



**REFEDs Meeting**  
**Sunday 7 June 2009**  
Málaga, Spain  
Author: Licia Florio

**Table of Contents**

|  |   |
|--|---|
| 1. Welcome and Apologies .....   | 1 |
| 2. Interfederation business – Mikael Linden (CSC).....                               | 2 |
| a. Identifiers and attributes .....  | 2 |
| a. JISC work on LoA – Nicole Harris (JISC).....                                      | 2 |
| b. Campus – Mikael .....   | 3 |
| c. InCommon – Ken Klingenstein (Internet2).....                                      | 3 |
| 5. Inter-federation Business.....  | 3 |
| a. Inter-federation agreement – Andrew Cormack (JANET(UK)) .....                     | 3 |
| b. The federation operator CPS – Alex Reid (AARNET) .....                            | 3 |
| c. Report from JISC on the study to assess federation policies – Nicole Harris ..... | 4 |
| d. CAUDIT IAM Federation – Patricia McMillan (Queensland Univ).....                  | 4 |
| STORK – Leif Johansson (Stockholm Univ).....   | 4 |
| Kantara – Lucy Lynch (ISOC).....   | 4 |
| Interoperability with other Identity spheres – Diego Lopez (RedIRIS) .....           | 4 |
| Tao of Attributes – Ken Klingenstein .....   | 5 |
| n. Date of Next Meeting, AOB and Close .....   | 5 |

**1. Welcome and Apologies**

Licia welcomed the participants and a round table of the attendees followed.  
Licia gave a brief update on REFEDs developments since the meeting in December 2008.

The REFEDs roadmap, approved in December, identifies the interest areas the group agreed to explore. Work has been undertaken mainly in the “Privacy and Data Protection” area for which documents are available on the REFEDs website.

Reports on the work carried out in the other areas and on future plans is detailed in the rest of these minutes.

Mikael Linden reported on the status of the REFEDs wiki ([refeds.terena.org](http://refeds.terena.org)). Mikael added a new section on the wiki to report experiences on product interoperability. All attendees are invited to report on their inter-operability experience.

Nicole Harris noted the work initiated by Jane Charlton to gather SPs would be continued by Mark Williams.

**Action:** All to populate the wiki section on the interoperability.

**Action:** TERENA to provide an account to Mark to access the REFEDs wiki.

## 2. Interfederation business – Mikael Linden (CSC)

### a. Identifiers and attributes

Mikael reported on the lesson learnt from Kalmar federation. To ease inter-operability among federation and to ease SPs in a confederated environment, Mikael proposed federations to standardise/agree the list of mandatory attributes. This would allow SPs to know which attributes they would be able to access from each of the federations participating in a confederation.

Further Mikael proposed to harmonise the semantic of attributes, which can be rather different among federations for the same attributes.

Andrew noted that in most of the cases the mandatory attributes collected by the federations concern personal data and that might be a concern. Mikael said that attributes should be populated but not always released.

Mikael also noted it might be worth using SAML2 persistent identifiers (eduPersonTargetedID, ePTID), rather than keeping using ePPN.

The uProve module, developed in SWITCH was also discussed. Leif proposed SPs to declare their needed attributes in metadata, so that IdPs can provide what needed. Andrew argued against this, as being a bad practise, as it would encourage SPs to request more attributes than needed.

**Action:** Mikael to circulate a request to collect the list of mandatory attributes.

**Action:** Mikael, Andrew to initiate the process to identify those attributes that have the same meaning across federation.

## 3. Federation business model – Mikael Linden

A discussion took place on how federation's costs are handled firstly in an inter-federation scenario. Mikael noted that in Kalmar's case federations do not charge each other, although at national federation level different models apply.

It was also noted that federations deal with SPs in different ways. HAKA federation for instance does charge commercial SPs but does not charge library SPs.

Thomas reported that SWITCH federation plans to expand beyond HE, which will imply a different business model than the current one.

## 4. LoA

### a. JISC work on LoA – Nicole Harris (JISC)

JISC funded a study to investigate how LoAs' definitions to achieve fine-grained access control to digital resources. The study covers current LoA standards in UK and beyond, addressing also the work done by the US government Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

On a more general note and mainly concerning LoA for HE federations, Nicole noted it would be

useful to separate the metadata registration from the metadata distribution and it would be useful to define how the assurance would flow across.

