AAI Pilots projects at the University of Lausanne

February 2003

UNIVERSITE DE LAUSANNE

Content of the presentation

- 2 pilots projects
- Present situation
  - home organization (origin)
  - resource (target)
- Implementation of AAI at Unil
  - home organization (origin)
  - resource (target)
- Demo
- First conclusion
- Open issues
- Next steps

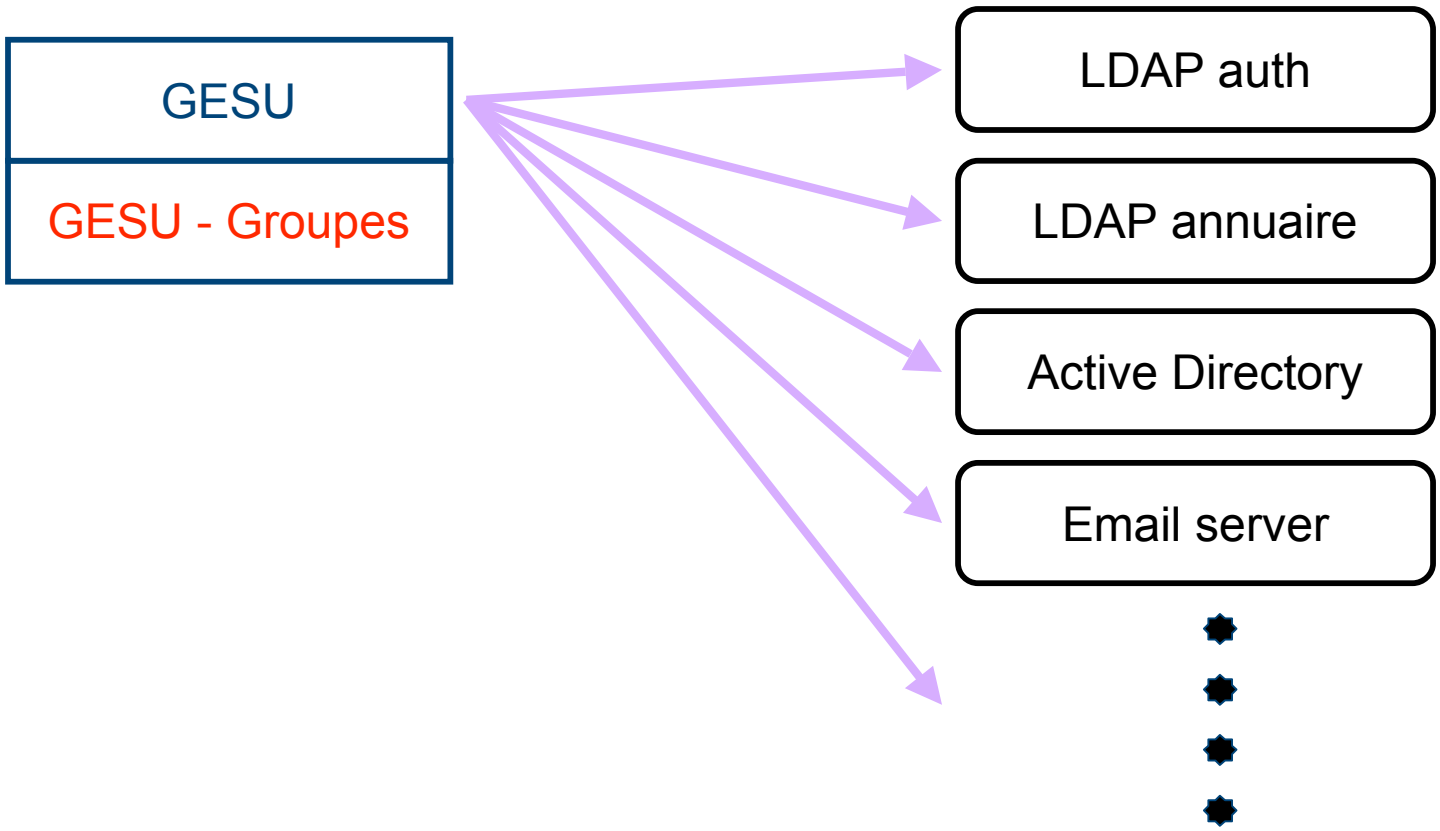
Pilot project: UNIL-EPFL Common Services for Students

- Exchange of authentication data regarding students registered at UNIL and EPFL. Use an **existing application**: Offre d'emploi et logement
- Replace an existing « bricolage » with Gaspar between UNIL and EPFL
- Resource owner: UNIL
- Home organizations: UNIL and EPFL
- Technical aspects:
  - application developed with Informix (Web datablade)
  - Web server is Iplanet (migration to Apache ?)
  - GASPAR at EPFL
  - Basic users attributes are exchanged
- Focus of pilot project
  - **Resource integration (Shibboleth and Tequila)**
  - **Integration of gaspar (home org.)**
  - Exchange user attributes between two organizations
- Advantage of this pilot project
  - no application development is needed
  - limited human resources is needed
  - may be started as soon as central AAI is available
  - collaboration between EPFL an UNIL on this application already exists

