centre informatique

AAI at Unil

Home Organization Integration

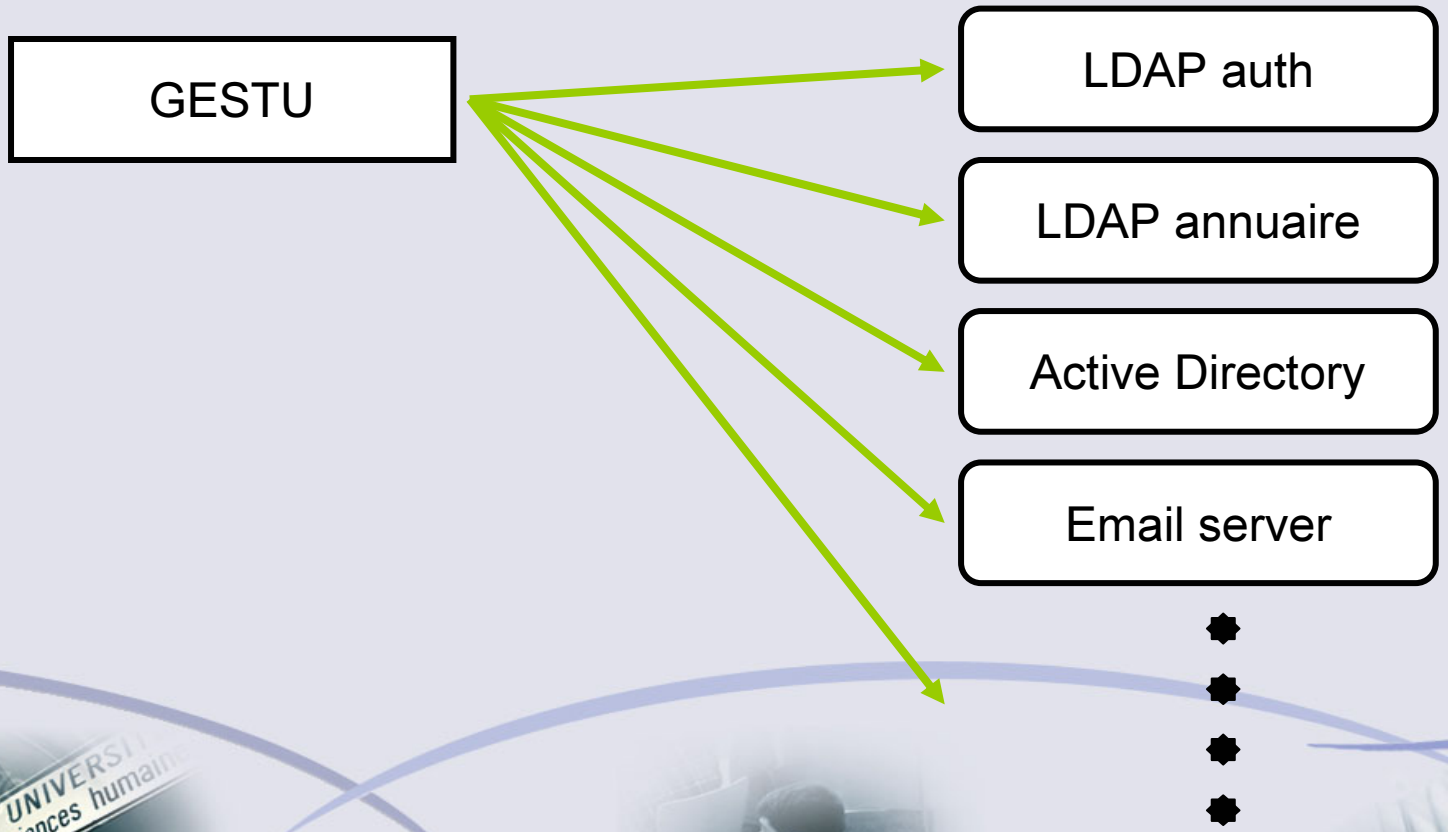
centre informatique

GESTU

- Gestion des utilisateurs
  - Accès informatique (username/password)
  - Mailbox and email address
  - Security groups
- Students: automatic
- Employees: web interface or paper formular
- Gestu is integrated in RH and students database


centre informatique

GESTU



A LDAP auth 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:****************
```

A LDAP auth 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
```

