« networking the networkers »

Internet2 Spring Meeting
Washington DC
27 April, 2009

Licia Florio
Project Development Officer
florio@terena.org

Middleware Developments in Europe

Agenda

- Background
- Network access: eduroam
- Application access: Identity Federations
- The policy side:REFEDs

- PKI

How it all started

- Problem to solve:
  - Provide wireless access only to authenticated users;
  - Provide access to shared (web) resources;
- Requirements:
  - Identify users uniquely at the edge of the network;
  - Multiple devices to get on-line with;
  - Guest access;
  - Scalable solution;
    - Following the model authenticate local, act global;
  - Easy for users;
  - Open standards.

First pan-European Identity federation

- eduroam = education roaming:
  - To provide federated network access;
  - For the institutions participating in eduroam;
  - Started in a very simple way:
    - NRENs active in the TERENA task-force on mobility share their wireless connections.
- eduroam technology:
  - 802.1X/EAP + RADIUS;
  - EAP can provide with the right EAP-method; protection of credentials;
- eduroam is single purpose federation, just for network access.

eduroam in Europe

- Most of EU connected
  - Plans to expand to Ukraine, Belarus, Armenia

eduroam Today

- Since 2005 part of GÉANT project:
  - In 2007 eduroam became an EU service;
- Model:
  - Confederation:
    - Federation of national eduroam federations;
- eduroam European policy:
  - Only regulates the peering among the national federations;
  - National policies applies at national level;
- Outside EU:
  - eduroam in Japan, Australia, Taiwan, China (not in all country!);
  - Canada;
  - US (not in place yet): UC Santa Barbara, UTK, Harvard (Boston area) and others.

eduroam Goes Global

- The good:
  - We can travel all over and we will be able to get on-line
- But…
  - How do we organise the peering internationally?
    - What is the model to follow?
  - How does the trust model evolves from national, to international?
    - In Europe, this is defined by the European policy;
    - How about the rest of the world?
    - Do we need/want a global policy?
  - Is eduroam implemented in the same way across the globe?

Identity Federations in Europe

- Mainly used to provide access to Web-based applications;
  - But plans are to support also other applications;
- Identity Federations have two main components:
  - Technology/protocols;
  - Trust;
- Technology:
  - All of them 'talk' at least SAML1.x;
  - Migration to SAML2 is ongoing;
  - Due to the convergence of SAML2 these different national federations can talk to each other;
- Trust:
  - Built via policies, which reflect a community understanding of trust, behaviours, laws.

Deployment in Europe

- Different level of deployment in EU:
  - Recently created federations: Italy, Germany, Ireland, France.
  - Operational: Switzerland, UK, Croatia, Netherlands, Spain, Czech Republic, Nordic countries.

- Different (open source) technologies are used
  - Shibboleth: UK, Finland, Switzerland, Germany, Italy;
    - Most used technology;
    - But not the only one :-)
  - PAPI: Spain;
  - A-Select: the Netherlands;
  - Sun Federation Manager based upon Liberty Alliance specification: Norway.
- GÉANT:
  - eduGAIN: to enable sharing of identity data among federations;

Federation 'Mess'

- Bilateral federation (Classical model):
  - Users trust their IdP, which establish relationships with one or more SPs;
- Confederation:
  - Different federations agree to share some common policies (see eduroam case);
- Interfederation:
  - Similar to the confederation, but with less formal agreements in place (see Kalmar Union).
- Leveraged federations:
  - Within a federation sub-groups agrees to share policies that do not apply to the all federation;
- Gateway of federations:
  - See eduGAIN
- And much more…

What is REFEDs?

- Is NOT by definition a technical group:
  - In most of the cases those working on policies and business model do not work on technologies;
    - But there are exceptions…
- What is REFEDs then?
  - REFEDs gather people interested in producing guidelines that might be useful for other identity federations all in the R&E landscape;
  - REFEDs aim to also lobby with some bodies with influence in other areas, such as Liberty Alliance, Article 29 Working Party and similar to get acknowledgment and possible endorsement.
- REFEDs is an international group:
  - Not only for Europe;
  - But also Australia, Americas, Asia.

Why REFEDs?

- REFEDs started with aim to assess the trust model in inter-federation context.
  - Discussion on this started a way back,
- Diversity in the way to implement federations has an impact on the inter-operability;
  - And the costs;
  - And can create barriers to the deployment of federations;
  - But communities do have different laws, requirements, behaviours;

REFEDs Scope

- REFEDs roadmap defines four main areas:
  - **Policy Coordination**
    - To define of policy template and guidelines for the new federations.
  - **Privacy and Data protection**
    - To develop good practice for identity federation operators and participants to use federated technologies to reduce the transfer of personal data.
  - **The (Inter)Federation business**
    - To document the federation process.
  - **Definition of LoA profiles**
    - In Identity Federations, LoA refers mainly to the way Identity Providers (IdP) establish the identity of the end user and how securely users credentials are stored.

