How the Home organisation should inform the End user

The Data protection laws create a set of requirements for the INFORM interactions with the user. This Data protection Code of Conduct recommends a division of responsibility where the INFORM interaction is carried out by the Home Organisation of the user, for instance, in an INFORM Graphical User Interface (GUI) installed at the Identity Provider server, whereas the data release is requested and subsequently processed by the Service Provider Organisation.

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

Law requirements

Informing the end user (“INFORM interaction”)

For a Home Organisation, informing the end user can be done when a new end user gets their account at the institution. At that time, the Home Organisation has the first opportunity to inform that the user's Attributes may also need to be released to a Service Provider Organisation when they wants to access it. However, the law requires the End User to be informed about the specific Attribute release every time the Attributes are to be released to a new Service Provider Organisation.

The Service Provider Organisation's obligation to inform the End User depends on whether it is acting as a Processor or a Controller. As a Controller, the Service Provider Organisation is responsible for communicating with the End User the issues above; which Attributes it will be using, and what it will be doing with them. As a Processor, a Service Provider Organisation can refer to the Home Organisation.

The European Data Protection Board, the EU advisory body contributing to the uniform application of the General Data Protection Regulation, took the view that the information must be given directly to individuals - it is not enough for information to be "available[1]". In the Internet, a standard practice to inform the end user on processing their personal data in Services is to provide them with a Privacy Notice web page in the Service.

In the Web Single Sign-On scenario of SAML 2.0, a convenient place to inform the end user is at the Home Organisation before the Attribute release takes place for the first time. Several federations supporting the European higher education and research communities have already developed tools implementing this approach (e.g. the Consent-informed Attribute Release system (CAR) module implemented for Shibboleth, the consent module implemented for SimpleSAMLphp). This allows the user's decision to directly affect the transfer of Attributes to the Service Provider Organisations; if the Service Provider Organisations were communicating with the user it might have already received all the Attributes and values.

General Principles for informing the user

Information dialogues should be short and concise.

The UK information commissioner proposes a "layered approach"[2], the basic information should appear on the main page, and a hyperlink shall be provided for detail. Merely having a clickable link labelled "Privacy Notice here" probably wouldn't be enough.

The goal 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 Acceptable Usage Policies 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 Organisation's name, description, logo and requested attributes on the main page. If a user wants to learn more, they can click a link resolving to the Service Provider Organisation's 's Privacy Notice. It is possible that users will actually not do the latter, but at least they have the choice to inform themselves of what is going on.

Layered notices can be particularly useful when describing the attribute values which will be released. In general, LDAP-style attributes are transferred to the Service Provider Organisation. 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. eduPersonEntitlement="`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 values 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 transferred".

Recommendations

For all Attributes (INFORM interaction):

1. The user MUST be informed of the attribute release separately for each Service.
2. The user MUST be presented with the `mdui:DisplayName` value for the Service, if it is available.
3. The user MUST be presented with the `mdui:Description` value for the Service, if it is available.
4. The user SHOULD be presented with the `mdui:Logo` image for the Service, 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 expected before release. (However, given how web browsers work, the user may have to click a CONTINUE button in order to continue in the sequence.)
   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 SPO for the last time, the user MUST be prompted again for the INFORM interaction
    a. the list of attributes the SPO requests
    b. the `DisplayName` of the SPO
    c. the `Description` of the SPO

Internationaliszation

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

Footnotes

[1] Opinion 15/2011 on the definition of consent, p.20.

[2] *"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).