

# Directories at UNIL

# UNIL Administration

- > Many databases and applications:
  - > ResHus: contracts with Etat de Vaud
  - > SAP: other contracts
  - > Immat: students
- > Physical persons in a single table
- > Moral persons in a single table
- > GESTU application is integrated in this system
  - > management of accesses to services
  - > management of groups



# GESTU

- > Based on the concept of « service » and « access to a service »
- > Master services
  - > eliot -> basic access (entry in the auth directory)
  - > ula -> access to a VMS machine
  - > ...
- > Dependent services: share the data with a master service
  - > mailbox -> mailbox on our mail server
  - > intranet -> access to our admin application
  - > argos -> access to our HPC server
- > Access to a master service
  - > Person
  - > Admin. unit / gidnumber
  - > username/uidnumber/initial-password
  - > state of the access: open, closed, blocked, « echu »
- > Access to a dependent service
  - > state of the access: open, closed, blocked, « echu »



# GESTU

- > Automatic procedures
  - > access creation for students: the day following the end of the immatriculation process (a letter is sent)
  - > closing access: 6 months after exmatriculation
  - > access creation for employees having a valid contract (through a web form)
  - > send notification of access termination by email (1-2 month before)
  - > ...
- > Manual procedure (operator)
  - > create, close, ...
  - > re-initialize password