Pilot project: AAI for students in medicine

- Provide an authenticated and controlled access to restricted databases @ HUG and to list of available courses
- Proposed by S. Spahni (HUG)
- Resource owner: HUG
- Home organization: UNIL and UNIGE
- Focus of pilot project
  - **Integration of UNIL LDAP Authentication**
- Advantage of this pilot project
  - resource already exists
  - may be started as soon as central AAI is available
  - collaboration between HUG an UNIL on this pilot project has already been discussed

Gestion des utilisateurs (before AAI)



UNIVERSITE DE LAUSANNE

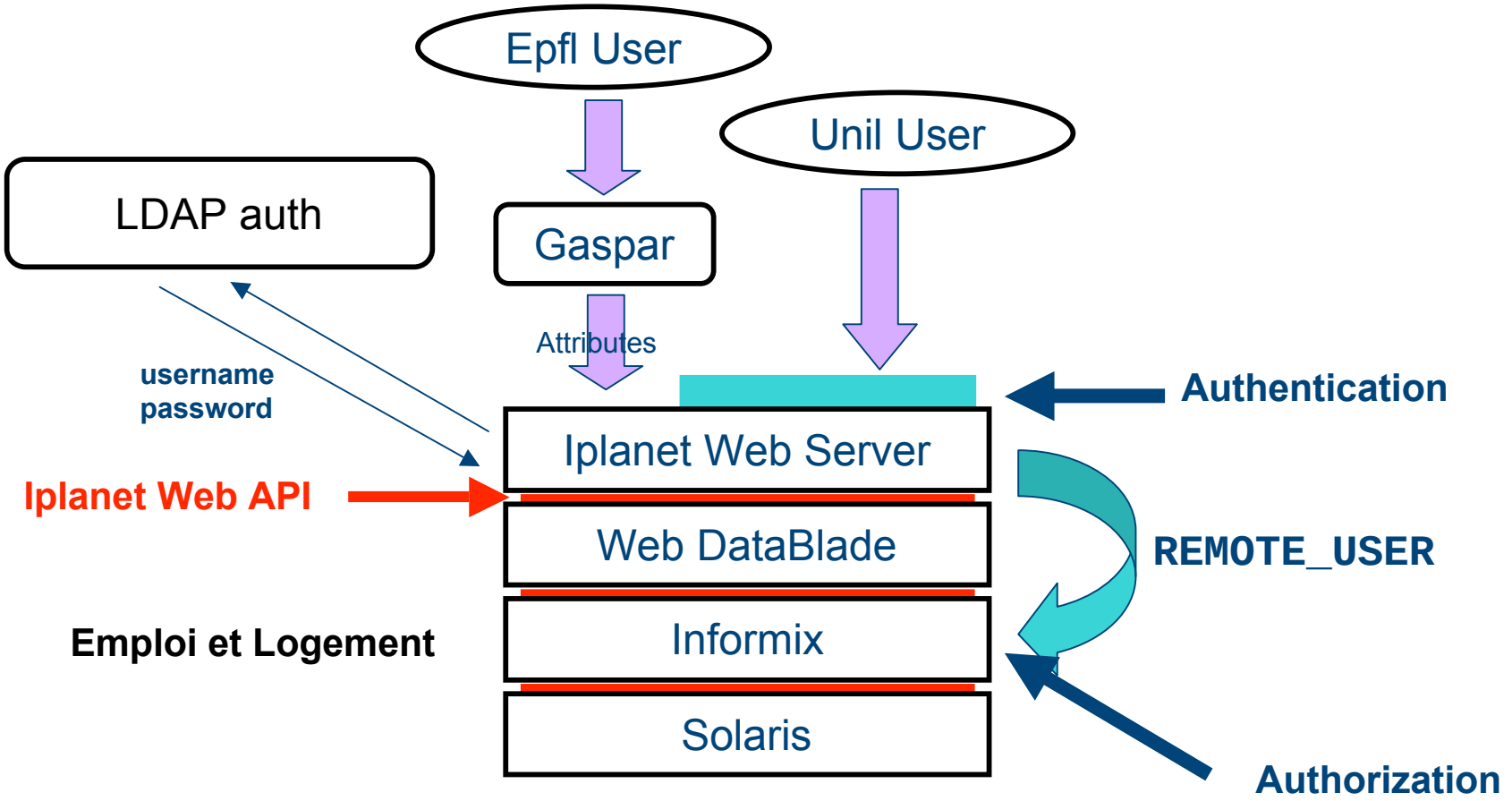
LDAP user

```
dn: uid=uone,ou=unil-users,ou=gesu,dc=unil,dc=ch
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uid: uone
sn: One
cn:User One
givenName:User
mail: User.One@ci.unil.ch
uidNumber: 10281
gidNumber: 10010
loginShell: /bin/ksh
gecos: User One
homeDirectory: /users/uone
userPassword:****************
```