#### **b. Campus – Mikael**

Mikael noted that in a federation environment the quality of the identity verifications becomes more important and it has to comply with federation's rules.

Haka has published a list of min require and self-audit guidelines to ensure compliancy.

Mikael reported that institutions could only join the HAKA federation if the minimum requirements are fulfilled.

#### **c. InCommon – Ken Klingenstein (Internet2)**

Ken reported that eduCause is about to join InCommon, which is now moving to SAML2.0. In what concerns LoAs, InCommon complies with the Silver LoA level, but there are requirements for LoA 0, for example to leave anonymous comments in websites and blogs.

Ken noted that InCommon would remain part of I2 for the next couple of years, but in the future it might be moved out due to the fact that the membership is expanding beyond I2 community.

Ken touched upon scalability of federations, as in being international, being able to support different market and reaching consumers.

Ken finally noted that I2 is about to launch a survey on 2<sup>nd</sup> factor authentication.

### **5. Inter-federation Business**

#### **a. Inter-federation agreement – Andrew Cormack (JANET(UK))**

A discussion took place on how a possible inter-federation agreement would work. Andrew presented his preliminary ideas.

Within a federation, metadata are handled according to the local process at federation level (local published process). If escalation processes occur they are dealt according to the 'home' federation rules.

In a multi-federation scenario all federation would deal with a central entity, which would have agreements with all federations and there would be a metadata terms of use agreed between the central entity and the other parties.

The inter-federation agreement would rule the flow of info.

Action: Andrew to circulate the inter-federation agreement made between UK and InCommon. More discussion will be needed on this.

#### **b. The federation operator CPS – Alex Reid (AARNET)**

Although Alex was not involved into this, he agreed to report on this topic on behalf of Rodney McDuff (Queensland Univ). During the REFEDs meeting in Utrecht it was agreed to create a document that would be the equivalent to the CPS for PKI. Rodney, who suggested the work, had asked for other people to be involved. However work has progressed very slowly, due to other commitments.

Ken noted that such a work would be very useful and it would be desirable to carry it in a broader group. Licia noted that having a small group to prepare an initial draft would be more efficient, but plans are to get consensus on the results from a large community.

It is worth noting that the document is meant to be provide a framework for "SAML Metadata Signing Policy and Aggregation Practice" in order to allow for comparison. The document would

be technology agnostic and it would be applicable to any SAML-related policies and practices.

**c. Report from JISC on the study to assess federation policies – Nicole Harris**

Jisc commissioned a study to analyse the various federation policies with the aim of discover reasons for big differences in the policy documents. Original idea was to investigate the need for a common policy template. The study has been completed and results are available.

Action: Nicole to circulate the report URL on the JISC policy study.

**d. CAUDIT IAM Federation – Patricia McMillan (Queensland Univ)**

Patricia reported on the CAUDIT IAM framework. CAUDIT is the association of IT Directors, CIOs from higher education and research.

A compendium is under preparation to provide policy considerations, risk assessment, risk management, LoAs, relevant standards and resources. Advices on how to federate with other institutions are also in the plan.

Patricia noted that contributions on case studies on Identity Access Management would be welcome.

For more info please refer to:

<https://wiki.caudit.edu.au/confluence>

**STORK – Leif Johansson (Stockholm Univ)**

Leif reported on his meeting with the Swedish STORK representative. STORK is an EC funded pilot to create a system able to recognise eID throughout Europe. The aim is to facilitate business and e-government transaction using eIDs.

Leif invited attendees to get in touch with their national STORK representative to bring to their attention the work done by the research and education community on Identity Management.

**Kantara – Lucy Lynch (ISOC)**

Lucy provided an overview on Kantara, the new initiative starting as a follow up of Liberty Alliance. Lucy invited attendees to join discussion on the relevant Kantara group.

Licia noted that TERENA had joined Liberty Alliance and that recently TERENA was asked to sign a new agreement to join Kantara. Plans are for TERENA to join Kantara as well.

**Interoperability with other Identity spheres – Diego Lopez (RedIRIS)**

Diego noted that the last trend seems to only recognise SAML as protocol for interoperability. As the key issue is transferring data, Diego suggested having a more agnostic approach, without binding to the nature of the protocol.

Normal users would ask HE federation to link their already existing identities.