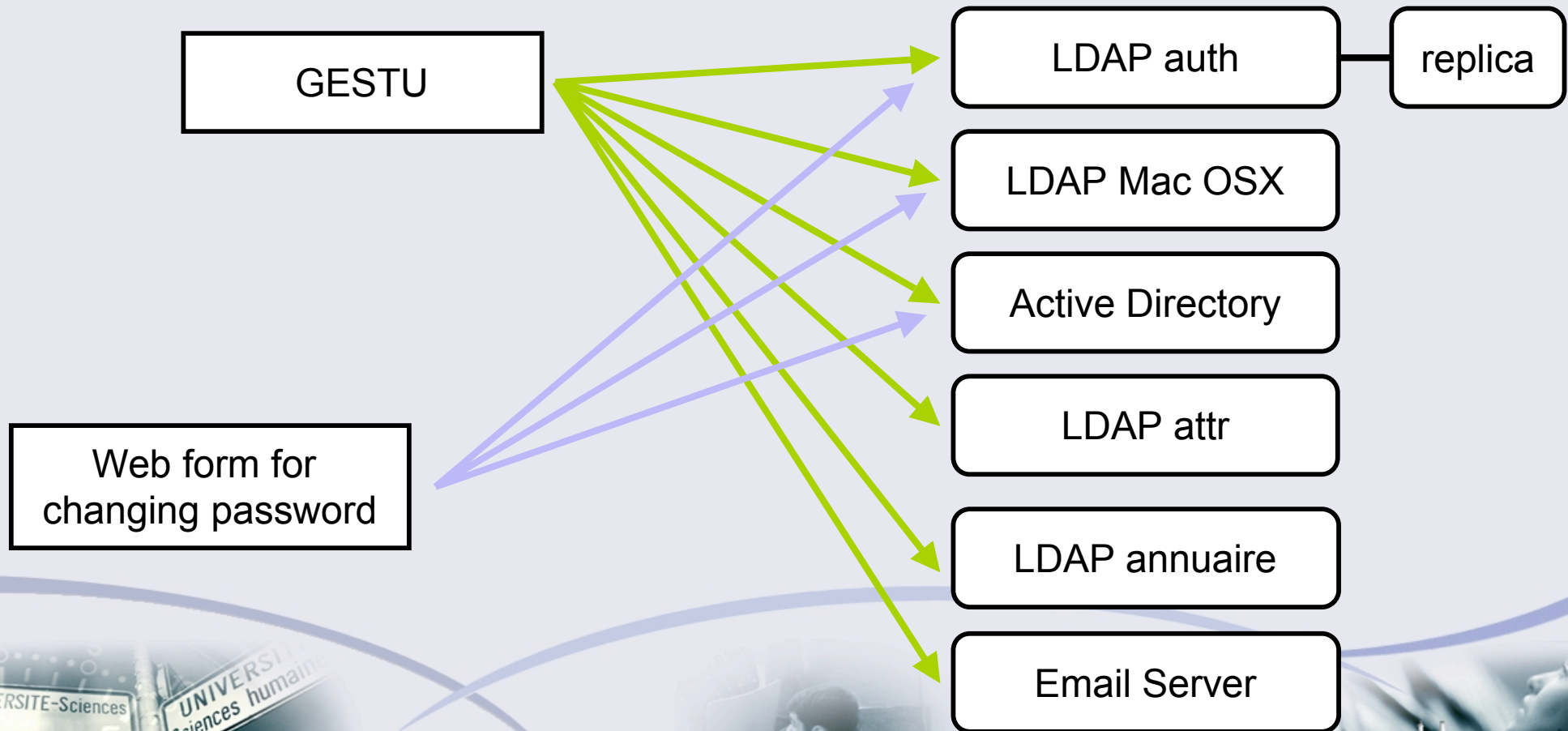


# Groups

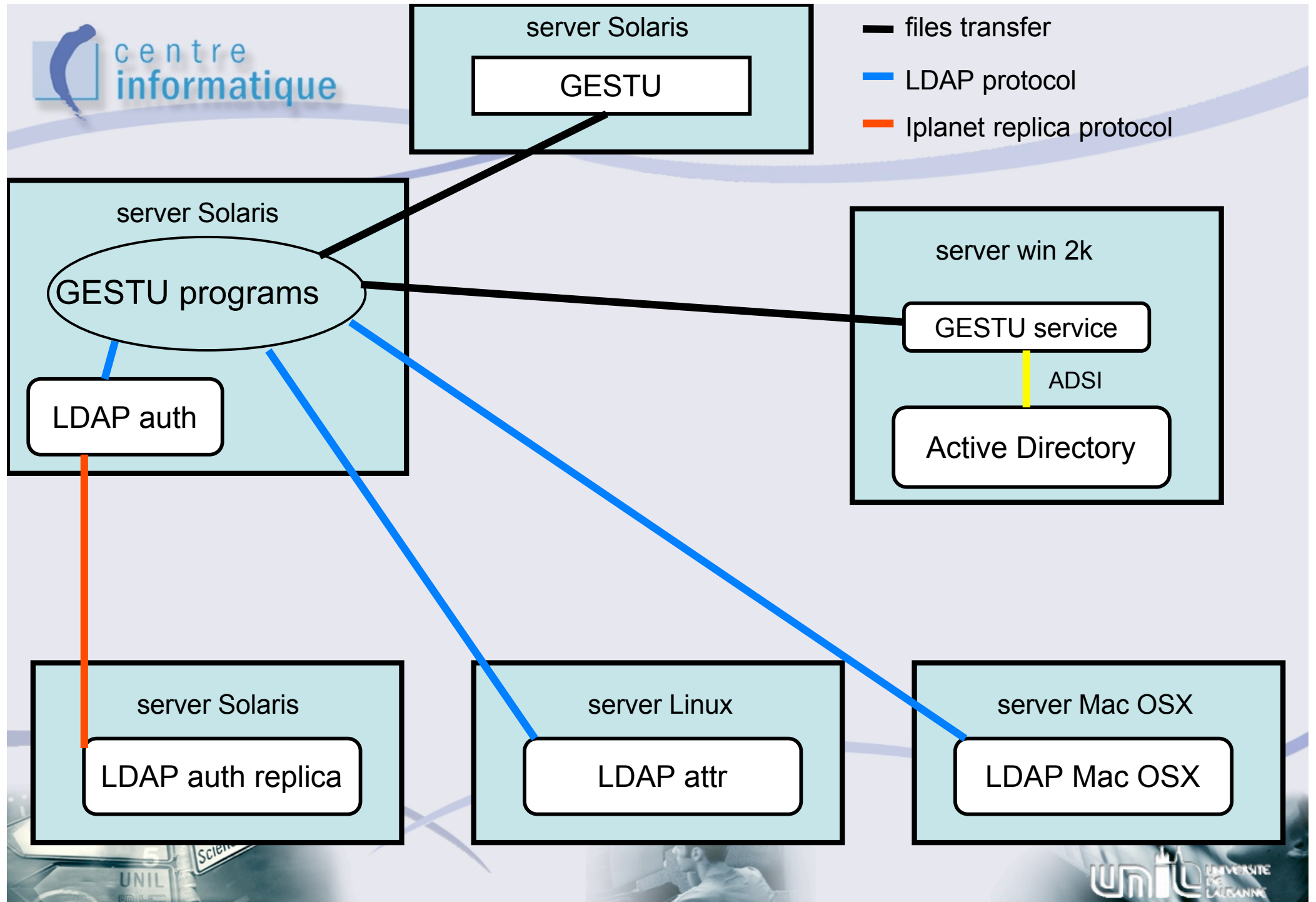
- > An authorized user is able to create a group/email-list
- > Groups
  - > members are computed with criteria (recomputed daily)
  - > members may be added manually



