

DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG

PROJET PORTAIL SIPG

Référence Agence : P3.PORTAIL.L4_Description_Integration_Portail_au_SIPG_v0.2.doc

Identifiant Agence : J:\EFG\Portail\Livrables\Phase 3\P3.PORTAIL.L4 - Description de l'intégration de l'application au SIPG\P3.PORTAIL.L4_Description_Integration_Portail_au_SIPG_v0.2.doc

Date d'impression : 08/09/10 11:09

Édition : 0

Révision : 2

État de validation : A valider

Rédaction :

Validation :

Liste de diffusion			
Agence :			
Christophe Valade	V		
Daouda Ndiaye	V		
Dominique Chambéry	O		
Cyril Jacquet	I		
Les chefs de projets de l'Agence	I		

A = mise en Application, O = Observations, I = Information – diffusion, V = Validation

Suivi des Mises à Jour

Mises à jour			
<i>Version</i>	<i>Date</i>	<i>Auteur</i>	<i>Objet de la mise à jour</i>
0.1			Version initiale
0.2	12/04/2007		Intégration des remarques de l'Agence

DSI	Portail SIPG	Émetteur :
		Date d'édition : 08/09/2010
	DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG	Version 0.2

Sommaire

1	VUE D'ENSEMBLE.....	3
2	LE PORTAIL DU SIPG ET LES APPLICATIONS DU SIPG	4
2.1	Lien du portail vers une application du SIPG	4
2.2	Lien de l'application vers le portail.....	7
2.3	Création de contenus dans le portail par les applications	7
2.3.1	Principe général	7
2.3.2	Format d'échange d'une news.....	8
2.3.3	Format d'échange d'un message	9
3	LE PORTAIL DU SIPG ET S&A.....	12
3.1	Lien de S&A vers le portail	12
3.2	Lien du portail vers S&A.....	13

DSI	Portail SIPG	Émetteur :
		Date d'édition : 08/09/2010
	DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG	Version 0.2

1 Vue d'ensemble

Le schéma qui suit, situe le portail dans le SIPG. Il fait apparaître l'intégration du portail dans les sous-ensembles du système d'information :

