

Best Current Practice

DRAFT

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)

	Global	
1	Signing certificate expired	Currently implemented as a validator warning. To be confirmed by the SG.
Entity level		
2	md:EmailAddress in md:ContactPerson element should start with mailto: prefix	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 contact found but no http://refeds.org/metadata/contactType/security contactType	SIRTFI specification error
4	SIRTFI attribute declared but no appropriate md:ContactPerson set	SIRTFI specification error
5	shibmd:Scope with no regexp attribute	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 EntityDescriptor	Since http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html does not define appearance of this element in places other than md:Extensions element of EntityDescriptor it is most likely that the condition is a result of a mistake.
7	mdrpi:RegistrationPolicy not found	eduGAIN SAML profile Section 3
8	mdattr:EntityAttributes element contains saml:AttributeValue with leading/trailing whitespaces	
Entity's role level		
9	mdui:UIInfo not found, no mdui:DisplayName and mdui:Description present	eduGAIN SAML profile Section 3
10	mdui:UIInfo with mdui:DisplayName found but mdui:Description not present	eduGAIN SAML profile Section 3
11	mdui:UIInfo found but mdui:DisplayName not present	eduGAIN SAML profile Section 3
12	mdui:UIInfo found but neither mdui:DisplayName nor mdui:Description present	eduGAIN SAML profile Section 3
13	mdui:UIInfo found but no mdui:Logo element	eduGAIN SAML profile Section 3
14	this SP does not provide requested attribute specification	left from saml2int - should it be kept?
15	Data Protection Code of Conduct declared but no mdui:PrivacyStatementURL found	Violates the CoCo spec
16	CoCo declared but md:RequestedAttribute element not found	Violates the CoCo spec
17	CoCo declared but mdui:PrivacyStatementURL and md:RequestedAttribute elements not found	Violates the CoCo spec