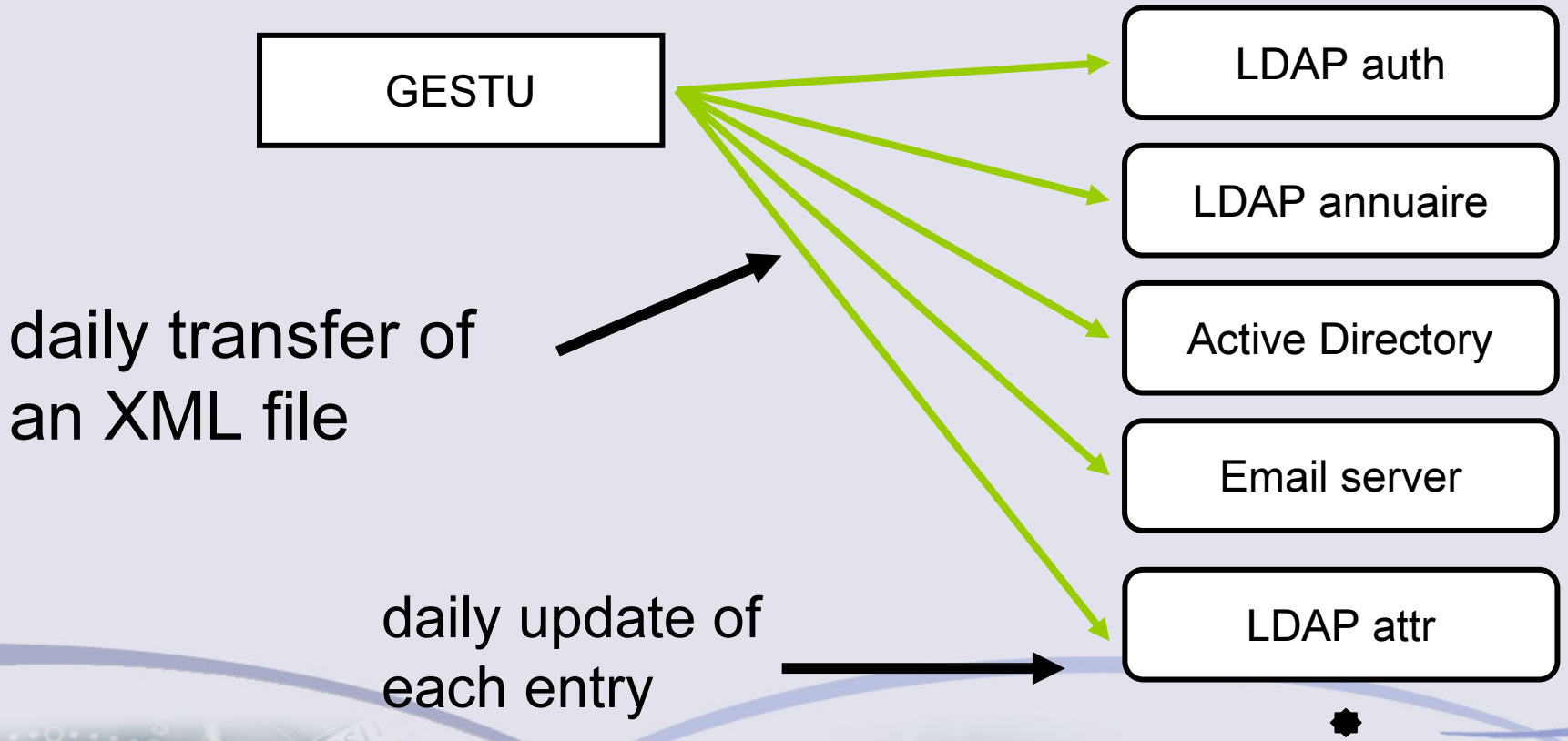
An other LDAP attr

- A LDAP that contains AAI attributres: LDAP attr
  - adapt the LDAP schema
- All students and staff: ~15000 entries
- Same dn as LDAP auth
- Implements the following attributes

eduPersonPrincipalName
swissEduPersonUniqueID
surName
givenName
preferredLanguage
swissEduPersonDateOfBirth
swissEduPersonGender
mail
swissEduPersonHomeOrganization
swissEduPersonHomeOrganizationType
eduPersonAffiliation
swissEduPersonStudyBranch3
swissEduPersonStudyLevel
swissEduPersonStaffCategory
eduPersonEntitlement

centre informatique

AAI: Home integration



XML entry (staff)

