

# Mise en oeuvre d'un intranet à partir de logiciels Open Source avec intégration des certificats numériques et login unique

N. Clément, F. Dal, X. Jeannin, M.T. Nguyen

**CNRS/UREC**

*<http://www.urec.cnrs.fr>*

# *Plan*

- Intranet tentative de définition
- Objectifs du projet
- Application A2C2
- Fonctionnalités développées
- Acteurs et notion de groupe de travail
- Architecture de l'application
- Module d'accès aux ressources
- Module d'administration
- Certificat et login unique
- Intégration d'applications dans A2C2
- Gestion des comptes des applications
- Synthèse sur la méthode d'intégration d'application
- Déploiement

# ***Tentative de définition d'un intranet***

- **Il existe plusieurs définitions, d'origine commerciale, de la notion d'intranet, les définitions généralement admises sont :**
  - Les communications dans l'entreprise : Intranet
  - Les communications avec les partenaires et clients : Extranet
  - Les communications avec tout le monde : Internet
  
- **Le périmètre de l'entreprise peut être difficile à définir surtout dans le cadre communauté recherche**
  
- **Les intranets et les extranets se caractérisent par le contrôle d'accès aux ressources : les données, les applications**
  
- **Le passage des applications sur le Web**
  - Les applications « groupware »
  - Les accès aux services réseau
  - Les applications métiers (Xlab, application scientifique)
  - Les applications Web sont moins performantes que les applications classiques.
  
- **Les intranets sont spécifiques à leur entreprise**

# ***Objectifs du projet***

- **Mise en place d'un outil sécurisé de communication Web**
  - Entre les membres de la direction du STIC
  - Entre la direction du STIC et les laboratoires du STIC
    - Par exemple : Intranet des directeurs du STIC
  - Entre des groupes de travail du département STIC
    - Réseaux thématiques pluridisciplinaires (RTP)
    - Réseau de technologie de base (RTB)
  
- **Objectifs**
  - Espaces coopératifs (GroupeWare)
  - Intranet sécurisé de personnes : certificats numériques
  - Usage du seul certificat pour
    - Contrôler les accès aux pages HTML et données
    - Contrôler les accès aux groupes de travail
    - Accéder aux applications de l'intranet
    - Administrer l'intranet
  
- **Pas d'outil libre et complet sur le marché**
  
- **Création d'un logiciel de gestion de groupes de travail**

# *Application A2C2*

## *Accès aux Applications Contrôlés par Certificat*

- **Besoins retenus pour un groupe de travail**
  - Partage de fichiers
  - Dépôt de pages HTML
  - Liste de diffusion (service externe sympa)
  - Intégration d'autres applications
  
- **Intranet sécurisé de personnes**
  - Usage de certificats numériques
  
- **Logiciels Libres**
  - Linux Apache Mod\_SSL PHP MySQL cURL
  - Réutilisable dans les laboratoires

# ***Fonctionnalités développées***

- **Gestion des utilisateurs**
  - Utilisation de l'annuaire des certificats
- **Gestion des groupes de travail et de sous-groupes**
- **Gestion des applications intégrées dans l'intranet et dans les groupes de travail**
  - WebCalendar, forum, liste de diffusion.
  - Application CNRS : Labintel
  - Autres
- **Login unique via le certificat**
  - Correspondance certificat / compte application Web
- **Module Application de Gestion de Fichiers**
  - Partage de données sécurisées
  - Publication de pages HTML avec gestion du contrôle d'accès
- **Module de gestion des droits d'accès**
  - Pages HTML
  - Données
  - Applications Web

