The Shibboleth-enabled WebDAV server used in ESUP-Portail and ORI-OAI projects

Raymond Bourges

UNIVERSITÉ DE RENNES 1

TERENA EuroCAMP

14 - 15 November 2007

Dubrovnik, Croatia

Shibboleth-enabled WebDAV server

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

Context

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

Context

- ESUP-Portail (since 2003)
  - ESUP-Portail is a consortium of French universities
  - Its goal is to provide a complete and open uPortal based solution to offer integrated access to services and information for students and staff
  - This includes user data storage with **Sharing** capacities provided by a **WebDAV server**

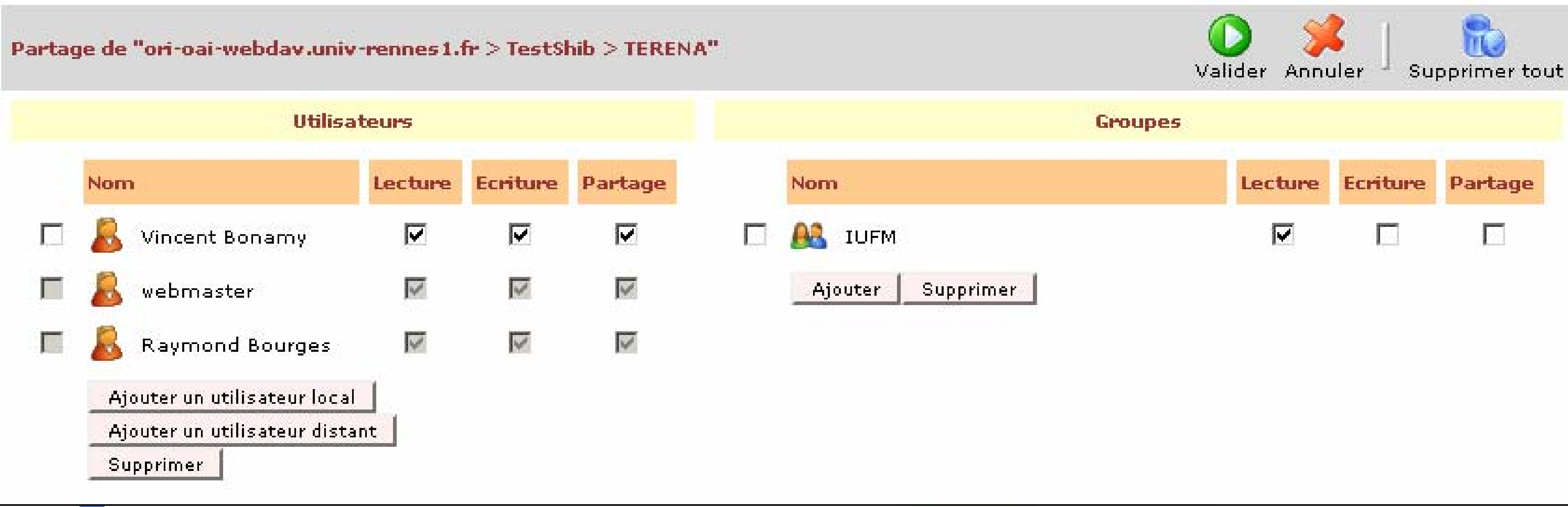
Context 2

- ORI-OAI (since 2006)
  - The ORI-OAI project seeks to create an open system
  - Build in part on ESUP-Portail project experience
  - This system allows users to:
    - Manage all the digital resources produced by universities
    - Share these resources with other universities
    - Valorize these resources with high-quality indexing
    - Make these resources **accessible** according to **well-defined access rules** with a **WebDAV server**

DEMO

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

I want to share a folder with users of another university



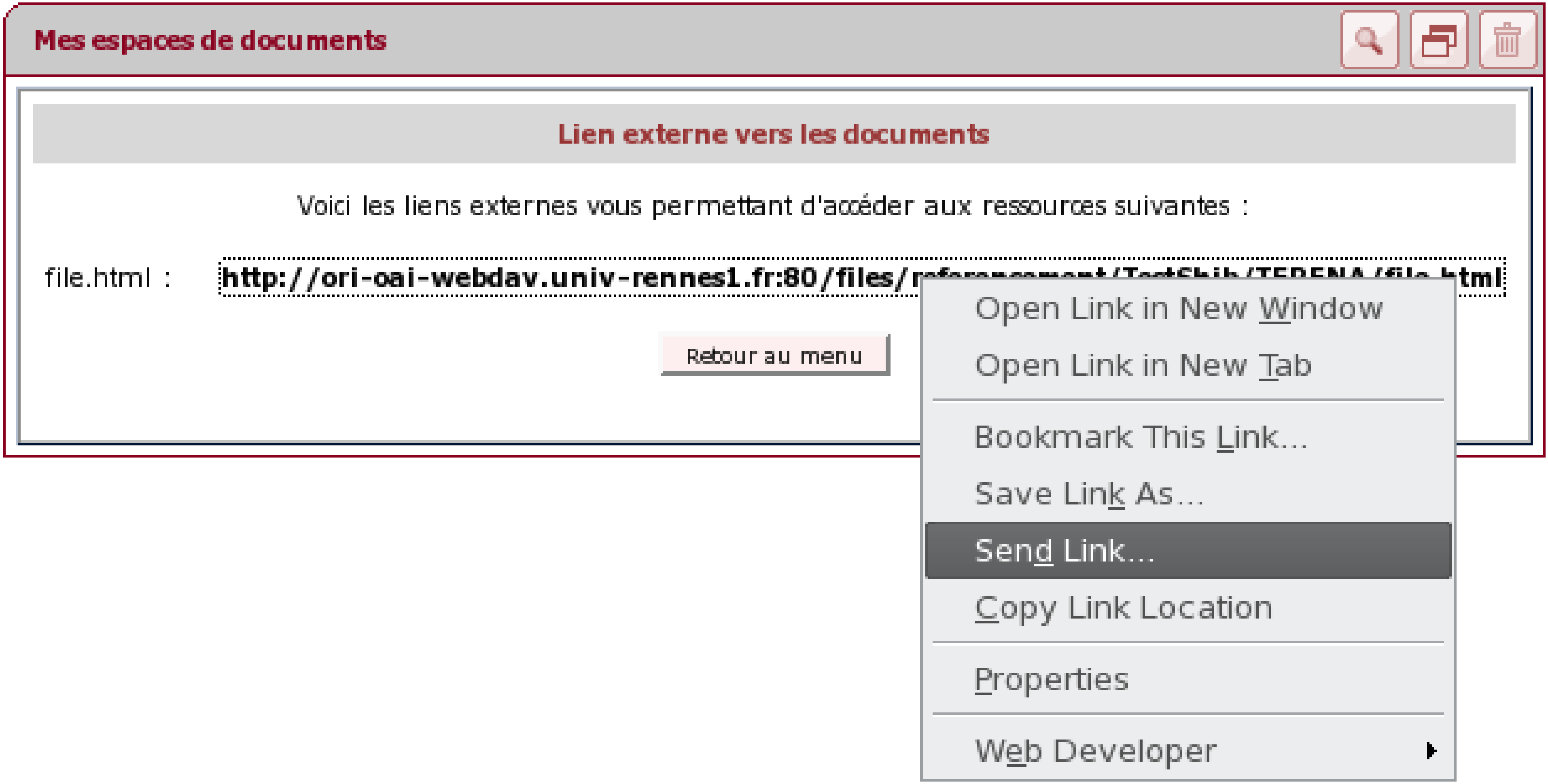
Partage de "ori-oai-webdav.univ-rennes1.fr > TestShib > TERENA"

