Attribute Release Recommendations

Status Update -- REFEDS Attribute Release Discussions

Goals:

1. define an approach to the data protection/privacy liability risks and exposures faced by IDPs and SPs in the worldwide Higher Education /Research environment when sharing attributes.
   a. Make it as simple as possible for campus users to successfully login and enter destination SP sites
   b. Remain compatible with regional and national laws and regulations guarding privacy
   c. Find an appropriate balance between risk and value for all parties
2. Define a scaleable approach to managing attribute release policies that works for all three parties (SP, Federation, IDP)
   a. Provide recommendations on metadata usage to support the scaleable approach
   b. Provide recomendations on GUI requirements to meet the legal and regulatory requirements.
   c. Provide suggestions to Federations, IDPs, and SPs on Business Practices that are believed to be compliant with EU regulations.

In developing these recommendations the Working Group has proceeded on the assumption that the combination of EU Privacy Regulations and European national laws will present the most difficult environment within which these recommendations will have to operate. Consequently, this document will frequently reference EU concepts and models. The Working Group considered the following issues to be out of scope for its efforts:

1. The end user has not reached the legal age, and parental involvement of some sort must be involved in the attribute release process.
2. The issues that arise if an an IDP in the EU releases PII attributes to an SP in the US (Safe Harbor framework)

Current Reading of EU Regulations

1. The starting points are:
   a. The EU Data Protection Directive 95/46/EC (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML,
   b. Additional material is provided by the Art.29 Data Protection Working Party http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm, in particular their Opinions on the Concept of Personal Data http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf and Consent http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.
   c. In addition, while the legal principles are buried in the Directive, the UK law provides a different presentation, which may be more readable: http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/I

```
Mikael: Alternatively, we could refer to the OECD privacy principles, which have been
the basis for the data protection directive. They are almost the same:
http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html
The benefit is, that OECD is not limited just to the UK or Europe.
```

1. This effort will rely on generally accepted interpretations of EU Regulations, while noting that there are interpretations that conflict with those presented in this paper.
   a. There is a reluctant conclusion that there are few, if any, attributes that every EU regulator will agree aren't PII when they are linked to an IP address or AAI session ID. We are therefore treating the class of guaranteed non-PII attributes as small to non-existent. Consequently, these recommendations do NOT categorize SPs into PII and non-PII categories, as was done by the eduGAIN DPGPD.
   b. The IDP bears primary responsibility when attributes are released.
   c. User Consent for Release is defined as any positive, unambiguous indication of the user's specific agreement; the user being fully informed of the consequences of their agreement and under no pressure to either grant or withhold consent. "No pressure" means, for instance, that accessing the SP is a) not a requirement for a person's job, or b) not a requirement for doing course work, c) etc.
   d. User consent must be "specific and informed" is the Art29WP mantra. i.e. given to each SP separately.
   e. The end user MUST be informed of the Service Provider's Privacy and Data Protection Policy.
2. This effort's recommendations, based on those interpretations:
   a. an SP MUST divide the set of attributes it is requesting into categories of NECESSARY and REQUIRING CONSENT
   b. An Attribute is NECESSARY if the service that the user has requested cannot be delivered unless the Attribute is released. (Minimal disclosure) "(David: it might be more complex: 'delivering' the service may be more than just access control. It might also cover important functionalities of the service. This makes the judgesment of 'necessary' somewhat harder... Related comment by Andrew below)"
   c. An Attribute is categorized as REQUIRING CONSENT if the service can operate without it, but the service will provide additional value to the user (or to other users of the site) if the Attribute is provided.
   d. Note that these interpretations are different from those used in the eduGAIN DPGPP document (URL).
      i. The eduGAIN DPGPP categorized services as being based either on consent or necessity. The interpretation presented in this report requires that individual attributes be defined as either consent or necessity. This model means that the list of necessary attributes for a particular service should be the same for all users.
      ii. The DPGPP defined NECESSARY as "necessary for doing one's job". That definition can produce a different answer for each user (and potentially, even for the same user at different times!). In addition, the IDP would still have to offer all users the choice of whether to release the attributes that *aren't* necessary for the service. Consequently, it seems simpler to use a crieria of "necessary to deliver the service" (Article 7f in the Directive), and then divide the attributes based on which *are* necessary to deliver the service and which are not necessary (but the service could make use of them if provided). Attributes in the latter (if any) are categorized as REQUIRING CONSENT.

