

Middleware integration in the Sympa mailing list software

Olivier Salaün - CRU

1. Sympa, its middleware connectors
2. Sympa web authentication
3. CAS authentication
4. Shibboleth authentication
5. Sympa and dokuwiki

CRU

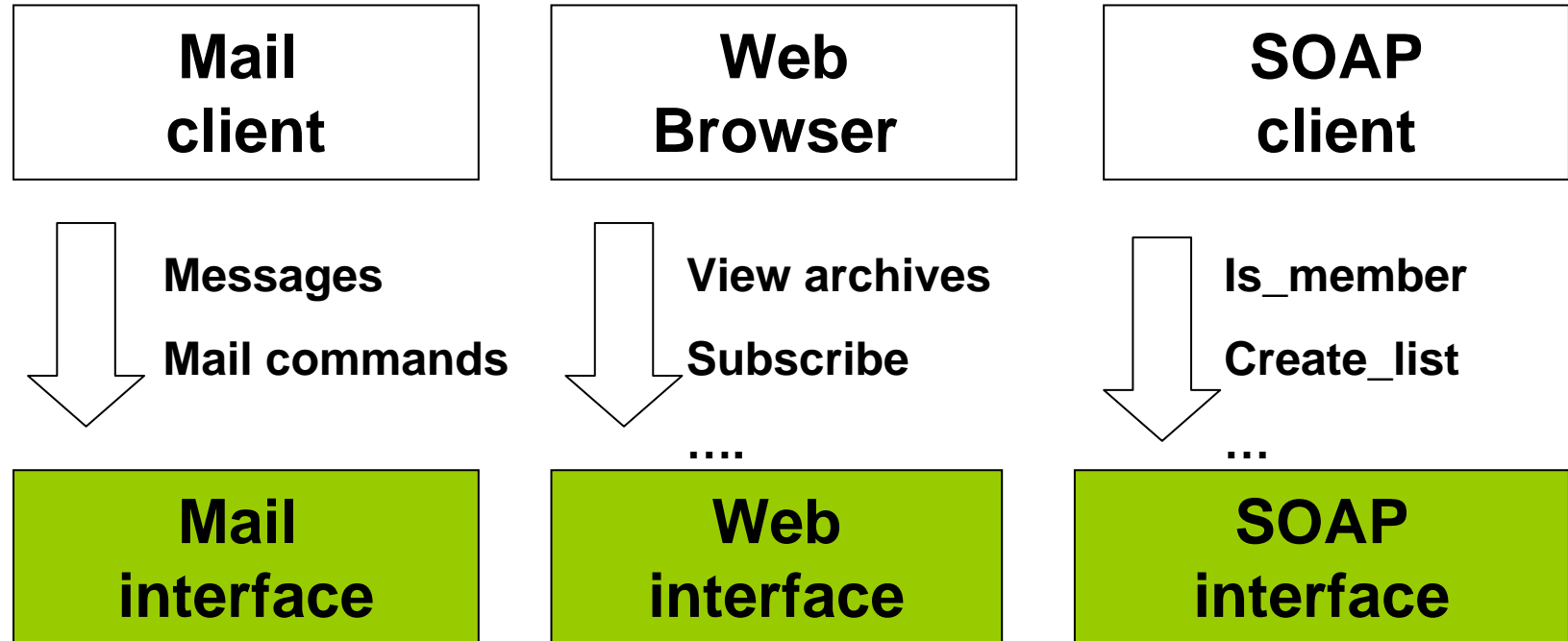
Comité Réseau des Universités

- Promoting internet services for French universities
 - Renater provides the network connectivity + CERT
 - CRU is working on middleware
- Our activities
 - Coordinating working groups
 - Organizing training sessions and conferences
 - Running services (federation, PKI, sourceforge,...)
 - Developing softwares : **Sympa**

Sympa

- An open source mailing list software
 - developed by the CRU
 - developed for French universities
- The user interface is internationalized
 - 12 languages
- Now widely used
 - universities, major companies, governments agencies, ...