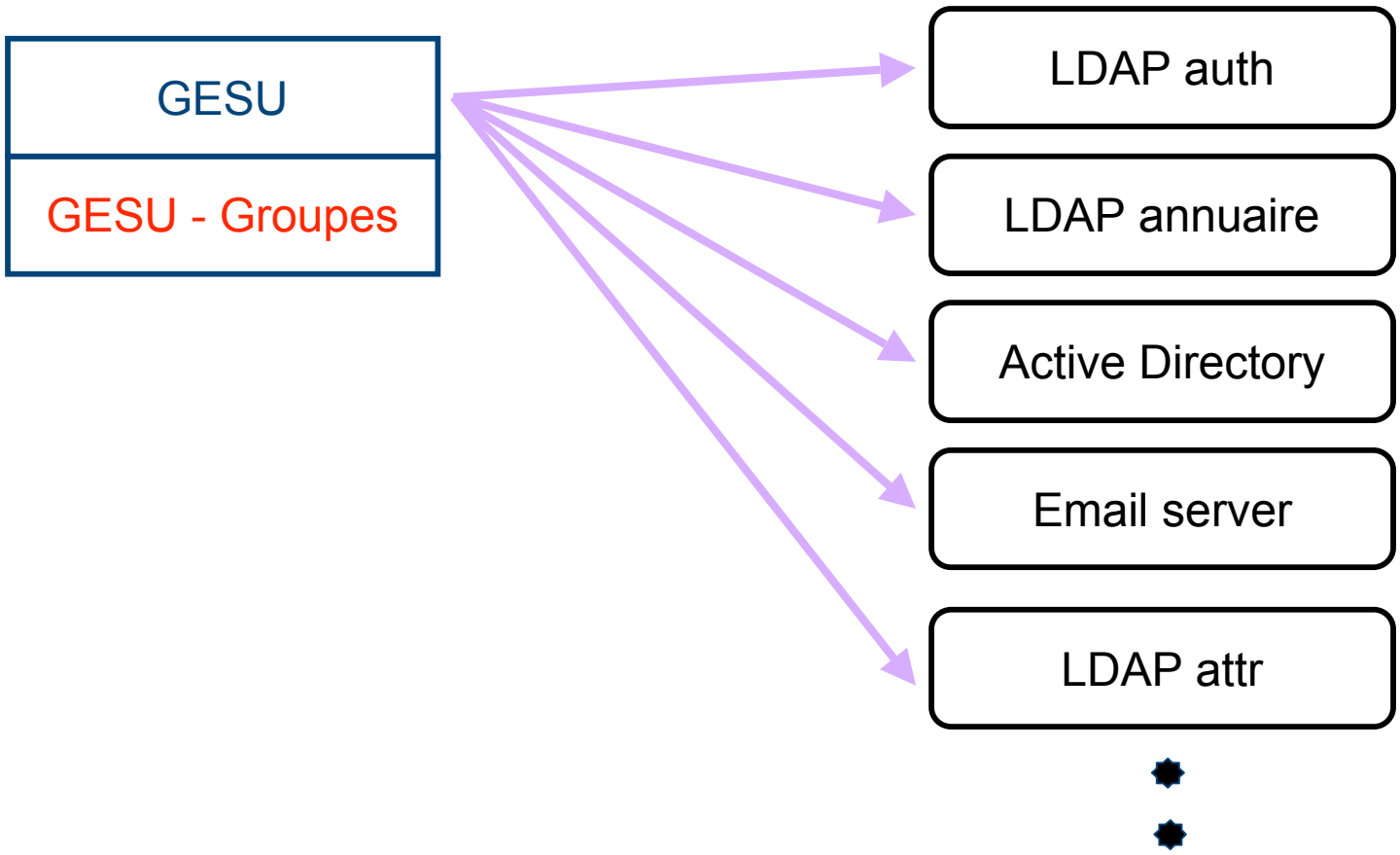
LDAP Group

```
cn=ci-g, ou=unil-groups,ou=gesu,dc=unil,dc=ch
objectClass=top
objectClass=groupOfUniqueNames
objectClass=posixGroup
cn=ci-g
description=ci-g
gidNumber=20001
uniqueMember=uid=uone,ou=unil-users,ou=gesu,dc=unil,dc=ch
uniqueMember=uid=utwo,ou=unil-users,ou=gesu,dc=unil,dc=ch
uniqueMember=uid=uthree,ou=unil-users,ou=gesu,dc=unil,dc=ch
memberUid=uone
memberUid=utwo
memberUid=uthree
```

Resource «Emploi et Logement» (before AAI)



AAI : Home Organization



LDAP attr

- All students and staff: ~15000 entries
- Implements the following attributes

```
eduPersonPrincipalName
  (not in the AAI Specification, userName)
swissEduPersonUniqueID
surName
givenName
swissEduPersonDateOfBirth
swissEduPersonGender
mail
swissEduPersonHomeOrganization
swissEduPersonHomeOrganizationType
eduPersonAffiliation
swissEduPersonStudyBranch3
swissEduPersonStudyLevel
swissEduPersonStaffCategory
eduPersonEntitlement
```