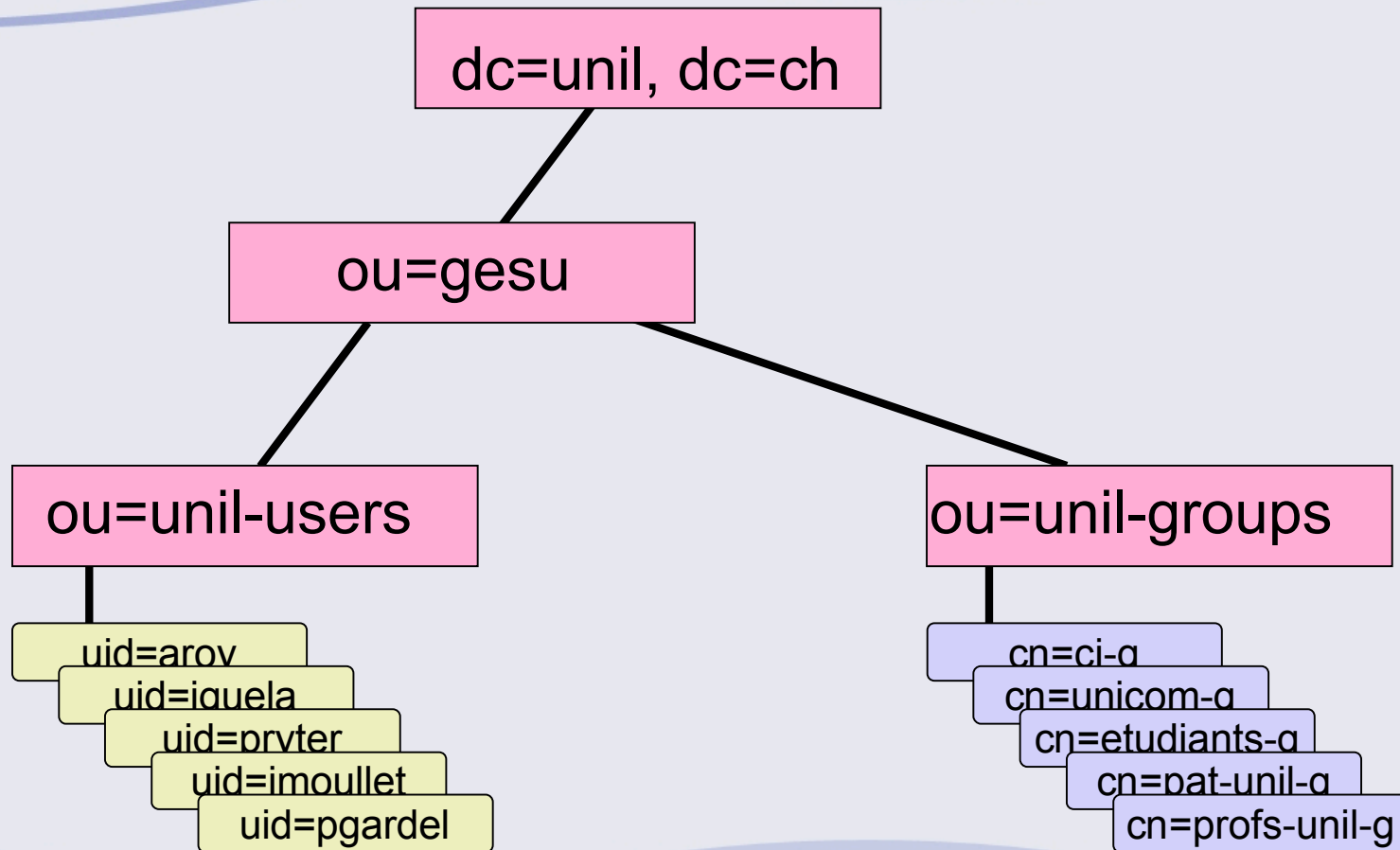
# Directories







# LDAP and AD DIT





# 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:*****
```

# 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
```