Utilisateurs

	Nom	Lecture	Ecriture	Partage
□	Vincent Bonamy	☑	☑	☑
□	webmaster	☑	☑	☑
□	Raymond Bourges	☑	☑	☑

Groupes

	Nom	Lecture	Ecriture	Partage
□	IUFM	☑	□	□

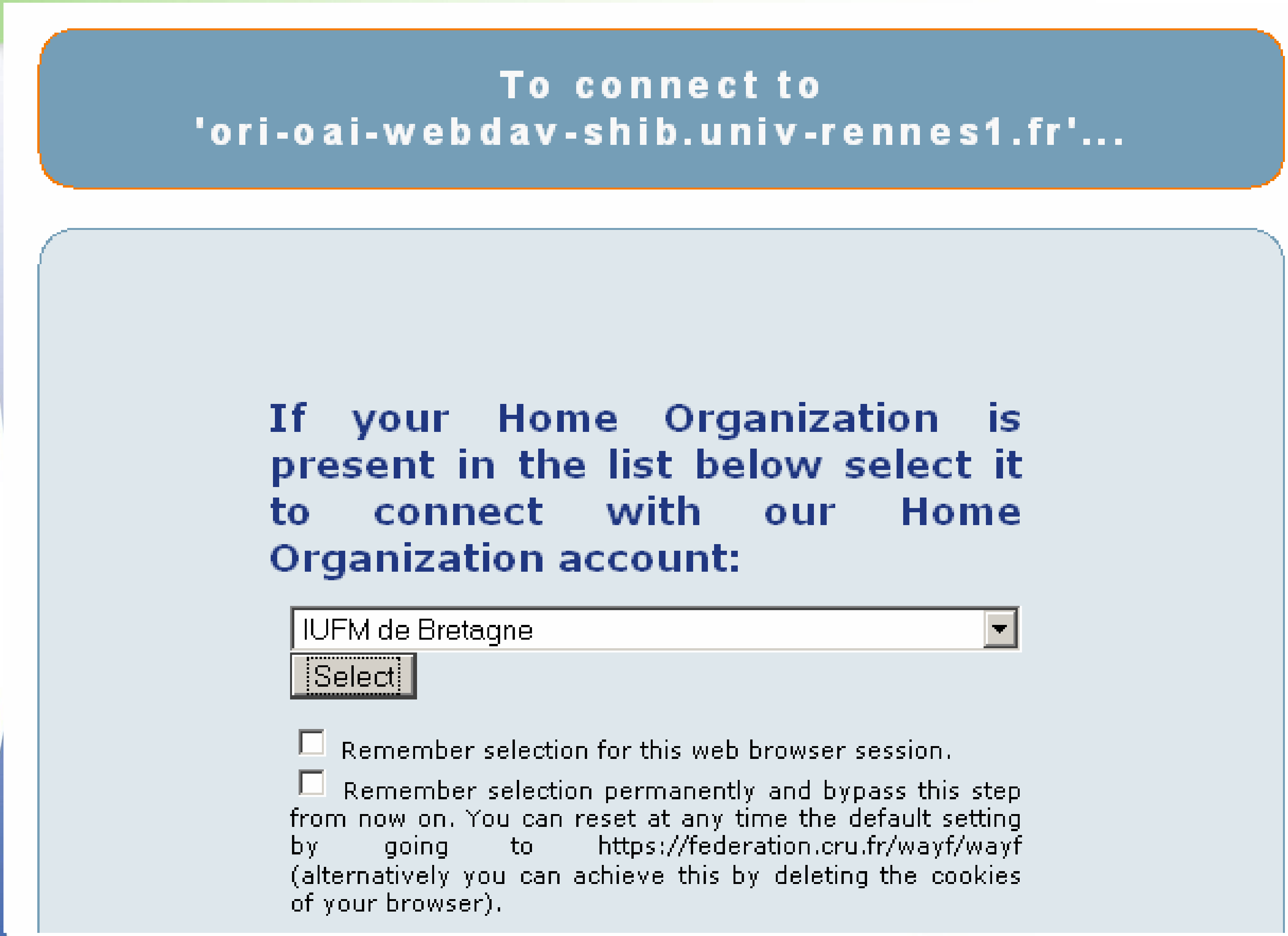


Mes espaces de documents

Lien externe vers les documents

Voici les liens externes vous permettant d'accéder aux ressources suivantes :

file.html : **http://ori-oai-webdav.univ-rennes1.fr:80/files/referencement/TestShib/TERENA/file.html**



To connect to 'ori-oai-webdav-shib.univ-rennes1.fr'...