# ***Acteurs et notion de groupe de travail (1)***

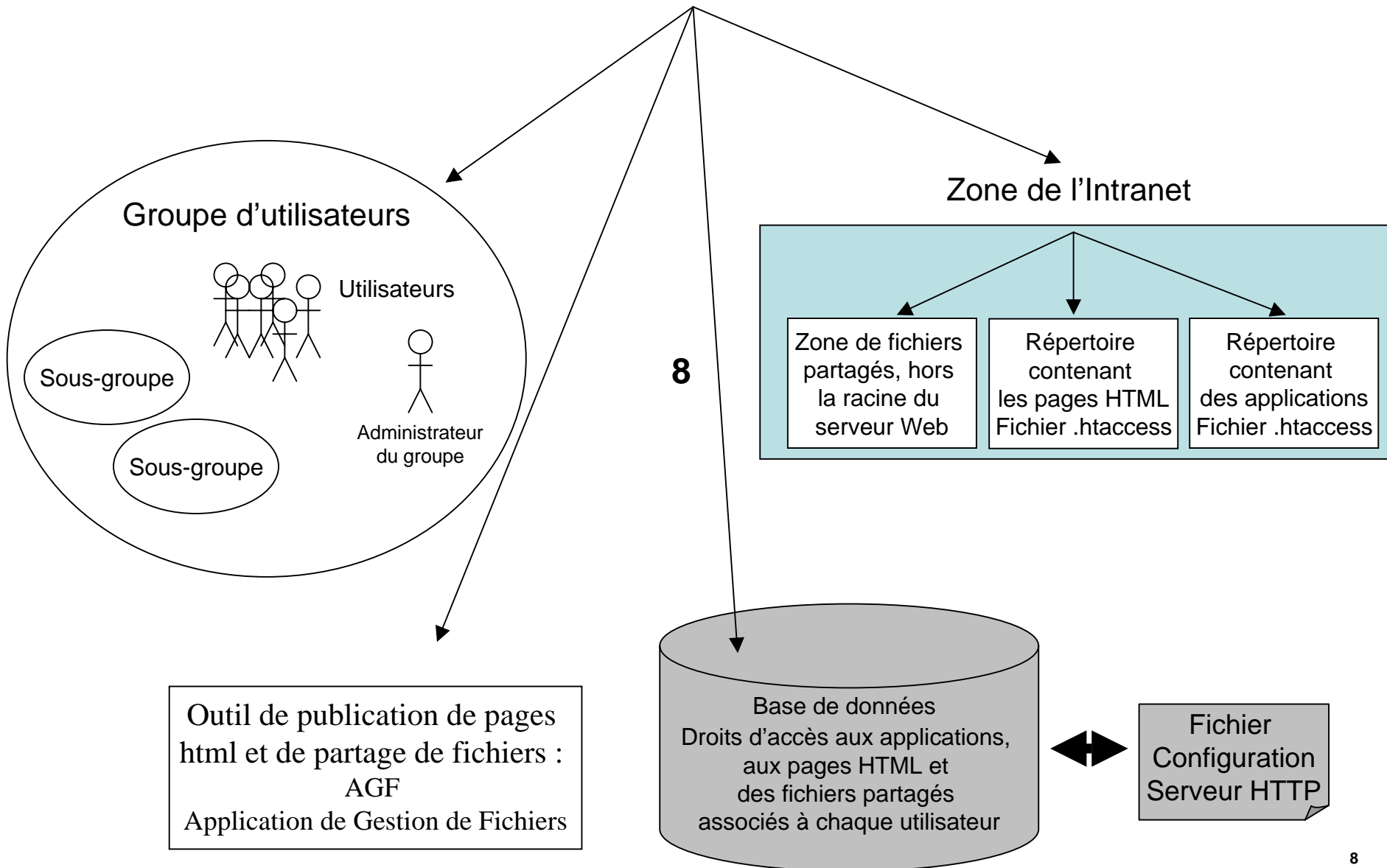
## **▪ Les acteurs**

- Super Administrateur
- Administrateur de groupe
- Utilisateur

## **▪ La notion de groupe de travail**

- Administrateur de groupe et membres du groupe
- Notion de sous-groupe
- Espace de publication HTML pour l'administrateur du groupe
- Espace de partage de fichiers pour les utilisateurs du groupe
- Intégration possible d'autres applications

## Groupe de travail





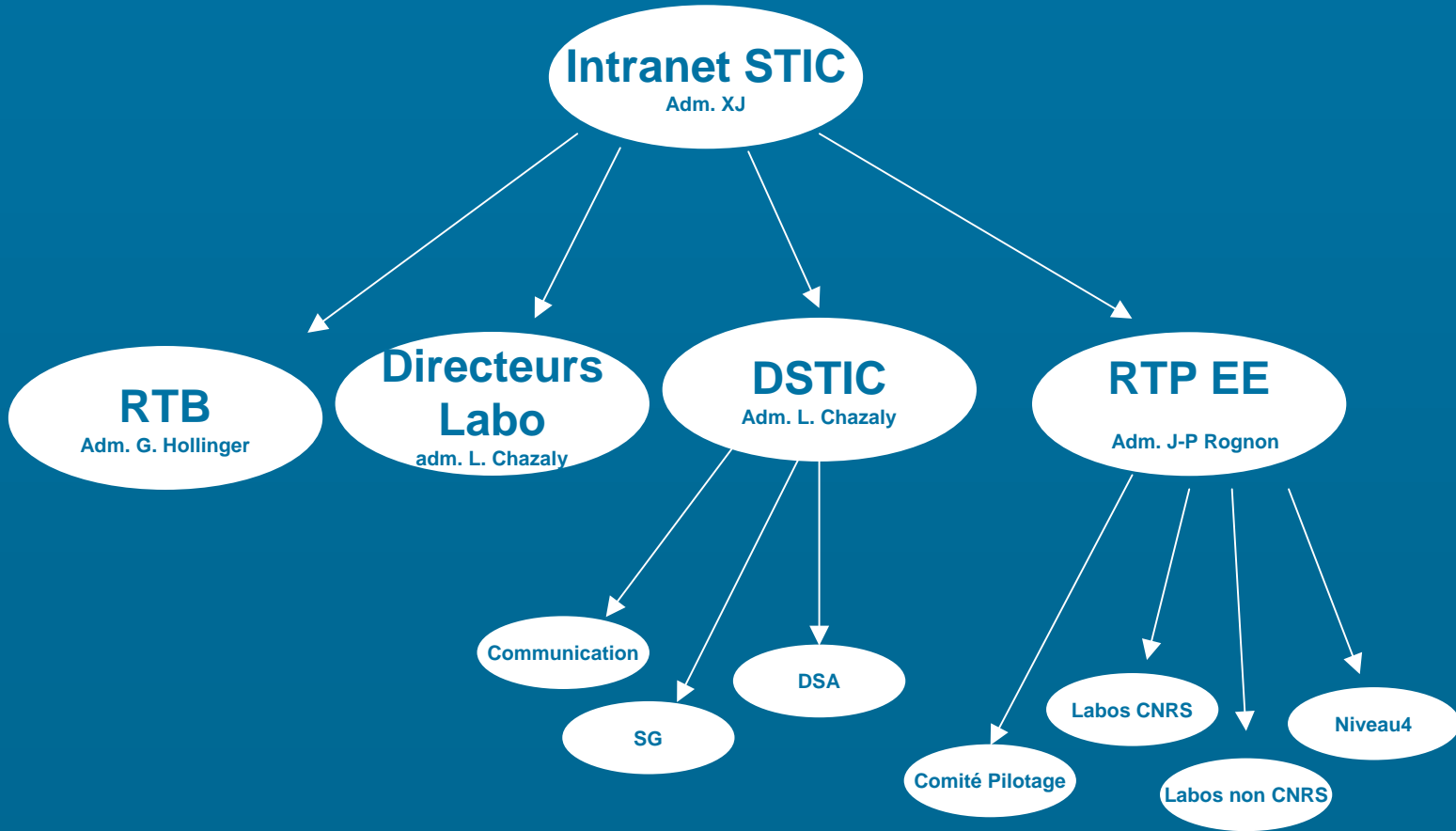
# Acteurs et notion de groupe de travail (3)

## Organisation de l'intranet STIC

Niveau Intranet

Niveau Groupe de travail

Niveau Sous-Groupe



# Acteurs et notion de groupe de travail (4) exemple RTP Energie Electrique

Bienvenue sur l'Intranet du département STIC du CNRS - Netscape

Fichier Edition Afficher Aller à Signets Outils Fenêtre Aide

https://intranet.stic.cnrs.fr/dess/intr

Le CNRS Annuaires Sites CNRS Autres sites

**Sciences et Technologies de l'Information et de la Communication**

Intranet STIC

**Fichiers partagés**

**Applications**

Labintel  
WebCalendar


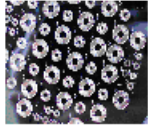
**Paramètres personnels**


**Administration Groupe**


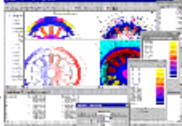
**Utilisateur connecté :**  
Xavier Jeannin

