eduGAIN policy comments

6nd Sep, 2010

www.edugain.org/policy

Initials	Commentator's name and contacts	In which role you have provided the comments
AS	Andreas Solberg	Comments from me personally. Not neccessarily representing UNINETT as an edugain member.
DL	Diego Lopez diego.lopez@rediris.es	
GW	Glenn Wearen (glenn.wearen@heanet.ie)	As federation operator of Edugate
NH	Nicole Harris. nicole.harris@jiscadvance.ac.uk, +44 (0)20 3006 6040.	On behalf of JISC and the UK federation.
SC	Scott Cantor (cantor.2@osu.edu)	Non-European, Shibboleth developer, shepherd of relevant standards and profiles
TL	Thomas Lenggenhager	
TW	Torbjörn Wiberg torbjorn.wiberg@adm.umu.se	Involved in policy decisions for SWAMID

Type: ge=general, te=technical, ed=editorial

Metadata profile (METAP)

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
1	DL	239	ge		Should not the metadata profile include the technical requirements on metadata made by the data protection profile, or at least mention it?	These are just extensions and only optional. The profile allows anything not specified or detailed.	It is only MAY, not MUST or SHOULD and therefore treated as any other extension. ⇒No effect on METAP
2	AS	239	ge	Who is responsible for the content of an Entity Descriptor in the metadata; the provider or the federation. In example; if required contact persons are lacking, who to blame?		A federation may only submit conformant entities. Entities must provide the info.	A federation may only submit conformant entities. Entities must provide the info required. ⇒No effect on METAP
3	AS	239	ge	Includes MUST include new stuff that AFAIK no one is yet using; such as MDattribs. Will that delay federations joining edugain?		Not the idea to just use the same metadata as today. Entites opting-in provide the enriched metadata.	Use MUST only for 'new stuff' which can easily be generated by the Participating Federation before submitting the metadata. They have anyhow to prepare a special eduGAIN metadata file with

Type: ge=general, te=technical, ed=editorial

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
							opted-in entities only. ⇒Update METAP
4	AS	239	ge	'DisplayName' element is mentioned. That is not part of SAML2Meta, where is this defined?		It is defined in mdui	This comes from the MDUI Working Draft which was recently uploaded to OASIS ⇒No effect on METAP
5	AS	239	ge	Dispute if one SP would like to be published to edugain through more than one federation... How is this sorted out? Example: Dreamspark, Elsevier.			The SP has to opt-in. It should only do it in a single federation or otherwise needs to use different EntityIDs. If they submit twice, the first wins until the conflict is sorted out. ⇒No effect on METAP ⇒Should go into an FAQ or HOWTO for SPs opting.in.
6	AS	239	ge	The document include a lot of fancy experimental metadata extensions that AFAIK nobody has started using in their own federation (yet).			Before 20110401 MDUI and MDAttribs should have made progress in the OASIS

Type: ge=general, te=technical, ed=editorial

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
				Warning: this will delay things... [MDattribs] and [IdPDiscovery]			process. See also 3) above. ⇒No effect on METAP
7	SC	274	te	Reference to SAML metadata spec should be supplemented by referencing the SAML 2.0 Approved Errata document.	Add a reference to the Approved Errata.	OK, I will add it.	⇒Update METAP
8	SC	328	te	(also 332)The namespaces here suggest OASIS official adoption of these profiles, but these have not been submitted yet.	Either remove such references, ask the editors to submit them to OASIS, or ask the editors to alter the namespaces to a non-OASIS value.	OK, I will check it out.	MDUI was already uploaded to OASIS, MDattribs will soon e uploaded as well. ⇒Update METAP
9	NH	339	ge	The particular values mandated for the validity interval are problematic for the UK federation, because at present we'd either have to pay people overtime to meet those constraints during holiday periods, or deploy on-line systems with knowledge of our signing keys. Mandating values for the validity interval is regarded as over-profiling by eduGAIN.	Maintain the statement but without specified values.	With or without values???	We drop specific values for validUntil or cacheDuration in the METAP. ⇒Update METAP
10	NH	346	ge	The use of 'MAY' with regard to the cacheDuration attribute is not required as this is already part of	Remove all reference to cacheDuration.	OK to drop it.	See 9) above ⇒Update METAP