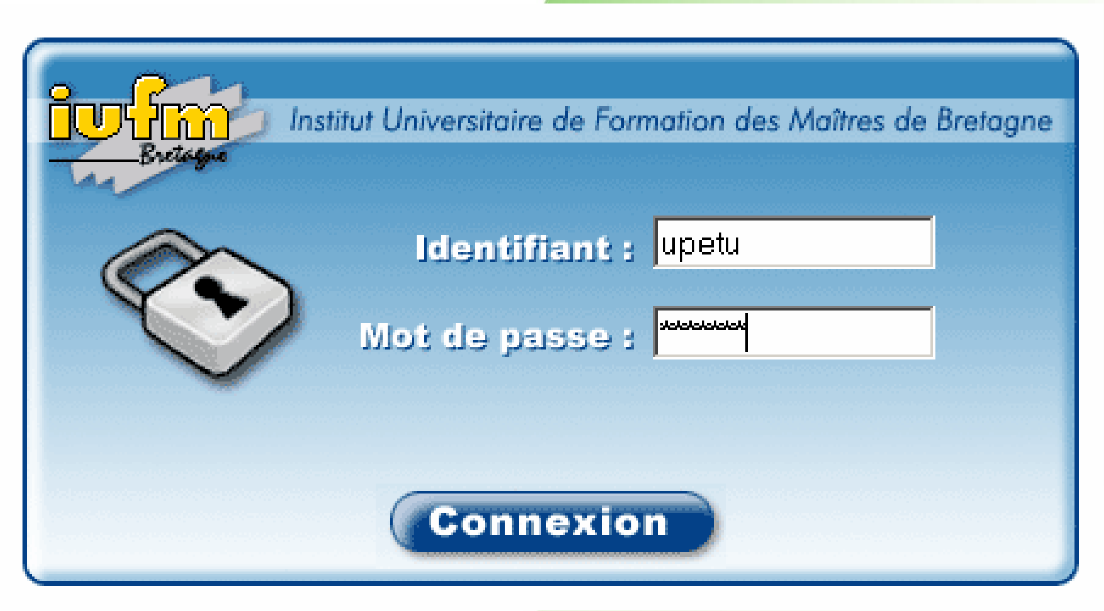
If your Home Organization is present in the list below select it to connect with our Home Organization account:

IUFM de Bretagne ▾

Select

□ Remember selection for this web browser session.

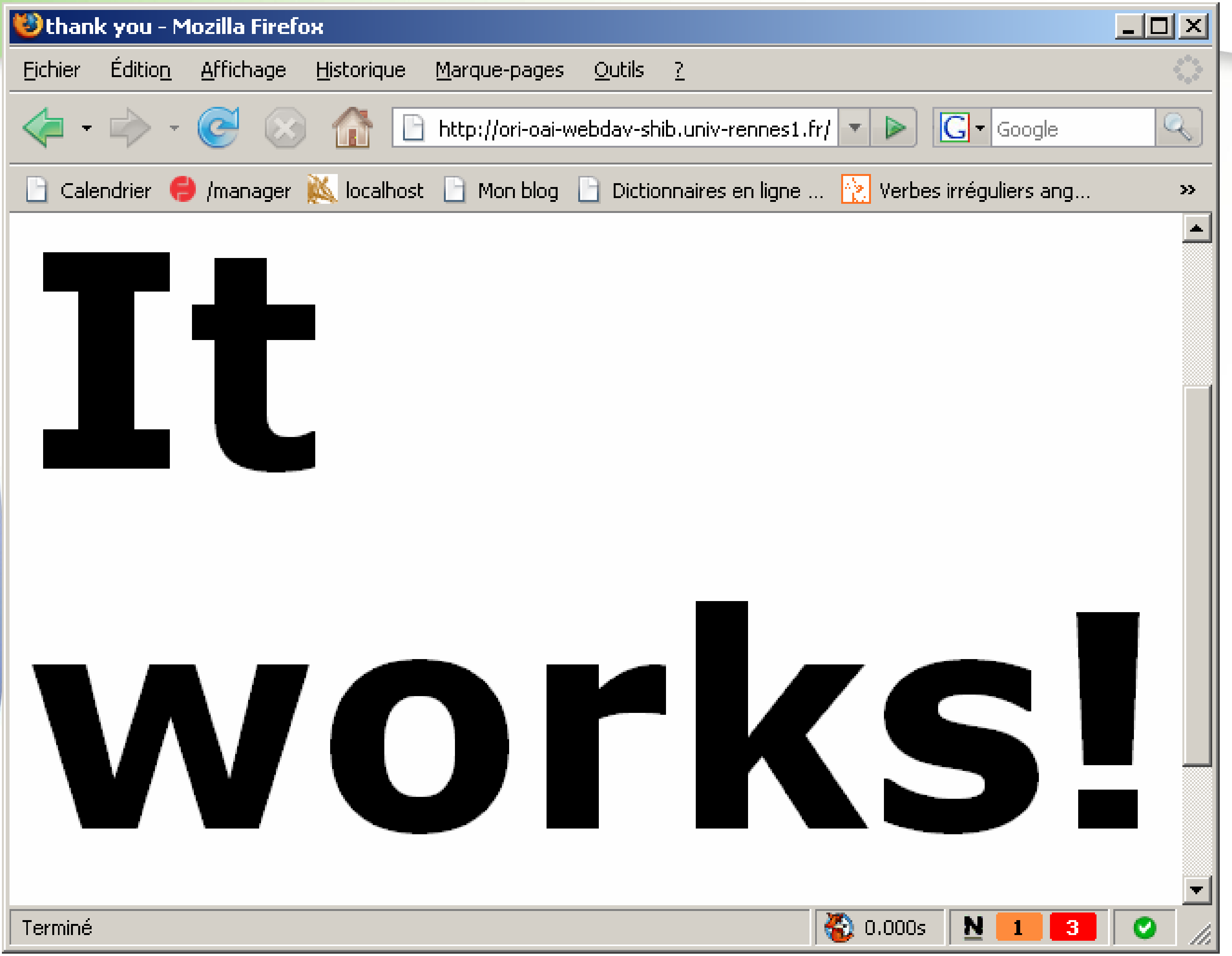
□ Remember selection permanently and bypass this step from now on. You can reset at any time the default setting by going to https://federation.cru.fr/wayf/wayf (alternatively you can achieve this by deleting the cookies of your browser).



Institut Universitaire de Formation des Maîtres de Bretagne

Identifiant : upetu

Mot de passe : ********



thank you - Mozilla Firefox
Fichier
Édition
Affichage
Historique
Marque-pages
Outils
?
http://ori-oai-webdav-shib.univ-rennes1.fr/
Google
Calendrier
/manager
localhost
Mon blog
Dictionnaires en ligne ...
Verbes irréguliers ang...
Terminé
0.000s
N
1
3

It works!