**Groupe actuel :**  
RTP Energie Electrique  
**Rôle actuel :**  
Administrateur Groupe  
[Changer groupe / rôle]

INTRANET RTP Energie Electrique

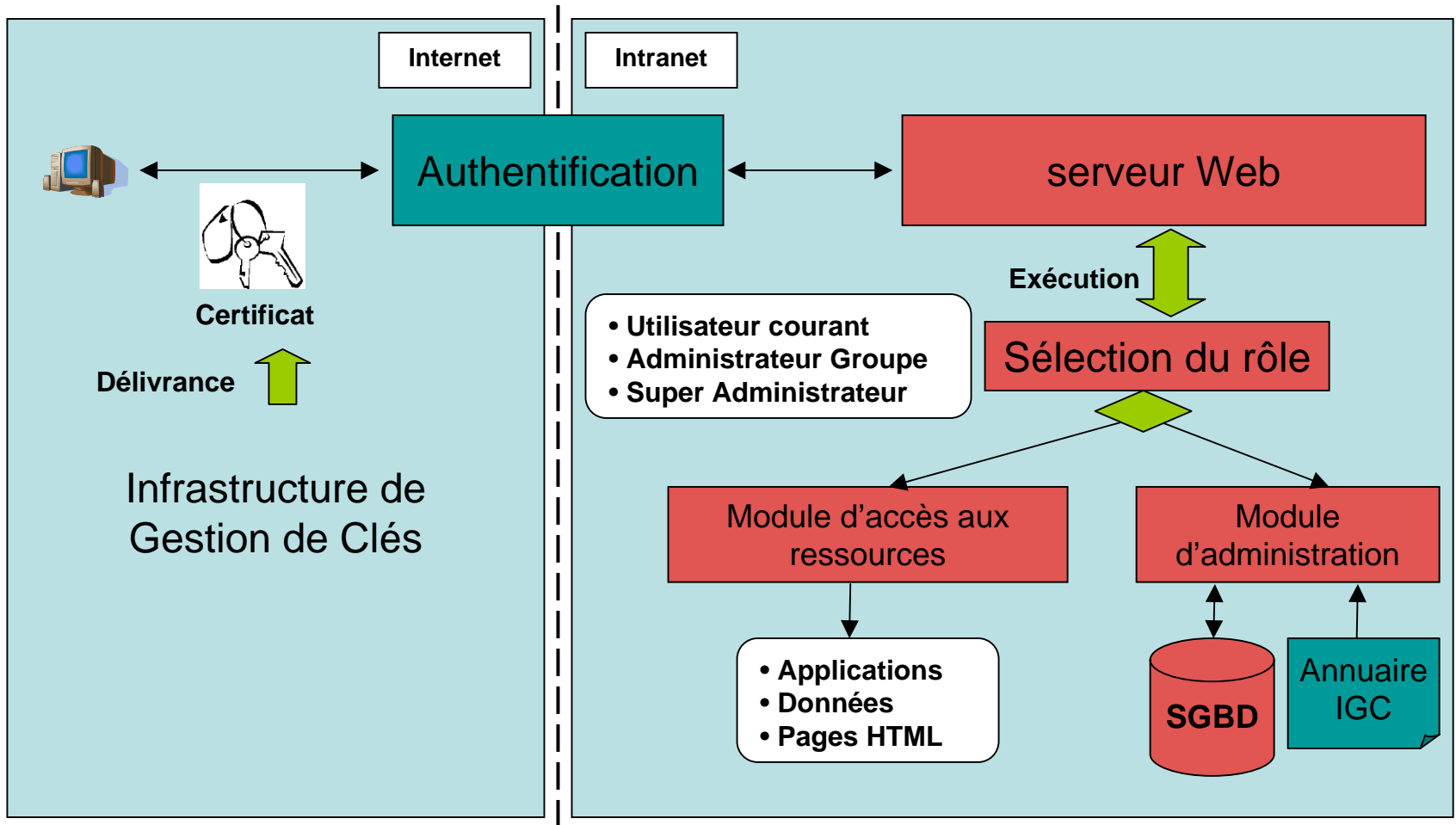
Vie du RTP  Vie des projets 

Vie des Laboratoires 

Propositions des laboratoires  Evaluations des propositions 

Document : Terminé (0.381 s)