Sympa architecture



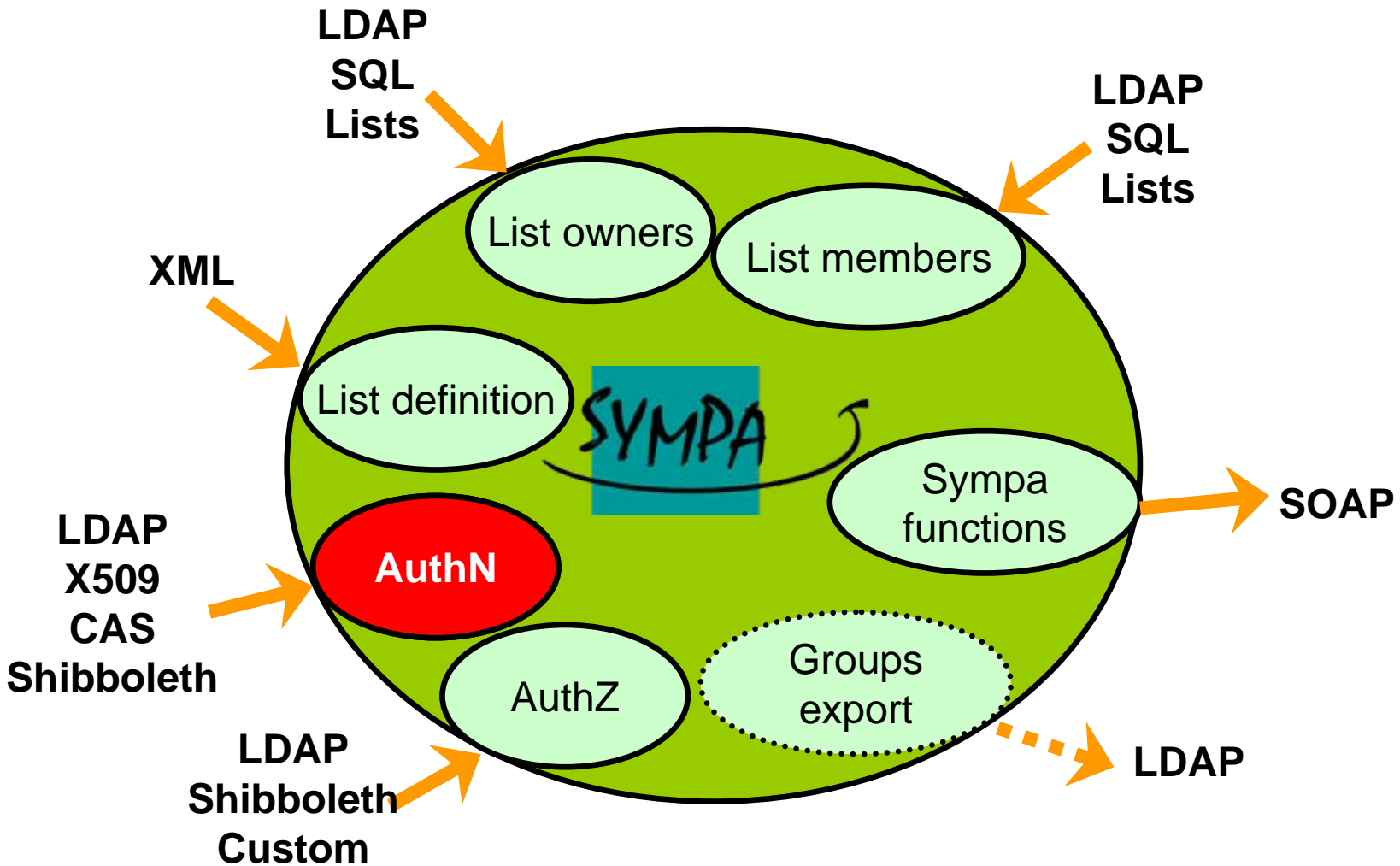
Sympa core features

Sympa is Middleware-enabled

- Our goal :

To make the software interact with its environment (LDAP directories, business databases, authentication services) as a data consumer / producer.