<swissEduPerson>
<uid>arootti</uid>
<unilPerNum>485</unilPerNum>
<swissEduPersonUniqueID></swissEduPersonUniqueID>
<surName>Rootti</surName>
<givenName>Aregg</givenName>
<swissEduPersonDateOfBirth>19640927</swissEduPersonDateOfBirth>
<swissEduPersonGender>1</swissEduPersonGender>
<mail>Aregg.Rootti@ci.unil.ch</mail>
<swissEduPersonHomeOrganization>unil.ch</swissEduPersonHomeOrganization>
<swissEduPersonHomeOrganizationType>university</swissEduPersonHomeOrganizationTy
pe>
<swissEduPersonHomeOrganization>unil.ch</swissEduPersonHomeOrganization>
<swissEduPersonHomeOrganizationType>university</swissEduPersonHomeOrganizationTy
pe>
<eduPersonAffiliation>staff</eduPersonAffiliation>
<swissEduPersonStaffCategory>300</swissEduPersonStaffCategory>
<eduPersonEntitlement>Acces-soft@unil.ch</eduPersonEntitlement>
<eduPersonEntitlement>All-users-portail@unil.ch</eduPersonEntitlement>
</swissEduPerson>

XML entry (student)

<swissEduPerson>
<uid>ostudent</uid>
<unilPerNum>58573</unilPerNum>
<swissEduPersonUniqueID></swissEduPersonUniqueID>
<surName>Student</surName>
<givenName>One</givenName>
<swissEduPersonDateOfBirth>19831228</swissEduPersonDateOfBirth>
<swissEduPersonGender>2</swissEduPersonGender>
<mail>One. Student@etu.unil.ch</mail>
<swissEduPersonHomeOrganization>unil.ch</swissEduPersonHomeOrganization>
<swissEduPersonHomeOrganizationType>university</swissEduPersonHomeOrganizationType>
<eduPersonAffiliation>student</eduPersonAffiliation>
<swissEduPersonStudyBranch3>1415</swissEduPersonStudyBranch3>
<swissEduPersonStudyBranch3>1600</swissEduPersonStudyBranch3>
<swissEduPersonStudyBranch3>1700</swissEduPersonStudyBranch3>
<swissEduPersonStudyLevel>1415-10</swissEduPersonStudyLevel>
<swissEduPersonStudyLevel>1600-10</swissEduPersonStudyLevel>
<swissEduPersonStudyLevel>1700-10</swissEduPersonStudyLevel>
<eduPersonEntitlement>All-etu@unil.ch</eduPersonEntitlement>
</swissEduPerson>

LDAP attr : a user (staff)