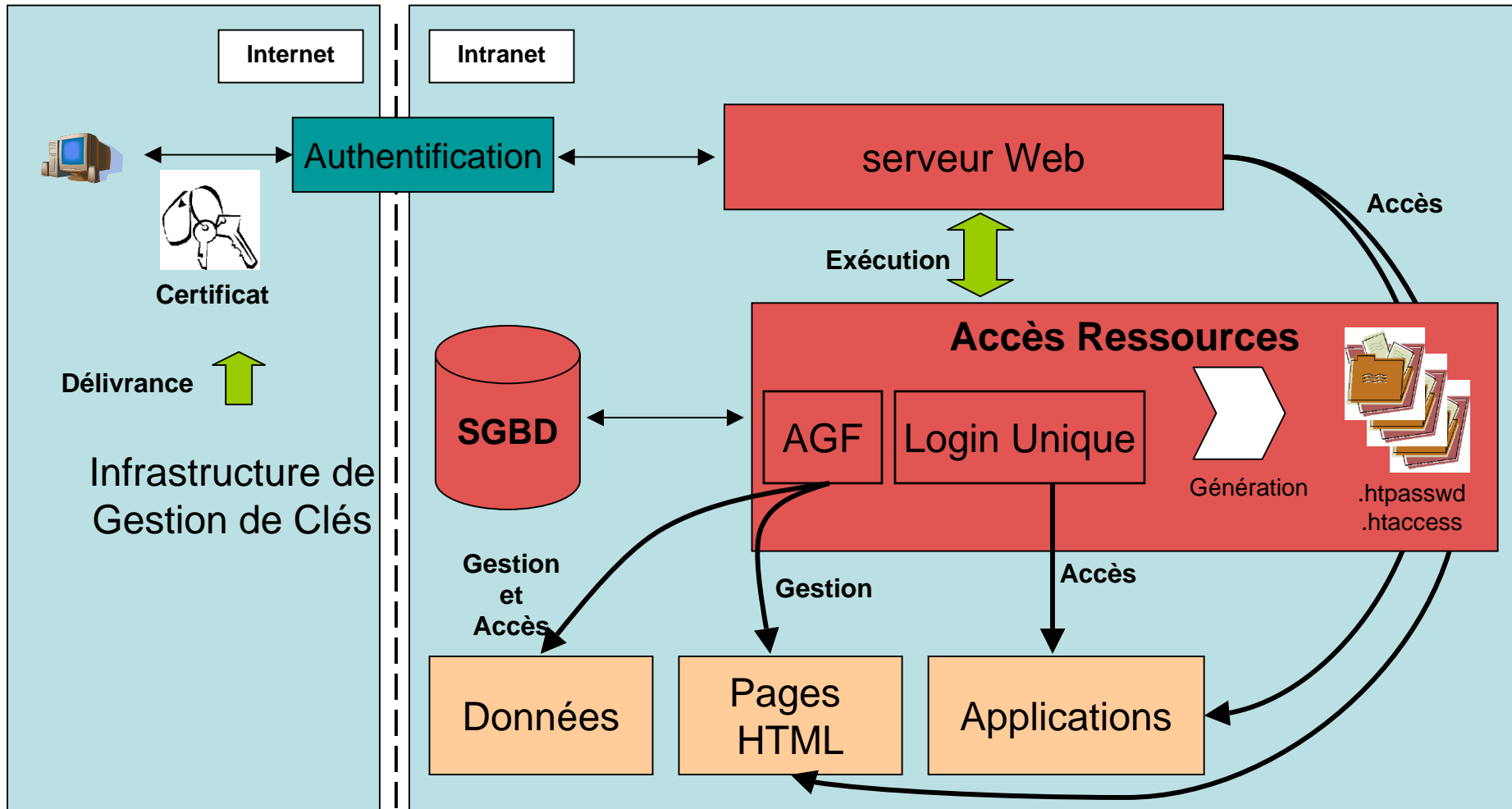
# Architecture de l'application



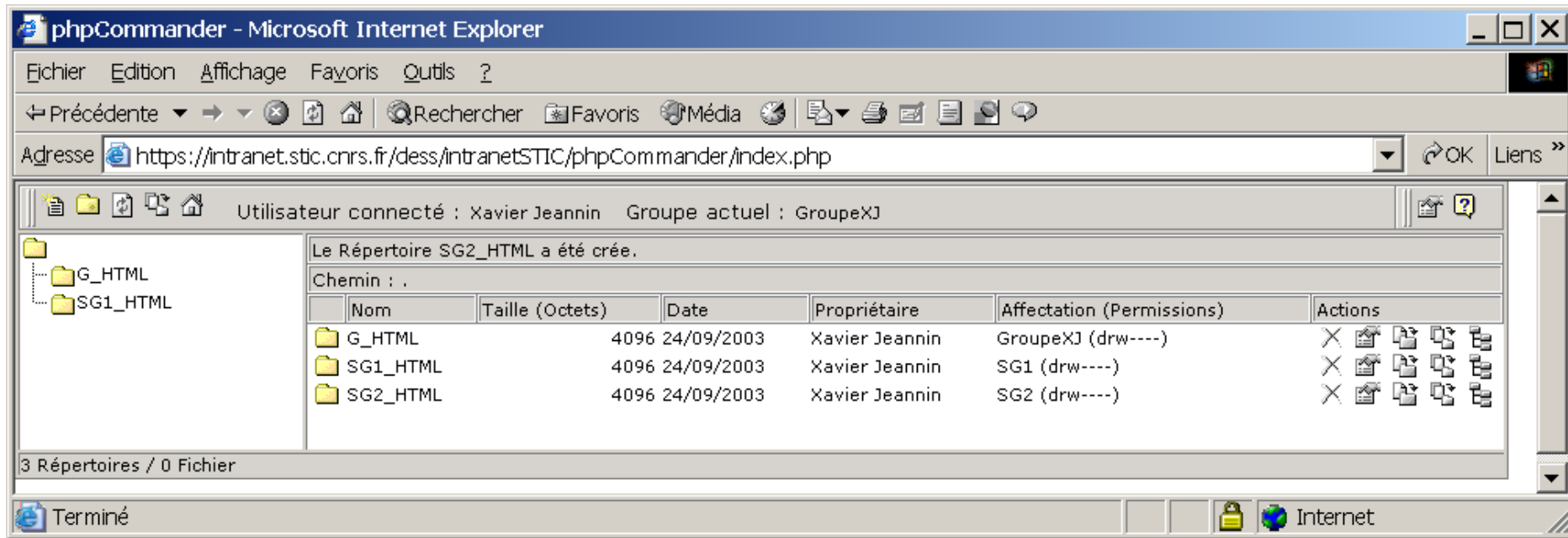
# ***Module d'accès aux ressources (1)***

- **Module de gestion automatique des accès aux ressources de l'intranet**
  - Utilisation de fichiers htaccess et de faux fichiers passwd incorporant le DN du certificat comme identifiant
  - Notion de groupe et de sous-groupe
  - Délégation d'administration
  
- **Modification d'un logiciel de partage de données : module AGF (Application de Gestion de Fichiers)**
  - Accès aux fichiers données
  - Hors de l'arborescence du serveur Web
  
- **Intégration d'applications avec utilisation des certificats comme login**

# Module d'accès aux ressources (2)



## Le module AGF publication Html



phpCommander - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

← Précédente → Recherche Favoris Média

Adresse <https://intranet.stic.cnrs.fr/dess/intranetSTIC/phpCommander/index.php> OK Liens »

Utilisateur connecté : Xavier Jeannin Groupe actuel : GroupeXJ

Le Répertoire SG2\_HTML a été créé.

Chemin : .