Middleware connectors in Sympa



Authentication in Sympa

- Mail authentication using challenges or S/MIME
- Web authentication
 - User logs in to subscribe, review list archives, share documents, manage groups
- Sympa native authentication :
 - email address + password
- Other authentication plugins :
 - LDAP
 - CAS
 - Shibboleth

Sympa web interface



A demo mailing list service

[List of lists](#) [Home](#) [Help](#)

Shibboleth login
 email address :

 password :
 [Login](#)

[First login ?](#)
[Lost password ?](#)

English

This demo mailing lists service is managed on our main server as a Sympa Vir

Once logged in, a "Create list" button will appear on the menu bar. This will a management.

Note that because this service is **only for test purpose**, we apply the folk

1. We are moderating mailing lists creation.
2. A mailing list population is restricted to 5 subscribers
3. Mailing lists will be automatically closed 7 days after their creation

Below are listed available mailing lists on this server :

123@demo.sympa.org
 456

actualites@demo.sympa.org
 test

alm@demo.sympa.org

Mixing authentication methods

- We've focused on flexibility :
 - Site administrator can allow one or more authentication methods
 - LDAP backend can be used depending on user email address format
 - CAS servers are listed in a drop-down menu (kind of WAYF)

CAS architecture

- CAS is a web Single Sign-On software
- Architecture includes
 - CAS server
 - CAS clients
 - Support for CAS proxies
- Until CAS 2.x only userID is carried
- Most CAS-enabled applications include CAS client code
 - Libraries for common languages (Java, PHP, Perl, Ruby, WebObjects,...)

CAS authentication in Sympa

- Implemented with the CAS 2.0 Perl library
- Sympa requires the user email address
 - Fetched from the university LDAP directory
 - Requires additional configuration
- Sympa provides a SOAP interface
 - login uses the CAS proxy mode
- Transparent login
 - Using CAS gateway feature
- Logout=Sympa logout + CAS logout

Sample CAS configuration

cas

base_url <https://cas.univ-x.fr>

non_blocking_redirection on

auth_service_name cas-cru

ldap_host ldap.univ-x.fr:389

ldap_get_email_by_uid_filter (uid=[uid])