WebDAV protocol

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

WebDAV

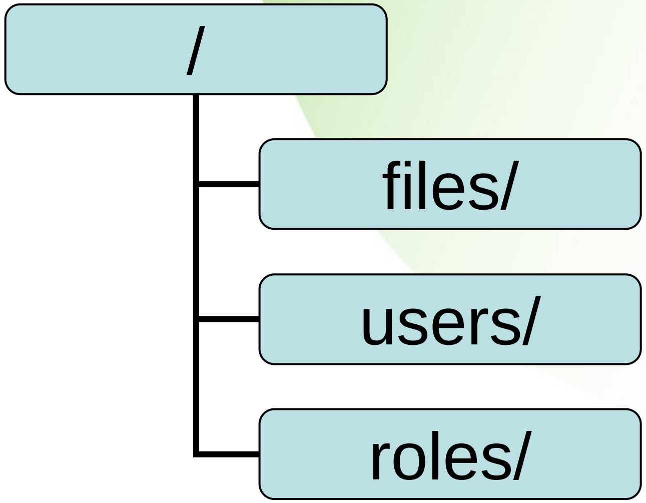
- WebDAV (RFC 4918) is an extension of HTTP/1.1, which initial goal was to permit remote editing through HTTP. To do so, WebDAV adds the following concepts:
  - Documents are no longer data, but also metadata, called **properties**. The value of these properties can be controlled by the server (Live property), or enforced by clients' requests (Dead property).
    - Ex: last file modification date, file display name
    - Document + metadata form a **WebDAV resource**
  - A resource can be locked by users for online editing

Webdav

- WebDAV introduces new HTTP methods:
  - PROPFIND/PROPPATCH respectively to get/set a property on a resource
  - LOCK/UNLOCK respectively to set/unset a lock on a resource
  - MKCOL to create a collection
- As other HTTP application WebDAV can support different authentication mechanisms:
  - LDAP
  - SSO
  - Shibboleth

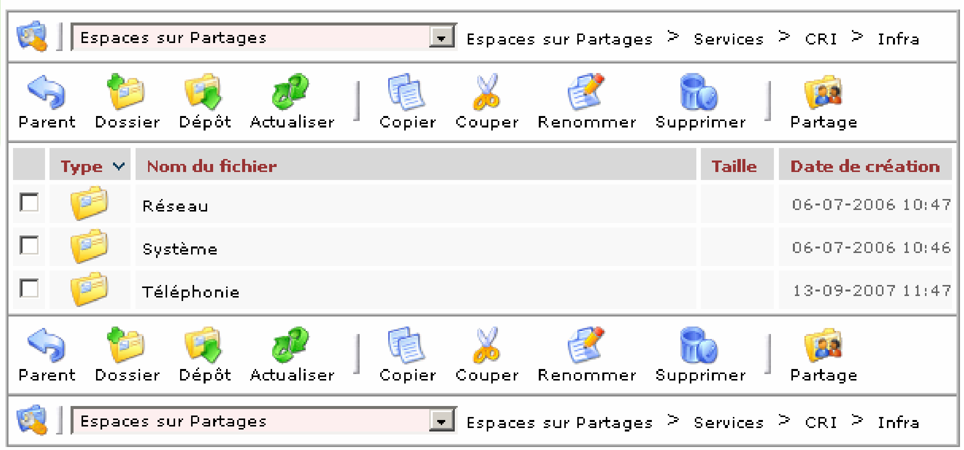
WebDAV resources

- WebDAV resources can be gathered into **collections**, much like files are gathered into folders within a file system. A collection is itself a resource, and thus can be moved, copied, deleted like another resource
- Resources can be files and folders but may represent, as we will see with ACP, other concepts like Users or Groups. So a typical WebDAV hierarchy looks like this:



Resources accessibility

- A big feature of WebDAV is his accessibility form different clients over the web
  - Explorer OS integrated
    - Rich editing capacity
  - Simple Web explorer
    - Easy read access
  - Web application
    - For portal integration

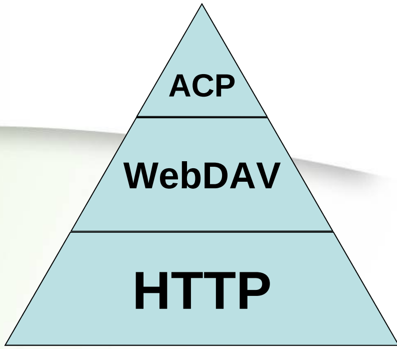


	Type	Nom du fichier	Taille	Date de création
□		Réseau		06-07-2006 10:47
□		Système		06-07-2006 10:46
□		Téléphonie		13-09-2007 11:47

ACP protocol

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

ACP



- Access Control Protocol (RFC 3744)
  - is an extension of WebDAV
- All possible requestors are called **principals** in ACP RFC
- A WebDAV server supporting ACP has to store a representation of each principal as a WebDAV resource
- Principal can be:
  - A user resource with at list a displayname property
  - A group resource with the special group-member-set property which reference users as members
    - A group resource can be a collection and containing other subgroups

ACP

- ACP defines a new resource property called **ACL** (**A**ccess **C**ontrol **L**ist) which contains **ACE** (**A**ccess **C**ontrol **E**lement)
  - This property is typically used to define authorizations on files or folders
- Each ACE represents a relation on the resource between a principal and a **privilege**
  - The relation can be to grant or to deny principal the use of the privilege
- Privileges define actions allowed on resources. Example:
    - read, write, write-acl

Slide WebDAV server

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

Slide

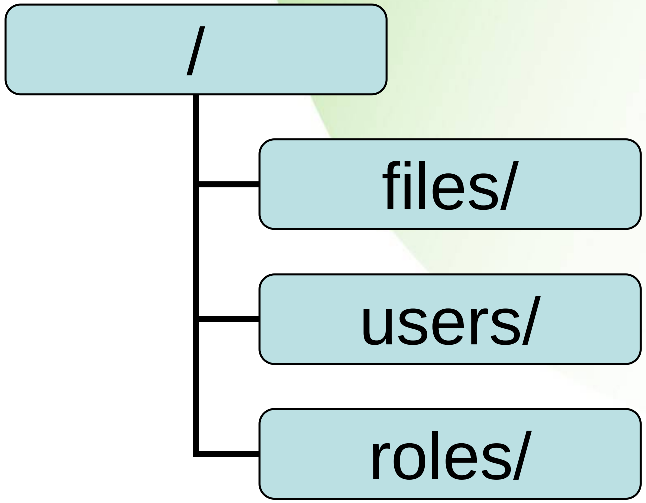
- Open Source Java WebDAV server **with ACP support** from Apache software foundation
- Extensible
  - J2EE filters compatibility
    - Used by ESUP-Portail project to provide LDAP, SSO (with CAS) or Shibboleth authentication capacities
  - Storage called Slide store
    - Used to plug different content and property storage implementations in different parts of the resources tree provided by the WebDAV server (files, users, roles)
  - Slide event mechanism
    - Used by ESUP-Portail project to provide an implementation of Quota for WebDAV (RFC 4331)

Slide store

- Out of the box you find
  - File system store
    - To store content as binary files and properties as XML files
    - Can also be used to store users or groups
  - LDAP store
    - Can be used to retrieve users and groups information from an LDAP directory
  - SQL Store
    - Can be used to store users, groups, properties but also files in a database