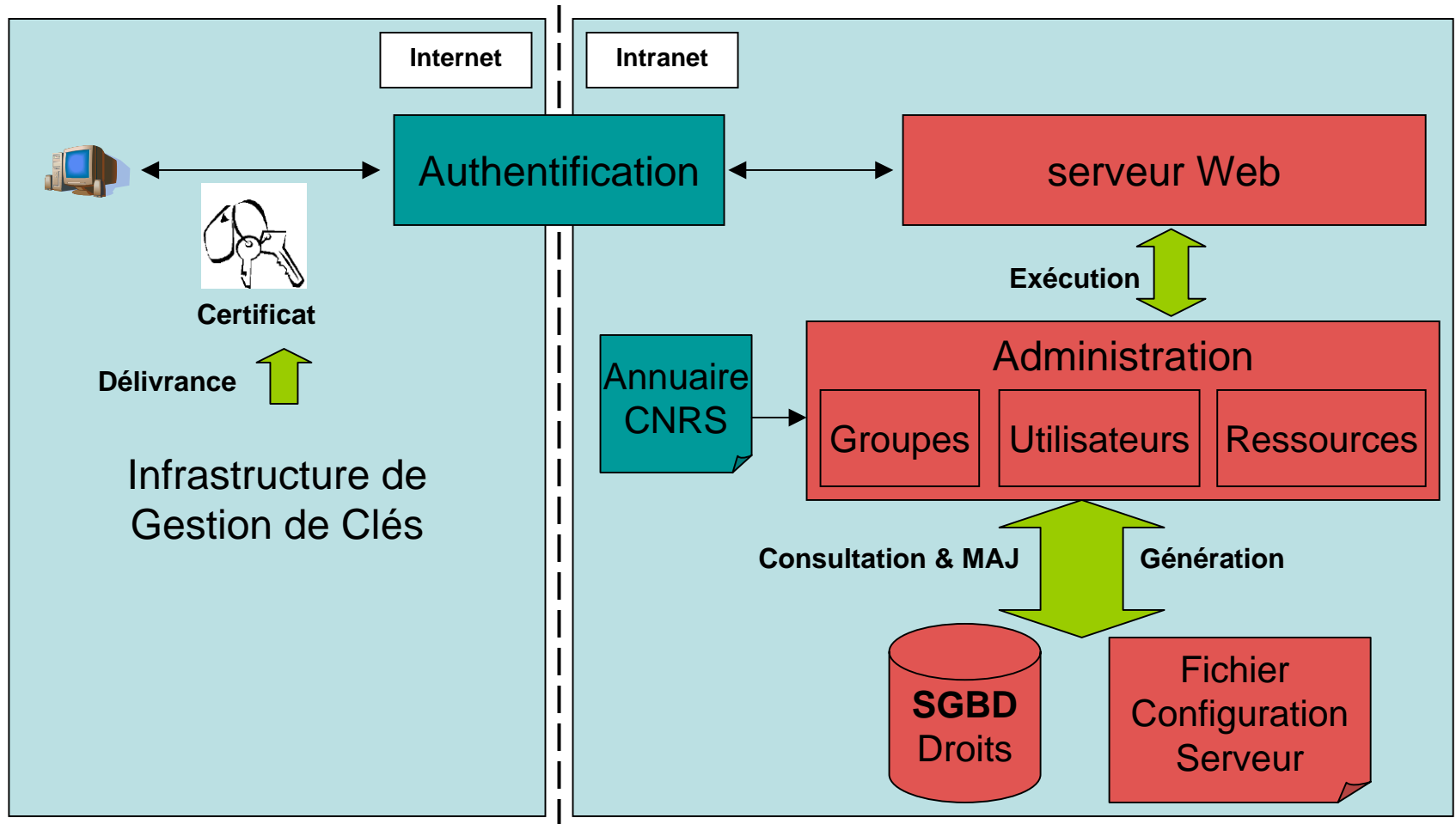
Nom	Taille (Octets)	Date	Propriétaire	Affectation (Permissions)	Actions
G_HTML	4096	24/09/2003	Xavier Jeannin	GroupeXJ (drw----)	✕ 📁 📄 📄 📄
SG1_HTML	4096	24/09/2003	Xavier Jeannin	SG1 (drw----)	✕ 📁 📄 📄 📄
SG2_HTML	4096	24/09/2003	Xavier Jeannin	SG2 (drw----)	✕ 📁 📄 📄 📄

3 Répertoires / 0 Fichier

Terminé

Internet

# Module d'administration (1)



# Module d'administration (2)


## Gestion des utilisateurs

Bienvenue sur l'intranet du département STIC du CNRS - Microsoft Internet Explorer

Echier Edition Affichage Favoris Outils ?

← Précédente → Recherche Favoris Média

Adresse <https://intranet.stic.cnrs.fr/dess/intranetSTIC/template/listeUtilisateurIntranet.php?selectedM> OK Liens »



CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Le CNRS Annuaires Sites CNRS Autres sites

**Sciences et Technologies de l'Information et de la Communication**






**Intranet STIC**

- Fichiers partagés
- Informations personnelles
- Administration Intranet**
  - Gestion Utilisateur Intranet
  - Gestion Groupe Intranet
  - Gestion Application Intranet
  - Gestion Application Groupe
  - Visualisation LOG

**Liste des utilisateurs de l'intranet :**

[Afficher le\(s\) 4 utilisateur\(s\) de l'intranet](#)

[A](#) - [B](#) - [C](#) - [D](#) - [E](#) - [F](#) - [G](#) - [H](#) - [I](#) - [J](#) - [K](#) - [L](#) - [M](#) - [N](#) - [O](#) - [P](#) - [Q](#) - [R](#) - [S](#) - [T](#) - [U](#) - [V](#) - [W](#) - [X](#) - [Y](#) - [Z](#) - [Autres](#)

Prénom Nom ▲	Mail	Statut	Actions
<b>Florence Dal</b>	florence.dal@urec.cnrs.fr	actif	
Minh-Tung Nguyen	minh-tung.nguyen@urec.cnrs.fr	actif	 
<b>Nicolas Clement</b>	nicolas.clement@urec.cnrs.fr	actif	
<b>Xavier Jeannin</b>	Xavier.Jeannin@urec.cnrs.fr	actif	

[\[Nouvel utilisateur\]](#) [\[Retour\]](#)

Internet



# Sélection et gestion des utilisateurs



CENTRE NATIONAL  
DE LA RECHERCHE  
SCIENTIFIQUE

[Le CNRS](#) | [Annuaire](#) | [Sites CNRS](#) | [Autres sites](#)

