Federated Access Management

Document Version: 2 DRAFT

Date: Oct 2011

Author (Version 2): Andrew Cormack (JANET(UK))

Authors (Version 1): Andrew Cormack (JANET(UK)), Eva Kassenaar (SURFnet), Mikael Linden (FUNET), Walter Martin Tveter (UNINETT),

Abstract

The document provides an overview and recommendations on how to implement Federated Access Management Systems in order to reduce the amount of personally identifiable data that is exchanged, in accordance with the Directive *95/46/EC*.

Contents

Federated Access Management

Traditionally, staff and students in research and education have gained access to licensed on-line resources such as electronic journals and discussion groups by having a personal login with the provider of the service and providing additional data about themselves to the provider. Federated Access Management represents a different approach, where the person logs into their home organisation – typically a university, college or school – and that organisation then provides the service provider with the information the service needs to make its access control and presentation decisions. For the many resources that are covered by site licences, this may require no more than a reliable assertion that the person is a member of the organisation. For some services it may be necessary to assert the person's status (staff, student, etc.) or their subject of study; if the service allows its users to make individual configuration choices or to retain information such as recent searches then the home organisation can provide a unique opaque persistent identifier, unique to that service, rather than the user's actual identity to allow this information to be recorded. Only a few services, for example where a resource is licensed to particular individuals or where e-mail is used to send results or notices, should need to handle information directly linked to an individual person.

Federated Access Management therefore represents an opportunity to greatly reduce the amount of personally identifiable data that is exchanged, in accordance with the aims of Directive *95/46/EC* on the processing of personal data. That Directive sets rules both for when personal data may be processed, and the actions that must accompany the processing. This paper seeks to apply the Directive to the particular case of Federated Access Management to determine how both home organisations and service providers should act in order to comply with the Directive.

Directive 95/46/EC on Personal Data

Definition of Personal Data

Article 2(a) of the Directive defines personal data as follows:

> "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

A full discussion of this definition may be found in the Article 29 Working Party's Opinion 4/2007 on the Concept of Personal Data.[1]

Since the home organisation knows the identity of the account holder who has logged in, it is likely that all use of information about that user by the home organisation will be considered as processing personal data and therefore subject to the Directive.

In most cases the processing of attributes by service providers will also be regulated by the Directive, however some European countries have a few court cases where information not associated with an individual or account was considered to be non-personal. Service Providers should normally treat all attributes as personal data unless they have confirmed that their own jurisdiction and those of the users and home organisations allows them to be treated as non-personal.

Processing Personal Data

The Directive permits personal data about a data subject to be processed in two different types of circumstances:

- Where processing is **necessary**, either for the performance of a contract with the data subject (Article 7(b)), to comply with a legal requirement (Art.7(c)), to protect the vital interests of the data subject (Art.7(d)), in the public interest (Art.7(e)) or, with some limitations, for the legitimate interests of the data controller or the third party to whom the information is disclosed (Art.7(f));
- Where processing is optional, and the data subject has freely given specific and informed **consent** (Art. 7(a)).

The Directive sets different requirements for processing in each of these circumstances. To comply with the Directive it is therefore necessary to know which circumstance is being used, and what duties that imposes. If neither circumstance applies, i.e. the processing is not necessary and the data subject has not consented, then personally identifiable data must not be processed.

The following sections consider the various transfers of data (possibly including personal data) that occur within a Federated Access Management system and seeks to identify the appropriate legal basis (if any) that applies to each of them. The appropriate conditions and requirements from the Directive are then used to derive

[1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

recommendations for Home Organisations and Service Providers to improve their compliance with the Directive.

Data Transfers in Federated Access Management

In a Federated Access Management system, information about a user will normally be provided by the user's home organisation to the service provider. However it is also possible for the service provider to ask the user to provide information directly, for example through a registration or configuration page. The Directive also distinguishes transfers of data to countries outside the European Economic Area (EEA), so it is necessary to consider what differences might apply if service providers are located outside Europe.

Transfer from Home Organisation to Service Provider

In most educational contexts a contract will exist between the user and their home organisation (their school, college or university), or there will be a legal duty to provide education. The home organisation might therefore (by Art.7(b) or Art.7(c) of the Directive) use the basis of **necessity** to process personal data, including disclosing it to service providers, so long as the processing is necessary to fulfil the contract with the user or the legal duty. However many external services will be necessary for one user but not for another – for example students and researchers studying different subjects will need to access different services – so the home organisation relying on Articles 7(b) or 7(c) would have to apply different attribute release rules to different users. For these services, at least, it may be simpler to use the basis that processing and disclosure are **necessary** in the legitimate interests of the service provider (Art.7(f)), notably the interest of providing the service to users who have requested it. Article 7(f) involves an additional restriction that even legitimate processing may not take place if the fundamental rights of the individual override the reason for processing. The fundamental right most likely to be damaged is privacy, so home organisations will need to be satisfied that any service providers to whom they release personal data on this basis will not breach the user's privacy. A home organisation may, for example, wish to know what other information about the user the service provider intends to obtain, either from the user themselves or from other services, and whether information will be used for any purposes other than delivering the service.

Whichever of the necessity grounds is used (Articles 7(b), 7(c) or 7(f)), home organisations must ensure that they do not disclose any more information to the service provider than is necessary for the delivery of the service (Art.6(1)(c)). Wherever a service can be delivered using only non-personal attributes and opaque identifiers then these are all that should be released. Service providers should expect to have to make a strong case for any requirement to disclose information directly linked to an individual and may find that such requests are refused if the home organisation is not satisfied that privacy and other rights will be protected. In particular, service providers and home organisations (or federations acting on their behalf) should agree in advance who will be responsible for investigating any instances of misuse. It will normally be more effective, and provide better privacy protection, if this is done by the home organisation using evidence from the service provider. However this does require the service provider to have confidence that home organisations will take effective action where necessary.