Slide store in ESUP/ORI Projects

- Naturally we used default Slide store:
  - Slide File system store is used for files and properties (files/)
  - Slide LDAP store is used for users (users/)
    - but this store was extended by ESUP/ORI for shibboleth needs
  - Slide SQL Store is not used



Slide store in ESUP/ORI Projects

- /roles branch is more complicated
  - /roles/local uses Slide file system store. It contains static technical groups like the admin one
  - /roles/uPortal uses a ESUP/ORI specific store (UPortalRoleStore) that exposes all uPortal managed groups with a Web Service mechanism for uPortal dialog
  - /roles/shib uses another ESUP/ORI specific store (ShibRoleStore) that allows groups definitions based on shibboleth attributes combinations

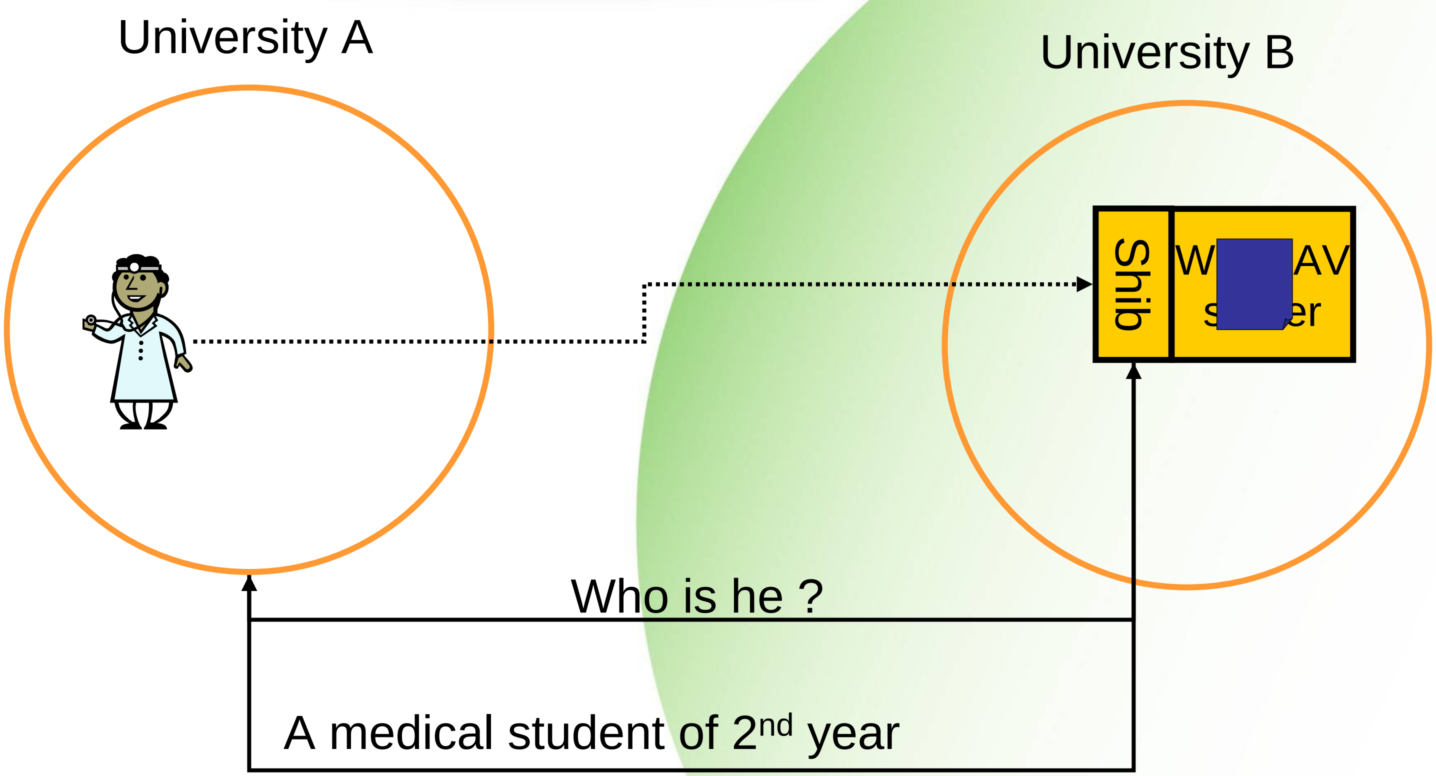
Shibboleth integration

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

Shibboleth

- Shibboleth provides mechanism to identify and authorize users over the web thanks to 3 components:
  - **SP** provide service (of course ☺) according to rules managed locally
  - **IdP** is based on the end user’s university and, after local authentication, gives chosen information (attributes) to the SP requested by the user
  - **WAYF** is used by SP to ask a user “Where Are You From” in order to interact with the right IdP

Shibboleth (practical example)



University A

University B

Shib

W AV
s er

Who is he ?

A medical student of 2nd year

- Try to access document in university B
- Query to university A « identity provider »
  - generally throw a WAYF
- Response to university B « service provider »
- Access to document

