Confederation Meeting Prague

2 September, 2007

Prague

Introduction

The first International confederation meeting organized under the umbrella of TERENA and hosted by CESNET took place on September 3 in Prague.
One of the aims of the meeting was to identify the major drivers for creating identity federations in the academic community as well as the drivers for interoperability among the various federations.
The workshop was highly interactive and provided a good overview on issues to address on federation interoperability scenarios.
Next federation meeting will take place in May (adjacently to TNC). Dates and venue will be announced on the refeds list.

Summary of actions

Action03092007-01: Licia to provide accounts for the wiki
Action03092007-02: All participants agreed to do some 'homework', identifying major research projects in their region that need cross-federation connections. This will help to clearly identify uses cases. Licia to chase people up to get contributions for the use cases.
Action03092007-03: Licia to collect the links to the policy for the refeds website.
Action03092007-04: Identify which part of eGovernment is interesting for refeds. Olivier to contact the French group and report on the results.
Action03092007-05: Jane and Andrew to circulate the material on the comparisons of federation policies that is being undertaking by JISC and UKERNA.
Action03092007-06: Robin Wilton to report on the developments of the Liberty Alliance eGovernament group.
Action03092007-07: OpenId and CardSpace integration in identity federations: Ken and Ingrid to report on this.
Action03092007-08: Andrew + Eva + Walter to get in touch with Article 29 Working Party (Art 29 WP) on behalf of TERENA refeds group.
Action03092007-09: Leif, Diego and Andreas to investigate attributes invitation and aggregation issues.
Action03092007-10: Leif to send his proposal to the refeds list describing his ideas for the min requirements.
Action03092007-11: Everybody with experience on the LoA to send info to the refeds list.
Action03092007-12: Leif to provide more inputs on how to proceed to use attributes to ship LoA.
Action03092007-13: Eva to put best practices on-line.

Meeting Report

The meeting was opened by Ingrid Melve, who reported on the needs for confederating in the Scandinavian countries. Andrew Cormack and Ken Klingenstein reported on the main concepts upon which UKAccessManagement Federation and InCommon are built.
The attendees agreed that collaboration and sharing each other resources to offer users more services than those available at their institutions is on of the main reasons why federations are needed. It was agreed that it is important to identify uses cases that request federation interoperability.
The exercise to produce use-cases was meant to understand which communities are potential candidates to liaise and interoperate with the identity federations run by the various NRENs. The discussion was not meant to analyze pros and cons of alternative approaches to identity federations.

A first attempt included the following scenarios:
1. Collaboration, such as sharing wikis, file systems and similar
2. Dealing with content providers, such as Elsevier, MSDN-AA, Apple iTunes
3. Network access and roaming users in particular temporary users, see for instance eduroam
4. Grid and research - IGTF (the International Grid Trust Federation) involves only authN. The cooperation between IGTF and identities federations is mainly at IdPs level, in order to use the campus credentials to get grid certificates. There are already on-going examples where grid certs are used to access non-Grid resources, such as eduroam. It was agreed that REFEDS group should get in touch with CERN and ESA.
5. Liaison with government
6. Supporting light path provisioning and related tools like PerfSonar
7. User support, in what concerns trouble tickets
8. A more generic use case identified was: What are the conditions for SPs to accept different credentials different from those handled by their federation?

There is currently lots of interest in OpenId (SUN and Liberty Alliance are testing with OpenId, InCommon is considering adding OpenId to the list of SPs, UNINETT has gained quite a lot of experience integrating OpenId with FEIDE) and how this can be integrated with the identity federations.
Ingrid and Ken will provide a report on the work done on the inter-operation between SAML-based Identity federations and OpenId will be provided as well on the work done in US on the interoperability between Shibboleth and CardSpace.

Further to this, the various models according to which federations can interoperate were also discussed. The models that were taken into account were: confederation, peering and leveraging. A discussion on the terms used followed:
- Confederation: mainly in Europe, see eduroam case. Typically a confederation implies an agreement among the various federations.
- Peering: members of different federations can peer among each other. This is typically a lightweight process compared to the confederation.
- Leveraging: specific to US. Universities join in federations, and at the same time they individually are members of a bigger federation, such as Incommon.

A discussion on the overlap between public sector, business sector and the social sector and how to handle this scenario followed.
Both Liberty Alliance and OASIS have established eGovernament working groups to examine how to liaise with government-centric identity initiatives. Robin Wilton (SUN and Liberty Alliance) will report about the developments of the Liberty Alliance eGovernament group.

Attributes – Diego

Diego highlighted issues involved with attributes exchange at (con)federation level; one the issues being users privacy. It was agreed that typically the institution that collects users' data is responsible for the data collected.
The model to exchange metadata (full metadata exchange vs dynamic access) was discussed. Leif suggested using an invitation solution.
Aggregation of attributes was also discussed. Participants agreed that this issue would become more and more important in the future.
Attendees agreed that allowing a SP to aggregate attributes from more IdPs should be regarded as bad practice.
Action: investigated invitation and aggregation issues Leif, Diego and Andreas.

LoA – Ken

LoAs were addressed and in particular the way to handle LoAs when crossing the border from one federation to the other. To better understand how LoAs work, when spanning over different federations, a comparison of the various policy would be helpful. In UK, JISC and UKERNA, are already undertaking a work to analyze the various policies; the results of this study will be made available to the refeds community.
It was agreed that the reason to get LoAs is for the universities to have a reasonable trust with the federation operator and for the SPs to feel more secure.
At the moment most of the federations seem to go for Level 1, which means a loose check on the IdP.
There is no standardised attribute that carries LoA and this is very much related to authN. Leif asked where a possible technical discussion on shipping LoA into attributes should take place, maybe OASIS?
Action: People that have experience on the LoA to send info to the refeds list.
Action: Leif to provide more inputs on how to proceed to use attributes to ship LoA.

Legal aspects

Leif proposed to define some min requirements for (con)federation agreements.
Leif also asked the reason for SPs to sign an agreement with the federations.
His suggestion was to only list the SPs and to provide mechanisms for authentication.
The agreements should only involve the IdPs and the federations.
A discussion took also place on European regulations on privacy, discussed by the Article 29 Working Party (Art 29 WP).

Action: Leif to send his proposal to the refeds list describing his ideas for the min requirements.
Action: Andrew, Eva and Walter would approach the Art 29 WP group, under the TERENA banner.

It was agreed to have a follow up meeting in the summer 2008. Licia will verify where and when this meeting can be organized.