# 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`



# UNIL Directories

- > LDAP is Iplanet Directory 5.1
- > operations on accesses:
  - > daily
  - > on demand by operator
- > change password: online
- > LDAP attr: updated daily
- > email and name in LDAP auth: updated daily
- > programs verifying directories
- > ...





# Management of LDAP attr

- > used by Shibboleth AA only
- > updated daily
  - > Gestu produces an xml files containing all the users with their attributes
  - > a program
    - > read the xml file
    - > load the list of the users in the LDAP
    - > one by one delete and recreate users entries with data from the xml file
    - > remove LDAP entries not in the xml file
    - > add new entries
- > ~ 18000 entries
- > updated in 25 minutes
- > function for computing `swissEduPersonUniqueID` from `perNum`





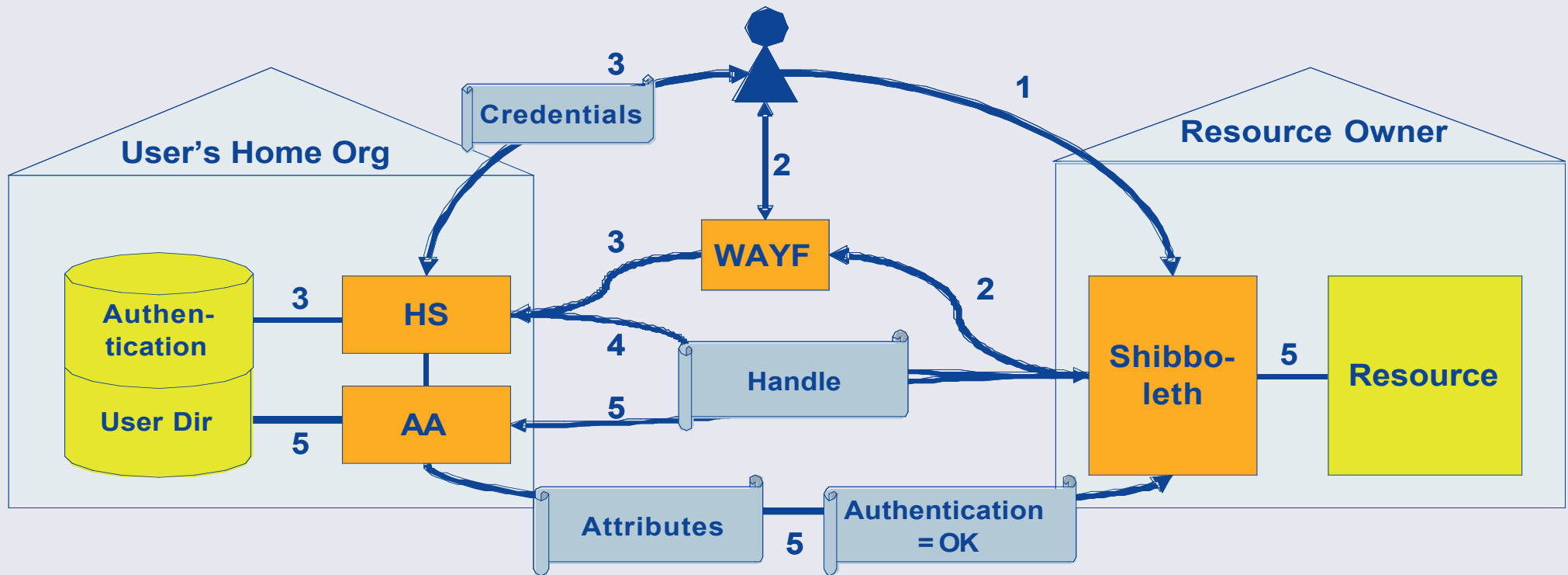
# XML entry (staff)

```
<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</swissEduPersonHomeOrganizationType>
<swissEduPersonHomeOrganization>unil.ch</swissEduPersonHomeOrganization>
<swissEduPersonHomeOrganizationType>university</swissEduPersonHomeOrganizationType>
<eduPersonAffiliation>staff</eduPersonAffiliation>
<swissEduPersonStaffCategory>300</swissEduPersonStaffCategory>
<eduPersonEntitlement>Acces-soft@unil.ch</eduPersonEntitlement>
<eduPersonEntitlement>All-users-portail@unil.ch</eduPersonEntitlement>
</swissEduPerson >
```