Managing Liability (the NEED FOR CONTRACTS)

'**Relevant Points'**

1. Contract or NOT. Much of the EU regulation and law expect an IDP and SP to sign a bilateral contract, and that this contract would address the sharing and handling of user attributes, and which party assumes which aspects of liability. When a contracts exists, it should help to clarify all of these issues. However, it is extremely rare to find research and collaboration situations where a contract has been signed between the two parties. In some cases, one of the parties may not be a legal entity. In these situations, clearly, there is no clarity.

Mikael:I’m not sure if this is a too strong statement. If the IdP is a data controller and SP a data processor (“processes personal data on behalf of the IdP”), this is true. Otherwise, it is unclear. For sharing liability, contract is necessary, but otherwise… Andrew may have an opinion here.

Andrew: See http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_1.aspx
"A decision to share personal data with another organisation does not take away your duty to treat individuals fairly. So before sharing personal data, you should consider carefully what the recipient will do with it, and what the effect on individuals is likely to be. It is good practice to obtain an assurance about this, for example in the form of a written contract."

1. Commercial SP vs non-commercial. Obviously, this is related to the contract issue. In most cases commercial SPs will require contracts before offering services. There are exceptions, however (eg DreamSpark). Commercial SPs can go bankrupt, in which case the bankruptcy lawyer might consider a collection of PII attributes to be an asset that could be sold.

Mikael: I doubt this can be easily done in EU… Personal data is collected to a specific purpose, and can't be further processed to a purpose which is conflicting with the original purpose.

1. There are actually two different risks in attribute sharing situations:
    a. Regulatory Risk. An appropriate contract *can* remove the risk of regulatory action. Some regulators are likely to consider that some kinds of PII should not be disclosed unless there's a contract between the parties. In this case there's a risk that the regulator will fine the IDP for an unlawful disclosure, or order that the disclosure stop until there is a contract.
    b. Harm to Users. If the release of attributes causes harm to a person then they can sue the IDP, possibly even if the harm is the SP's fault. Potentially, a contract between the IDP and the SP could transfer this risk from the IDP to the SP (e.g. who bears the cost of the court case and paying the damages). Without a contract, the IDP alone bears this risk. Presumably, before signing such a contract, the SP needs to have both a reason to accept the risk and some ability to control the level of risk it is accepting.
2. The EU Data Privacy Guidelines define two other Roles in the attribute release process: data controllers and data processors. Originally the distinction was straightforward: controllers had independence in choosing how personal data were used, processors didn't as they only did what they were told by the controller. But various types of joint and sub-contracted activity are organized in ways that do not neatly fit that model. The latest Article 29 WP guidance [1] takes 35 pages to try to provide clear explanations. Some Member States (like Finland) don't use the concept of processor at all.

- For the attribute release discussion I suspect it doesn't make much difference: at most it's a sub-bullet within the "do we need a contract" section. Being a data processor means that some of the SP's duties are transferred to the IdP, but to achieve that there has to be a contract between the two setting out the relationship. "(David: If an SP recieves attributes it becomes responsible for the received data: data controller. It may be different in other countries (even though I doubt it) but there is no way that an SP in the Danish context can be 'data processor'. Mikael: that's not true. A software-as-a-service provider is a typical data processor, and a typical SP at least in Finland.)". Hence I think it is at most a comment that "a contract may also be used to establish that the IdP and SP are in a data controller/data processor relationship, rather than both being data controllers".
- Incidentally DLA Piper considered that it would be rare for an SP to have so little freedom of decision making that they'd count as a data processor (even though they did expect that there would be contracts in the majority of cases). Within UK interpretation I suspect it could be more common than that, but it doesn't feel like an approach that's going to be a big win in inter-federation activities. [1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

'**Recommendations'**

1. If there is a contract, then the IDP should ensure that the contract address all of the liability issues.
2. If there is no contract, then the IDP should identify approaches to lower the risk.
    a. (Mikael) article 17 introduces the idea that the measures to protect PII are lower for low-risk-attributes:

Article 17. Security of processing.
1. Member States shall provide that the controller must implement appropriate *technical and organizational* measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of *security appropriate to the risks* represented by the processing and the nature of the data to be protected.

