

FederID



Clément OUDOT

Table of contents

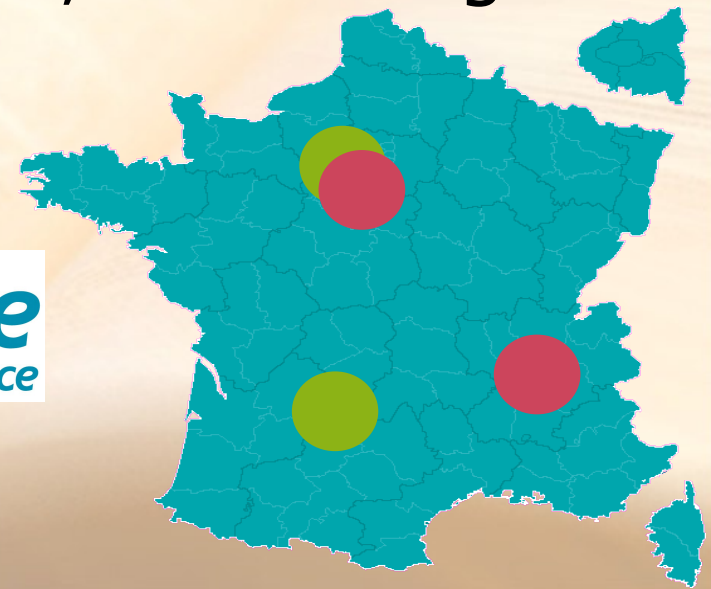


- LINAGORA Group
- A question of Identity
- Liberty Alliance
- The FederID architecture
- Advanced use of LDAP
- Conclusion

LINAGORA Group



- LINAGORA Group, this is:
 - 100 persons
 - Implantations in Paris, Lyon and Toulouse
 - Results: 9 billions euros for 2007
 - Training, Support, Integration, Consulting
 - Only Free Software !





- Open Source Software Assurance :
 - Bring our customers support on more than 250 Free Softwares
 - Patches delivered within 8 hours
 - Patches always submitted to the communities
 - Bugs report on critical architectures, not tested by the community developers



Table of contents



- LINAGORA Group
- A question of Identity
- Liberty Alliance
- The FederID architecture
- Advanced use of LDAP
- Conclusion