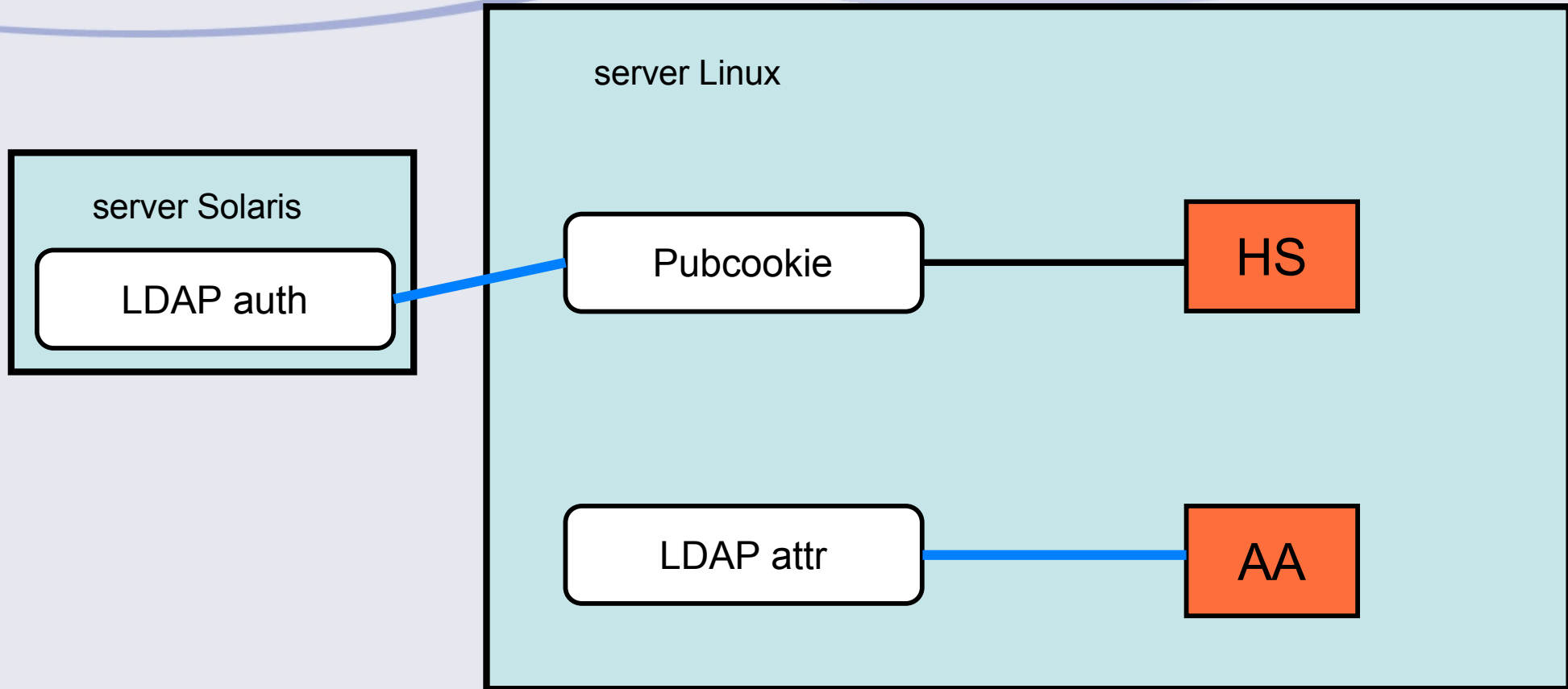
# XML entry (student)

```
<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>
```

