eduGAIN policy comments

6th 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	
EH	Eefje van der Harst, Surfnet	
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

Data Protection Provile (DP)

Id	Who	Line	Type	Comment (justification for change)	Proposed change by the commentator	Discussion in the policy subtask	Resolution by the policy subtask
1	AS	787	ge	How many federations do we think will support the data protection profile?		Hopefully they will, it's what we can do to ease IdP-side opt-in. Support in SAML2 products and marketing needed.	no changes done
2	EH	787	ge	How is the profile related to the policy		The DP profile is an optional profile which supplements the eduGAIN constitution.	Added REQUIRED/RECOMMENDED/OPTIONAL to all profile cover pages
3	EH	787	ge	The profile is very complex, maybe because technical and juridical are mixed. Maybe the profile can be split up in 1. The data-protection rules that apply 2. The consequences for the SP en the IP (home organisation) 3. The technical implementation		1. and 2. Of course the whole data protection directive (and national implementations) apply, if personal data is processed in EU. Directive's articles relevant to federated identity management are explained in Appendix B. 3. The technical implementation is section 4.	no changes done
4	TL	809	ed		1.1 Terms now: Home Organisation	The text from eduGAIN constitution will be copied here	Copied the section 1.1 of the Constitution to the end of this document ("glossary").

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 organisation which the end users are affiliated to and which is responsible for authenticating end users and maintaining their Attributes. Home Organisation is responsible of setting up and operating an Identity Provider, either by itself or as an outsourced service. In this document, a Home Organisation refers to an organisation whose Identity Provider a Participant Federation has exposed to eduGAIN new: Home Organisation The organisation to which an end user is affiliated to and which is responsible for authenticating the end user and keeping his/her Attributes up-to-date. Home Organisation is responsible for setting up and operating an Identity Provider, either by itself or as an outsourced service. In this document, a Home Organisation refers to an organisation whose		

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
					Identity Provider gets exposed to eduGAIN by a Participant Federation Oh, I just noticed that this definition should be aligned to the constitution. I assume the pale blue background means that this term is elsewhere defined. Make it explicit from where. BTW: the SP definition should then also have a blue background.		
5	TL	813	ed	Requirements and categories for Service Providers The first sentence does not provide much information, but PII is not explained.	now: Service Providers have different characteristics with regards to the end users accessing the Service Provider. Considering the data protection directive's implications, Service Providers are divided into the following two categories: category PII: the Service Provider processes personal data category non-PII: the Service Provider processes no personal data The categories are further elaborated below and summarized as a table in	ok	changed

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
					Appendix A. new: Considering the data protection directive's implications, Service Providers are grouped into these two categories: - category PII: the Service Provider processes personal data - category non-PII: the Service Provider processes no personal data PII stands for 'Personally Identifiable Information'. The categories are further elaborated in section 2.3 and 2.4 and summarized in a table in Appendix A.		
6	TL	828	ed	Registering to a category The responsibility referring to 'it' could be interpreted as the SP or the Home Federation. Meant is the SP, so be more specific.	now: If a Service Provider is registered to the category non-PII, it takes the responsibility of ensuring that	Ok	changed

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
					new: If a Service Provider is registered to the category non-PII, the Service Provider takes the responsibility of ensuring that		
7	TL	840	ed		jurisdictions not jurisdictions	Ok	changed
8	TL	846	ed	Service Providers manifesting no category The last sentence does not provide additional info. It is obvious since the profile requires the choice of one of the two categories.	now: If a Service Provider does not manifest any category, it is assumed that the Home Organisations and Identity and Service Providers have fulfilled the obligations set by the data protection directive using an out-of-band mechanism. This is the default for Home Organisations and Identity and Service Provides who have not adopted this profile. new: If a Service Provider does not manifest any category, it is assumed that the Home Organisations, Identity Providers and the Service Provider will fulfil	ok	changed

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 obligations set by the data protection directive using an out-of-band mechanism.		
9	TL	851	ed		Category PII: SP processes personal data now: In category PII, the Service Provider is processing personal data because it receives Attributes which are considered personal data from the Identity Provider. new: In category PII, the Service Provider is processing personal data because it requests Attributes from the Identity Provider which are considered personal data.	Not ok. Juridically, processing of personal data starts when it receives (not requests) PII.	no changes
10	TL	863	ed		now: The Service Provider being a data processor or data controller may depend on the Home Organisation. The Service Provider may have a data processing agreement with	ok	changed