Diego reported on the Concordia group and in particular on the Identity Metasystem discussion, on how to exchange identities with the aim of ensuring inter-operability. Diego noted this activity would be very relevant for REFEDs.

Questions to address concerns things like what makes an OpenId account suitable to be used into a SAML assertion or what makes an X.509 certs suitable to be used with OpenId and so on. Diego noted that PKI might be in business for longer than expected and currently it seems

the only technology to enable trust in a distributed environment.

Diego noted that it would be worth exploring the possibility of engaging in reciprocity principle with big players, namely accepting IDs issued by a provider such as Facebook, but asking the same provider to accept HE IDs.

### **Tao of Attributes – Ken Klingenstein**

Ken noted that OpenID would be used to deliver attributes for the White House. A workshop on attributes is being organised by I2 in September.

One of the issues to address is how to deal static and dynamic provision of attributes.

### **n. Date of Next Meeting, AOB and Close**

To be decided on the list.

### **Action List**

| <b>Reference</b> | <b>Who</b>        | <b>Action</b>  | <b>Status</b> |
|------------------|-------------------|--|---------------|
| 07062009-01      | TERENA            | to provide an account to Mark to access the REFEDs wiki.   |               |
| 07062009-02      | All               | All to populate the wiki section on the interoperability.  |               |
| 07062009-03      | Mikael            | to circulate a request to collect the list of mandatory attributes.                                |               |
| 07062009-04      | Mikael,<br>Andrew | to initiate the process to identify those attributes that have the same meaning across federation. |               |
| 07062009-05      | Andrew            | to circulate the inter-federation agreement made between UK and InCommon.                          | Done          |
| 07062009-06      | Nicole            | to circulate the report URL on the JISC policy study.  |               |

### **List of Participants**

|                             |  |
|-----------------------------|--|
| Kristof Bajnok              | NIIF / Hungarnet                       |
| Valentino Cavalli           | TERENA                                 |
| Andrew Cormack              | JANET(UK)                              |
| Ana Lúcia de Moura          | RNP                                    |
| Licia Florio                | TERENA                                 |
| Victoriano Giralt           | University of Malaga                   |
| Maja Gorecka-<br>Wolniewicz | PIONIER/Nicolaus Copernicus University |
| Nicole Harris               | JISC                                   |
| Roland Hedberg              | Umeå University                        |
| Avgust Jauk                 | ARNES                                  |

---

|                      |  |
|----------------------|--|
| Leif Johansson       | Stockholm university/SUNET             |
| Toshiyuki Kataoka    | National Institute of Informatics      |
| David Kelsey         | STFC-RAL                               |
| Jean-Paul Le Guigner | CRU-RENATER                            |
| Thomas Lenggenhager  | SWITCH                                 |
| Mikael Linden        | CSC                                    |
| Diego Lopez          | RedIRIS                                |
| Lucy Lynch           | Internet Society                       |
| Iara Machado         | RNP                                    |
| Patricia McMillan    | The University of Queensland           |
| Aleks Mihićinac      | ARNES                                  |
| Miroslav Milinovic   | Srce                                   |
| Janos Mohacsi        | NIIF/Hungarnet                         |
| Christian Panigl     | ACOnet                                 |
| Rok Papež            | ARNES                                  |
| John Paschoud        | LSE                                    |
| Dubravko Penezic     | Srce                                   |
| Juergen Rauschenbach | DFN-Verein                             |
| Alex Reid            | AARNet                                 |
| Brook Schofield      | TERENA                                 |
| David Simonsen       | WAYF                                   |
| Hideaki Sone         | NII / Tohoku Universit                 |
| Hannes Tschofenig    | Nokia Siemens Networks                 |
| Niels van Dijk       | SURFnet                                |
| Joost van Dijk       | SURFnet                                |
| Glenn Wearen         | HEAnet                                 |
| Torbjörn Wiberg      | SWAMI/Umeå Universitet                 |
| Klaas Wierenga       | Cisco Systems                          |
| Mark Williams        | JISC Collections                       |
| Stefan Winter        | RESTENA                                |
| Tomasz Wolniewicz    | PIONIER/Nicolaus Copernicus University |
| Kazu Yamaji          | National Institute of Informatics      |
| Hans Zandbelt        | SURFnet                                |