ShibRoleStore and Shibboleth attributes

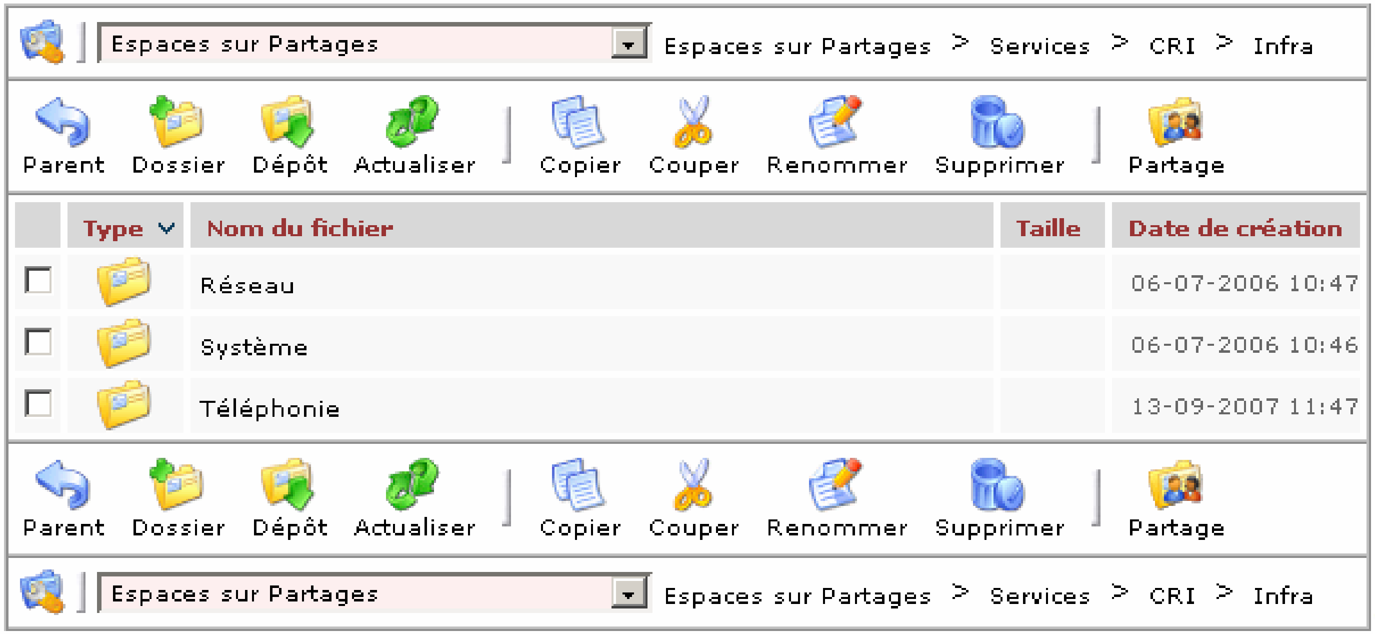
- ShibRoleStore has 2 functions
  - **Storage of Shibboleth groups definitions** (done with administrator rights)
    - MKCOL “shib group” in /roles/shib branch
    - PROPPATCH the *shib-eval-exp* property of “shib group” in order to store the new shibboleth attributes based rule
  - **Dynamically evaluate rule during ACE parsing**
    - Use of a JSR-94 compatible rule engine (JBoss Drools)
    - If rule is successfully evaluated the *group-member-set* WebDAV property of “shib group” reference the current connected user
    - If rule isn’t successfully evaluated the *group-member-set* WebDAV property is empty and ACE isn’t verified
- Rules can contain equal, not, or, and, etc.

Portal integration for management

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

ESUP Storage Channel

- This channel provides uPortal users with access to all their files
- It has CIFS, WebDAV and FTP capacities
  - You can, for example, cut a CIFS folder and paste it in an WebDAV server



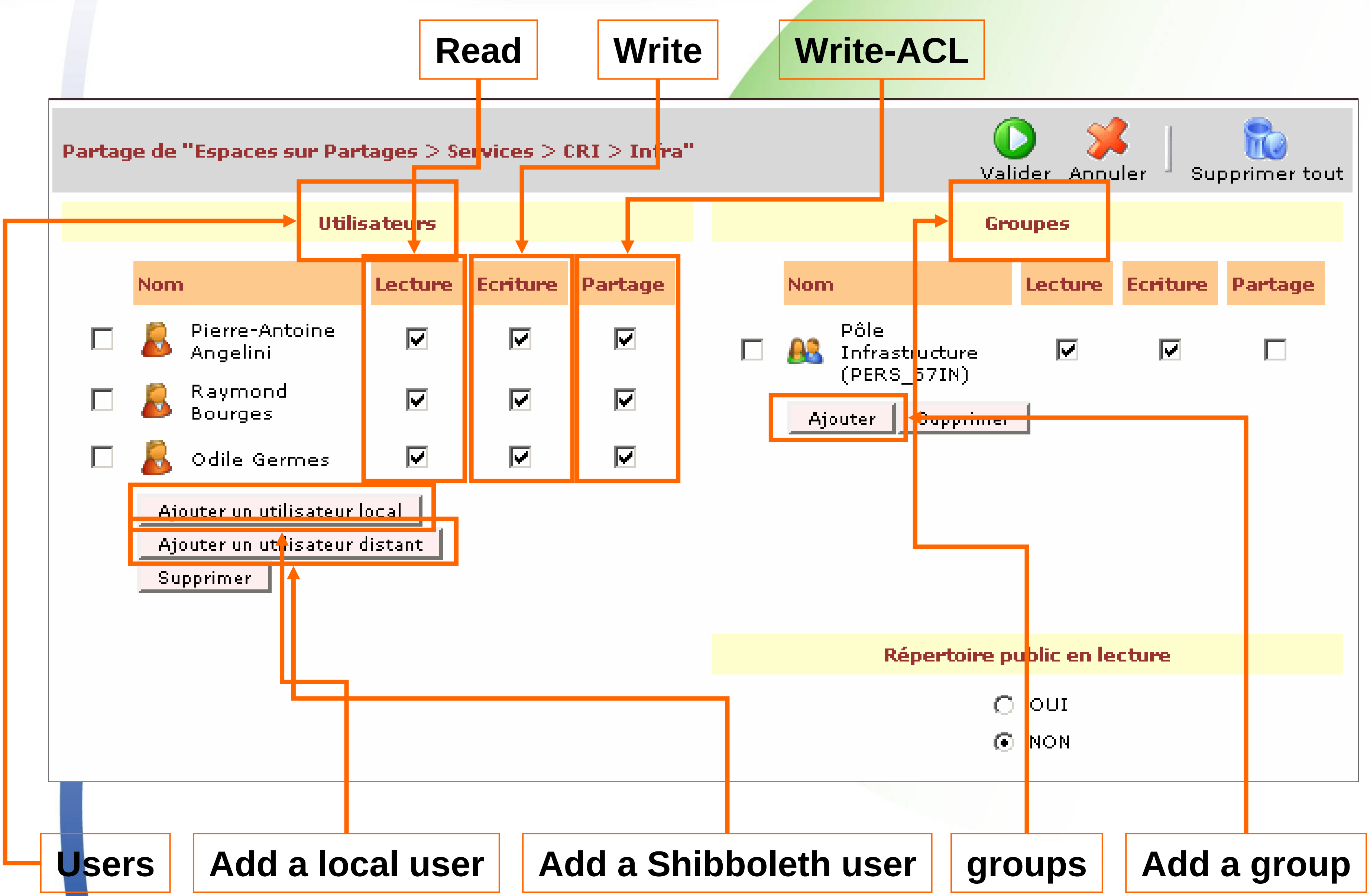
	Type	Nom du fichier	Taille	Date de création
□		Réseau		06-07-2006 10:47
□		Système		06-07-2006 10:46
□		Téléphonie		13-09-2007 11:47

ESUP Storage (ACL management)

- If you have write-acl privilege in a WebDAV server, you have a “share” button

- With it, you can manage ACL on WebDAV current folder
- Please note that if you give write-acl to others you can delegate ACL management. It is particularly useful in a large organization like a university
- You also have facilities to select users or groups
  - With a directory browser for users and a groups explorer

