SWITCH

The Swiss Education & Research Network

Technical Background Information

Ueli Kienholz, SWITCH
Rolf Gartmann, SWITCH
Claude Lecommandeur, EPFL

December 2, 2002

SWITCH aai

SWITCH

The Swiss Education & Research Network

PAPI

Rolf Gartmann, SWITCH Security Group

December 2, 2002

SWITCH aai

PAPI 1.1.0 - Open Issues

- 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

- 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

- 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

- 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

SWITCH

The Swiss Education & Research Network

Shibboleth Technical Info

Ueli Kienholz, SWITCH

2. December 2002

SWITCH aai

Shibboleth Technical Info

SWITCH
The Swiss Education & Research Network

❑ Status of Shib

❑ Technologies involved

❑ How to implement an origin site

❑ How to implement a target site

❑ Need to know & pitfalls

Status of Shib

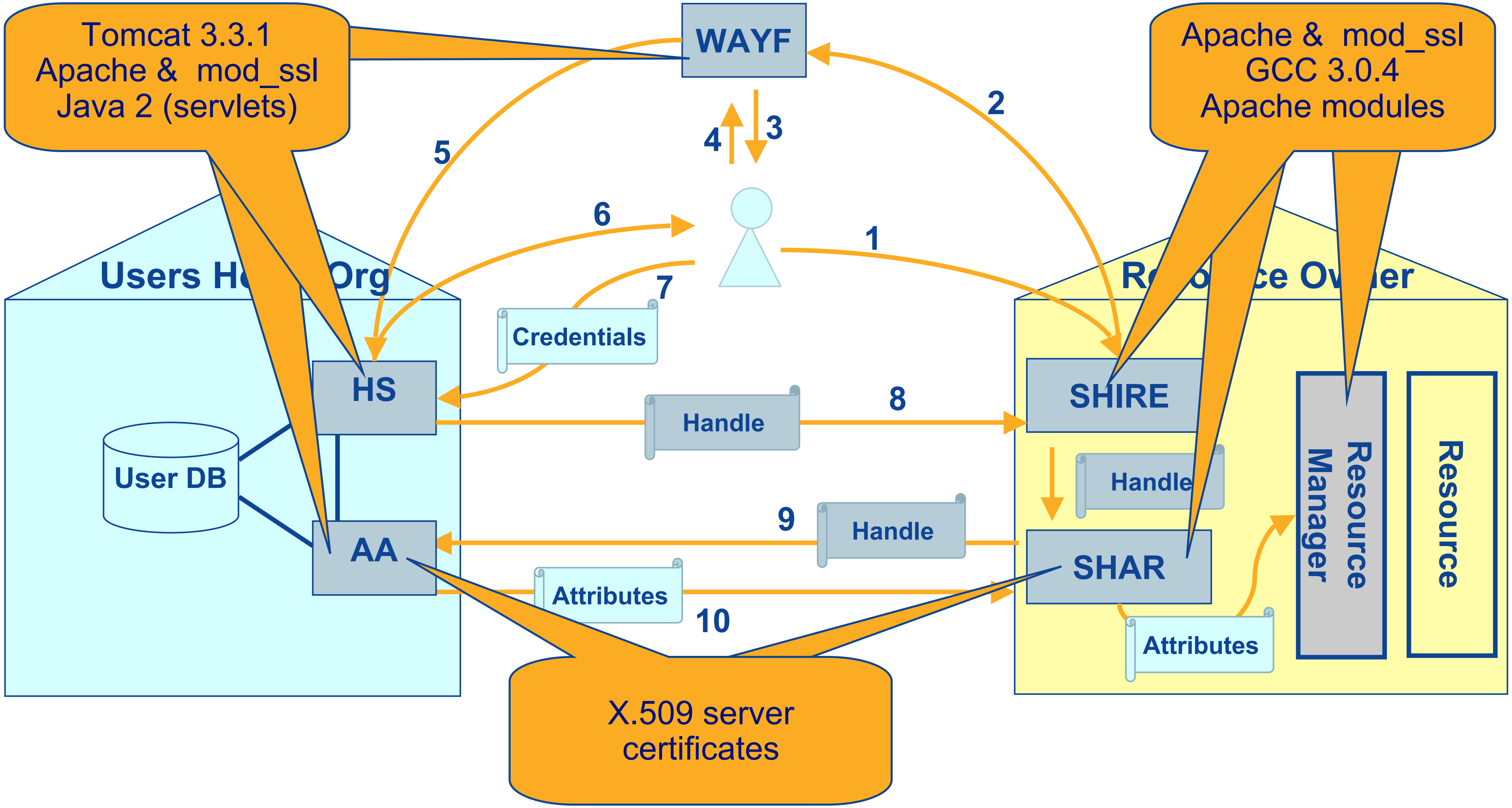
Latest Version: 0.7

- Just enough functionality for a working Shib implementation
- Not recommended to protect sensitive data with this version
- Attribute release policy tools and config will change dramatically at the next version

➢ For tests and pilots OK,
but not easy

Technologies involved

The Swiss Education & Research Network



Tomcat 3.3.1
Apache & mod_ssl
Java 2 (servlets)

Apache & mod_ssl
GCC 3.0.4
Apache modules

X.509 server
certificates

Installation of an Origin Site

Installation

❑ Download Shib Distribution (http://wayf.internet2.edu/shibboleth/)

❑ Follow instructions in

❑ Origin Deployment Guide (see http://shibboleth.internet2.edu/)

❑ http://www.switch.ch/aai/pilot-docs/shibboleth/origininstall.txt
(Installation Notes for an Origin installation at SWITCH)

Suggested Reading