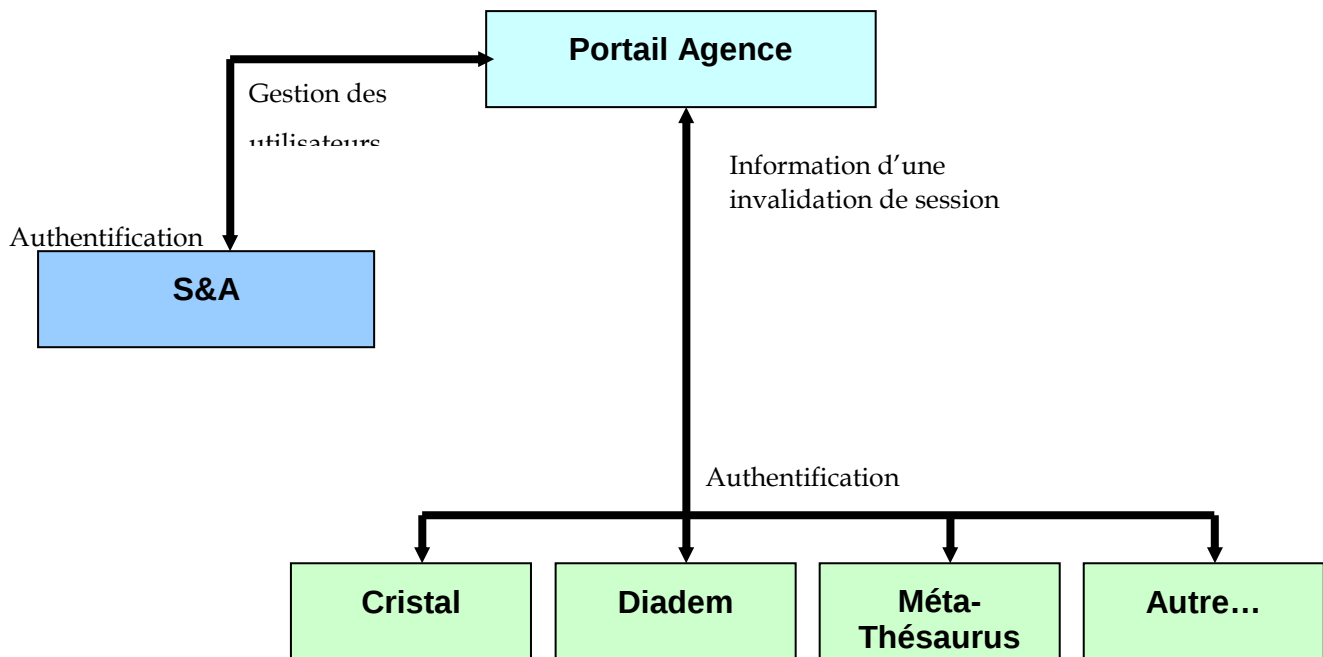


Figure 1

- **Le Portail du SIPG**, point d'entrée sécurisé du SIPG pour de nombreux acteurs.
- **Cristal**, système de gestion de greffes d'organes.
- **Diadem**, outil de recueil national des données concernant les patients dialysés du projet REIN.
- **Structures et Autorisations**, référentiel des structures de prélèvement et de greffe.
- **Le Méta-Thésaurus**, référentiel de concepts médicaux relatifs au prélèvement et à la greffe.
- **Les autres applications du SIPG**, existantes ou futures

DSI	Portail SIPG	Émetteur :
		Date d'édition : 08/09/2010
	DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG	Version 0.2

2 *Le Portail du SIPG et les applications du SIPG*

Le portail de l'Agence est lié à chaque application à laquelle il donne accès. Cette liaison est une liaison dans les deux sens.

2.1 **Lien du portail vers une application du SIPG**

Le but du portail Agence est de permettre un accès à toutes les applications du SIPG via une authentification unique. Le portail inter-agit donc avec les applications pour négocier une session pour chaque utilisateur demandant un accès.

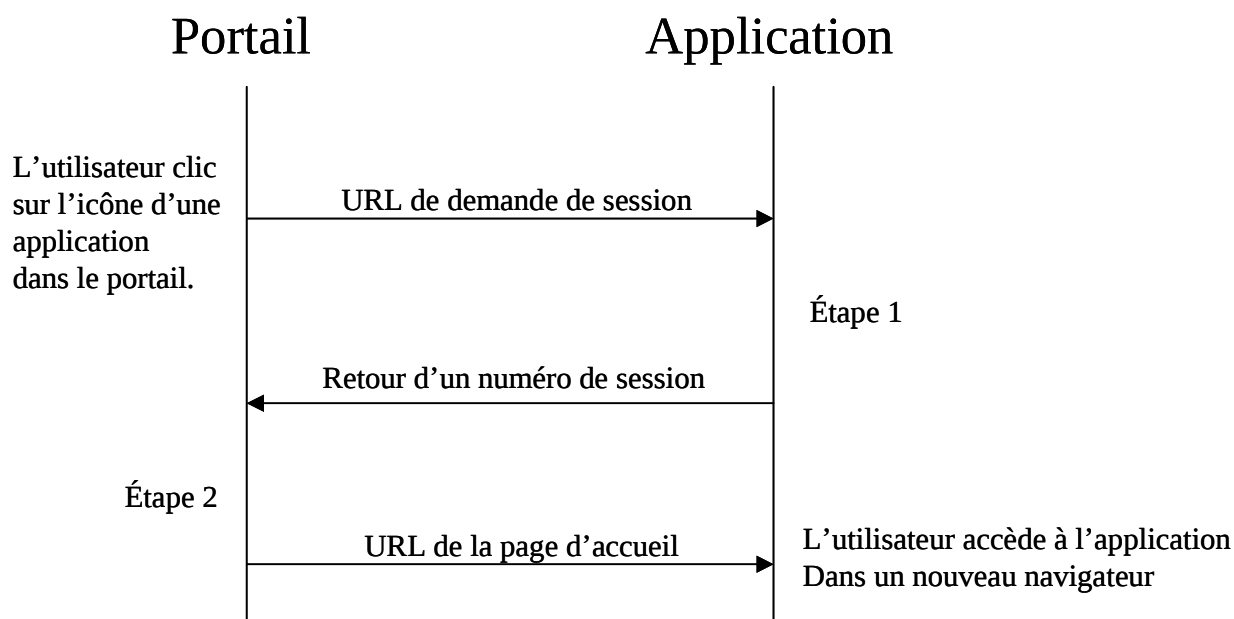
Chaque application disposant d'un mécanisme d'authentification unique possède trois URL :