ldap_timeout 7

ldap_suffix dc=cru,dc=fr

ldap_scope sub

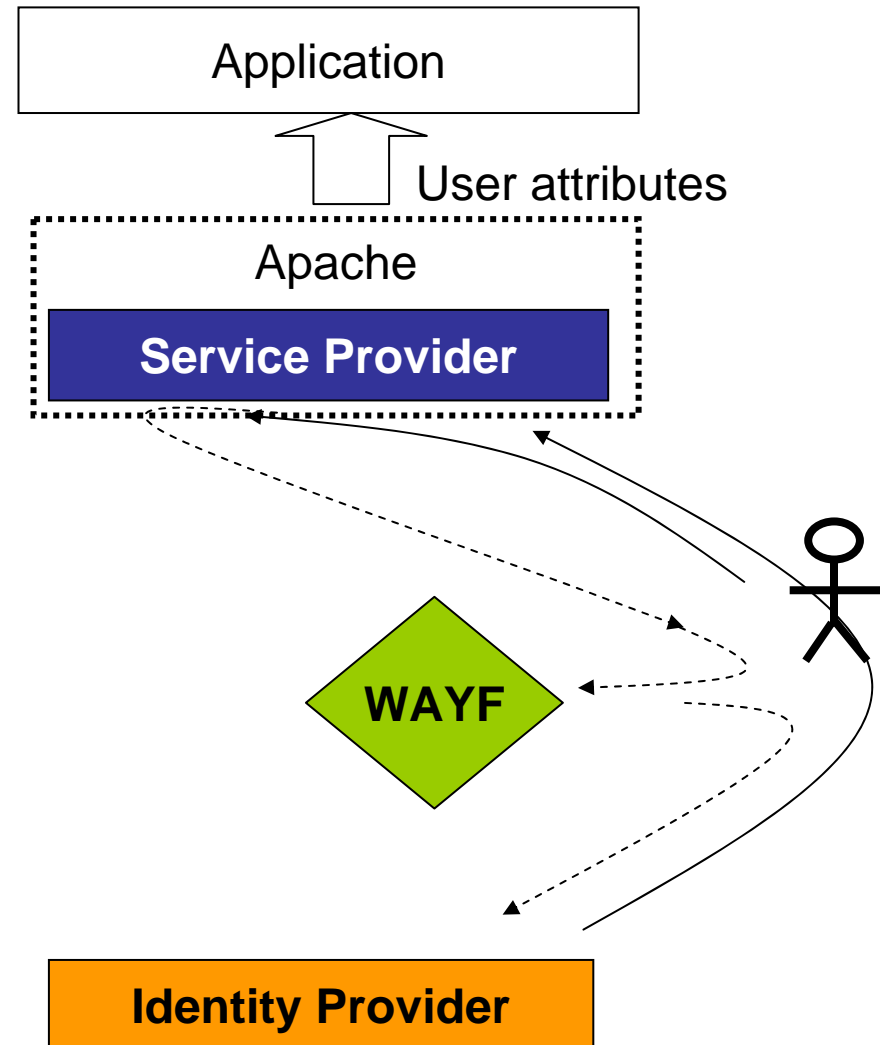
ldap_email_attribute mail

CAS demo

- <https://listes.univ-rennes1.fr/www>

Shibboleth architecture

- Shibboleth is a distributed web SSO
- Authentication is handled by an Apache module
 - Standard API to carry user attributes via environment variables



Shibboleth authentication in Sympa

- Implementation is not Shibboleth specific
 - Plugin named *generic_sso*
 - tested with PAPI, Feide
- User attributes used by authorization engine
- Logout currently not handled

Configuring Shibboleth authentication

- Apache configuration

```
<Location /sympa/sso_login/cru_federation>  
  AuthType shibboleth  
  ShibRequire Session On  
  require mail ~ @  
</Location>
```
- Sympa configuration

```
generic_sso  
service_name CRU Federation  
service_id cru_federation  
http_header_prefix HTTP_SHIB  
email_http_header HTTP_SHIB_INETORGPERSO_MAIL
```

Handling Shibboleth user attributes

- Sympa uses the email address as a primary key
- First implementation
 - Mapping with incoming user email
- Security issues
 - Privileges mapped to user email address
- Second implementation
 - Due to JP.Robinson, univ of Birmingham, Alabama
 - Incoming email addresses are validated via a challenge email