http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-arch-v05.pdf

Configuration of an Origin Site

Main configuration file:

- ❑ web.xml

PKI:

- ❑ Generate a server.key with openssl, and send CSR to aai@switch.ch
- ❑ Overwrite server.crt with the one that is signed and returned from SWITCH
- ❑ Add certificate of Test-CA to ca_bundle.crt
  download it from
  http://www.switch.ch/aai/pilot-cert/ca-vho-t_PEM.crt

For more details see:

http://www.switch.ch/aai/pilot-docs/shibboleth/origininstall.txt
(Installation Notes)

Installation of a Target Site

Installation

- ❑ Download Shib Distribution (http://wayf.internet2.edu/shibboleth/)
- ❑ Follow instructions in
- ❑ Target Deployment Guide (see http://shibboleth.internet2.edu/)
- ❑ http://www.switch.ch/aai/pilot-docs/shibboleth/targetinstall.txt
  (Installation Notes for a target installation at SWITCH)
- ❑ RedHat 7.2 or 7.3 suggested when installing binaries
- ❑ Compilation from source not easy, yet

Suggested Reading

http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-arch-v05.pdf

Configuration of a Target Site

Main configuration file:

- ❑ shibboleth.ini

PKI:

- ❑ Generate a server.key with openssl, and send CSR to aai@switch.ch
- ❑ Overwrite server.crt with the one that is signed and returned from SWITCH
- ❑ Add certificate of Test-CA to ca_bundle.crt
  download it from
  http://www.switch.ch/aai/pilot-cert/ca-vho-t_PEM.crt

For more details see:
http://www.switch.ch/aai/pilot-docs/shibboleth/targetinstall.txt
(Installation Notes)

Need to know & pitfalls

- ❑ First call after restart of origin server very slow (needs compilation of Java-servlets)
- ❑ Permissions of /etc/httpd/conf/ssl.* should be 755
- ❑ Origin site and target site need to be synchronised (+/- some minutes) -> use NTP
- ❑ Remove php4_module from httpd.conf at target site