- l'URL de demande de session ;
- l'URL d'accès (page d'accueil) ;
- l'URL de déconnexion.

Contenu	Catégories	Droits de consultation	Droits de modification	Workflow	Avancé
* Titre S&A					
* Code SA					
Description Ceci est l'application S&A. Il s'agit du référentiel de l'Agence de la biomédecine					
 Icône					
Visuel					
Documentation					
URL de demande de session					
* URL d'accès					
URL de déconnexion					

Figure 2

Ces trois URL sont renseignées pour chaque application dans le portail. Lorsqu'un utilisateur clique sur l'une d'entre elle dans celui-ci, le mécanisme suivant s'opère :



Le portail accède donc aux deux premières URL d'une application lorsque l'utilisateur y accède pour la première fois. Le numéro de session négocié est alors stocké pour chaque utilisateur et pour chaque application, afin de ne pas avoir à renégocier celui-ci si la session ; le portail n'accède alors qu'à l'URL de la page d'accueil dans ce cas.

La troisième URL, celle de déconnexion est appelée lorsque l'utilisateur se déconnecte du portail ou lorsque la session de celui-ci a expirée.

Pour les applications qui ne possèdent pas ce mécanisme d'authentification unique, une seule URL est appelée, l'URL d'accès.

L'URL de demande de session attend trois paramètres :

- **UPP_ID** : l'identifiant de l'utilisateur. Cet identifiant est stocké dans S&A, il correspond à la partie numérique de l'identifiant JCMS du membre.
- **TIMESTAMP** : un timestamp du moment exact de la demande, au format timestamp SQL
- **HASH** : un hash de type MD5 de la chaîne de caractère composé de la concaténation stricte du login du membre, de son mot de passe et du même timestamp que celui fourni dans la paramètre précédent.

L'application fournit en retour une page HTML simple avec comme corps :

```
<body>jsessionid=XXX;</body>
```

ou XXX est le code de session négocié ou -1 en cas d'erreur.

Une fois la session négociée, l'application s'affiche dans une pop-up, cette pop-up est en fait composée d'un code permettant de gérer l'audience et d'une « i-frame » occupant

DSI	Portail SIPG	Émetteur :
		Date d'édition : 08/09/2010
	DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG	Version 0.2

toute la fenêtre et affichant l'application cible. Cette pop-up n'est pas bloquée par les bloqueurs de pop-up à la date de rédaction du document.

2.2 Lien de l'application vers le portail

Le lien entre les applications du SIPG et le portail concerne la gestion de l'expiration des sessions de ces applications.

Lorsqu'une application invalide la session d'un utilisateur, le portail doit en être informé afin qu'il puisse renégocier une session avec celle-ci si l'utilisateur clique sur l'application dans le portail.

Aussi, à chaque fois qu'une session d'une application expire, celle-ci doit appeler l'URL d'invalidation d'une session du portail. Ce mécanisme existait sur la précédente version du portail, il a été repris de façon identique dans la refonte, aussi aucune application n'a besoin d'être modifiée, seul le paramètre désignant l'URL de l'ancien portail doit être mis à jour.

