An eduGAIN Update

Diego R. Lopez
RedIRIS
TF-EMC2. Utrecht, December 2008
What eduGAIN Offers

• Take advantage of existing identity infrastructures
  – Easing the path to a global system
  – Keeping the federation promise
• Oriented towards the confederation schema
  – But can support the others
• SAML 1.1 (and soon SAML 2.0) is the lingua franca
  – Profiles for WebSSO and other scenarios
• Software
  – Base, Conversion and Validation libraries (Java)
  – simpleSAMLphp (PHP)
  – eduGAINFilter (javax.servlet.filter), a.k.a. Java SP
  – Direct use of Shibboleth 2.0 being investigated
eduGAIN Elements

- The Metadata Service – MDS
  - Updated by authorised components
  - Queried by user interfaces or autonomous services
- PKI
  - Multi-rooted
  - Includes component identifiers
- Identifier Registry, based on URNs
  - Unique, well-structured component identifiers
  - Delegation schema
- Bridging Elements – BE
  - Are the eduGAIN endpoints
  - Adapt protocols when required
  - Should we talk of different BE types?
    - BE -> Federation gateway
    - IFEP (*Inter-federation endpoint*) -> Direct connection to eduGAIN
eduGAIN Architecture
eduGAIN Architecture (rewritten)
The Current eduGAIN Architecture

Connect. Communicate. Collaborate
eduGAIN Profiles

- Different clients - different profiles
  - WebSSO: Stand-alone web-based application
  - Automated Client (AC): Client without human interaction
  - Client in a Web containEr (WE): Web-based applications
  - User behind a Client (UbC): Non-web applications

- Transmission of credentials (except in Web SSO)
  - Clients embed security tokens in their requests
  - According to the Web Service Security (WS-SEC) standard
The Web SSO Profile

- Current status
  - Compatible with Shibboleth 1.3
  - Tested in direct connections to Shibboleth SPs
- SAML 2.0 profile defined
  - Aligned with the SAML2 basic inter-federation profile
Preparing for WebSSO

- Select a suitable BE/IFEP and put it at the appropriate place
  - Top of your federation (BE!)
  - Co-located with your SP/IdP (IFEP)
  - As your only SP/IdP (IFEP)
- Optionally, register with your local federation
- Get component identifier(s)
- Obtain certificate containing component identifier(s)
- Deploy the BE/IFEP using the certificate
- Register your metadata at the MDS
Neutral Access with eduGAIN

• Registry controls the entities able to use it
  – Delegation supports distributed management
• PKI leverage X.509-based profiles
  – Information can be derived from certificate extensions
• MDS allows the link from credentials to attribute sources
  – Dynamic association
• eduGAIN libraries provide an abstraction layer
  – Abstract operational model
  – Plus attribute translation if required
• BEs/IFEPs provide identity source adaptation
The AC profile

- Unique and non-transferable ID for each client
  - URN obtained from eduGAIN registry service
- Certificate in the eduGAIN trust fabric
  - Subject Alternative Name of the cert contains the URN
  - Obtained from the eduGAIN PKI
- Authentication information is based on the X.509 certificate
Preparing for AC

- Incorporate software able to generate requests according to the profile
  - Currently, part of the perfSONAR codebase
  - Seems easy to generalize
- Deploy and configure a BE/IFEP (H-BE) if you do not have one
  - Including registration and certificate
- Register an URN/branch for your client(s)
  - Optionally, assign individual identifiers
- Obtain certificate(s) containing component identifier(s)
- Incorporate data about the clients at your H-BE
- Deploy the clients
The Current UbC profile

- Similar to AC
- Online CA providing the certificate
  - SASL CA
Preparing for UbC

• Incorporate software able to generate requests according to the profile
  – Currently, part of the perfSONAR codebase
  – Seems easy to generalize
• Deploy and configure a BE/IFEP (H-BE) if you do not have one
  – Including registration and certificate
• Deploy and configure a SASL online CA
  – Including certificate
  – It must have direct access to user credentials
  – It must be able to provide a session to user attributes
• Deploy the clients
Why Current UbC Does Not Fly... And How To Fix It

• Deployment and configuration of the SASLCA
  – Certificate... Stretches CA policy to the limit
  – User credentials... Where to locate it
  – Session to user attributes... How to establish the link
• Use an already existing credential exchange infrastructure
  – Aligned with CA policies
  – Pervasive
  – With a profile allowing attribute retrieval
• Hey, we have the eduroam infrastructure!
  – DAMe extensions to convey attributes
  – And RadSec to enable H-BE location
The UbC Profile Revisited

- **Authentication protocols**
  - RADIUS/Radsec, applying results from DAMe
  - HTTP Auth

1: User tries to access client

2: Authentication

3: Get credentials + SAML assertions

4: Sends a request + relayed-trust SAML assertion

5: Forwards relayed-trust SAML assertion

6: Attribute request

7: Attribute response

8: Returns the authR decision

9: Sends a response
Preparing for New UbC

- Incorporate software able to generate requests according to the profile
  - Can be based on the DAMe codebase
  - And the relayed-trust management library
- Deploy and configure a BE/IFEP (H-BE) if you do not have one
  - Including registration and certificate
- Deploy and configure a RadSec server
  - Including certificate
  - Several choices: FreeRadius, radsecproxy,…
  - Enable the DAMe extensions
- Deploy the clients
The WE Profile

1: User tries to access client
2: SSO redirect
3: Authenticate
4: SSO response + SAML assertion
5: Sends a request + relayed-trust SAML assertion
6: Forwards relayed-trust SAML assertion
7: Returns the authR decision
8: Sends a response

- SAML assertions contain user’s credentials
- Clients must have a certificate in the eduGAIN trust fabric
Preparing for WE

• Deploy a H-BE according to WebSSO requirements
• Deploy and configure eduGAINFilter as R-BE for the client
  – Similar solution for other environments being considered
• Install and configure the relayed-trust software
  – In the perfSONAR codebase
  – Working in its generalization
  – Needs a specific identifier and certificate
External Attribute Authorities

- R-BE has configured a list of Attribute Authorities
- AA is connected to a set of Attribute Stores
Where We Are

• Not at service level
  – MDS, PKI and registry in operation
    • Policies being discussed
    – In use by demonstrators and perfSONAR
• Software available
  – As RC4
  – Previous to first official release
• Polishing general information resources
  – www.edugain.org
• Discussing how the service shall look like
  – And how to evolve it