First Results

- First documents have been produced in the area of "Privacy and Data Protection":
  - Federated Access Management [Dec 2008] [Draft]
  - Pseudonymous Identifiers [Dec 2008] [Draft]
  - Good Practice for Federated Access Management [Dec 2008] [Draft]
- The federated access management paper was sent to the Article 29 WP in July 2008.
  - We asked them to validate the work and eventually endorse it.
  - Thanks to Andrew Cormack (JANET(UK))!
- REFEDs wiki has become a reference for many publishers, who make explicit references to it.
  - The wiki contains data on 17 federations;

In the pipeline

- Work on all topics in REFEDs roadmap;
  - Hopefully some more documents available before the next REFEDs meeting;
    - June 2009 @ TERENA Networking Conference.
- Keep the wiki up-to-date:
  - Gathering data from the missing federations;
  - Mikael Linden (CSC) coordinates this.
- Strengthen contact with relevant bodies and projects:
  - STORK, pilot co-funded by EU that aims to implement an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State.
    - Discussion started with STORK seems promising.
  - Liberty Alliance.

PKI developments in Europe

- PKI
  - Comparable to Beckett's play "Waiting for Godot";
  - It is always about to happen, but it never really happens.

- Idea:
  - Address PKI in a different way;
  - Solve the server certificates issue first;
  - What if you could contract a service with a commercial CA for an unlimited amount of SSL certificates for a flat rate per NREN?
  - How many NRENs would you need? Would there be an interested vendor?

SCS: Making PKI happen

- Fall 2005:
  - TERENA opens a Call for Proposals;
  - First contract with GlobalSign BV in 2006;
- SCS (Server Certificate Service)
  - NRENs participating would get SSL certificates against a yearly flat-fee;
- Started with 8 NRENs (in 2006):
  - Now 19 NRENs participate;
  - More than 20.000 SSL certificates issued in Europe;
- March 2009:
  - As result of a new Call for Proposal, Comodo appointed as new supplier;

SCS → TCS

- New SCS service:
  - Expected to start in May 2009;
- Model:
  - Yearly flat fee per NREN;
  - TERENA contractual party;
  - A dedicated TERENA sub-CA;
- NRENs participating can also buy client certificates and code-sign certificates:
  - Upon an extra flat fee;
  - TCS: TERENA Certificate Services
- At this moment lots of working is ongoing to launch the new service:
  - Testing certificate profiles and interfaces;
  - Writing CPS for the TERENA sub-CA.

Who is in SCS

NREN	NREN service	Country
ACOnet	ACOnet TLS/SSL Server-Certificates	Austria
ARNES	Overjena digitalna potrdila za strežnike	Slovenia
BELNET	BELNET SCS Certificates	Belgium
CARNet	CARNet SC servis	Croatia
CESNET	Certifikáty SureServer EDU	Czech Republic
CRU/RENATER	SCS, Server Certificate Service (CRU) RENATER - Certificats Serveurs (RENATER)	France
FCCN	ServerSign EDU	Portugal
GARR	Istruzioni per certificati server SCS	Italy
HEAnet	HEAnet SCS	Ireland
HUNGARNET	Server Certificate Service	Hungary
JANET(UK)	Server Certificate Service	United Kingdom
LITNET	LITNET SCS	Lithuania
RedIRIS	Servicio de Certificados de Servidor para la comunidad RedIRIS	Spain
PSNC	PSNC SCS	Poland
SUNET	SUNET SCS Service	Sweden
SURFnet	SURFnet SCS	Netherlands
SWITCH	SWITCHpki SCS	Switzerland
UNI•C	UNI-Certifikat	Denmark
UNINETT	SCS (Server Certificate Service)	Norway

- New SCS:
  - Switzerland not participating;
  - Greece and Finland will now participate.

Conclusions

- Trust
  - We need fewer and easier to compare policies;
  - REFEDs can make this happen;
- Hopefully more results will be available during the next year:
  - LoAs;
  - Guidelines to develop and harmonise federation policies and processes.
- Identity impacts all parts of the network infrastructure, not only middleware.
  - Especially in the new vision of expanding the federated framework to support different set of applications and network.

Links

- REFEDs:
  - http://www.terena.org/refeds/
  - https://refeds.terena.org/
- SCS:
  - http://www.terena.org/activities/scs/
- eduroam:
  - http://www.eduroam.org
- eduGAIN:
  - http://www.edugain.org/