UNIVERSITE DE LAUSANNE

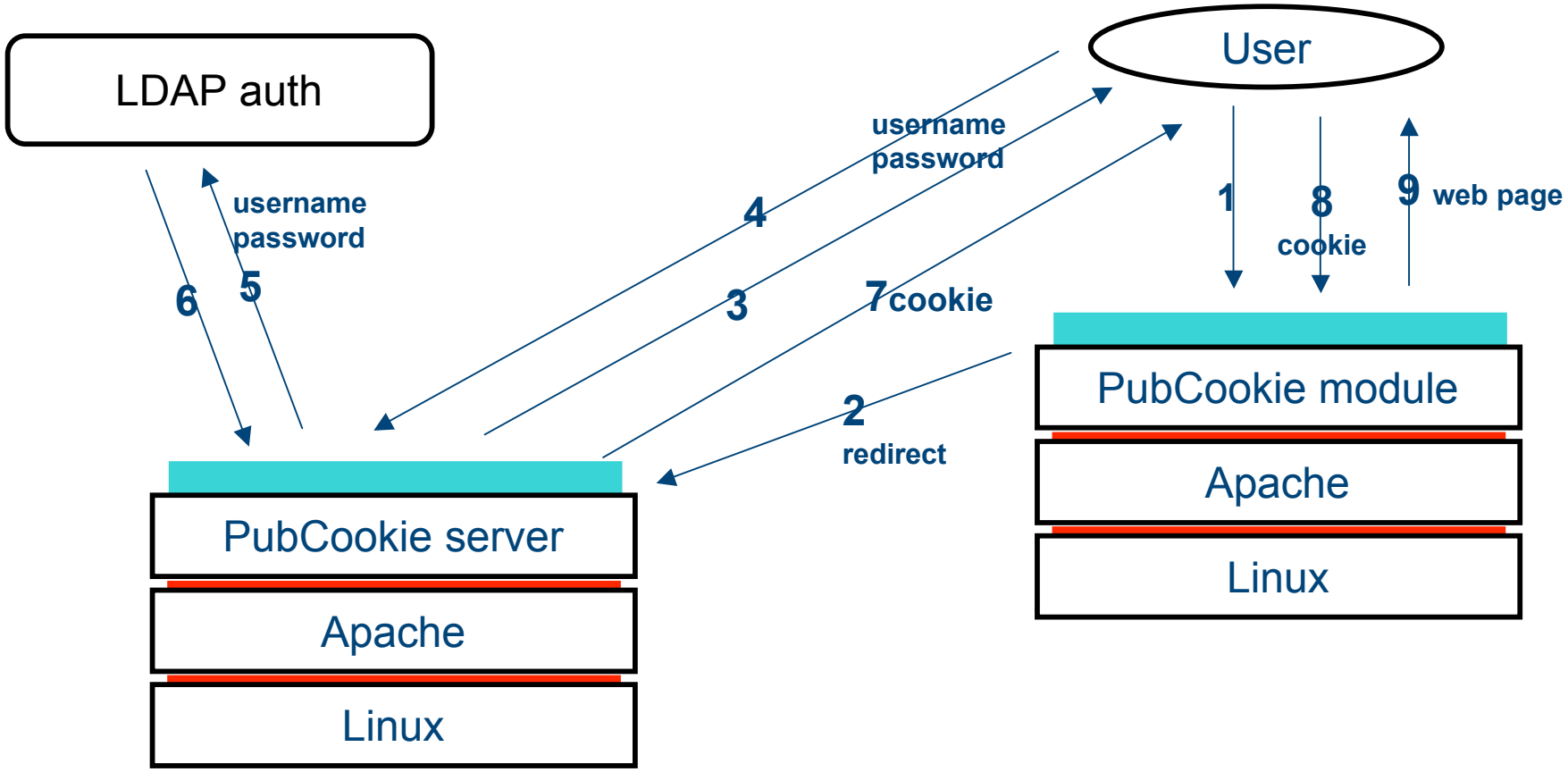
LDAP attr : a user entry (staff)

```
dn: uid=uone,ou=unil-users,ou=gesu,dc=unil,dc=ch
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: swissEduPerson
cn: User One
eduPersonPrincipalName: uone
swissEduPersonHomeOrganizationType: university
swissEduPersonGender: 1
uid: uone
swissEduPersonHomeOrganization: unil.ch
swissEduPersonDateOfBirth: 19640821
swissEduPersonUniqueID: 578067
swissEduPersonStaffCategory: 300
eduPersonAffiliation: staff
sn: One
eduPersonEntitlement: Pat-unil@unil.ch
eduPersonEntitlement: Gesu@unil.ch
eduPersonEntitlement: Ci@unil.ch
eduPersonEntitlement: Argos-users@unil.ch
eduPersonEntitlement: Acces-soft@unil.ch
eduPersonEntitlement: Rect-da-services@unil.ch
eduPersonEntitlement: Switch-oper@unil.ch
mail: User.One@ci.unil.ch
givenName: User
```