ESUP Storage (ACL management)



Read

Write

Write-ACL

Partage de "Espaces sur Partages > Services > CRI > Infra"

Utilisateurs

	Nom	Lecture	Ecriture	Partage
□	Pierre-Antoine Angelini	☑	☑	☑
□	Raymond Bourges	☑	☑	☑
□	Odile Germes	☑	☑	☑

Groupes

	Nom	Lecture	Ecriture	Partage
□	Pôle Infrastructure (PERS_57IN)	☑	☑	□

Répertoire public en lecture

○ OUI

● NON

Users

Add a local user

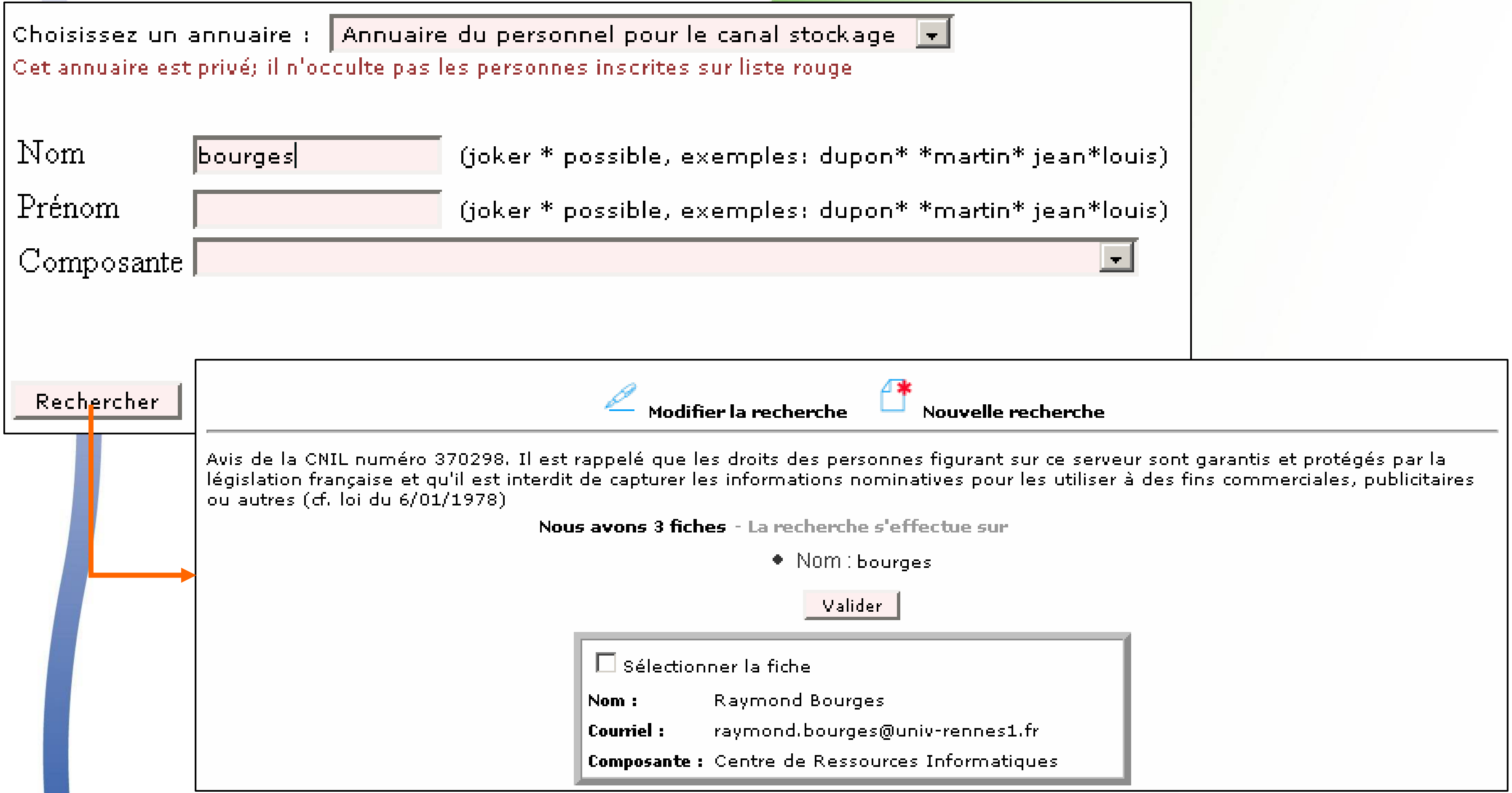
Add a Shibboleth user

groups

Add a group

ESUP Storage (Add a local user)

- Directory browser



Choisissez un annuaire : Annuaire du personnel pour le canal stockage

Cet annuaire est privé; il n'occulte pas les personnes inscrites sur liste rouge

Nom bourges (joker * possible, exemples: dupon* *martin* jean*louis)

Prénom (joker * possible, exemples: dupon* *martin* jean*louis)

Composante

Avis de la CNIL numéro 370298. Il est rappelé que les droits des personnes figurant sur ce serveur sont garantis et protégés par la législation française et qu'il est interdit de capturer les informations nominatives pour les utiliser à des fins commerciales, publicitaires ou autres (cf. loi du 6/01/1978)