The home organisation must also (by Art.10) inform the user what personal data is being disclosed to service providers and (by Art.6(1)(b)) for what purposes. This information is commonly presented in the form of a Fair Processing Notice. There are at least three opportunities for this to be done: when personal data is collected from the user, when the user signs up for a particular service, and when the user accesses the service. Circumstances will determine which of these are appropriate: for example if the user is not able to understand the notice then information must be given to a responsible adult before the user accesses the service.

Finally, the Directive recognises the right of a user to object to the processing of their personal data if there are "compelling legal grounds" for the objection (Recital 25 and Art.14). Home organisations must therefore have a clear policy and process for dealing with such objections. The process must include consideration of whether there is an alternative to the processing that can achieve the same ends, and must ensure that the correct balance has been achieved between the rights of the individual and the obligations of the organisation.

If it wishes, the home organisation may also process personal data on the basis of the user's **consent** (Art.7(a)). However this basis cannot be used for processing that is necessary for the user's education or employment, since in that case the consent would not be freely given (as required by Art.2(h)). Consent should only be used, if at all, either for services that are optional or to provide optional information to services that are necessary. Furthermore a home organisation using consent must also keep individual records of which users have consented to the processing or release of which data to which services, and allow all users to withdraw or modify their consent at any time. To avoid this burden the home organisation may prefer to limit disclosure to non-personally identifiable information. Further guidance on the use of consent is available in Article 29 Working Party Opinion 15/2011 on Consent.[2]

If personal data is to be exchanged, either on the basis of **necessity** or **consent**, the home organisation and service provider may enter into a data controller/data processor arrangement. If this is not done then both home organisation and service provider will be data controllers and the service provider must also (by Art.11) provide the user with a Fair Processing Notice, no later than the user's first contact with the service, informing them of the provider's identity, the personal data received and the purpose(s) for which it will be used.

Transfer from User to Service Provider

For some services it may be appropriate for the service provider to ask the user to provide additional personal information, for example an e-mail address for sending notification of service updates. In the usual case, where there is no contract between the service provider and user, this processing can only take place on the basis of the user's **consent** (Art.7(a)).

Since consent must be free and informed (Art.2(h)), the Service Provider must ensure that users who refuse to provide personal information are not unreasonably disadvantaged. For example service update information, if offered, should also be available on a web page for users who do not wish to provide an e-mail address.

[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Furthermore, the service provider must be able to deal with the user withdrawing their consent at any time. If personal data is essential for the provision of the service (e.g. to authorise access to the service) it should therefore be obtained from the home organisation as described above, since this is less likely to become unavailable and may also be more accurate than the user's self-declaration.

Where a service provider does obtain personal data from a user, the service provider will be the data controller for that data and carries the normal data controller responsibilities and liabilities, including informing the user what the data will be used for (Art.11), only collecting necessary data (Art.6(1)(c)), and only using the data for the declared purpose(s) (Art.6(1)(b)).

Services outside European Economic Area

In general, transfers of personal data to countries outside the European Economic Area (EEA) are prohibited unless the receiving country provides equivalent protection of personal data (Art.25).

If a service provider is not located in one of the countries that have been formally recognised as providing equivalent protection (a current list is available from the EC Data Protection home page) and no other arrangements, such as the US Department of Commerce's Safe Harbor scheme, cover the transfer, then personal data can only be disclosed under one of the derogations provided by Article 26. These permit transfers based on both contractual necessity and free individual consent. However the burden on a home organisation that transfers personal data to a service provider outside the EEA is heavier. Since it cannot be assumed that the service provider will automatically provide European levels of protection these are likely to have to be specified by the terms of a contract. Approved model contract terms can be found in the Documents section of the EC Data Protection home page.[3]

[3] http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Summary of Recommendations

This section summarises the recommendations for home organisations and service providers when transferring information within a Federated Access Management system. Both will also have responsibilities under the Directive for the personal information they hold, but these apply no matter how the information was obtained.

Home Organisations

- Must identify which information is necessary to provide each service
  - Must consider whether directly identifiable information is needed, or whether opaque identifiers or attributes are sufficient;
  - Unless use of the service is necessary to support a user's education, research or employment, must consider whether releasing the information will infringe the user's privacy or other rights;
  - Must inform users what information will be released to which service providers, for what purpose(s);
  - May release that necessary personally identifiable information to those services.
- May seek users' informed, free consent to release personal data to services where the user is able to give valid consent
  - Must inform users what information will be released to which service providers, for what purpose(s);
  - Must maintain records of individuals who have consented;
  - Must allow consent to be withdrawn at any time;
  - May only release personal information where consent is currently in effect.
- Should have a data processor/data controller agreement with all service providers to whom personally identifiable data is released.
- Should agree how misuse of services will be investigated and dealt with.
- Must ensure adequate protection of any data released to services outside the European Economic Area.

Service Providers

- Must consider whether directly identifiable information is necessary for their service, or whether opaque identifiers or attributes can be used;
  - Should obtain that information from home organisations;
  - Should inform home organisations if any other information about the user will be obtained, and if information will be used for any purpose other than delivering the service;
  - Should have a data processor/data controller agreement with all home organisations from whom personally identifiable data is obtained;
  - If no such agreement is in place, must inform users what personal information will be obtained, by which service providers, for what purpose(s).
- May request personal information from users
  - Must inform users what information will be processed by which service providers, for what purpose(s);
  - Must ensure that users who do not provide information are not unreasonably disadvantaged;

- Must maintain records of individuals who have consented;
- Must allow consent to be withdrawn at any time;
- Must cease processing data when consent is withdrawn.