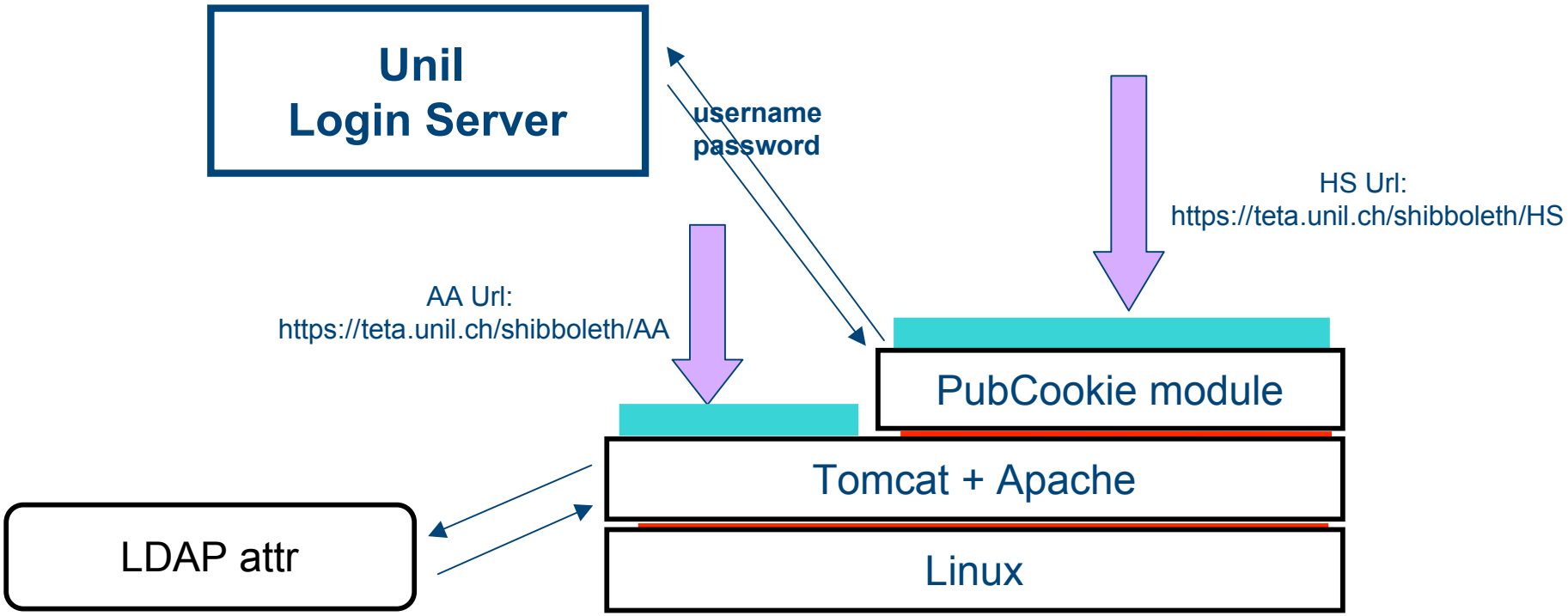
LDAP attr : a user entry (student)

```
dn: uid=sone,ou=unil-users,ou=gesu,dc=unil,dc=ch
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: swissEduPerson
cn: Student One
eduPersonPrincipalName: sone
swissEduPersonHomeOrganizationType: university
swissEduPersonGender: 1
uid: sone
swissEduPersonHomeOrganization: unil.ch
swissEduPersonDateOfBirth: 19831224
swissEduPersonUniqueID: 589456
eduPersonAffiliation: student
sn: one
eduPersonEntitlement: All-etu@unil.ch
eduPersonEntitlement: Etu-lett-hist@unil.ch
eduPersonEntitlement: Etu-lett@unil.ch
eduPersonEntitlement: All-users@unil.ch
eduPersonEntitlement: Etu-lett-geographie@unil.ch
swissEduPersonStudyLevel: 1600-10
swissEduPersonStudyLevel: 4905-10
swissEduPersonStudyLevel: 1415-10
mail: Student.One@etu.unil.ch
swissEduPersonStudyBranch3: 1600
swissEduPersonStudyBranch3: 1415
swissEduPersonStudyBranch3: 4905
givenName: Student
```