1.
    a. When there is no contract, then it's up to the IdP's risk appetite - the regulations assume that each IDP will assess the risk with each SP. In the absence of any additional information, suggestions, or hints, it is reasonable to assume that a group of IDPs will produce a variety of answers. One problem with this approach is that it is not scaleable -- it is extremely unlikely that every IDP would be able to assess every SP. The problem for SPs in this environment is that they cannot know how many IdPs are going to be willing to release, so will always have to cope with less than 100% coverage of its users.
    b. The Federation Participation Agreement, signed by all Federation members operating IDPs and SPs, addresses risk situations and imposes requirements on how SPs process and handle attributes [approach used by InCommon].

-
    - The intent of the language in the PA is to help SPs persuade IdPs that the risks of releasing attributes without a contract (plural because as previously discussed there's the risk of harm to the user and the risk of regulatory action) are acceptable. The SP

needs to make the case that the benefit to the IdP of its users accessing the service outweighs the risks to the IdP of uncontrolled attribute release. I would expect that case to involve at least explaining that the SP has done all it can to minimise the risk: at least by requesting only the minimum attributes needed, choosing less potentially harmful options (e.g. ePTID rather than ePPN)), and making some sort of statement about how the information will be protected. "(David: don't expect the SP (in most cases) to neither understand the true meaning of the individual attributes nor respect 'minimal disclosure'. Our experience is that ARP must be negotiated and the meaning of attritbutes explained thoroughly. We have also seen SPs walk away because they did not get what they wanted (phone number, email, social security number etc.)"

- [Nicole has done a fairly extensive mapping of Federation agreements, and is reseaching how many of them have language governing the SP's use of attributes.]

1.
    a. The SP could provide a statement of practice to reassure some IdPs that the risk of disclosing PII was acceptably low. However, the law that the regulator will be concerned about talks about a "contract *between* the parties", not a declaration by one of them.
    b. The French Federation has created a process where the Federation investigates each SP and places them into categories; in addition, the Federation developed for each SP a recommended set of attributes to be released. Thw IDP can then decide whether or not to accept the Federation's recommendations. This approach doesn't cause the IDPs liability to disappear, but MAY result in an IDP being more comfortable releasing attributes.

There are four different deployment models in common use. Each should be examined separately for risk; each probably requires its own unique approach.

Bilateral Relationship with Contract

This situation is the best fit with the common interpretation of the EU Guidelines. The contract between the IDP and the SP should address which entity is responsible for the various risks.

Unfortunately, even where contracts do exist, i.e. contracts for library resources, they rarely cover DPA issues etc. I've spoken to JISC collections about it in the past and they have said there is zero interest in including this information.

Central IDP providing Attribute Release

[This sections needs to be fixed.] An approach (used by WAYF, SIR, ?FEIDE since a few years now) is to let all SPs and IDPs in the federation sign an agreement, as part of joining to the federation, that they live up to XX requirements.

Feide does not sign contracts with individual applications, but with service provider organizations. Any participating educational institution have a SP-clause in their IdP contract (in our case, the Home Organization contract, as we are single-IdP). In practice, this leads to a situation where any service provided by a university may submit information for setting up a Service Provider

1. Application for attribute release this is input to our IdP portal, where each "IdP" decide if the service information flow is acceptable for their users a decision made by designated administrators used as input to the "consent/infoflow" UI, displaying info for each individual user at first-time login to the SP
2. Metadata for the SP We have separated the metadata from the application for attribute release, since we want a two-step process for attribute release. Most VO and HEI-related SPs currently fall into the operated-by-university category, and do not require separate contracts.

"(David: WAYF signs a contract with each individual SP (not service provider organisations) which describes the purpose of the service (same wording as presented in the end user consent dialogue) and the attribute release policy (the result of negotiation with WAYF, balanced with the purpose of the service). If the ARP needs to be changed later, a new contract is written and signed. The overall architecture is 'opt-out' meaning that attributes may be released from any IdP to any SP, except if the IdP has decided to block (opt-out) of data release to a given SP.)"