A question of Identity

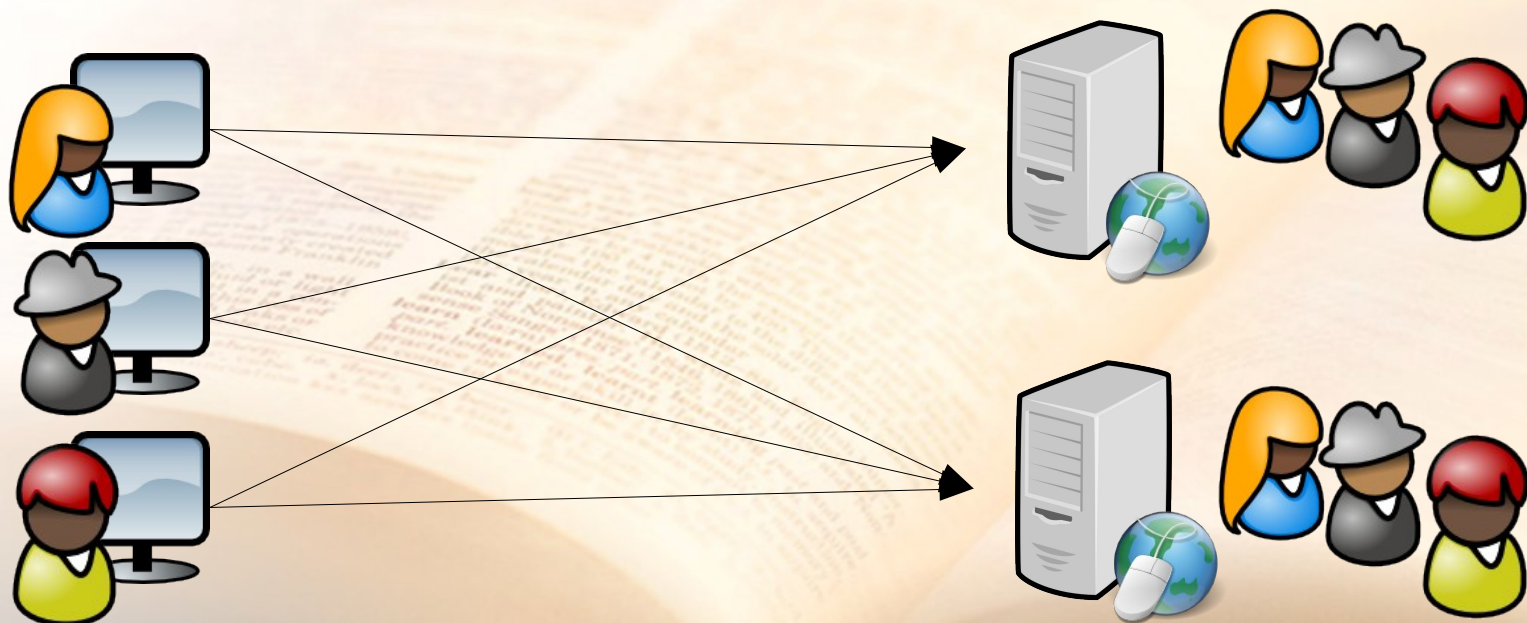


- A digital entity is a set of attributes describing an entity
- A subset named credentials are used for authentication
- An entity (a user) can own many identities
- Each identity has roles and rights within an application (service provider)

A question of Identity



- Services provider manage the identities :
 - For a service provider : 1 user = 1 identity
 - For an user : 1 service = 1 identity



A question of Identity



- We need Identity Management !
 - Referential of identities (LDAP Directory)
 - Provisioning services
 - Access control on data (LDAP ACLs)
 - Access control on applications (SSO rules)
- We need Identity Federation !
 - Keep different identities for private life purpose
 - Federate accounts to benefits from other services

Table of contents



- LINAGORA Group
- A question of Identity
- Liberty Alliance
- The FederID architecture
- Advanced use of LDAP
- Conclusion

Liberty Alliance



- Grounded in 2001 by SUN and 13 others partners
- More than 1500 members
- Goals :
 - Open Federation Standard
 - Respect of private life in numeric space