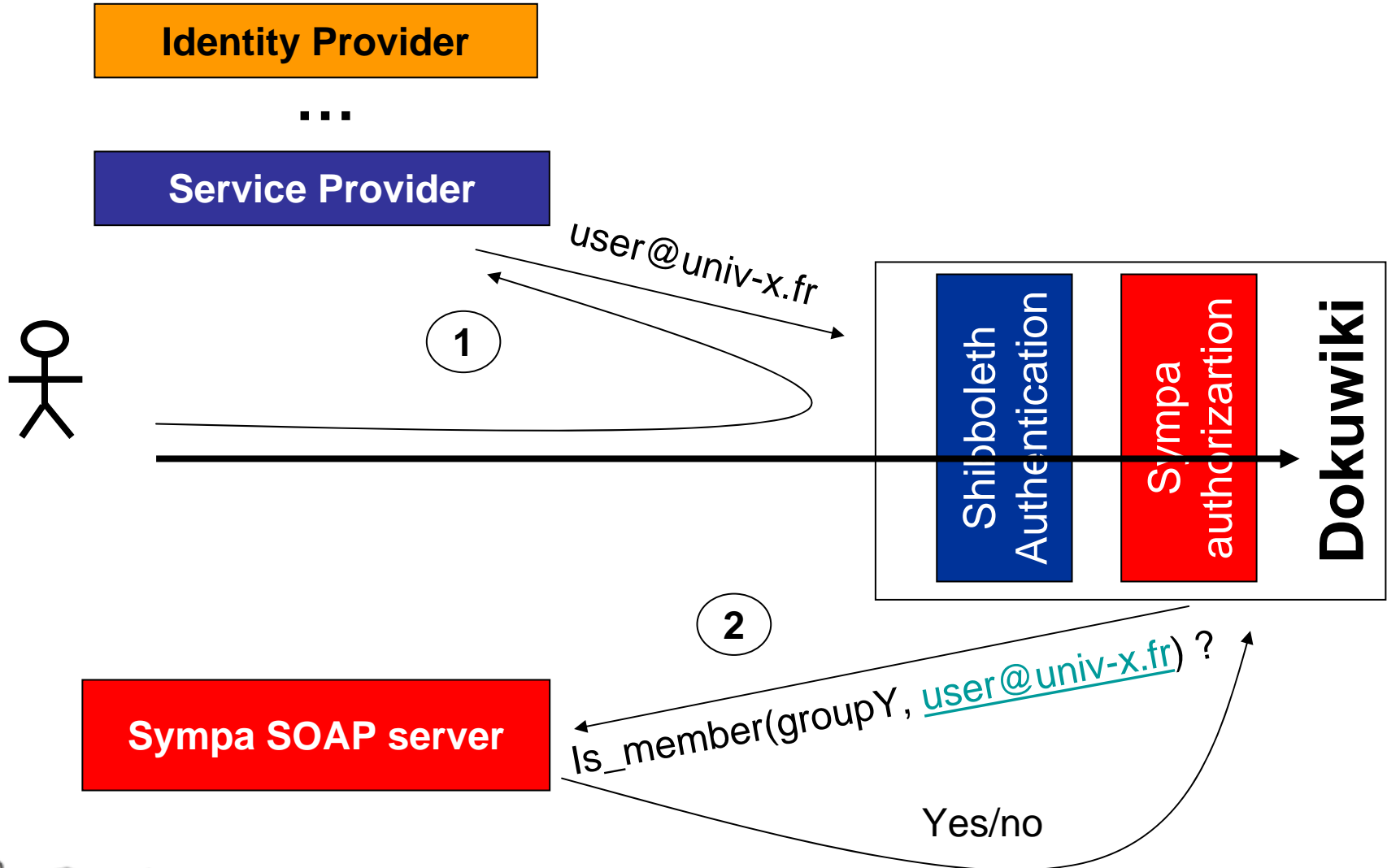
Sympa and dokuwiki

- Requirements :
 - Access control for web resources
 - Authentication is handled by Shibboleth
 - authorization requires groups definition
 - Groups include members from different institutions
 - Group membership is not defined in LDAP
 - So called Virtual Organizations
- Example:
 - Access control to a wiki for a group of researchers

Sympa and dokuwiki

- Dokuwiki
 - <http://wiki.splitbrain.org/wiki:dokuwiki>
- Group definition in Sympa
 - Mailing list = Group
 - Natural way of managing groups (Yahoo Groups, Google groups,...)
- Dokuwiki plugin
 - Authentication uses Sympa or Shibboleth
 - Authorization uses Sympa groups (via SOAP)

Sympa and dokuwiki



Sympa and dokuwiki demo

- https://www.cru.fr/activites/groupe_travail/test

Lessons we've learnt...

- Making application AA-enabled is a significant work
- Preserving native authentication method
- Transparent login increases the usability
- Email addresses as the user identifier
 - Not always provided
 - Not always reliable (privileges mapped to it)
- Global logout is difficult to implemented

Thank you for your attention

<http://www.sympa.org>