Sciences et Technologies de l'Information et de la Communication

*Intranet STIC*

Fichiers partagés

Informations personnelles

Administration Intranet

Gestion Utilisateur Intranet

Gestion Groupe Intranet

Gestion Application Intranet

Gestion Application Groupe

Visualisation LOG

**Utilisateur connecté :**  
*Florence Dai*

**Groupe actuel :**  
*IntranetSTIC*

**Rôle actuel :**  
*Super Administrateur*  
[Changer groupe / rôle]

### Sélection de l'accès aux groupes

*Vous êtes membre des groupes et sous groupes suivants, veuillez sélectionner **un groupe** pour accéder à l'ensemble de ses ressources :*

Groupe de travail	Sous Groupe	Accéder en tant que
<b>IntranetSTIC</b> (défaut)		[Super Admin] [Utilisateur]
Direction		[Utilisateur]
Equipe Grenoble		[Utilisateur]
	Stagiaires	
Projet Alexandria		[Admin] [Utilisateur]
	Developpeurs	
	Test	
Projet Intranet		[Utilisateur]
ProjetFutur		[Admin] [Utilisateur]
	Sauvegarde	

# *Certificat et login Unique (1)*

## ■ Principe

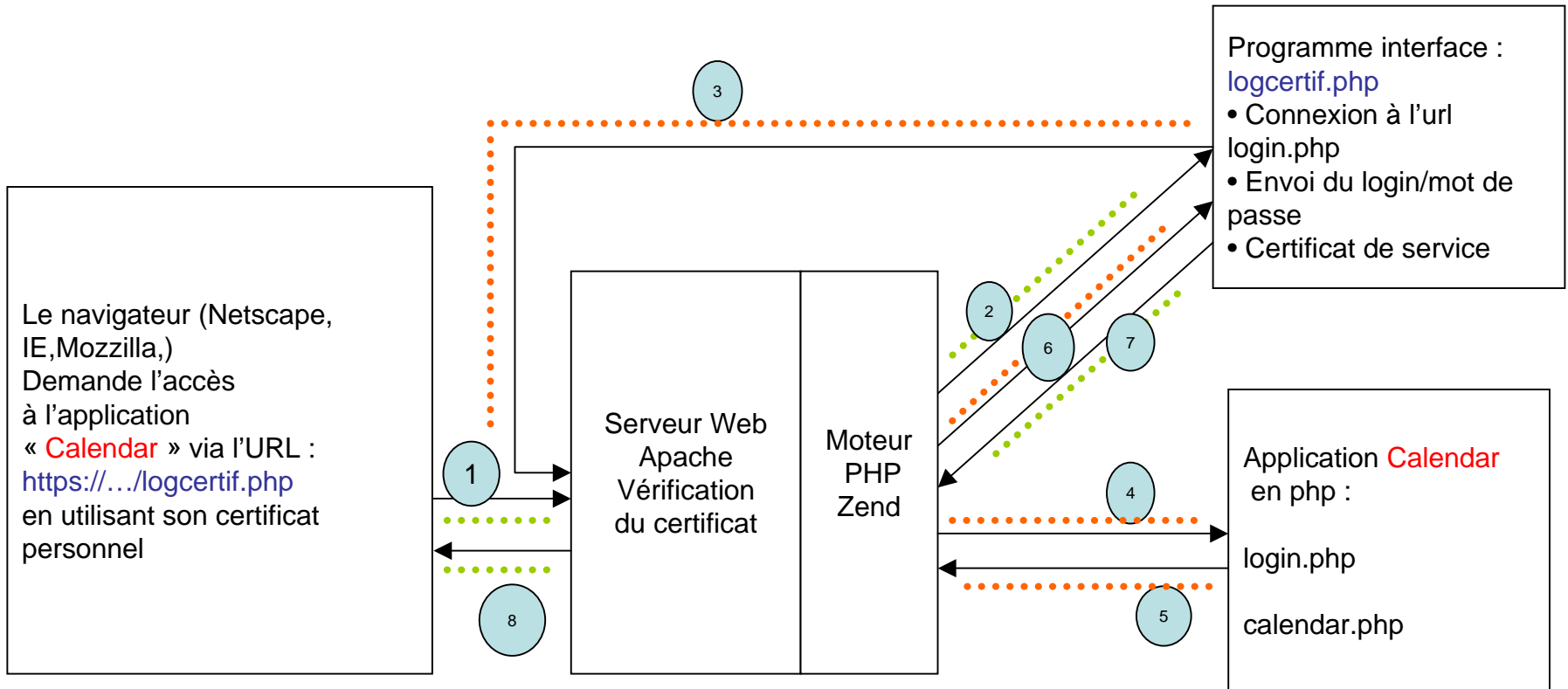
- Postage des arguments des formulaires HTML de connexion de l'application (bibliothèque cURL)

## ■ Caractéristiques

- Méthode simple mais limitée
- Nécessite un programme d'interface
  - Utilisation d'un certificat de « service »
- Possibilité de se connecter à des applications externes (Labintel)
- Non applicable à certaines applications
- Pas de modification de l'application
  - Pas de maintenance des applications ajoutées
  - Double gestion de bases de comptes utilisateurs
- Transmission des paramètres de la session applicative
  - cookie

