How to satisfy the data protection regulations in federated identity management?

Mikael Linden, CSC – IT Center for Science, P.O. Box 405, FI-02101 Espoo, Finland, Mikael.Linden@csc.fi

Keywords

Identity federation, data protection, eduGAIN

Abstract

The EU directive on Data protection [1] regulates the release of personal data if the Identity or Service Provider or both of them reside in EU/EEA. The objective of the directive is the free flow of personal data between the EU countries without infringing the data subject's privacy.

The EU directive on data protection is a non-technical issue which any Identity or Service Provider administrator and federation operator needs to be aware of. The topic is interesting for TNC, because the directive and its implications are not well understood by the technical people forming the main audience of the conference. Several kinds of misunderstandings have risen, such as "you can release whatever attributes if the end user consents to it." The rise of Identity Provider extensions (such as uApprove [2] of Shibboleth) asking user consent for attribute release has feeded this view.

The eduGAIN project of GN3 is aiming at releasing a pan-European interfederation service in April 2011. In the eduGAIN policy design work, considerable amount of effort is put on developing a data protection profile which covers the data protection issues in the attribute release between an Identity and Service Provider.

Requirements set by the directive and how the eduGAIN data protection profile covers them

To cover the directive's requirements, the eduGAIN data protection profile translates the directive's implications into requirements for Identity and Service Providers and proposes a procedure that the Providers need to take together to fulfill the directive's requirements. Following paragraphs introduce the fundamentals of the profile.

Personal data. The directive defines personal data as any information relating to an identified or identifiable natural person. The ambiguity of this definition is one of the main difficulties of the directive. Is attribute "user1234567" personal data for a Service Provider if there is no means to find out who this person is in real life? To avoid problems with this definition and its conflicting interpretations in European courts, the DP profile proposes a conservative approach.

Minimal disclosure. The directive requires that personal data must be adequate, relevant and not excessive in relation to the purpose of processing. In federated identity management, this translates to the principle of minimal disclosure. The Identity Provider shall release only attributes which are relevant for the service in question. In the data protection profile, the Service Provider weights its attribute needs against this requirement and provides a list of requested attributes to the Identity Provider.

Informing the end user. The directive requires that the end user is informed on releasing his/her personal data to a third party. The end user must be told what attributes are released, to whom and for what purposes. Services on the Internet do this usually via a Privacy Policy page, and the data protection profile

suggests that the Service Provider mediates this URL to the Identity Provider, which shows it to the end user before the attribute release takes place.

Criteria for making data processing legitimate. The directive requires that an attribute release is based on an end user's unambiguous consent, or the release is necessary for a variety of reasons, such as for performing a contract to which the data subject is party. Some national interpretations of the directive seem to emphasise consent, whereas others think necessity is the primary grounds for attribute release. In the front-channel binding of SAML, the end user can be informed and s/he can give his/her consent, if necessary, at the time when the Identity Provider has authenticated him/her but before the SAML authentication response is send from the Identity Provider to the Service Provider.

Attribute release to 3rd countries. The Directive's intention is that, in order to release personal data to non-EU/EEA countries (dubbed as 3rd countries), one must ensure that personal data has adequate protection in the receiving site. For some countries (such as Switzerland) the European Commission has decided that the local laws ensure adequate protection. In the United States, the Department of Commerce and the EC have negotiated the Safe Harbour framework that provides streamlined means for US organisations to comply with the directive. The Data Protection profile expects the Service Providers to reside in a country with adequate level of protection or that the US Service Provider has committed to the US Safe Harbour principles.

Technical implementation

The data protection profile relies on SAML 2.0 metadata as the vehicle that is used for expressing the Providers' privacy-related characteristics.

- The Service Provider inserts the list of requested attributes to its metadata, and uses a specific tag to indicate if it thinks some of the attributes count as personal data. If none of the attributes is personal data, the data protection laws are not applied and release of attributes is relaxed.
- The Service Provider places its Privacy Policy URL to its metadata element, and the Identity Provider presents the SP's clickable URL to the end user before attribute release takes place for the first time.
- The Service Provider uses a metadata tag to indicate if it thinks attribute release should be based on user's consent. Otherwise, it is enough that the Identity Provider just informs the end user on release of his personal data to the Service Provider, as described above.
- The Service Provider affirms that it resides in EU/EEA or in a country with adequate data protection.

In general, the Identity Providers receives the eduGAIN SAML 2.0 metadata from its own federation, and uses a local risk management practices to decide if it wants to release attributes to a foreign Service Provider in the metadata. The metadata tags ease development of tools which support the Identity Providers in their decision. Instead of the data protection profile, the Identity and Service Providers may also decide to use any other framework and/or bilateral arrangements to fulfill their responsibilities with regards to the data protection directive.

Acknowledgements

Acknowledgements to Andrew Cormack and Walter Tveter on the fruitful discussions on the data protection directive.

References

[1] 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

[2] http://www.switch.ch/aai/support/tools/uApprove.html

Vitae

Mr. Mikael Linden received his doctoral degree from Tampere University of Techology in 2009. He has been operating the Haka federation of the Finnish higher education since 2005 and chairs the subtask for the eduGAIN policy development.