Nous avons 3 fiches - La recherche s'effectue sur

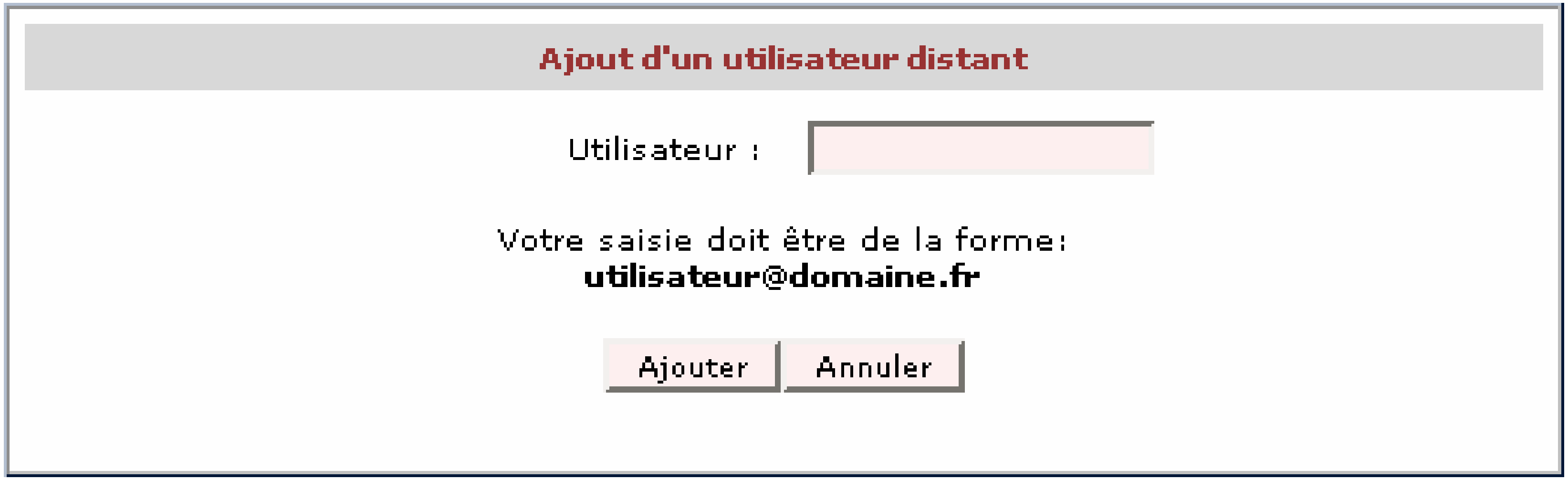
- Nom : bourges

□ Sélectionner la fiche

Nom :	Raymond Bourges
Courriel :	raymond.bourges@univ-rennes1.fr
Composante :	Centre de Ressources Informatiques

ESUP Storage (Add a shibboleth user)

- With Shibboleth each user over the world have an unique "NetID“
  - **eduPersonPrincipalName** or EPPN
- With ESUP Storage you can enter any EPPN to give direct access to a resource
  - example: bourges@univ-rennes1.fr



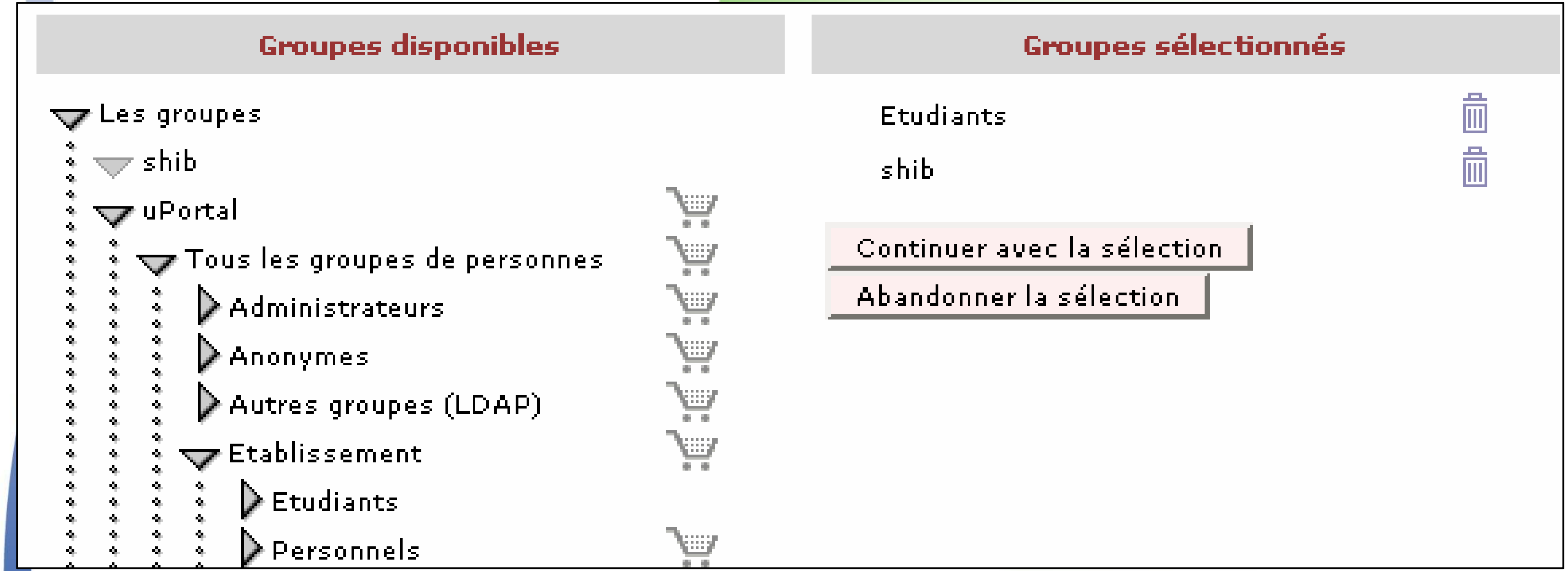
Ajout d'un utilisateur distant

Utilisateur :

Votre saisie doit être de la forme:
utilisateur@domaine.fr

ESUP Storage (Add a group)

- You have a group explorer of /roles branch of your WebDAV server in order to select one or more LDAP, uPortal and/or shibboleth groups



About future

- 1) Context
  - Demo (if it works…)
- 2) Protocols
  - WebDAV protocol
  - ACP protocol
- 3) Implementation
  - Slide WebDAV server
  - Shibboleth integration
- 4) Portal integration for management
- 5) About future

About future

- WebDAV server and ESUP Storage channel are used in many universities
- Shibboleth support is recent and not full tested at this time
- Apache Slide is not an active project
  - Worse, It Died 2 weeks ago! ☹
  - So we decided to work on WebDAV library proposed by Jackrabbit project
    - This one is ACP compliant and Store mechanisms exist
    - But, as I know, it’s only a library and not a server like Slide
    - Quota and authentication layers must be adapted

About future

- ESUP Storage Channel
  - We have a roadmap (first half of 2008) to transform it with esup-commons development framework in order to:
    - Run it as a servlet (standalone mode) and/or as JSR 168 Portlet (portal and not just uPortal mode) with the same java code
    - Have a full and flexible i18n support
    - Integrate WebDAV server administration like entering Shib evaluation rules or manage quota

Links

- ESUP-Portail
  - http://www.esup-portail.org/
  - http://sourcesup.cru.fr/projects/esup-webdav-srv/
  - http://sourcesup.cru.fr/projects/esup-stockage/
- ORI-OAI
  - http://www.ori-oai.org/
  - http://www.ori-oai.org/media/ORI-OAI%20EUNIS%20(en).pdf
  - http://www.ori-oai.org/media/EUNIS_2007.pdf

Rule example

- ESUP:shib-eval-exp property
  - eval(shibAtt.getAttributeUser("Shib-Supann-supannOrganisme","{EES}0352291A"))