# Shibboleth



# Unil Directories and AAI



# Origin site: httpd.conf Authentication

```
<IfModule mod_jk.c>
```

```
Include /etc/httpd/conf/mod_jk.conf
```

```
</IfModule>
```

```
# Pubcookie Configuration
```

```
PubcookieAuthTypeNames EGNID
```

```
PubcookieInactiveExpire -1
```

```
PubcookieLogin https://login.unil.ch/
```

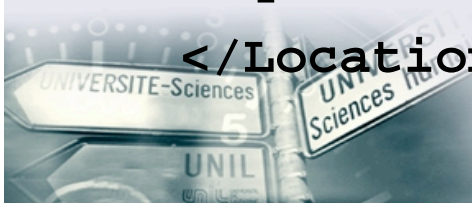
```
<Location /shibboleth/HS>
```

```
AuthType EGNID
```

```
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.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="xxxxxx" />
</JNDIDirectoryDataConnector>
```



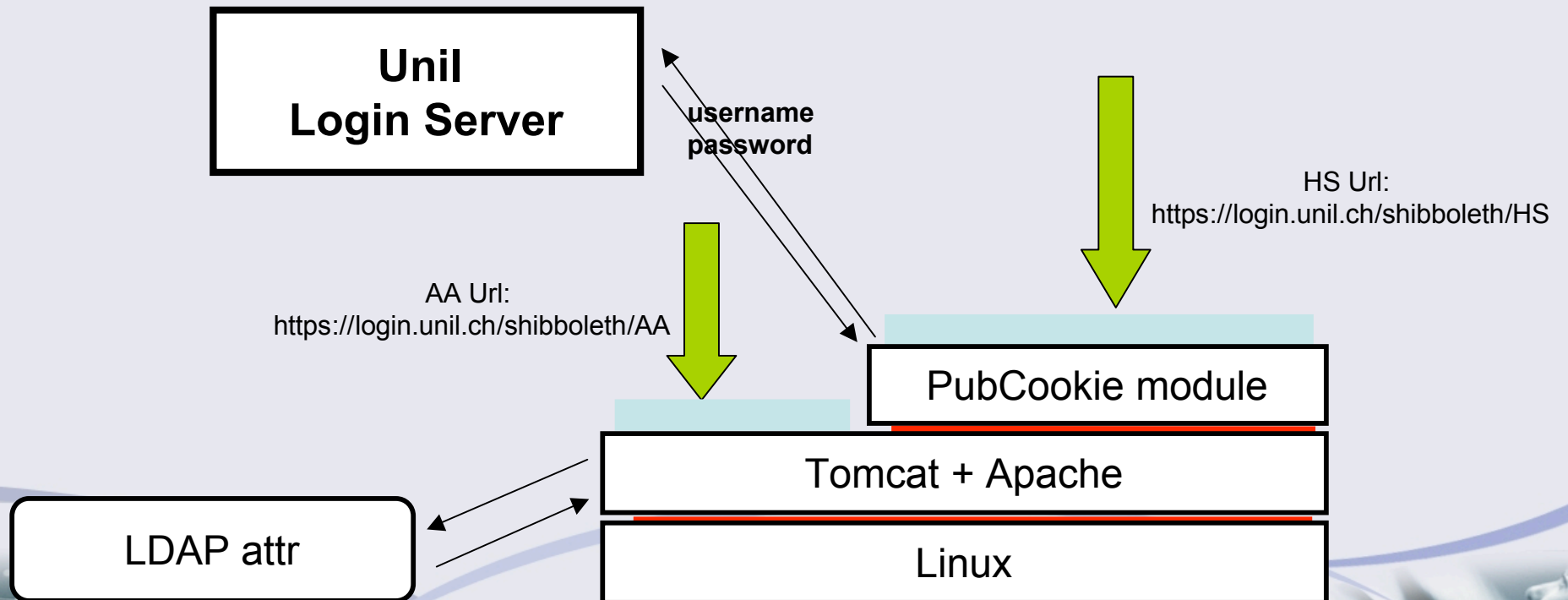


# Conclusion

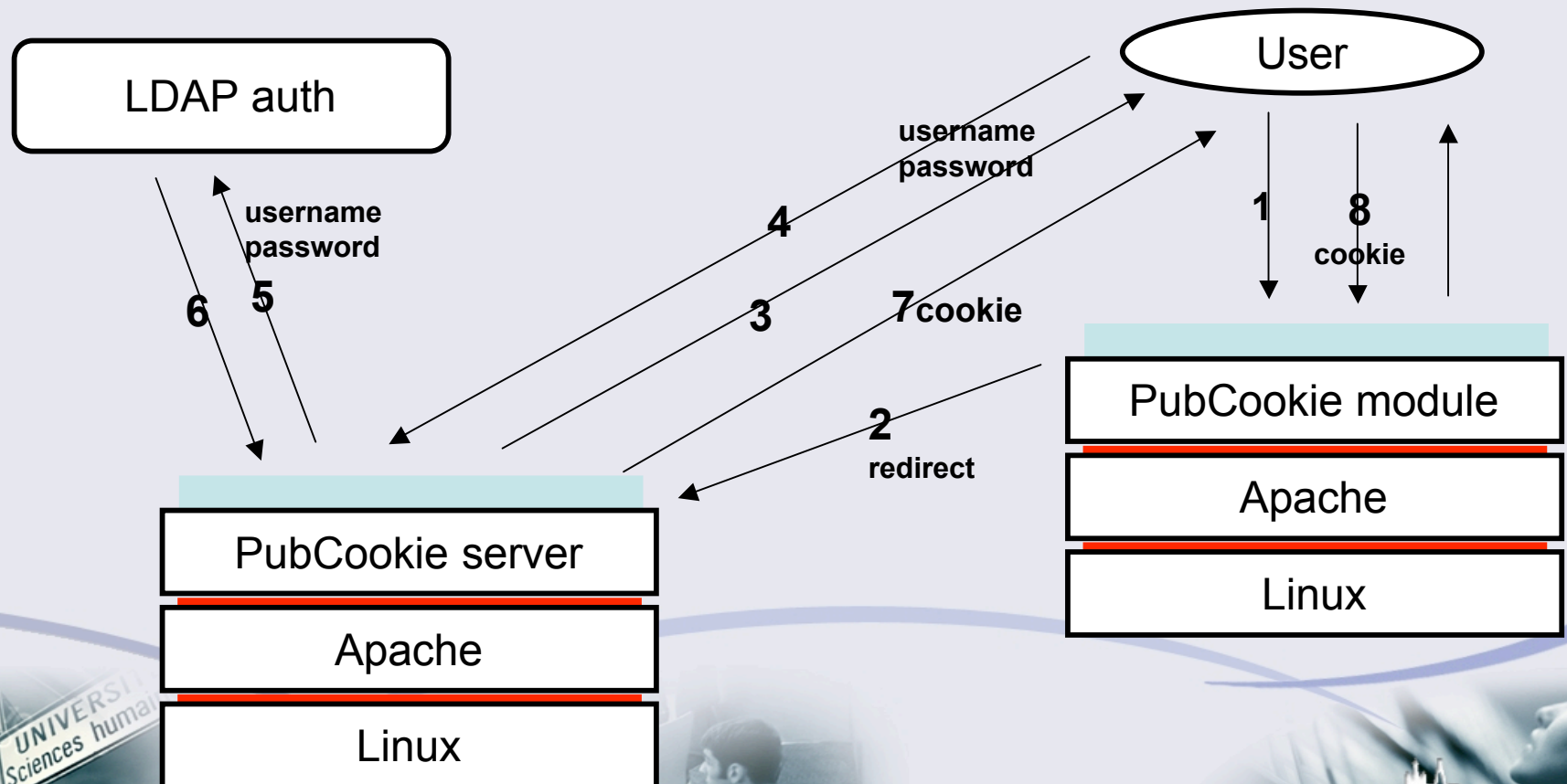
- > GESTU : central management of users
- > Two LDAP
  - > LDAP for authentication
  - > LDAP for attributes
- > Extracting data (XML file) -> easy in our case
  - > xml : future extension
- > GESTU : evolution ...



# Shibboleth: origin site



# Pubcookie login server





## 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 complète est effectuée en fermant toutes les fenêtres de votre navigateur et en quittant l'application.