# Certificat et login Unique (2)

## Connexion à une application Web



Méthode de « Postage » des paramètres

# *Intégration d'applications dans A2C2 (1)*

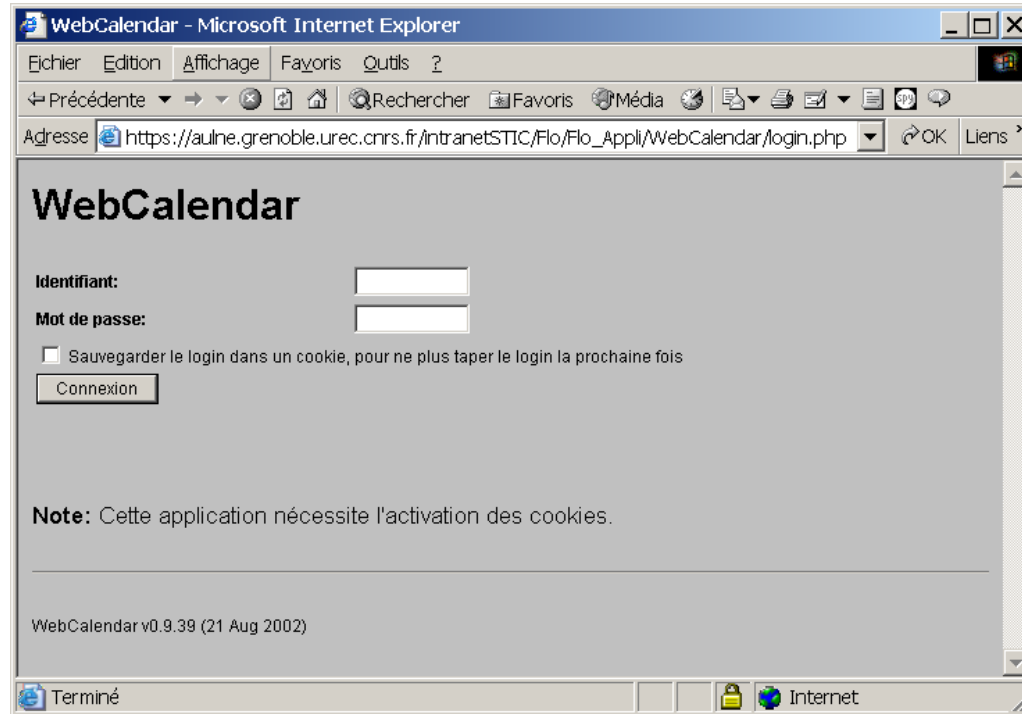
- **Principe de l'intégration**
  - Au niveau des groupes de travail
  - Utilisation du modèle pour créer le programme d'interface spécifique à l'application
  - Délégation de la gestion de l'application à l'administrateur de Groupe
- **Étapes de l'intégration**
  - Dans l'intranet
    - Le super administrateur intègre l'application dans A2C2 (étape manuelle)
    - Le super administrateur crée le programme d'interface (étape manuelle)
  - Dans un groupe
    - Le super administrateur installe l'application pour le groupe de travail (étape manuelle)
    - L'administrateur de groupe prépare les comptes pour les utilisateurs du groupe

## *Intégration d'applications dans A2C2 (2)*

# ***Type d'applications intégrables***

- **Les applications intégrables sans modification**
  - CGI-BIN / Mod\_Perl
  - PHP
  - Java théoriquement oui mais non testées
- **Les applications qui acceptent les certificats s'intègrent par simple lien hypertexte (Sympa)**
- **Possibilité de se connecter à des applications externes (Labintel) de manière limitée**
- **Limitations**
  - Les applications qui contrôlent la correspondance entre numéro IP et Session
  - Les applications qui utilisent des cookies comprenant l'adresse IP du client de manière chiffrée (cookies « non rejouables »)
  - Les applications (externes) situées hors de votre domaine DNS (RFC 2109)

# Exemple d'intégration d'une application dans l'intranet : WebCalendar



Méthode de « Postage » des paramètres

# Récupération des paramètres de connexion

- Il faut repérer dans le code de cette page HTML la partie entre les balises <FORM> et </FORM> :

```

<FORM NAME="login_form" ACTION="login.php" METHOD="POST" ONSUBMIT="return
valid_form(this)">
<TABLE BORDER=0>
<TR><TD><B>Identifiant:</B></TD>
  <TD><INPUT NAME="login" SIZE=10 VALUE="" TABINDEX="1"></TD></TR>
<TR><TD><B>Mot de passe:</B></TD>
  <TD><INPUT NAME="password" TYPE="password" SIZE=10 TABINDEX="2"></TD></TR>
<TR><TD COLSPAN=2><INPUT TYPE="checkbox" NAME="remember" VALUE="yes" >
Sauvegarder le login dans un cookie, pour ne plus taper le login la prochaine fois</TD></TR>
<TR><TD COLSPAN=2><INPUT TYPE="submit" VALUE="Connexion"
TABINDEX="3"></TD></TR>
</TABLE>
</FORM>

```

## Intégration d'une application dans l'intranet

Intégration d'une application dans l'Intranet STIC - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

← Précédente → Recherche Favoris Média

Adresse <https://intranet.stic.cnrs.fr/dess/intranetSTIC/template/integrerApplicationIntranet.php?select> OK Liens »

**Administration Intranet**

- Gestion Utilisateur Intranet
- Gestion Groupe Intranet
- Gestion Application Intranet
- Gestion Application Groupe
- Visualisation LOG

---

**Utilisateur connecté :**  
Xavier Jeannin

**Groupe actuel :**  
IntranetSTIC  
**Rôle actuel :**  
Super Administrateur  
[Changer groupe / rôle]

Avant de remplir ce formulaire, vous devez avoir installer manuellement l'application dans l'Intranet.  
Ce formulaire termine la procédure d'insertion d'une application dans l'Intranet.

Pour plus d'informations sur l'installation manuelle cliquer [ici](#)

---

Nom de l'application \* :

Version de l'application \* :  (ex : 0.1.0)

Nom du répertoire des fichiers \* :

Nom du fichier de connexion \* :

Nom du fichier de connexion login unique :

Version du dernier patch :  (ex : 0.1.0)

Date du dernier patch :  (jj/mm/aaaa)