SWITCH

The Swiss Education & Research Network

Téquila

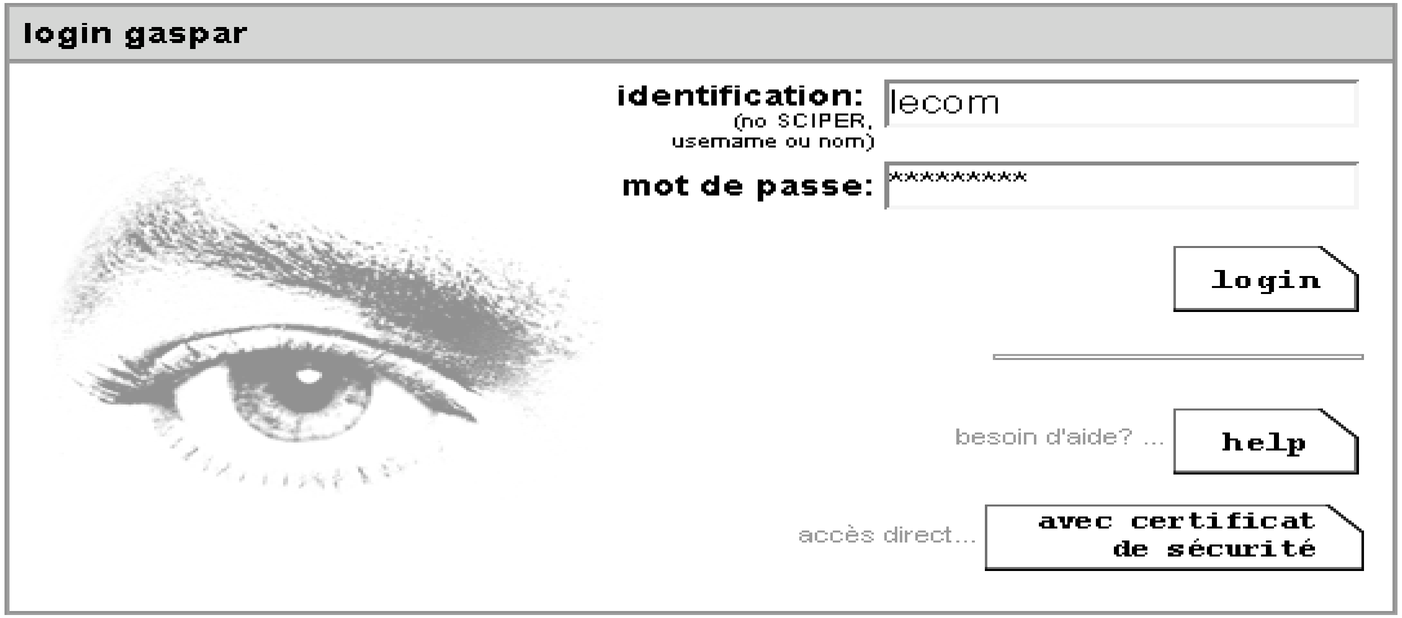
Claude Lecommandeur, EPFL

December 2, 2002

SWITCH aai

GASPAR

- Used at EPFL for more than 3 years.
- Authenticates dozens of Web applications.
- Manages authentication and central services.
- Authentication attributes mapped to several other servers (AD, LDAP, Radius...).