Liberty Alliance



Desk

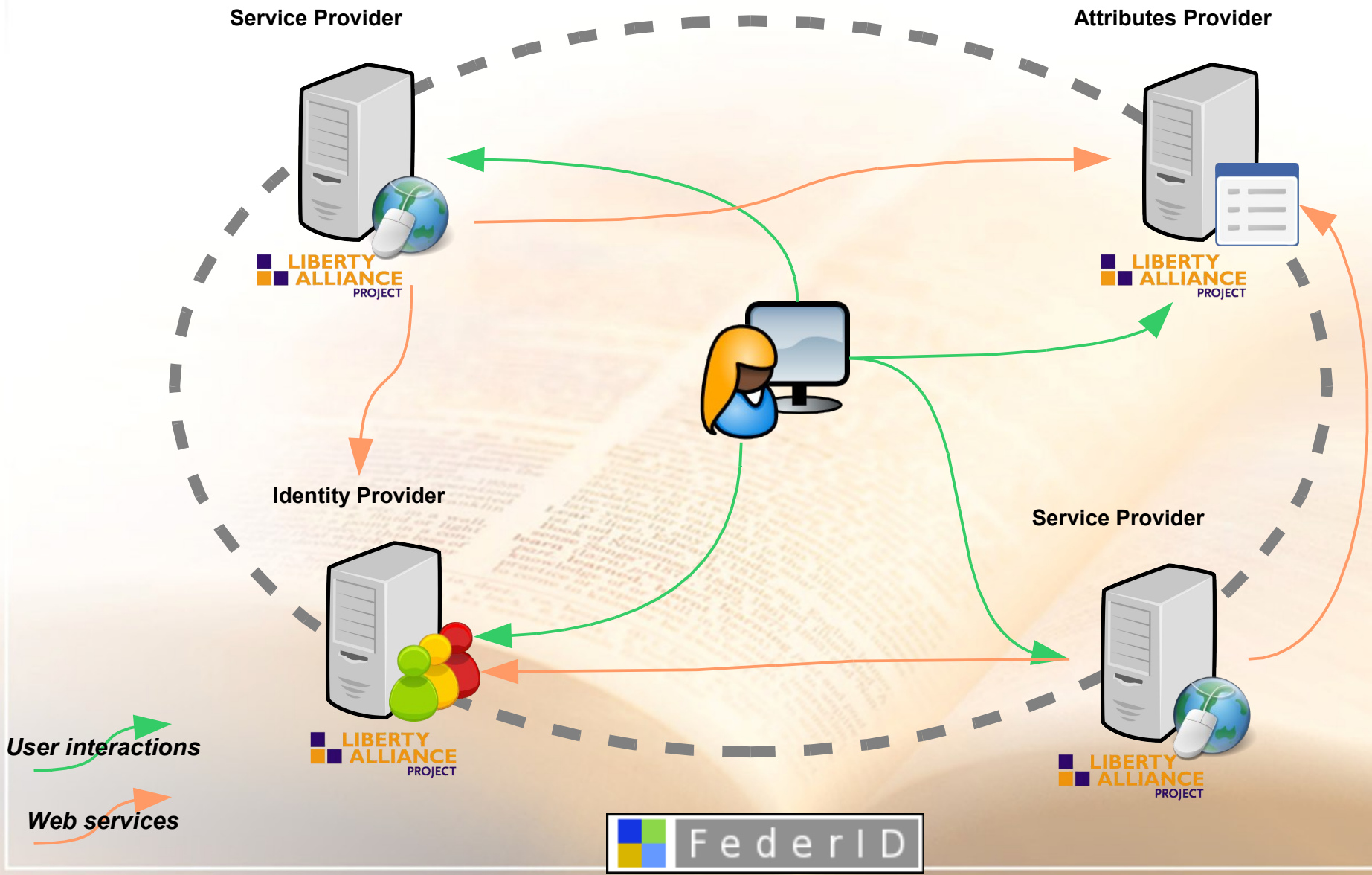
Sponsors

Liberty Alliance

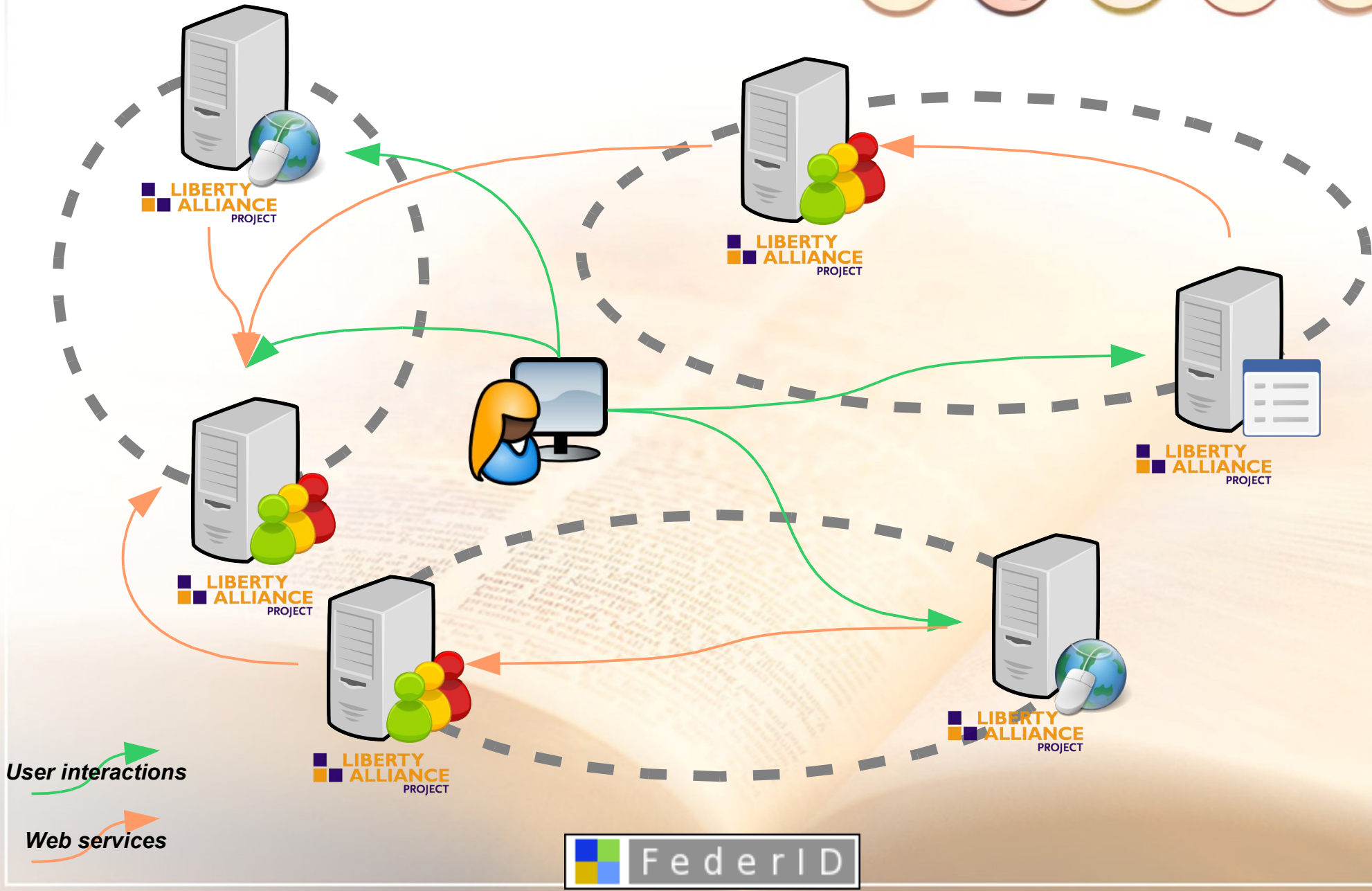


- Three standards frameworks :
 - ID-FF (Federation Framework) :
 - SSO, SLO
