

# **Good Practice for Federated Access Management**

Document Version: 02 DRAFT

Date: Dec 2008

Author: Andrew Cormack (JANET(UK))

## **Abstract**

This paper summarises the good practice recommendations contained in two papers on Federated Access Management and Pseudonymous Identifiers. Federated Access Management Technologies are recognised by a number of European privacy authorities as beneficial for individual privacy; the recommendations in this paper suggest how such technologies can be used both to minimise the transfer of personal data and to provide accurate access control decisions for protected resources.

The paper does not constitute legal advice and no responsibility is accepted for any errors. Readers should note in particular that the case law and opinions in this area are particularly unclear, and may vary between different European countries.

TERENA's REFEDs group has published two papers on the implications of European data protection law for Federated Access Management systems. The papers, and their principal sources, are as follows:

- Federated Access Management (Cormack, Kassenaar, Linden, Tvester) based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Pseudonymous Identifiers and the Data Protection Directive (Cormack) based on the Article 29 Working Party's Opinion 4/2007 on the Concept of Personal Data.

This paper is a summary of the recommendations contained in those two papers. The following recommendations constitute good practice for the use of Federated Access Management technologies to protect the privacy of individuals while permitting accurate access control decisions. Following the recommendations may also increase the likelihood that a given system will be compliant with European Data Protection law.

For clarity the recommendations are presented separately for Service Providers and Home Organisations (and their Identity Providers) though, since many of them relate to transfers of information between those two types of organisation, matching recommendations appear in both lists.

## **Service Providers**

- Must consider whether personally identifiable information is necessary for their service, or whether anonymous identifiers or attributes can be used;
  - Should obtain that information from home organisations;
  - 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
  - Should not collect personally identifying information from a user who was otherwise only identified by a pseudonymous identifier;
  - Should not seek to obtain information linking a pseudonymous identifier to a user from any other source; in particular they should not aggregate information collected from different services;
  - Must inform users what information will be released to 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.
- Should provide evidence to Identity Providers to permit them to investigate and deal with any misuse or other problem in the use of the service

## Home Organisations

- Must identify which services are necessary for education/research
  - Must consider whether personally identifiable information is necessary for those services, or whether anonymous identifiers or attributes are sufficient;
  - 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 other services that are not necessary for education/research
  - 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 construct pseudonymous identifier values in ways that conceal as far as possible the identity of the user, for example by using one-way hash functions and providing different values to each service provider;
- Should declare that they will not disclose the identity of the person to which a particular pseudonymous identifier value was assigned, other than when required by law to do so.
  - In particular, reports of misuse or other problems should be investigated by the Identity Provider, who is anyway most likely to be able to hold the user to account, and not the Service Provider.
- Should have a data processor/data controller agreement with all service providers to whom personally identifiable data is released.
- Must ensure adequate protection of any data released to services outside the European Economic Area.