Type: ge=general, te=technical, ed=editorial

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
				the base specification. Any required constraint on the cacheDuration interval should it be present would be again regarded as over-profiling, as eduGAIN systems would in any case be at liberty to apply their own refresh rules.			
11	AS	347	ge	cacheDuration of minimum 1 hour is way to short.	If it is common to pull metadata once an hour, I would say 4 hour validity is a minimum. To allow a 4 hop metadata relay without expiration.	[ANC] Our current recommendation is to fetch metadata once a day!	See 9) above ⇒Update METAP
12	NH	357	ge	The UK federation does not believe that administrative contact addresses should be published due to problems with spam. We currently insist on 'real person' addresses for the administrative contact to ensure response times and it is deemed inappropriate to publish such data.	Remove requirement for inclusion of the administrative contact. Administration is between the home federation and the member in question, and should not be necessary for interfederation communication and issue resolution.	If others agree, we drop it.	Only MUST for tech contact with a SHOULD for choosing a role address. ⇒Update METAP
13	NH	359	ge	The spamming implications of publication of technical and support contacts should be seriously considered. Role rather than real person contact addresses should be encouraged.	Justify requirement for the publication of these contacts within the eduGAIN context. What purpose does publication serve?	We have otherwise no reasoning in the profile doc and semantic hints.	See 12) above, no further action. ⇒No effect on METAP
14	NH	363	ge	363-369 This references an experimental specification and it is inappropriate to include as a mandated element at this stage.	Propose that should eduGAIN require this information, the service should undertake the process of marking registration origin itself	But federations register entities not eduGAIN. Important to get the trace and resolve duplicate submissions. We	This info can be generated by the Federation when preparing the

Type: ge=general, te=technical, ed=editorial

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
					rather than passing the burden to participating federations.	need something like that to know from where the metadata originated.	metadata for eduGAIN. ⇒No effect on METAP
15	SC	384	ge	(also 390) This material on formats seems to be more about what formats IdPs have to support.	I would move the focus here away from specific formats to list, but to ”SHOULD list all the formats you support”. Move material on what deployers have to support to some other section.	Into which part should ‘deployment requirements‘ go? A section or a new doc?	Probably best to separate out an ‘eduGAIN Metadata deployment’ document. ⇒ Do we want this?
16	NH	385	ge	This is the only point where a SAML 2.0 spec is insisted upon. If this could be made SAML version agnostic, it would allow a greater number of entities to participate in eduGAIN.	Make this statement SAML version agnostic	ditto	Same as 15) above
17	NH	386	ge	It is inappropriate for eduGAIN to be enforcing minimum key lengths. This again places a burden of change on federations and entities with no perceptible benefits.	Change this statement to SHOULD rather than MUST.	Do we want this? We lower the barriers further.	Should that also go to the MD Deployment doc? ⇒ Do we want this?
18	NH	394	ge	394-401 This references an experimental specification and it is inappropriate to include as a mandated element at this stage.	Remove requirement.	Who submits the first entity with unrecognizable strings only…	Turn all MUST into SHOULD ⇒Update METAP
19	AS	410	ge	Profile say MAY use RequestedAttribute.	I would say MUST or SHOULD. There is no alternative ways of handling ARP, or is it?	Profile says MAY contain `<md: AttributeConsumingService>` which requires at least one `<md:RequestedAttribute>`. It is valid to require no attribute at all!	Leave it as it is ⇒No effect on METAP

Type: ge=general, te=technical, ed=editorial

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
20	SC	417	ge	This seems to rule out URL naming, and doesn't really motivate the requirement for OID names by noting what kinds of attributes would have such names.	I would move material on attribute naming to a deployment profile section. As with the previous comment, metadata should simply describe what **is** deployed.	OK, see above	Drop this from here. See 15) above
21	AS	418	ge	Profile allows the use of non-oid attribute names 'otherwise other URN formats may be used.' Why not require oid only?		SAML1 endpoints use generally other URNs.	Same as 20) above
22	NH	427	ge	427-434 These elements are NOT part of a metadata profile, and should be included elsewhere within the policy / constitution documentation.	Remove.	427-438 can go to the 'deployment requirements' part.	Move it to MD Deployment doc. ⇒ Do we want this?

Type: ge=general, te=technical, ed=editorial