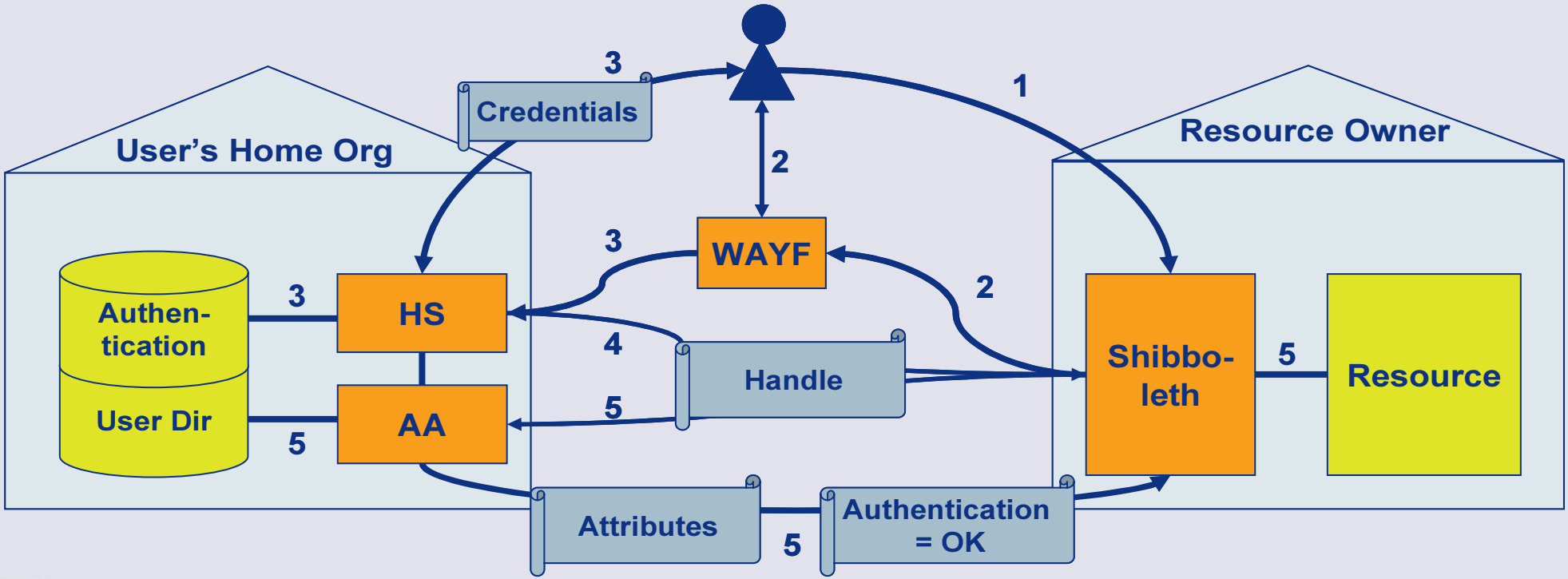
```
> dn: uid=uone,ou=unil-users,ou=gesu,dc=unil,dc=ch
> objectClass: swissEduPerson
> cn: User One
> eduPersonPrincipalName: uone
> swissEduPersonHomeOrganizationType: university
> swissEduPersonGender: 1
> uid: uone
> swissEduPersonHomeOrganization: unil.ch
> swissEduPersonDateOfBirth: 19640821
> swissEduPersonUniqueID: 578067@unil.ch
> 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 (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@unil.ch
> eduPersonAffiliation: student
> sn: one
> eduPersonEntitlement: All-etu@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
```