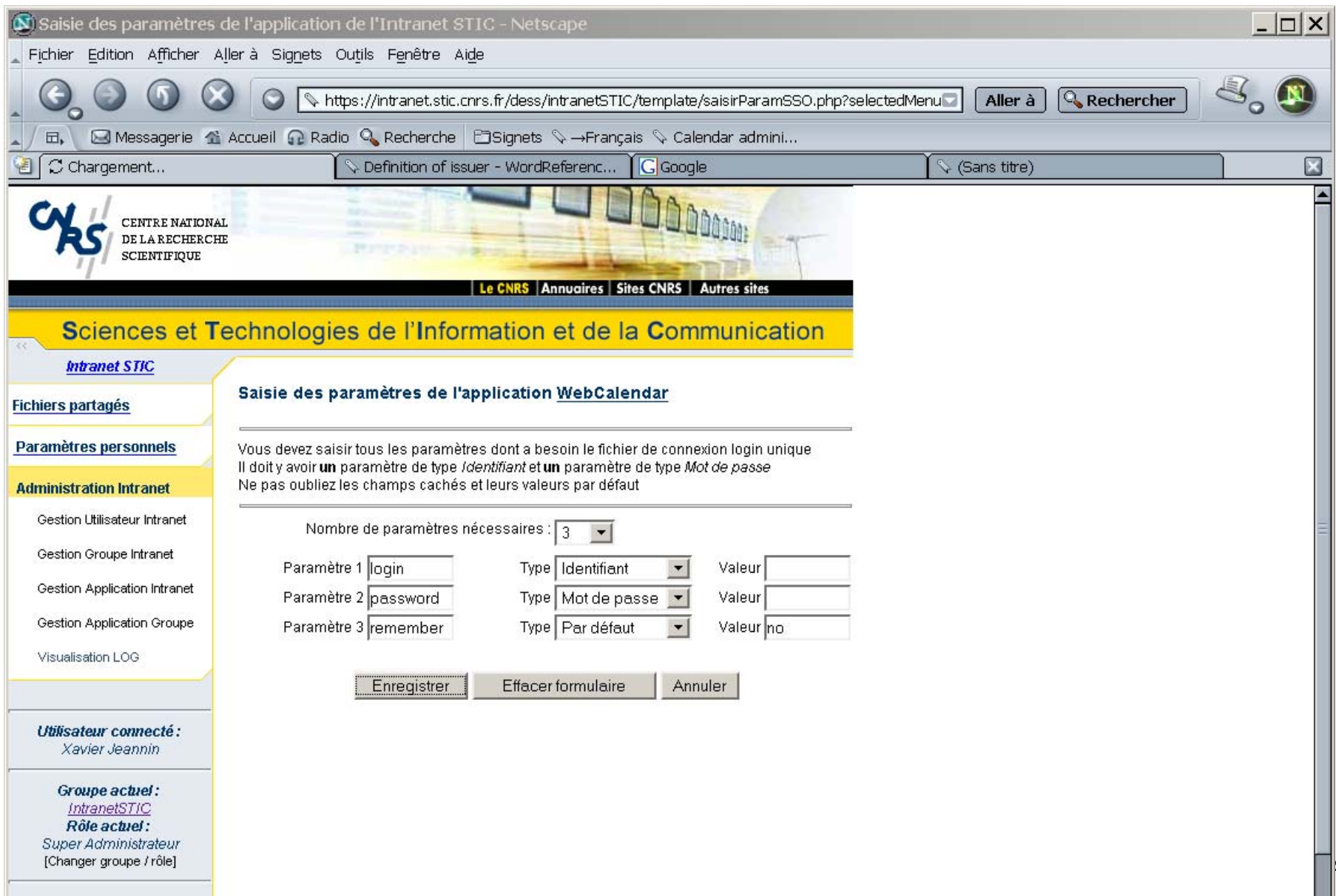
\* : champs obligatoires

Terminé Internet



# Intégration d'applications dans A2C2 (7)

## Saisie des paramètres à « Poster »



Saisie des paramètres de l'application de l'Intranet STIC - Netscape

https://intranet.stic.cnrs.fr/dess/intranetSTIC/template/saisirParamSSO.php?selectedMenu

Le CNRS | Annuaires | Sites CNRS | Autres sites

Sciences et Technologies de l'Information et de la Communication

[Intranet STIC](#)

**Fichiers partagés**

**Paramètres personnels**

**Administration Intranet**

- Gestion Utilisateur Intranet
- Gestion Groupe Intranet
- Gestion Application Intranet
- Gestion Application Groupe
- Visualisation LOG

**Utilisateur connecté :**  
Xavier Jeannin

**Groupe actuel :**  
IntranetSTIC

**Rôle actuel :**  
Super Administrateur  
[Changer groupe / rôle]

### Saisie des paramètres de l'application WebCalendar

Vous devez saisir tous les paramètres dont a besoin le fichier de connexion login unique  
Il doit y avoir **un** paramètre de type *Identifiant* et **un** paramètre de type *Mot de passe*  
Ne pas oublier les champs cachés et leurs valeurs par défaut

Nombre de paramètres nécessaires : 3

Paramètre 1	<input type="text" value="login"/>	Type	Identifiant	Valeur	<input type="text"/>
Paramètre 2	<input type="text" value="password"/>	Type	Mot de passe	Valeur	<input type="text"/>
Paramètre 3	<input type="text" value="remember"/>	Type	Par défaut	Valeur	no

Enregistrer    Effacer formulaire    Annuler

# ***Gestion des comptes des applications***

- **Les applications sont accessibles via l'ancienne procédure de login**
  - Les utilisateurs ne doivent pas accéder au compte d'un autre utilisateur du groupe
  - Dans certains cas, l'administrateur de groupe ne doit pas connaître le mot de passe d'un utilisateur
  
- **Les mots de passe sont chiffrés dans la base de données, mais**
  - A2C2 est obligé de les manipuler en clair à un moment.
  - Impossibilité de cacher les mots de passe au super administrateur
  
- **Gestion des mots de passe**
  - Les utilisateurs ne gèrent pas leur mot de passe
  - Les utilisateurs gèrent leur mot de passe
  
- **Les utilisateurs et l'administrateur de groupe ne voient jamais l'ancien mot de passe lors d'une modification**

# *Synthèse sur la méthode d'intégration d'application (1)*

- Permet l'intégration d'applications d'origines diverses
- Pas de modification de l'application
- Solution simple à mettre en place
- **Limitations**
  - Les applications qui contrôlent la correspondance entre numéro IP et Session
  - Les applications qui utilisent des cookies comprenant l'adresse IP du client de manière chiffrée (cookies « non rejouables »)
  - Les applications (externes) situées dans votre domaine DNS
- **A2C2 permet un login unique « local »**

# *Synthèse sur la méthode d'intégration d'application (2)*

- **Gestion complexe et lourde des bases de comptes pour chaque application**
- **Ecriture du programme logcertif.php**
- **Méthode transitoire en attendant**
  - de véritables solutions de SSO
  - l'adaptation des applications aux certificats
  - la mise en place d'infrastructure de gestion de privilèges

# *Déploiement*

- **Projet en phase pilote**
  - intranet Urec, Intranet STIC
  - 6 applications interconnectées
  - Tutos, WebCalendar (Php), WebCalendar (CGI/BIN ModPerl), Php2BB (avec modification), SquirrelMail, Labintel
  - Les limites du programme inconnues
  
- **A2C2 prévu pour des groupes de travail de 250 personnes maximum**
  
- **Open Source et diffusable**
  
- **Autres développements possibles suite au retour d'expérience**

***Questions ?***