Inter-Federation Situations

Federations rely on each other, and common approaches to handling risk.

SAML 2 Metadata Recommendations

SAML 2 Metadata is defined in Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0), with various addenda, and in assocaited specifications.

1. RequestedAttribute elements in each SP entry are used to describe the attributes that that the SP needs and desires.
2. The metadata MUST indicate whether an attribute is in the NECESSARY or CONSENT REQUIRED category.
3. For each CONSENT REQUIRED attribute, the metadata SHOULD provide a textual description of why the SP is asking for this attribute (eg what added value a user would obtain by releasing it)
4. Entity Attributes in each SP entry are used to assign each SP to one or more categories.
    a. (need to describe what this element would be used for; this is a way to support "SP Categorization"; possibly, each category has associated with it a default set of attributes for release).
    b. list of recommended TAG values for various categories
5. SP entries MUST contain elements for DisplayName, Description, Logo, and PrivacyStatementURL. The requirements for the content of the PrivacyStatement are listed in the next section. These elements are defined in SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0.
6. If we agree that attribute release in general is always based on necessity (+ optional attributes on consent), then the DPGPP document's LegalGrounds element becomes unnecessary.
7. The metadata SHOULD include a way of indicating that an IDP or SP operates in conformance with these recommendations.

```
Mikael: This could mean in practice a metadata extension element which carries a URL which
resolves to a digitally signed document or a scanned paper with a handwritten signature, where
the IdP/SP owner commits to certain rules.
```

GUI Recommendations

1. The IDP MUST present the DisplayName and Logo of the SP, and SHOULD present the Description (this information can be obtained from Federation metadata; see SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0) "(David: I would go for 'MUST present the description' - in stead of SHOULD)."

Mikael: Why logo is MUST? I understand logos are good for usability, but is it a must
from privacy perspective? Or do we just want to enforce a good practice?

Nicole: How can we say must display when this information is available at all in the metadata as yet?
What does the IdP do if the information is absent?

1. The IDP MUST present the SP's PrivacyStatementURL. This is done even if all attributes are released based on NECESSITY.
2. The Privacy and Data Protection Policy policy must be available at least in English and address the issues presented in Article 11 of the data protection directive:
    a. Identity of the controller and of his/her representative, if any
    b. Purposes of the processing
    c. Any further information such as;
        i. Categories of data concerned
        ii. Recipients or categories of recipients
        iii. Existence of the right of access to and the right to rectify the data concerning him/her

Mikael: In Finland, we have issued a template (in Finnish/English) for an SP's privacy policy:
http://www.csc.fi/hallinto/haka/ohjeet/palvelut-yllapitajille/tietosuojaseloste.html

Nicole: As above, how can you enforce presenting information that isn't currently available in the metadata?

1. The IDP MUST present a list of the attributes defined as NECESSARY. No user consent is required before release. (However, given how web browsers work, the user may have to click a CONTINUE button in order to continue in the sequence.) (I don't actually think the "notify" one needs a button: so long as it's clear to the user that the consequence of their next action will be to release the attributes then that seems to satisfy the requirements of the Directive. So, for example, I'd see no problem in putting up a description of the attribute release on the same screen as the username/password entry boxes, making clear that *if* you login then this is what'll happen. NOTE -- the attribute values for the specific browser user are not available when the login screen is presented, since the user's identity is not yet known.))
2. The IDP MUST present a list of the attributes in the REQUIRING CONSENT category. The user MUST be able to consent/block each individual attribute (and value?). We may come back to this in talking about attribute groups, where it really doesn't make functional sense to consent to only one of a set of attributes, but if the attributes are separate (e.g. suppose a site that asks for display name and date of birth, both on grounds of consent rather than necessity) then you have to be able to consent separately too. Saying "we can only address you by name if you tell us your birthday too" sounds to me like invalid consent to both :(
3. The IDP should provide the ability to configure localised descriptions of the attributes (e.g. what PersistentID means)
4. The IDP MUST remember which attributes' release the user has consented to (if consent is used), or been informed of (if NECESSITY is used). If an SP's attribute release policy changes, the user MUST be prompted again for INFORM and/or CONSENT.
5. (major issue, creating confusion) There are sets of attributes that are very similar, sometimes overlapping. The best example of this is the set of attributes related to a person's name(s). An SP may request all of a person's name attributes, which will result in a cluttered and confusing attribute release GUI. (suggest some standards for handling these reaquests?) More information available in this posting from Scott.