 - Federation mechanisms
 - ID-WSF (Web Services Framework) :
 - Attribute sharing
 - Interaction service
 - ID-SIS (Service Interface Specifications) :
 - Interface between services

Liberty Alliance



Liberty Alliance



User interactions
Web services



Table of contents



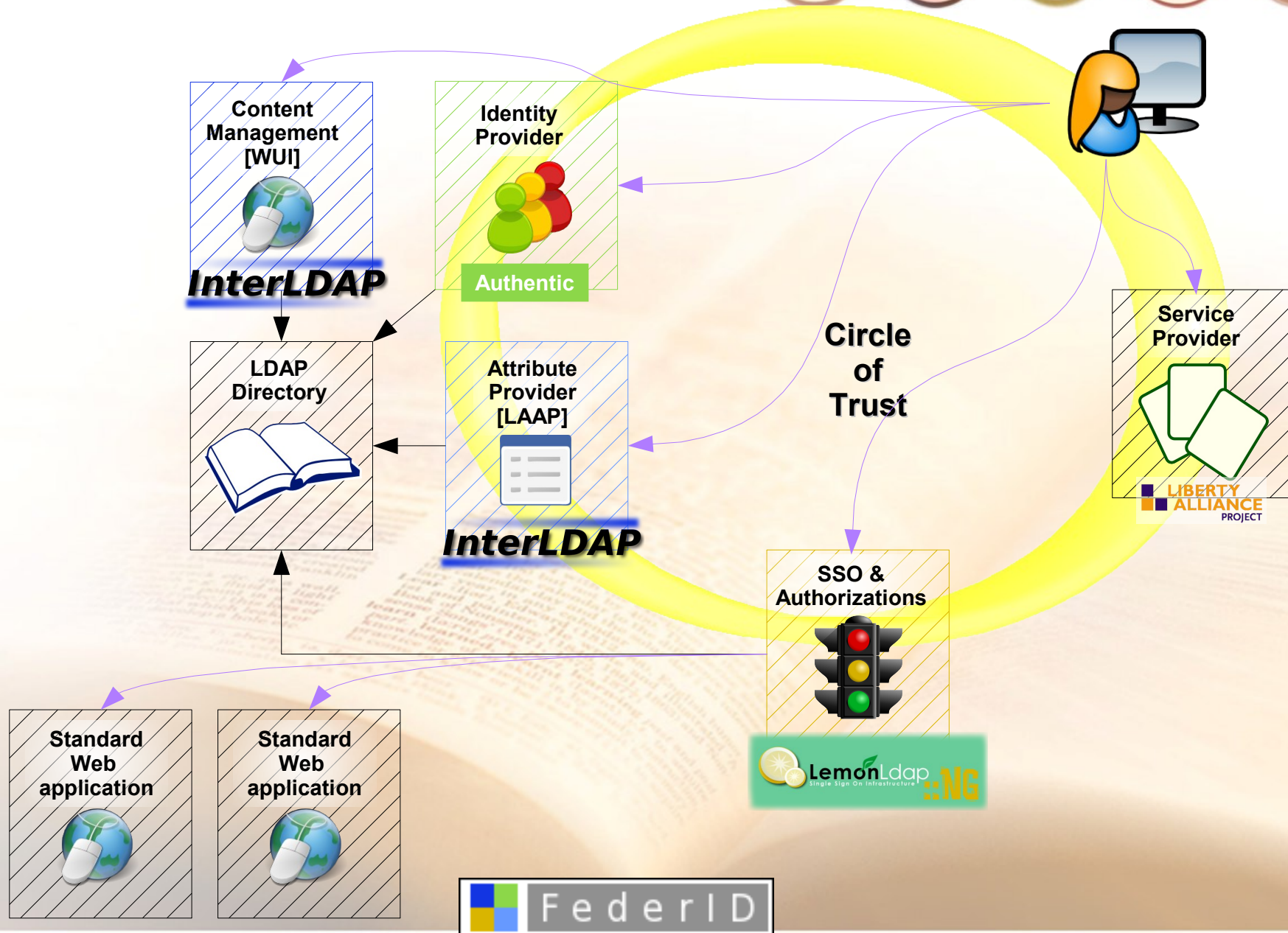
- LINAGORA Group
- A question of Identity
- Liberty Alliance
- The FederID architecture
- Advanced use of LDAP
- Conclusion