login gaspar

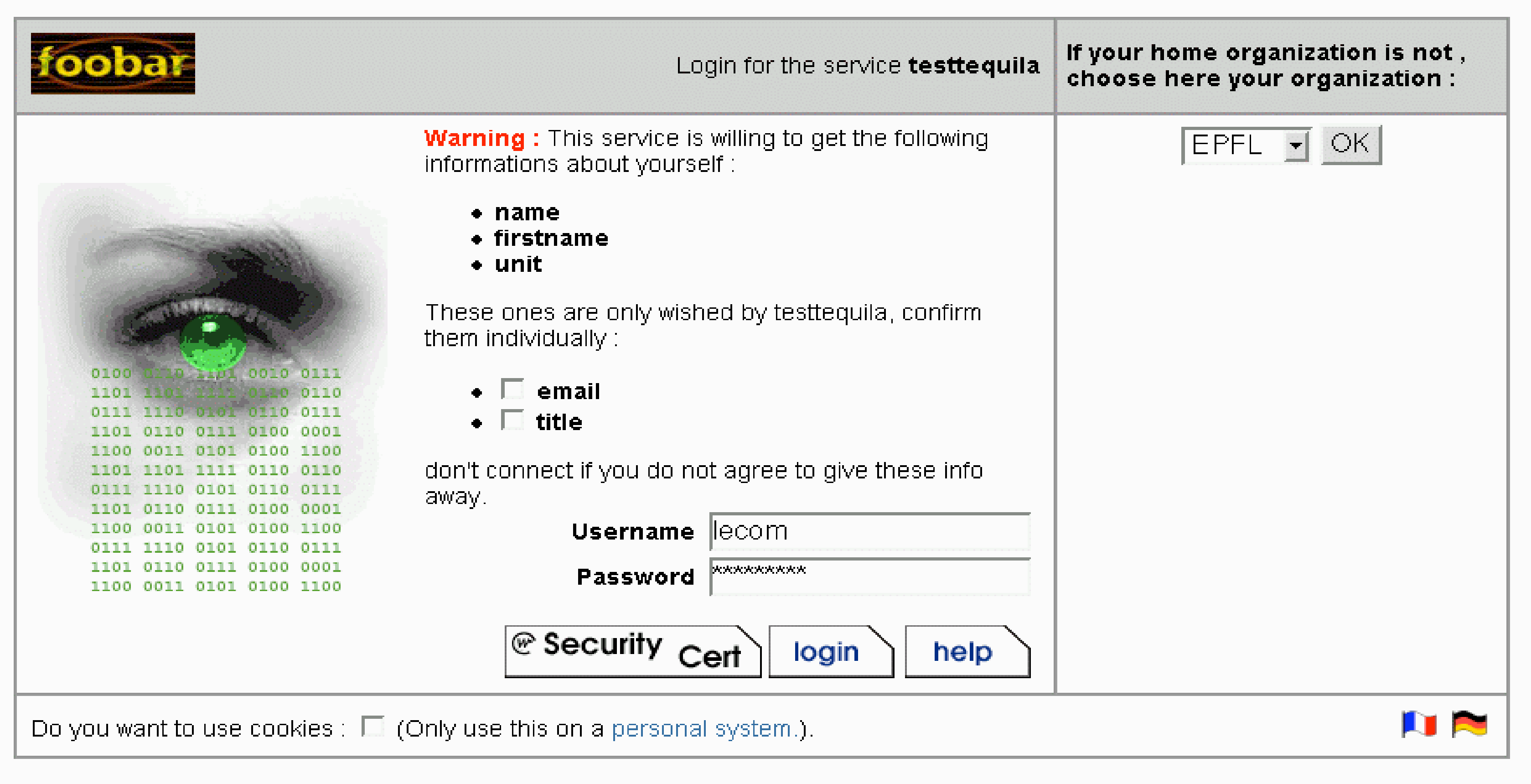
identification: (no SCIPER, username ou nom) lecom

mot de passe: **********

Téquila (1)

- Based on Gaspar.
- Rewritten in Perl.
- Handles multiple institutions.
- Take care of user data protection and privacy.
- Very customizable.

Téquila (2)



Login for the service **testtequila**

If your home organization is not , choose here your organization :

Warning : This service is willing to get the following informations about yourself :

- **name**
- **firstname**
- **unit**

These ones are only wished by testtequila, confirm them individually :

- □ **email**
- □ **title**

don't connect if you do not agree to give these info away.

Username	lecom
Password	**********

Do you want to use cookies : □ (Only use this on a personal system.).

How does it work ?
Scenario 1

- The Web application that wants authentication redirects the user to the Tequila login window.
- Tequila authenticates the user.
- Tequila tells the Web application about the successful login.
- Tequila redirects the user to the application.
- The application accepts the user.

How does it work ?
Scenario 2

- The Web application that wants authentication redirects the user to the Tequila login window.
- Tequila authenticates the user.
- Tequila stuffs user attributes in the application URL and signs it (public key signature).
- Tequila redirects the user to this signed URL.
- The application verifies the signature and accepts the user.

Across institutions

- When using a remote Tequila server (the user is trying to authenticate in an institution other that his home institution), the local Tequila redirects the authentication request to the user's home institution.
- The local Tequila, has no information on the user.
- User's security (password) and privacy (attributes) is protected.