Attribute Harmonization

1. start with eduPerson
    a. In the eduGAIN policy work we discussed what to do with the inconsistent semantics of eduPersonAffiliation. This Doodle poll presents the alternatives and the preferred one: http://doodle.com/me2xgh4ctgrypbg7
    b. However, we concluded that the fastest way forward for eduGAIN is that we don't introduce a new attribute but use ePA and just declare some ePA values (staff, employee) unrealiable.
2. is this a document where we want to make recommendations on persistentID vs ePTID vs ePPN? Or ePA vs ePSA?
3. Need to identify specific attributes that are "standard"

SP Categorization

SP Categorization is a service provided by Federations. They review and examine member SPs, paying particular attention to their business processes and handling of received attribute values. They also evaluate the set of attributes requested by the SP, assigning them to the NECESSARY, REQUIRING CONSENT, and UNNEEDED categories. The goal is to reduce the effort that each individual IDP must make in deciding which attributes to release to each SP. IDPs might use the Federation's opinion as supporting evidence for their decisions about attribute release.

Federations use several different models to share their conclusions with IDPS:

1. RequestedAttribute elements in the SP's metadata entry. IDPs could create release policies triggered by these elements.
2. EntityAttributes elements in the SP's metadata entry. IDPs could create release policies triggered by these elements. These elements could contain different values, assigning the SP to one of several different categories. Each category has associatted with it a set of attributes to be released.

Federations would have to take some care in defining categories. For instance, it seems to me that sites supporting Collaborative Work will likely all require the same (or extremely similar) attribute sets. Sites providing utility services (eg Foodle) will likely require a similar (but different) set.

CONCERN: If we associate different set of attributes to different categories, this might be going against minimal disclosure principle. Behind a same category, we can have different applications with different attributes needs. I doubt that we can standardize this way. Even if it's more work for federation operators we should stick to necessity, i.e. minimal disclosure. "(David: WAYF has been recommended to created categories (attritbute profiles, see http://wayf.dk/wayfweb/attribute_profiles.html) - but not for specific services or groups of services. Any deviation from these profiles, when assigning ARPs to SPs should be explained in the contract)."

1. The Federation could publish recommendations as to which attributes should be released to each SP. Individual IDPs would each make their own decisions about each SP, consulting the Federation's recommendations but making their own decisions about which attributes to release. "(David: I would strongly recommend this approach as I believe most IdPs will see it as a big help if the federation operator takes position and helps in defining ARPs.)"

Mikael: I'm not against IdPs making individual decisions, but I would still emphasise on trying
to ensure the RequestedAttributes elements are reliable and the IdPs can normally rely on it.
If there is a problem in RequestedAttributes, the issue should be escalated to the federation
which has registered the SP.
This is a scalable approach. Individual IdPs one-by-one challenging the SPs
RequestedAttributes scales poorly in a federation and especially in an interfederation.
Of course this expects a globally shared practice on the interpretation of "minimal disclosure" and
"NECESSITY vs CONSENT REQUIRED".

But, perhaps, most of the work is the process of analyzing an SPs requirements; entering information into an SP's metadata element may be just a very small part of the overall effort.

How does the RENATER approach work today -- It's not exactly that way. As you can see on this link (https://services-federation.renater.fr/renater/filtres/) we do have these categories of SPs but the set of attributes can differ from a SP to another in the same category. It's just a way of sorting to help IDP managers to select and configure more easily relevant resources. But, as federation's operator we moderate some SPs attributes demands, explaining that the more attributes they ask (see PII), the more inconveniences with the regulator they will have. (But, would it reduce the risk sufficiently that many IDPs would be willing to proceed under this system ? It depends if PII are involved or not, if yes, IDPs have no choice, they have to contract with the SP.)