The FederID architecture



- LASSO API: Library of the Liberty Alliance specifications, C
- InterLDAP: LDAP tool suite for content management, J2EE (Spring-LDAP, Tapestry 5)
- LemonLDAP::NG: Web SSO tool with authorization management, Perl
- Authentic: Liberty Alliance identity provider, Python

The FederID architecture



The FederID architecture



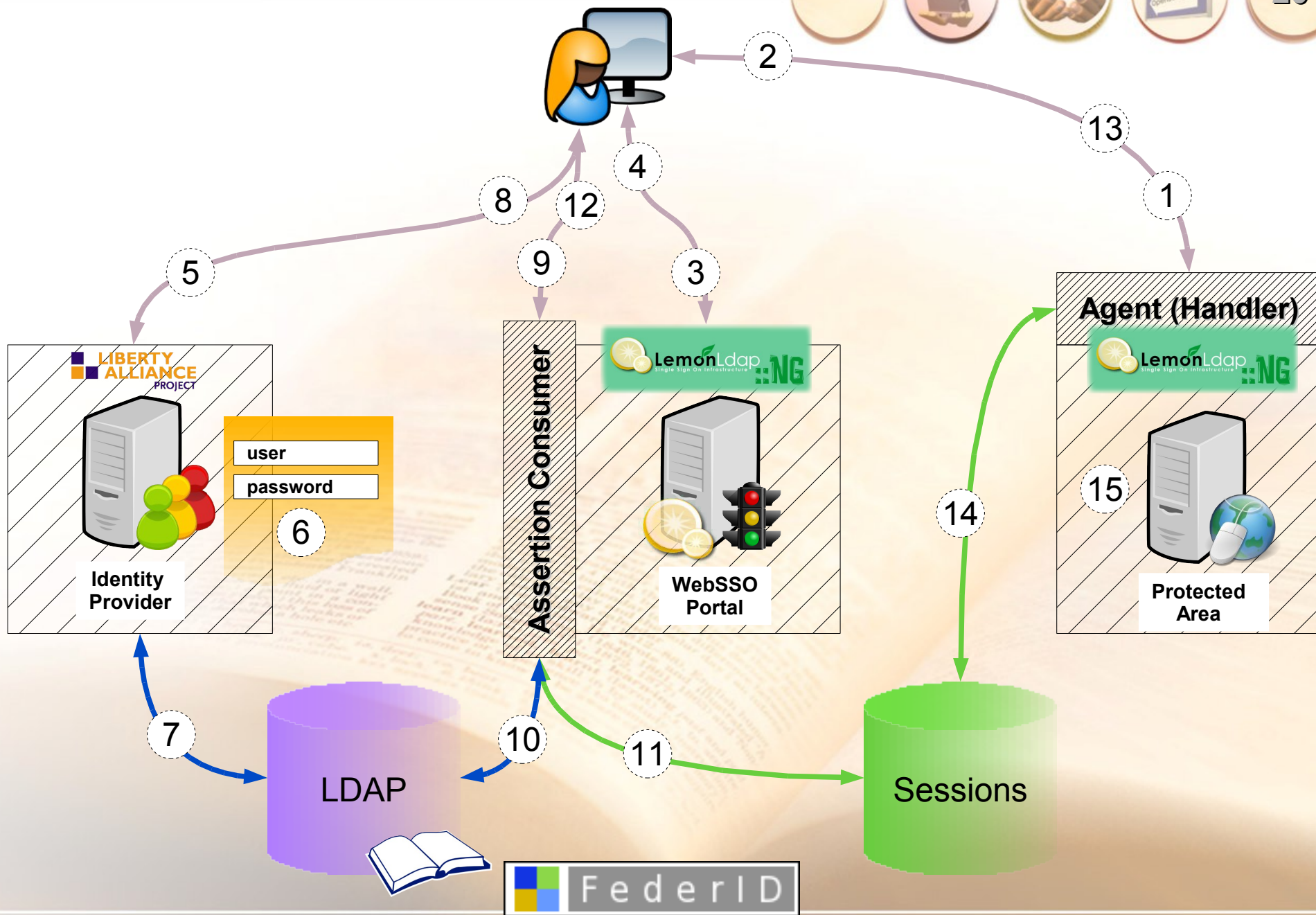
- Authentic :
 - Liberty Alliance identity provider
 - Authentication of users against an LDAP server, a database or simple flat text files
 - Forcing LDAP authentication within FederID
 - Capable of forwarding LDAP attributes into SAML responses