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
					some Home Organisations in eduGAIN, making the Service Provider a data processor for those Home Organisations. For the rest of the Home Organisations, the Service Provider may be a data controller. new: Whether the Service Provider is a data processor or data controller may vary per Home Organisation. With some Home Organisations in eduGAIN, the Service Provider may have a data processing agreement and acts as a data processor. For the other Home Organisations, the Service Provider acts as a data controller.		
11	TL	871	ed		Purpose of processing now: The data processing agreements signed by the data controllers and processors may be more specific on what is the purpose of processing.	ok	changed

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
					new: A bilateral data processing agreement signed by a data controller and a data processor is likely to be more specific on the purpose of processing.		
12	TL	878	ed		Informing the data subject now: and expose it to the eduGAIN metadata. new: and expose this URL to the eduGAIN metadata.	ok	changed
13	AS	886	ge	Before releasing the end user's Attributes to the Service Provider for the first time, the Identity Provider must provide the Service Provider's clickable privacy policy URL to the end user. Who is responsible for making sure that the identity provider do this right? The federation or the idp		This is not different from responsibility on metadata in general. Home Federation rejects the metadata if mandatory parts are missing, the rest is up to the provider. Instructions to the Provider need to be given by the Home Organisation, of course.	no changes

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
				themselves?			
14	TL	887	ed	Since it is marked as an example we can drop the 'if necessary'.	now: This can be done, for instance, when an end user consents, if necessary, to Attribute release (see next section). new: For instance, the Identity Provider displays the URL, when an end user consents to Attribute release (see next section 2.3.4).	Not ok. If attribute release is based on necessity (not on consent), the URL need to be shown to the end user. The current wording supports this alternative better.	not changed
15	TL	890	ge	> What if the Attribute requirements or other issues above change? > Anything about re-consent? It could be included into the paragraph above, where it now just refers to the first time.		OK to add that to lines 886-889. This still leaves an open question if implementations keep track on the list of attributes to which an end user has consented, and is able to spot if the list has changed.	changed "Before releasing the end user's Attributes to the Service Provider -for the first time, or -for the first time after an extension in the Attribute set for this Service Provider, the Identity Provider must..."

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
16	TL	892	ed	If the SP is a data processor, the Home Org has to be a data controller, so we can drop that. It is anyhow obvious.	now: The data controller is responsible for informing the end user on processing his/her personal data. If the Service Provider is a data processor and the Home Organisation is the data controller, the Service Provider may refer to the Home Organisation in its privacy policy web page. new: The data controller is responsible for informing the end user on processing his/her personal data. If the Service Provider is a data processor, the Service Provider may refer to the Home Organisation in its privacy policy web page.	ok	changed
17	TL	911	ed		replace 'providers' with 'provides'	ok	changed
18	GW	911	ed	This assumes that the end user was not forwarned about the processing (for example, when the data was first collected by the home organisation), in which case this prompt would be unnecessarily	If Attribute release is based on necessity, and the end-user has previously consented to his/her data being processed having been previously informed, the end-user should not be prompted, otherwise	Not ok. Proposed text does not clarify but confuses the reader. According to the law, the Home Organisation needs to inform the user on processing personal data in the Home Organisation's local	Refined text in 2.3.3, 2.3.4 and 4.5. Now requirements are in 2.3.3 and 2.3.4 and suggested technical implementation is

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
				inconvienient	a prompt with the following or equivalent text should be presented 'I am informed on release….'	identity management system even if federated identity management and eduGAIN never existed… It's better that eduGAIN policy covers only issues which follow from eduGAIN. Informing an end user on eduGAIN when his/her personal data is collected for the first time in the Home Organisation does not set the Home Organisation free from the duty of informing the end user on release of his/her personal data to a Service Provider (see lines 880-885).	placed to 4.5.
19	TL	915	ed		now: Provider's privacy policy (see the previous section). new: Provider's privacy policy (see the previous section 2.3.3).	ok	changed
20	TL	945	ge	> Attributes revealing racial or ethnic origin, political opinions, > religious or philosophical beliefs,		(ref. vc 6.9) Replace the sentence by a reference to the DP directive: "Attributes revealing data that the	changed: "Attributes revealing data that the data protection