Suggestions about some possible categories and their associated attribute bundles:

1. collaboration: persistendID(Mandatory),mail(Optional),cn(Optional)
2. library: ePSA(M),ePE(M),mail(O)
3. elearning: persistentID(M), cn(M),mail(M), ePSA(M), eduCourseMember(M), schacUniquePersonalID(M)
4. escience: persistentID(M),ePSA(M),schacHomeOrganization(M),mail(O)
5. VOs/Collab: name (displayName? formal name?), eppn, email, affiliation, project?), students (class enrollment?)

I am trying to map the requirements onto something like page 4-6 of the Feide attribute specification http://www.feide.no/sites/feide.no/files/documents/norEdu_spec.pdf

Outstanding Questions

1. "an SP MUST divide the set of attributes it is requesting into categories of NECESSARY and REQUIRING CONSENT" -- does an SP still need to identify whether any of the requested attributes are in the PII category ?

Mikael: Perhaps we just assume that all atributes are PII

1. guidelines on how often the same user needs to consent to the attribute release to the same SP? The EU directive says that just once is enough, a recent usability study [1] proposes end users want to reconsent every now and then (like 6 months). [1] https://tnc2011.terena.org/core/presentation/71
2. Which attributes are considered to be PII ? "(David: presume that any information about any user IS PII and treat it as such)."
    a. Probably varies from one country to the next....
    b. EPTID is PII. It's safe to assume it is.
    c. But an even stricter view is that any attribute (eg. EPSA) is PII, because the SP can reveal the end user's identity if it combines its log files with the IDP. What will we do with this? (Federation contracts prohibit such collaboration between IDPs and SPs. eg IDP to agree that it will never provide an SP with the identity of any anonymised user, but will investigate and deal with any complaints itself.) "(David: I doubt a federation policy can prohibit any lawful investigation which includes tracking down a user in case of breach. I you look at the anti-terror legislation already implemented, it does not make sense for a federation policy to have opinions going in the oposite direction...)". "(Andrew: I'm not trying to prevent lawful investigations, I'm trying to prevent unlawful ones, where the IdP decides to tell the SP the real identity of the user (in breach of minimum disclosure) just because the SP feels it has a complaint against them. This doesn't stop the SP, or anyone else, using a legal process (e.g. a court order) to obtain that identity, but I'm assuming that most problems can actually be resolved without legal action, and in that case it's the Home Organisaiton that needs to do it)"
3. And, unfortunately, "comply to EU regulations" means different things in different countries
4. if the purpose of the service provider changes radically, the user may need to be informed on the attribute release again, and, if attribute release is based on consent, s/he may need to re-consent to the attribute release. How does the IDP-side consent/necessity module learn the change in the purpose of the SP, if the SP does not change its entityID "(David: information about prior consents could include a hash of the purpose description. If it changes, new consent is needed. Mikael: You mean hash of <mdui:Description> ? Interesting idea... This would imply <mdui:Description> is MUST)".
5. We need to vet the principle "an IDP can release attributes if the SP decribes them as NECESSARY" against the various national laws. (However, the interpretation that attributes can be released based on necessity (article 7f) needs to be verified against the national laws. For instance, it appears that in Finland we must use consent if PII is released to a service which is not related to research and education (the purpose of processing changes). This may imply that, in the consent/necessity module implementation, there should be support to a metadata extension tag that, if present, overrides the per-attribute consent/necessity thing. Haka federation operator could then flag these SPs from the Haka federation metadata using the XML tag, and the IDP consent module would always ask user consent for them.)
6. How to indicate that an IDP or SP is operating in conformance with these recommendations ?

Out of Scope

1. end user is under the legal age
2. If PII is released from an IDP in EU to an SP in the US (or other country with incompatible privacy laws), the EU law expects the SP to sign a contract where it commits to the European data protection principles. How to organise this in a scalable manner?

RESOURCES

1. The original REFEDs paper - and, on a UK level, our Federation recommendations - were attempts to codify good practice in a way that referenced the law but didn't depend on it. The REFEDs paper is definitely out of date following the Art29WP Opinion, but it might be the sort of approach we could use.
2. The eduGAIN Policy Framework Data Protection Good Practice Profile (
3. The final ver 1.0 is available in http://www.geant.net/service/edugain/resources/

Threads user to create this document:

- Summary So Far………
- Data protection and attribute release issues
- when can user consent be provided....
- Remaining Steps
- technical recommendations....