Report on the DASISH SSH AAI strategy meeting March 10, 2014 at the MPI for Psycholinguistics

Present: Hilary Beedham, John Shepherdson (CESSDA), Dieter van Uytvanck (CLARIN), Peter Gietz, Wolfgang Pempe (eduGAIN, DARIAH), Lukas Haemmerle, Ann Harding (eduGAIN), Daan Broeder, Przemek Lenkiewicz, Kees-Jan van Looij (DASISH)

Report by Daan Broeder et al.

Introduction

This meeting was organized by DASISH, partly as a follow-up of a previous DARIAH/DASISH AAI workshop at GESIS in Cologne, to (1) discuss the current status of the AAI approach of the different SSH ESFRI projects, (2) investigate possibilities for collaborations, and (3) see where the eduGAIN project fits in the different strategies.

The presentations from CESSDA, DARIAH, CLARIN and eduGAIN can be found on: http://www.clarin.eu/event/2014/dasish-aai-workshop

Short summary

CLARIN: the CLARIN model of an ESFRI specific service provider federation that makes contracts with the national IDFs, can be taken over by other ESFRI projects. The contract is almost completely independent from CLARIN, i.e. the CLARIN ERIC as legal entity can be replaced by another such entity.

DARIAH: DARIAH has now implemented a number of software modules that together provide functionality for: Homeless users, external attribute provider that together compensate for home organizations lacking sufficient attribute provisioning and lacking connection to eduGAIN.

CESSDA: although CESSDA has a long history as an infrastructure with also pilot-projects with AAI, currently there is yet no formulated AAI strategy. CESSDA is now closer to establishing a board and representatives. This is should facilitate the communication and cooperation with CESSDA as a whole.

Although CESDDA accepts crossover data and thus also crossover users, the priority is delivering CESSDA data to CESSDA users. CESSDA may be somewhat more self-contained than the other ESFRIs. UKDA has currently 22000 active users from the UK of which 15% do not have a academic account (use homeless solution)
UKDA has a preference developing AAI solutions with the UKAMF.

We established that although institutions can have different (incompatible) access levels for their resources, that shouldn't be an issue for common AAI solutions, if a common AAI is only used for authentication. But one common need for access levels is nevertheless about distinguishing the academic users from non-academic ones. This should be possible using the current national IDFs and ESFRI homeless IdP solutions, although not with a very high level of assurance.

It is clear that some data would need a very high level of assurance of the authentication; such data will probably always need to be provided under special conditions. For the over great majority of all data-sets, the level of assurance we can currently get is sufficient.

There was broad interest in using 'federation as a service' services, but they should preferably also be inclusive of components as "homeless IdPs, external attribute providers, etc." it was accepted that such services should be managed by the communities themselves. This is in line with GEANT to move its focus from providing base connectivity more to providing useful services, as this is where more innovation can be created. Network facilities have become a commodity. So service-providing projects like eduroam, eduGAIN will have strong support and are likely to receive funding and keep being developed.

With respect to new technologies solutions like OAuth2 and OpenID Connect[1] [2] should be considered, how to interact with them and include them in the common AAI framework. Although it is very clear that the level of assurance is low, such authentication via social networks can be useful for tracking users.

Results

1. All ESFRIs think that availability of SAML FIM infrastructure (as a service) is very worthwhile. Examples are: homeless IdP, external attribute provider, and discovery services. The proposed integrated software from DARIAH is a good example. This can be offered as software only or as a to be managed service. eduGAIN should be encouraged in a follow up project proposal to offer this.

---

[1] See http://security.stackexchange.com/questions/44611/difference-between-oauth-openid-and-openid-connect-in-very-simple-term
[2] http://openid.net/connect/

2. All ESFRIs think supporting the Data Protection CoCo is worthwhile and will (recommend) to do so. DASISH will also sign a support letter.
3. For connecting ESFRI SPs to IdPs in national IDFs with an (eduGAIN) opt-out policy, connecting to eduGAIN is the best option
4. For connecting ESFRI SPs to IdPs in national IDFs with an (eduGAIN) opt-in policy opinions differ:
    a. CLARIN needs access to as many relevant IdPs as possible and therefore uses a CLARIN specific federation that connects directly to the national IDFs. In this way the approach of an ESFRI specific SPF can be seen as complementary to eduGAIN.
    b. DARIAH is content to wait on further eduGAIN penetration and relies on its homeless store for the moment to support users from IdPs not yet connected via eduGAIN.
5. (a) DARIAH offers it homeless & external attribute store for the Humanities. (b) CLARIN offers the CLARIN SPF for services 'in need' to connect to IdPs. However they need certification to become a CLARIN "T-center".
6. All ESFRIs would like to collaborate further on further FIM related work as SAML ECP, OpenID (Connect).
7. A possible DASISH follow-up project, should further try to work on common AAI, possibly in collaboration with other interested ESFRIs working at the same type of FIM. (although perhaps in a different setup, combinations of ESFRIs more based on their common work topics, rather than general SSH community).