/contactType/security	2-entity	2	SIRTFI specification error
4	SIRTFI attribute declared but no appropriate md:ContactPerson set	2-entity	2	SIRTFI specification error
5	shibmd:Scope with no regexp attribute	2-entity	5	https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0 recommendation
6	mdattr:EntityAttributes placed in md:Extensions element of SPSSODescriptor/IDPSSODescriptor, expected in md:Extensions element of md:EntityDescriptor	2-entity	1	Since http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html does not define appearance of this element in places other then md:Extensions element of EntityDescriptor it is most likely that the condition is a result of a mistake.
7	mdrpi:RegistrationPolicy not found	2-entity	3	eduGAIN SAML profile Section 3
8	mdattr:EntityAttributes element contains saml:AttributeValue with leading/trailing whitespaces	2-entity	3	
9	mdattr:EntityAttributes element contains duplicated saml:Attribute / saml:AttributeValue declaration	2-entity	??	
10	mdui:UIInfo found but mdui:DisplayName not present	3-role	3	eduGAIN SAML profile Section 3
11	mdui:UIInfo found but no mdui:Logo element	3-role	1	eduGAIN SAML profile Section 3
12	mdui:UIInfo / mdui:DisplayName does not have English value	3-role	??	
13	mdui:UIInfo not found, no mdui:DisplayName and mdui:Description present	3-role (SP-only)	3	eduGAIN SAML profile Section 3
14	mdui:UIInfo with mdui:DisplayName found but mdui:Description not present	3-role (SP-only)	3	eduGAIN SAML profile Section 3
15	mdui:UIInfo found but neither mdui:DisplayName nor mdui:Description present	3-role (SP-only)	3	eduGAIN SAML profile Section 3
16	Data Protection Code of Conduct declared but no mdui:PrivacyStatementURL found	3-role	4	Violates the CoCo spec
17	Data Protection Code of Conduct declared but md:RequestedAttribute element not found	3-role	4	Violates the CoCo spec
18	mdui:Logo content size is larger than 40000 and smaller than 50000 characters	3-role		Decided by eduGAIN SG
19	mdui:Logo content size is 50000 or more characters	3-role		Decided by eduGAIN SG
20	R&S Category declared but the SP does not provide required mdui:DisplayName	3-role	4	R&S spec 4.3.3
21	R&S Category declared but the SP does not provide required mdui:InformationURL	3-role (SP only)	4	R&S spec 4.3.3
22	R&S Category declared but the SP does not provide the required Binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST in md:AssertionConsumerService	3-role (SP only)	4	R&S spec 4.3.1

23	R&S Category declared but the SP does not provide any technical contact	2-entity	4	R&S spec 4.3.4
24	Some entities do not have an encryption certificate	1-global		
25	SP has a wrong signing certificate	3-role (SP-only)		
26	SP has no encryption certificate	3-role (SP-only)		