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
				trade-union membership, and > the processing of data concerning health or sex life should not be > released in eduGAIN. Do we really need this? I do not understand what 'the processing of data' has to do with 'released in eduGAIN'. A simple cn may reveal or at least strongly hint at someones religious origin...		data protection directive defines as sensitive personal data should not be released in eduGAIN”. The reason for this is that if sensitive data is not processed, risks are lower and IdPs less reluctant to release attributes. There are no known court cases on person’s common name counting as sensitive personal data.	directive defines as sensitive personal data should not be released in eduGAIN. “
21	GW	953	ed	Spelling mistake ’categoty’	catagory	ok	changed
22	TL	959	ed	Registering a Home Organisation's conformance The last sentence does not provide additional info. The profile requires one or both of the two categories.	now: If a Home Organisation does not manifest conformance to this profile, it is assumed that the Home Organisation and the Service Providers have fulfilled the obligations set by the data protection directive using an out-of-band mechanism. This is the default for Home Organisations and Identity and Service Provides who	ok	changed

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
					have not adopted this profile. new: If a Home Organisation does not manifest conformance to this profile, it is assumed that the Home Organisation and the Service Providers will fulfil the obligations set by the data protection directive using an out-of-band mechanism.		
23	SC	964	ge	Introduction of new metadata extension to capture adherence to DPP.	I would suggest this be expressed using a SAML Attribute via the EntityAttributes extension. Whenever something can naturally be expressed as an attribute of the entity, this is usually the best way to express it to make the information available to implementations.	Not ok. This element is a child of a <RoleDescriptor> element. Metadata EntityAttributes spec (Committee specification 01, 4.8.2009) defines EntityAttributes only for <EntitiesDescriptor> and <EntityDescriptor> elements: *"180: The meaning of this element is undefined by this profile if it appears anywhere else within a metadata instance, or within any other XML document"*	not changed
24	TL	964	ed		Technical implementation I would move chapter 4 to Annex A and rename the existing annexes to	Not ok. The technical implementation of the DP profile in SAML metadata is integral part of it, not just an appendix.	not changed

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
					B and C.		
25	AS	964	ge		XML Extension to data protection profile: what about using entityattributes instead of a new namespace?	see item DP-23	See DP-23
26	TL	1040	ge		line 1040: Include the xml:lang="en" into the example. Good examples generlly help for wide adootion later on. <mdui:PrivacyStatementURL xml:lang="en"> http://www.example.org/privacypolicy.html </mdui:PrivacyStatementURL>	ok	changed
27	TL	1046	ed		ff: 4.4. Criteria for making data processing legitimate Here you should refer to 2.3.4 and the hints provided there for necessity or conent.	ok	added a reference to 2.3.4
28	GW	1071	ed	This repeats parts of 907-915	Merge or reference both sections to improve legibility	ok	See DP-18
29	TL	1074	ed		4.5. Identity Provider behaviour	see DP-14	no changes

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
					now: ask him/her to consent, if necessary, to the Attribute release. new: ask him/her to consent the Attribute release, if necessary.		
30	TL	1076	ed		4.6. Service Provider behaviour now: A Service Provider relying on the data protection mechanisms provided in this document and belonging to category PII must, before accepting any Attributes, ensure that the Identity Provider manifests conformance to category PII. new: Relays a Service Provider on the data protection mechanisms defined in this document and belongs to category PII, the Service Provider must ensure that the Identity Provider manifests	ok	changed: Relays a Service Provider on the data protection mechanisms defined in this document and belongs to category PII, the Service Provider must ensure that the Identity Provider manifests conformance to category PII before the Service Provider accepts any attributes.

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
					conformance to category PII before it accepts any Attributes.		
31	TL	1079	ed		4.7. Service Providers which have "multiple faces" new title: 4.7. "Multy faced" Service Providers	ok	changed
32	TL	1084	ed		now: the Service Provider registers several entries (with separate entityIDs) in the metadata, or new: the Service Provider registers multiple entities (with separate entityIDs), or	ok	changed
33	GW	1381	ge	If the SP changes their attribute requirements, it should be up to them to inform IdP's using whaterver means they have available		The other alternative, on which the profile currently counts, relies on the Identity Provider remembering the list of attributes (just attribute names, not values) whose release the user has consented to. At least uApprove for Shibboleth supports this.	See DP-15

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
34	GW	1385	ge	It may not make a difference to implementations, but the information is very useful for IdP's to gain a greater understanding of the SP expectated attributes		Probably yes. Current DP profile does not make any difference between Required and non-Required attributes. The profile assumes that both Required and non-required attributes are Relevant for the service (see section 2.5 of the profile). If non-Required attributes were not relevant for the service, then, following from the directive, the service should not get them, at all.	no changes

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