Unil Login server : pubcookie

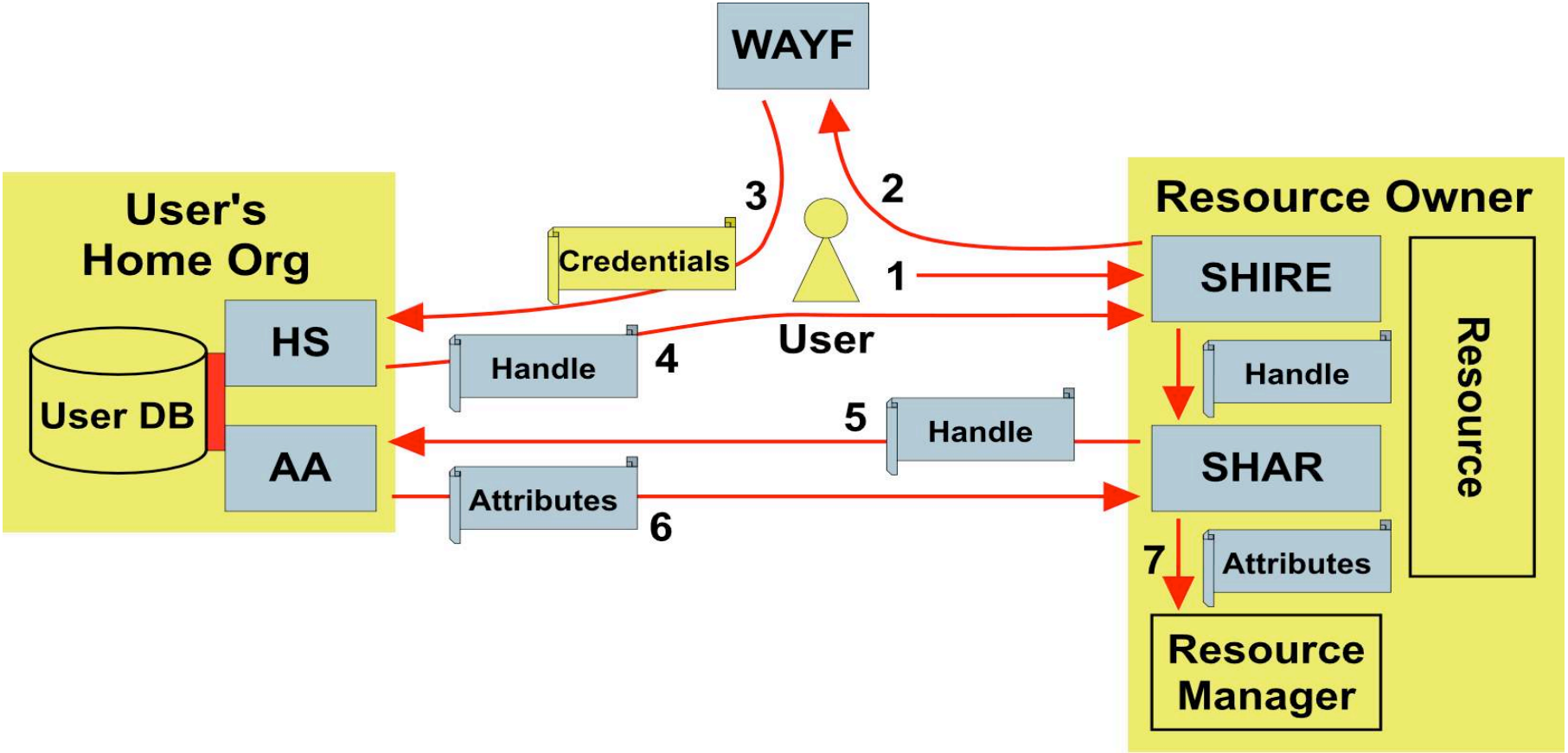


Shibboleth : Origin site



UNIVERSITE DE LAUSANNE

Shibboleth

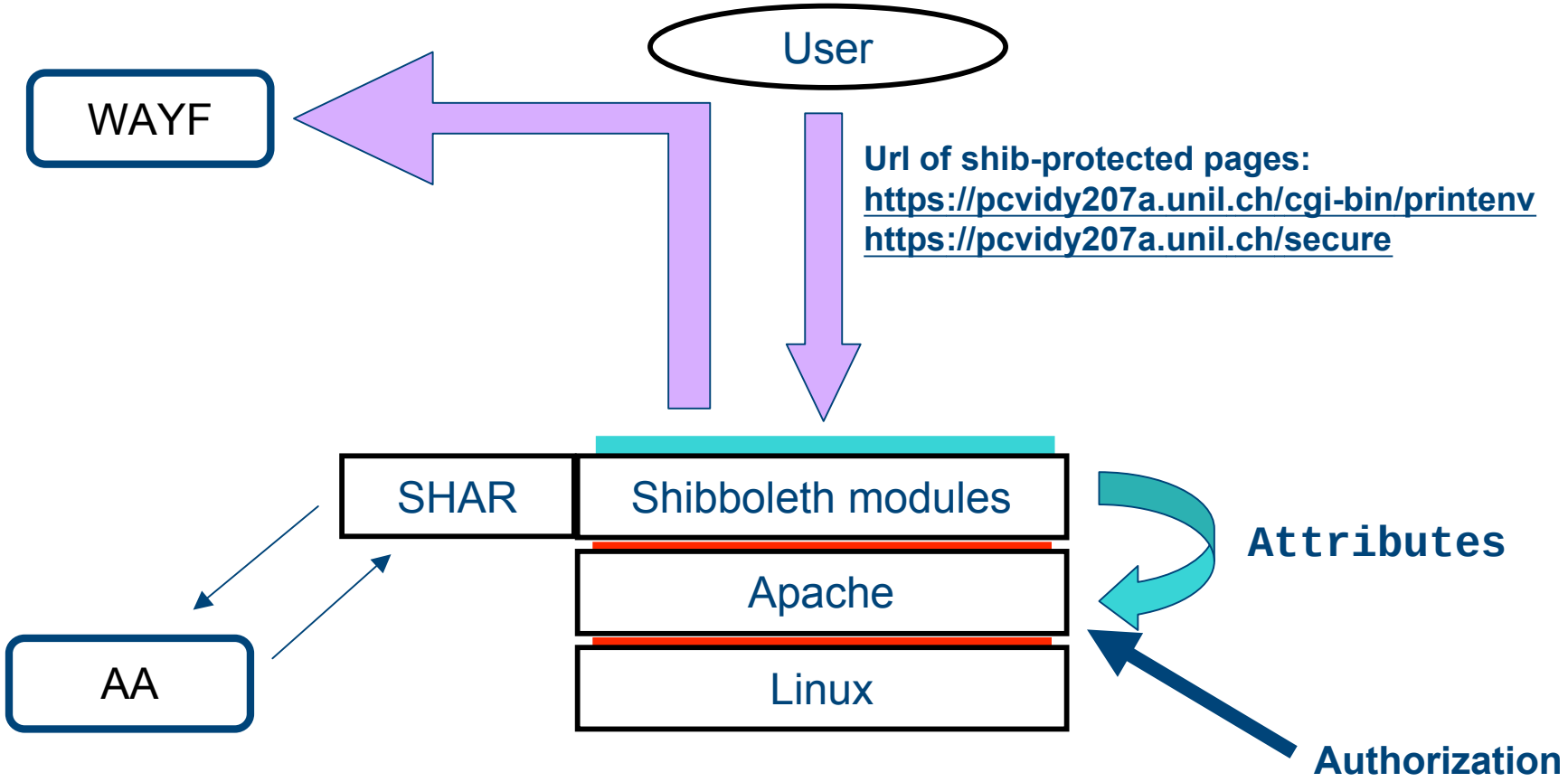


UNIVERSITE DE LAUSANNE

Origin site: httpd.conf

```
<IfModule mod_jk.c>
Include /usr/local/apache/conf/mod_jk.conf
</IfModule>

# Pubcookie Configuration
PubcookieAuthTypeNames EGNetID
PubcookieInactiveExpire -1
PubcookieLogin https://teta.unil.ch/

<Location /shibboleth/HS>
AuthType EGNetID
AuthName "shibboleth/HS"
require valid-user
</Location>
```

Target side: first try



Target side: httpd.conf

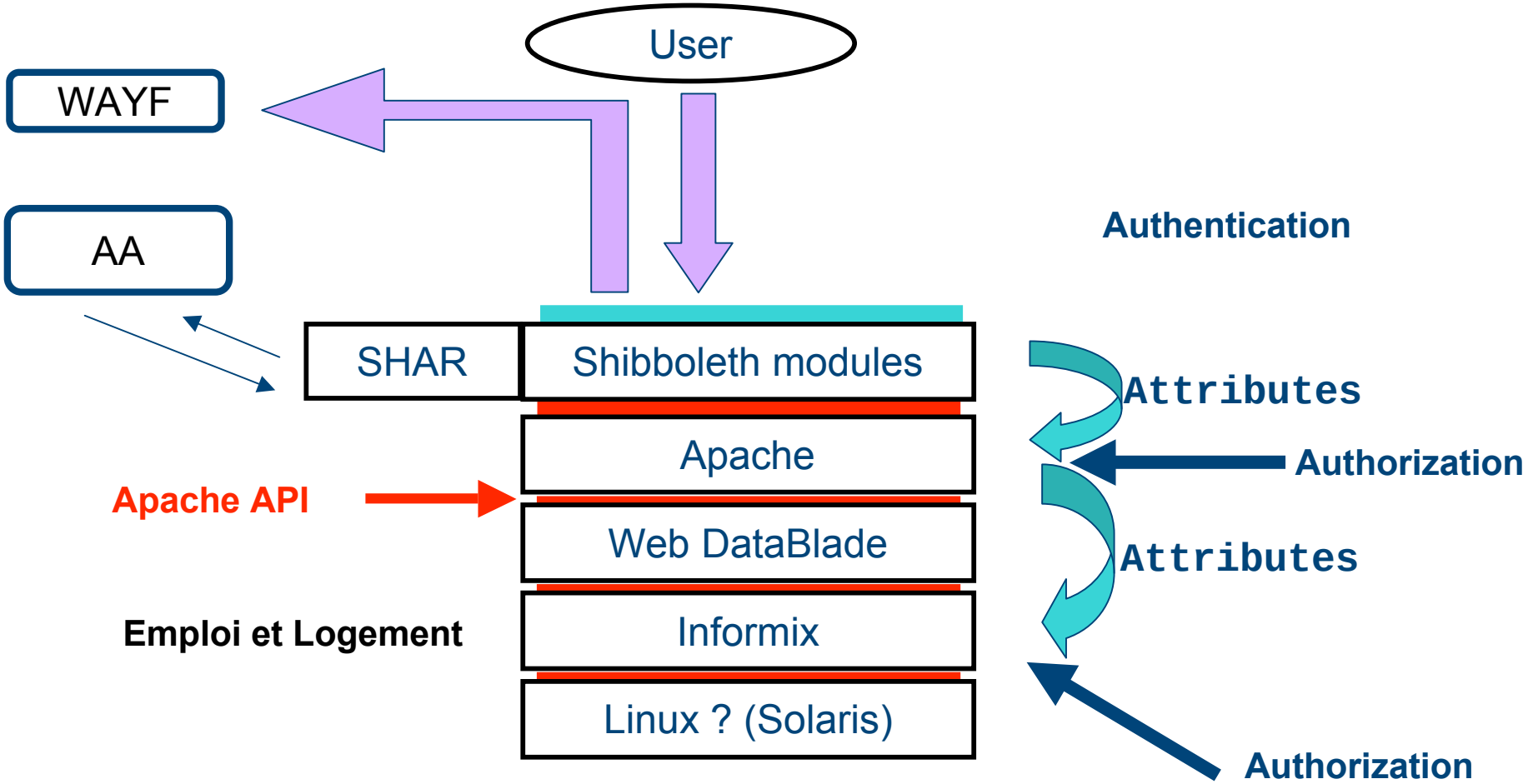
```
SHIREConfig  /opt/shibboleth/etc/shibboleth/shibboleth.ini
SHIREURL /shibboleth/SHIRE
<Location /shibboleth/SHIRE>
SetHandler shib-shire-post </Location>

ShibMapAttribute urn:mace:eduPerson:1.0:eduPersonPrincipalName REMOTE_USER
ShibMapAttribute urn:mace:eduPerson:1.0:eduPersonAffiliation Shib-EP-
   Affiliation affiliation
ShibMapAttribute urn:mace:eduPerson:1.0:eduPersonEntitlement Shib-EP-
   Entitlement entitlement

<Directory "/usr/local/apache/htdocs/secure">
  AuthType shibboleth
  require affiliation staff@unil.ch
</Directory>

<Directory "/usr/local/apache/cgi-bin">
  AuthType shibboleth
  require valid-user
  ShibExportAssertion On
</Directory>
```