The FederID architecture



- LemonLDAP::NG:
 - WebSSO product based on Apache Perl Handler technology.
 - Offering three modules :
 - Handler: protect the application
 - Portal: where the user is redirected when not authenticated
 - Manager: graphical interface enabling the configuration of LemonLDAP::NG.

The FederID architecture

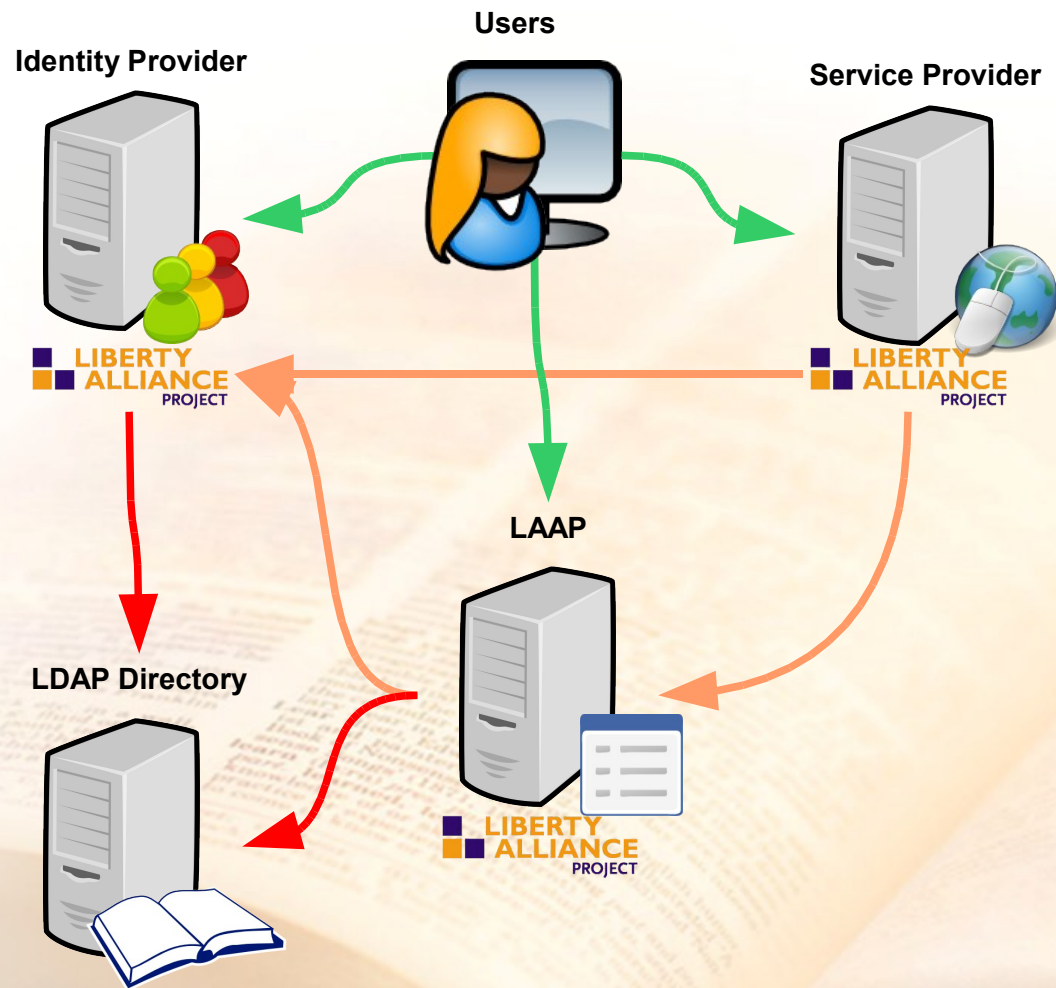


The FederID architecture



- InterLDAP-LAAP:
 - Liberty Alliance Attribute Provider
 - IF-FF and ID-WSF frameworks
 - Mapping of the representation of a person between LDAP and Liberty Alliance
 - Share LDAP attributes through normalized Web Services

The FederID architecture



HTTP
LDAP
XML/SOAP

The FederID architecture



- InterLDAP-WUI:
 - Content Management System for an LDAP directory
 - Enriched schema designing the interface “on the fly”
 - Authorization back-end
 - Delegation is enabled by setting trees and groups properties for each part of the Directory Information Tree

Table of contents



- LINAGORA Group
- A question of Identity
- Liberty Alliance
- The FederID architecture
- Advanced use of LDAP
- Conclusion

Advanced use of LDAP



- SSO stack:

- Authentication against LDAP (or LA IdP)
- Authorizations against LDAP Filter :

- First select the attributes needed for the filter

- Define logical groups :

business => '(departmentUID=MyBusinessEntity)'

- Protect your area :

^/site/.*\$ => \$groups =~ /bbusinessb/

^/(js|css) => accept

default => deny

=> No need to manage groups into Directory !

Advanced use of LDAP



- Standard LDAP Schema: mono/multi-valuated, syntax, matching rules, ...
- Enriched schema:
 - Labels/descriptions
 - List of values/Default value
 - Visible/filterable/modifiable
 - Double capture

Advanced use of LDAP



- The power of SQL for LDAP:
 - LDAP Query Language
 - For reading only
 - Doing searches on results of a primary search
 - LQL request stored as an LDAP attribute value

Advanced use of LDAP



- LQL functions:
 - search/list/read (DN, FILTER)
 - sup (DN, N): raise the tree from "DN" for "N" levels
 - fsup (BASE, FILTER): return the first parent of "BASE" selected by "FILTER"
 - and/or: union/intersection
 - group (DNGROUP, DNMEMBER): check if "DNMEMBER" belongs to "DNGROUP"
 - concat: strings concatenation

Advanced use of LDAP



- And some variables:
 - \$namingContext: suffix of the tree.
 - \$targetDN: DN targeted by the operation.
 - \$targetRDN: RDN targeted by the operation.
 - \$authorDN: DN of the author of the operation (as it is bound on the directory).
 - \$authorRDN: RDN of the author of the operation.

Advanced use of LDAP



- LQL example :

```
attribute(attribute(sup(search(ou=structs,$  
namingContext,$targetRDN),1),manager)  
,cn)
```

Advanced use of LDAP



- Proxy-Authz control:
 - Before this control, need to maintain a connection on the directory per user
 - Now, we can use pool of connection with rootdn binds + Proxy-Authz
- No-op:
 - Goal: know if a user can write before writing!
 - Need to test the alternative 'Get effective rights'

Table of contents



- LINAGORA Group
- A question of Identity
- Liberty Alliance
- The FederID architecture
- Advanced use of LDAP
- Conclusion

Conclusion



Join us!

<http://www.federid.org>
federid-dev@federid.org

<http://www.interldap.org>
interldap-dev@objectweb.org



Thank you – Danke sehr



<http://www.federid.org>
<http://www.interldap.org>