

Status Update
REFEDS Working Group
Attribute Release Recommendations

Steve Carmody

Mikael Linden

Sept 14, 2011



REFEDS

TOPICS

- Goals
- A new(er) interpretation of the the EU Data Protection Directive
- Preliminary Recommendations
- Next Steps
- Questions.

Goals

- Find an approach to the data protection/privacy liability risks and exposures faced by IDPs and SPs in the worldwide Higher Education/Research environment
 - That makes it as simple as possible for campus users to successfully login and enter destination SP sites
 - Is compatible with regional and national laws and regulations
 - Finds an appropriate balance between risk and value
- Find a scaleable approach to managing attribute release policies.



In Scope

- Provide suggestions to Federations, IDPs, and SPs on Business Practices and Policies that are believed to be compliant with EU regulations.
- Provide recommendations on GUI requirements to meet the legal and regulatory requirements.
- Provide suggestions to Federations, IDPs, and SPs on scaleable approaches that simplify the management of attribute release policies.
- Provide recommendations on metadata usage to support the scaleable approach



Out of Scope

- Browser user is under the legal age
- Issues that arise if an an IDP in the EU releases PII attributes to an SP in the US (Safe Harbor framework)

The New Interpretation

- There are few, if any, attributes that every regulator will agree are not PII when they are linked to an IP address or AAI session ID.
- An Attribute is **NECESSARY** if the service that the user has requested cannot be delivered unless the Attribute is released. (Minimal disclosure)
- 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.



Major Differences with the DPGPP Interpretation

- SPs self-assigned themselves to categories (category PII or non-PII)
 - All attributes now considered to be PII
- **NECESSARY** was defined as
 - related to an employee doing his work
 - related to a student taking his courses and otherwise being educated
- That definition comes up with a different answer for each user (and potentially, even for the same user at different times!)



Recommendations Brought Forward Today

- Policy Framework
- Consent GUI Recommendations
- SAML 2 Metadata Recommendations



Policy Framework

- An SP **MUST** divide the set of attributes it is requesting into categories of **NECESSARY** and **REQUIRING CONSENT**
- An Attribute is **NECESSARY** if the service that the user has requested cannot be delivered unless the Attribute is released. (Minimal disclosure)
- Services with **NECESSARY** attributes must use a UI to notify the user of the release.



Policy Framework (more)

- 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.
- 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.
- The user **MUST** provide Consent before **REQUIRING CONSENT** attributes are released.



Policy Framework (more)

- Services with some **NECESSARY** and some **CONSENT**-based attributes will require a hybrid release UI (notification and consent).



Consent GUI Recommendations

- When requesting Consent, The IDP MUST present the DisplayName, Logo, and Description of the SP
- The IDP MUST present the SP's PrivacyStatementURL. This is done even if all attributes are released based on NECESSITY.
- The SP's 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



Consent GUI (more)

- The IDP **MUST** present a list of the attributes and values the SP has defined as **NECESSARY**. No user consent is required before release.
- The IDP **MUST** present a list of the attributes and values the SP has defined as **REQUIRING CONSENT**. The user **MUST** be able to consent/block each individual attribute and value.
- 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 **NOTIFY** and/or **CONSENT**.



Consent GUI (more)

- The IDP should provide the ability to configure localised descriptions of the attributes (e.g. what PersistentID means)
- Major Issue -- There are sets of attributes that are very similar, sometimes overlapping (eg names) An SP may request all of a person's name attributes, which will result in a cluttered and confusing attribute release GUI.

SAML 2 Metadata Recommendations

- RequestedAttribute elements in each SP entry are used to describe the attributes that the SP needs and desires.
- The metadata **MUST** indicate whether an attribute is in the **NECESSARY** or **CONSENT REQUIRED** category.
- 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)



SAML 2 Metadata (more)

- SP entries **MUST** contain elements for `DisplayName`, `Description`, `Logo`, and `PrivacyStatementURL`.
- the DPGPP document's `LegalGrounds` element is no longer unnecessary.
- The metadata **SHOULD** include a way of indicating that an IDP or SP operates in conformance with these recommendations.



Next Steps (discussions already underway)

- Develop recommendations related to risk and the need for contracts
- Develop recommendations on Attribute Harmonization
- Develop recommendations to simplify the process IDPs would use to manage attribute release policies
- Projected delivery date --



Questions ?



Slide title goes here

www.internet2.edu

INTERNET[®]
2