UNIVERSITE DE LAUSANNE

DEMO

- User with affiliation = staff
  - https://pcvidy207a.unil.ch/cgi-bin/printenv
  - https://pcvidy207a.unil.ch/secure
- User with affiliation = member
  - https://pcvidy207a.unil.ch/cgi-bin/printenv
  - https://pcvidy207a.unil.ch/secure

Resource «Emploi et Logement» (with AAI)



UNIVERSITE DE LAUSANNE

First conclusion

- No problems at installation
- Resource integration is not a big deal
- Home organization needs more work (not due to Shibboleth)
- Shibboleth is a great and promising product
  - Stable
  - Fast
  - Flexible
  - Works on Solaris and Linux
- Good integration of PubCookie and Shibboleth
- TLS : everything is OK
- The choice of the attributes is good: easy to extract from DB

UNIVERSITE DE LAUSANNE

Open issues

- Attributes
  - givenName mandatory
  - attributes are associated with an account; accounts are associated only to a real person?
  - eduPersonAffiliation : choices of the home organization ….
  - eduPersonAffiliation needs a more detailed specification
  - eduPersonPrincipalName : REMOTE_USER
  - swissEduPersonUniqueId

UNIVERSITE DE LAUSANNE

Open issues

- Ressource side
  - problem: Linux – Apache – Web DataBlade – Informix
  - try with Solaris instead of Linux -> not yet finished

UNIVERSITE DE LAUSANNE

Open issues

- Shibboleth
  - only 3 attributes are implemented (eduPersonPrincipalName, eduPersonAffiliation, eduPersonEntitlement)
  - write a Java class (origin side) for each attribute -> easy
  - write a C++ class (target side) for each attribute -> easy
  - Shib add @unil.ch to some attributes
  - target implementation not yet available for IIS
  - release of attributes not yet controlled by the user
  - Attribute Release Policy is rudimentary
  - Resource Manager (Apache « require ») is rudimentary
  - How to bypass the WAYF

UNIVERSITE DE LAUSANNE

Open issues

- Tequila
  - Not yet the time to try it: but now all the pieces are ready -> easy
  - Shibboleth-origin at EPFL for the pilot ?

UNIVERSITE DE LAUSANNE

Next steps

- Use Shibboleth with « Emploi et logement » inside Unil
- Implements the AAI attributes in Shibboleth
- Wait for the next version of Shibboleth for a better ARP
- Try Tequila with EPFL
- Use Tequila and (or ?) Shibboleth to access « Emploi et logement » from EPFL
- Open the Shibbolized and (or ?) Tequilized application to the students of Unil and EPFL
- Wait the Shibboleth target implementation @ HUG (2nd pilots)