Notes on Implementation of INFORM/CONSENT GUI Interfaces

1. Notes on Implementation of INFORM/CONSENT GUI Interfaces

The Data protection directive and interpretations create a set of requirements for the INFORM and CONSENT interactions with the user. This Data protection Code of Conduct proposes a division of responsibility where the INFORM and CONSENT interaction is carried out by the Home Organisation of the user, for instance, in an INFORM/CONSENT Graphical User Interface (GUI) installed to the Identity Provider server.

However, the Data protection regulators and the groups developing and enforcing these regulations recognize that there is a balance between full disclosure to meet the requirements and usability. A poor design of the user interaction screens can actually reduce the likelihood that users will understand what is happening.

1.1 Requirements from the Directive

For the requirements on informing the end user, see Introduction to Data protection directive, section 8.

For the requirements on user consent, see Introduction to Data protection directive, section 9.

Note: Introduction to Code of Conduct proposes to defer release of optional extra Attributes based on user consent until Phase 2.

1.2 General Principles for informing the user

Inform dialogues should be short and concise. If not, users will not read them.

The UK information commissioner proposes a "layered approach"; the basic information is on the main page, and there is a hyperlink for detail. Merely having a clickable link labelled "privacy policy here" probably wouldn't be enough.

"A layered notice usually consists of a short notice plus a longer notice. The short notice contains basic information, such as the identity of the organisation and the way in which the personal information will be used... The short notice contains a link to a second, longer notice which provides much more detailed information." (the UK information commissioner's Privacy Notices Code of Practice, page 18)

The goal here is to provide a human readable form as the primary interface with the ability to click further to see what the 'technical' data is. The AUPs presented by most Internet services do not suffice as they are rarely read nor understood by the users. The basic information should be provided as short accurate "user-friendly" descriptions; detailed information about "exactly what's going on" can be provided as a link.

Consequently, **this profile recommends displaying the Service Provider's name, description, logo and requested attributes on the main page**. If a user wants to learn more, he/she can click a link resolving to the Service Provider's Privacy policy.

It is not expected that "normal" users will actually do the latter, but at least they have the ability to inform themselves of what is going on. The Norwegian Feide federation uses this approach; normal people do not follow the links, but there are several persons who over the years where this has been operational have given favorable feedback on this approach. Including the Data Protection Agency.

Layered notices can be particularly useful when describing the attribute values which will be released. In general, LDAP-style attributes are transferred to the SP. However, very few users have any familiarity with the conventions and usage of LDAP attributes. Instead, the Identity Provider could ask the user to release "name"; the link would take the user to a page listing all of the LDAP name attributes and values.

There are other attributes where the values are intentionally opaque (e.g. ePE="urn:mace:rediris.es:entitlement:wiki:tfemc2"). It is NOT reasonable to expect the end user to understand what this value means and to pick up a particular value to be released. Instead, natural language descriptions of the vallues should be provided.

A good way to explain to a user why there is a transfer of information is "your email, name and affiliation will be transfered, as we do for international projects like Zyzzy, VO2 and Tjollabong". Explaining by analogy is human, albeit not necessarily academic in all disciplines.

1.3 Recommendations

See SAML 2 Profile for the Data Protection Code of Conduct for details on the related SAML2 metadata elements.

For all attributes (INFORM interaction)

1. The user MUST be informed on the attribute release separately for each SP.
2. The user MUST be presented with the mdui:DisplayName value for the SP, if it is available.
3. The user MUST be presented with the mdui:Description value for the SP, if it is available.
4. The user SHOULD be presented with the mdui:Logo image for the SP, if it is available.
5. The user MUST be provided with access (e.g. a clickable link) to the document referenced by the mdui:PrivacyStatementURL.
6. The IDP MUST present a list of the RequestedAttributes 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.)

    a. The IDP MAY list the NECESSARY attributes on the same screen as the username/password entry boxes, making clear that *if* you login then this is what will happen. It MUST be clear to the user that the consequence of their next action will be to release the attributes. NOTE -- the attribute values for the specific user are not available when the login screen is presented, since the user's identity is not yet known.
7. The display software SHOULD provide the ability to configure and display localised descriptions of the attributes (e.g. what PersistentID means) and their values (e.g. what eduPersonEntitlement="urn:mace:rediris.es:entitlement:wiki:tfemc2" means)
8. The display software MAY inform the user of the release of an "attribute group" (eg attributes expressing the user's "name"), and then release all requested attributes in the group (e.g. various forms of the user's name such as cn, sn, givenName and displayName).
9. The display software MAY give the user the option to remember that they have been INFORMed of the release of the necessary attributes.
10. If any of the following has changed since the user accessed this SP for the last time, the user MUST be prompted again for the INFORM interaction
    a. the list of attributes the SP requests
    b. the DisplayName of the SP
    c. the Description of the SP

Additionally, for release of optional extra attributes (CONSENT interaction)

1. The display software MUST ask the user to consent to release of attributes tagged as REQUIRING CONSENT
    a. the user MUST have an opportunity to give his/her consent to each attribute separately
    b. however, the display software MAY allow the end user to consent to the release of an "attribute group" as a whole (eg attributes expressing the user's "name"), and then release all requested attributes in the group (e.g. various forms of the user's name such as cn, sn, givenName and displayName)
2. The user MUST be prompted for the CONSENT interaction separately for each SP.
3. If any of the following has changed since the user accessed this SP for the last time, the user MUST be prompted again for the CONSENT interaction
    a. the list of attributes indicated as REQUIRING CONSENT
4. The user MUST have an opportunity to withdraw his/her consent at any time
5. The display software MUST produce reliable log files on the users' decision to consent to attribute release

Internationalization

The lang attribute of the mdui elements can be used to match the user's preferred language settings.