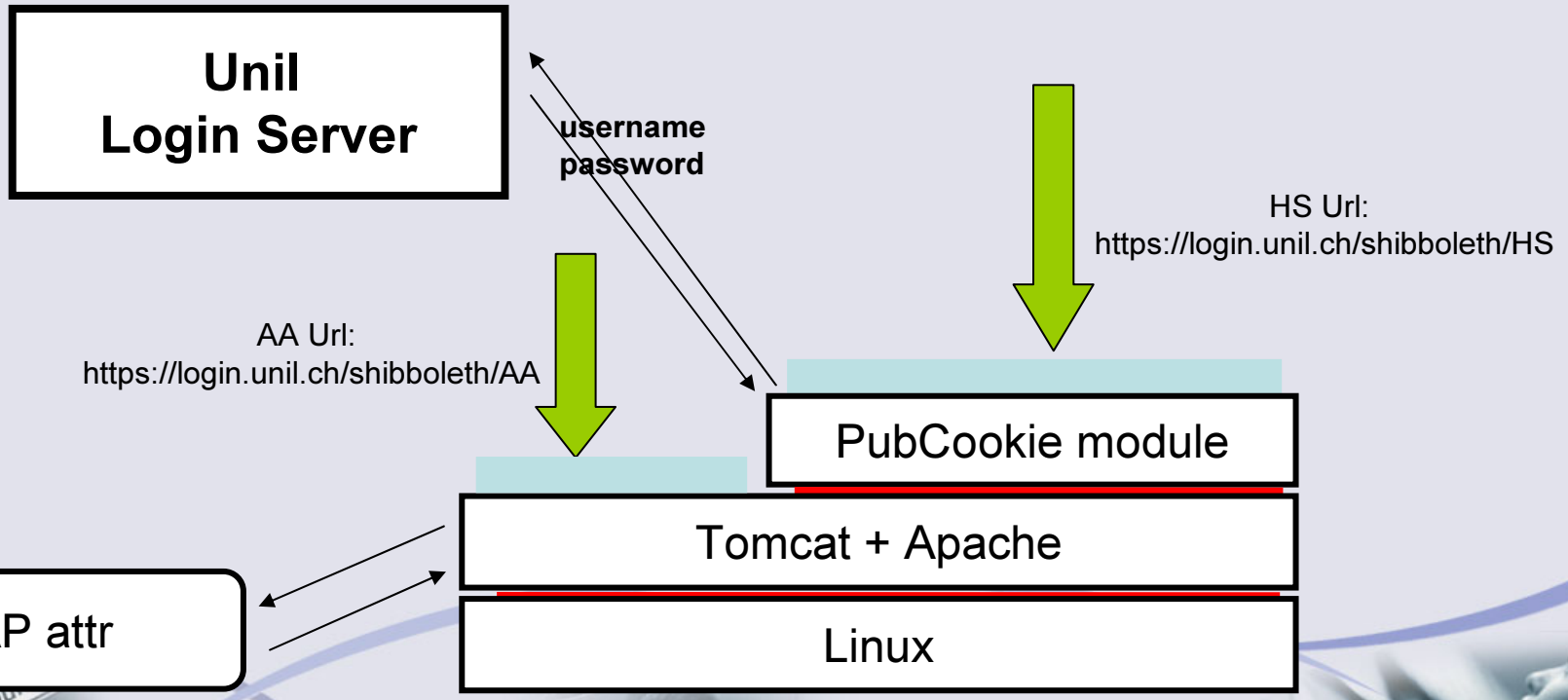
centre informatique

Shibboleth



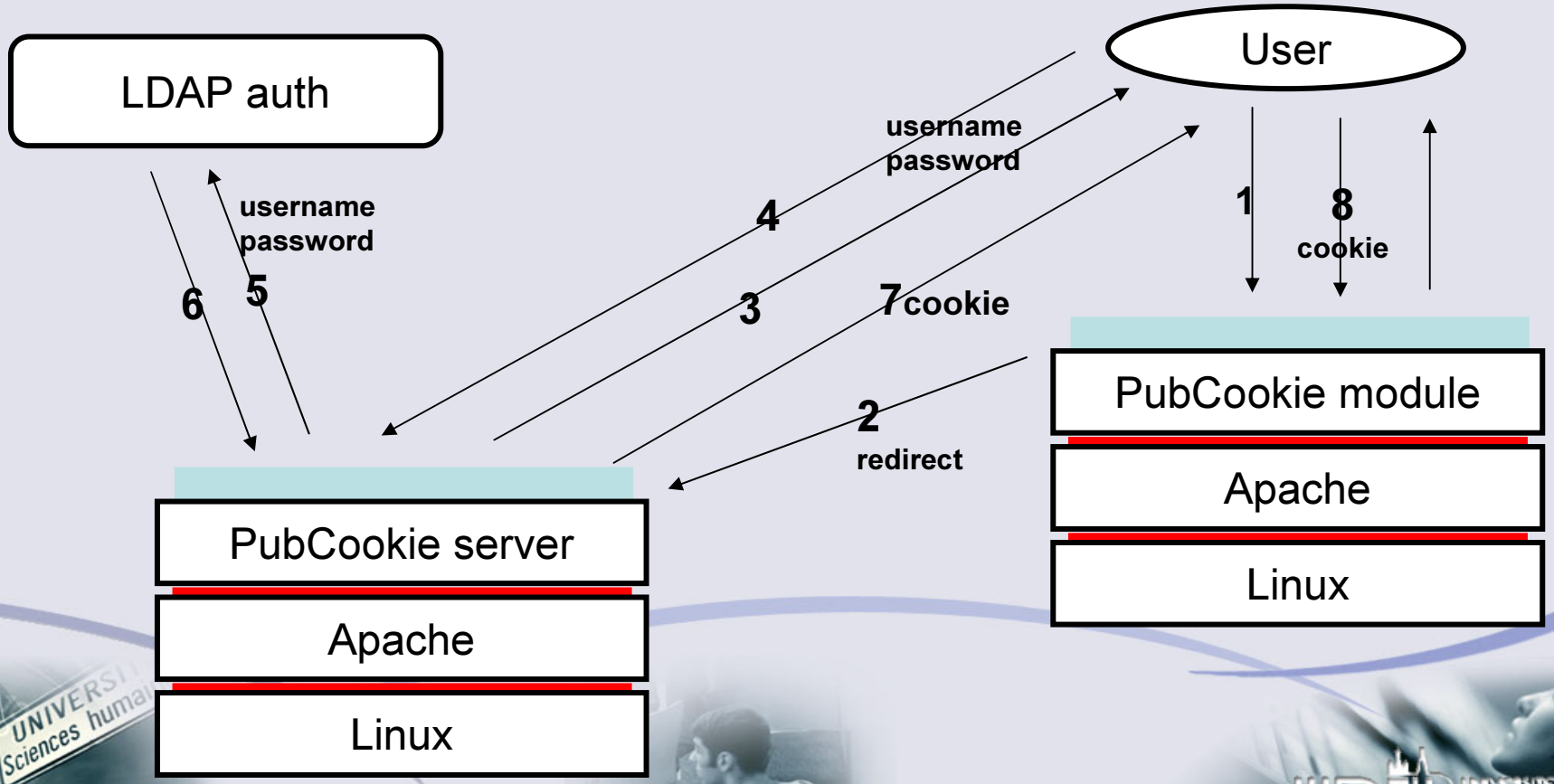
centre informatique

Shibboleth: origin site



centre informatique

Pubcookie login server



Origin site: httpd.conf Authentication

```
> <IfModule mod_jk.c>
> Include /etc/httpd/conf/mod_jk.conf
> </IfModule>

> # Pubcookie Configuration
> PubcookieAuthTypeNames EGNetID
> PubcookieInactiveExpire -1
> PubcookieLogin https://login.unil.ch/
>
> <Location /shibboleth/HS>
> AuthType EGNetID
> AuthName "shibboleth/HS"
> require valid-user
> </Location>
```

Origin site: resolver.xml Attributes

```
> <SimpleAttributeDefinition id="urn:mace:switch.ch:attribute-
  def:swissEduPersonUniqueID" > <DataConnectorDependency requires="directory"/>
     </SimpleAttributeDefinition>
  ….
> <JNDIDirectoryDataConnector id="directory">
  <Search filter="uid=%PRINCIPAL%">
  <Controls searchScope="SUBTREE_SCOPE" returningObjects="false" /></Search>
  <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory"
  />
  <Property name="java.naming.provider.url" value="ldap://cati.unil.ch:390/ou=unil-
  users,ou=gesu,dc=unil,dc=ch" />
  <Property name="java.naming.security.principal" value="uid=xxxxxx,dc=unil,dc=ch" />
  <Property name="java.naming.security.credentials" value="xxxxx"  />
> </JNDIDirectoryDataConnector>
