SWITCH

The Swiss Education & Research Network

International Update

Thomas Lenggenhager, SWITCH

2. December 2002

SWITCH aai

AA in General

SWITCH
The Swiss Education & Research Network

- Many local activities in the queue
  - Different foci due to different environments

- Need for interoperability will arise
  - Common understanding of the architecture
    - Which pieces within 'Middleware Puzzle'?
  - Authorization Attributes
    - Common syntaxes, common semantics
  - Use same protocols 'on the wire'
  - Understand underlying trust models

  TERENA Task Force, together with Internet2, started working on it

Shibboleth

SWITCH
The Swiss Education & Research Network

- **Version 0.7 is out** http://shibboleth.internet2.edu
  - **New versioning schema replaces alpha and beta versions**
  - **Available as binaries (RedHat 7.2 & 7.3, Solaris 2.8) and source**
  - **Target side without Java**
  - **Easier installation**

- **Version 0.8 planned for March 2003**
  - **Attribute Release Policy will be redone**
  - **Configurable Attribute Requestor at target side**

- **Version 1.0 planned for April 2003**
  - **Bug fix release, no new features**

Shibboleth (2)

SWITCH
The Swiss Education & Research Network

They are working on:

- **Personal Information Manager**
  - **Ease sharing of web contents with buddies**
    - **User friendly generator for Apache .htaccess files**
- **Privacy Management System**
  - **User can review to which resource which personal information was released**

- **WebCT release of April 2003 will include Shibboleth support**
- **uPortal and Open Knowledge Initiative (OKI) will use Shibboleth**

  http://www.ja-sig.org http://web.mit.edu/oki
- **Convergence with PAPI is longer term issue**
- **Future software maintenance is an open issue**

Europe

SWITCH
The Swiss Education & Research Network

- **UK – Athens** http://www.athensams.net
  - **Centralized access management system**
  - **249 resources by 51 providers, 2 Mio accounts, 86'000 accesses/day**
  - **Decentralization with campus LDAP servers now possible**
  - **Shibboleth compliance planned for 2003**

- **NL – A-select** http://a-select.surfnet.nl
  - **Authentication system in testing phase**
  - **'Hitchhike' on existing authentication service providers**
    - **RADIUS (available from remote login service)**
    - **SMS – One-Time-Password sent to mobile phone**
    - **Dutch bankcards**

Europe (2)

SWITCH
The Swiss Education & Research Network

- **NO – FEIDE** http://www.uninett.no/feide/index.en.html
  - **Building a common electronic ID for education**
  - **Coordinated user database through indexed LDAP servers**
  - **Authentication system for web services named Mellon & Moira**
    - **Implementation as Java servlets**
    - **Similarities with Tequila**

- **FI – FEIDHE** https://hstya.funet.fi
  - **Trials based on national ID smart-card not full success**
  - **'We must live with username/password for the next years'**
  - **Virtual Polytechnic is driver for AAI project**

Authorization

SWITCH
The Swiss Education & Research Network

- Authorization gets soon complex – requires programming
- Policy and rule based authorization
  - promises to be easier to manage and to keep consistent
- Two approaches for policy based access control
  - PERMIS – Project of University Salford, UK http://sec.isi.salford.ac.uk/permis
    - Based on XACML
    - Implemented as C-library
  - SPOCP – Project of Swedish Universities http://www.umu.se/it/projupp/spocp
    - Based on S-expressions
    - Can use LDAP and other dynamic data
    - Implemented as C-library, Apache module and standalone server
  - Both are in an early stage, missing is e.g.
    - Deployment
    - User interfaces to generate and check policies and rules

Liberty Alliance

SWITCH
The Swiss Education & Research Network

- **Version 2 planned for 2003** http://www.projectliberty.org
  - **Will not be backwards compatible with version 1.x**
  - **Bob Morgan & Scott Cantor (Shibboleth development team) invited experts for the design of version 2**

SWITCH

The Swiss Education & Research Network

PAPI

Rolf Gartmann, SWITCH Security Group

December 2, 2002

SWITCH aai

PAPI 1.1.0 - Open Issues

SWITCH
The Swiss Education & Research Network

- Well suited at an enterprise level
- Group based assertions about users (and not Attribute based)
- Transmitted information to Resources
- Different assertions about users to different PoA's
  not solved in this version (no Attribute Policy)
- Most authorization is done at the AS (and not at the PoA as needed in our environment)
- N x M dependency (AS, PoA's)
- Personalized Resources

PAPI 1.2.0 - New Features

SWITCH
The Swiss Education & Research Network

- Still based in Perl
  - And Perl-ish configuration and features
- Support for attribute-based authorization
  - Assertions sent by the AS can be individualized
  - PoAs can specify richer authz filters on these assertions
- Better personalization mechanisms
  - Individual accept/reject objects
  - Automatic redirection at the AS
- Extended proxy mode
  - Applicable to a whole domain
  - Support for HTTP authentication

PAPI 1.2.0 - New Features

SWITCH
The Swiss Education & Research Network

- For each (G)PoA an AS is going to contact an assertion format string is derived from:
  - User and group data
  - The (G)PoA definition
  - The AS defaults
- Inside the assertion format string, the AS can substitute
  - Connection variables
    - » Username (or a hash of it), a nonce, anything else passed through the HTML forms or the configuration
  - Attributes of the user entry
    - » Based on LDAP although other sources are possible
- A Perl-ish way to ARPs

PAPI 2.0 - New Features

SWITCH
The Swiss Education & Research Network

- Apache & IIS module written in C
- PAPI Proxy will stay in Perl (at least for the moment)
- Java implementation at the AS side
- extended trust model
- available in spring 2003