```

centre informatique

Demo

> Shib Secure page on lita (valid user)

> Shib Secure page on lita (staff)

> Shib Secure page on lita (student)

> Secure page on exptest (staff only)

Fichier Edition Affichage Favoris Outils ?

Précédente Rechercher Favoris Média

Adresse C:\temp\aai\aai\index.html OK Liens

Université de Lausanne
Centre informatique

Serveur d'authentification

nom d'utilisateur

mot de passe

Envoyer

The resource you requested requires you to authenticate.

- Cette connexion vous donne accès aux applications utilisant ce système d'authentification (AAI) durant une période de 4 heures.
- **ATTENTION**: Pour protéger vos accès et éviter un accès non autorisé, la déconnexion compléte est effectuée en fermant toutes les fenêtres de votre navigateur et en quittant l'application.

unil Université de Lausanne centre informatique SWITCH aai

Collège Propédeutique 2 - CH-1015 Lausanne - Suisse - Tél. +41 21 692 22 00 - Fax +41 21 692 22 05

Poste de travail

centre informatique

Conclusion

- Installation of Shibboleth-Origin
  -> No problem on Linux (RedHat, Debian)
- Two LDAP
  - LDAP for authentication
  - LDAP for attributes
- Extracting data (XML file) -> easy in our case
  - GESTU integrated in RH and Students databases
  - A single IT team at Unil -> cooperation