Ce paramètre se configure pour la plupart des applications du SIPG dans le fichier web.xml de l'application web. Exemple pour S&A :

```
<init-param>
  <param-name>efg.session.notification.url</param-name>
  <param-value>http://uranus/portail/custom/sipg/applicationSession/kill.jsp</param-value>
</init-param>
```

L'URL à renseigner pour toutes les applications est <http://uranus/portail/custom/sipg/applicationSession/kill.jsp>

Cette URL accepte un paramètre : **ID_VAL**, qui doit contenir le numéro de session à invalider

2.3 Création de contenus dans le portail par les applications

2.3.1 Principe général

Le portail donne la possibilité à une application externe de créer des contenus dans celui-ci en utilisant un fichier d'échange de type XML.

Pour cela il est configuré pour « écouter » un répertoire donné. Tout fichier possédant l'extension XML déposé dans ce répertoire sera intégré dans le portail. Le mécanisme d'import utilise trois répertoires donnés :

- Un répertoire d'écoute ;
- Un répertoire dans lequel seront déplacés les fichiers XML importés correctement ;
- Un répertoire dans lequel seront déplacés les fichiers XML qui n'ont pu être importés correctement.

DSI	Portail SIPG	Émetteur :
		Date d'édition : 08/09/2010
	DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG	Version 0.2

De plus en cas d'erreur, le log de JCMS possède des informations sur le problème survenu.

Ces trois répertoires sont différents pour chaque type de contenu « importable ». Il y a à l'heure actuelle deux types de contenus importables, les news et les messages. Les répertoires de gestion de l'import se paramètrent dans le fichier de paramétrage de JCMS webapp.prop. Viennent s'ajouter deux autres paramètres, le premier permet d'activer ou de désactiver l'import tandis que le second définit dans un format de type « crontab » la fréquence d'écoute du répertoire.

Exemple de ces cinq paramètres pour les news :

```
import.news.actif: 1
import.news.schedule: * * * * *
import.news.dossierSource: C:/importXML/news/src
import.news.dossierTraite: C:/importXML/news/traite
import.news.dossierErreur: C:/importXML/news/erreur
```

2.3.2 Format d'échange d'une news

Le format XML attendu pour une news est le suivant :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PPP_NWS>
  <NWS_ROW>
    <NWS_TIT>le titre de la première news</NWS_TIT>
    <!-- =====
           date de publication format YYYYMMDD HH24:MI:SS
           ===== -->
    <NWS_DAT>20020325 15:24:12</NWS_DAT>
    <NWS_RES>le résumé de la news</NWS_RES>
    <NWS_MES>le corps de la news qui peut être
              au format html</NWS_MES>
    <!-- =====
           Les échéances possibles (calcul du délai d'expiration)
           dans ECH_KEY, la valeur dans ECH_VAL
           - 0 : en secondes
           - 1 : en minutes
           - 2 : en heures
           - 3 : EN JOURS
           - 4 : en semaines
           - 5 : en mois
           - 6 : en années
           - dans l'exemple le délai est exprimé en jours et vaut 1
```

```

===== -->
<ECH_KEY value="3">
  <ECH_VAL>1</ECH_VAL>
</ECH_KEY>
<!-- =====
      Les destinataires possibles dans DST_KEY, les valeurs
dans DST_VAL
      - 0 : tout le monde
      - 2 : Utilisateurs (le login JCMS)
      - 4 : Groupes (l'identifiant JCMS du groupe)
      - 5 : Applications (le code de l'application)
      - dans l'exemple on cible une liste d'utilisateurs
===== -->
<DST_KEY value="2">
  <DST_VAL>dfleury</DST_VAL>
  <DST_VAL>omercier</DST_VAL>
  <DST_VAL>mtettekpoe</DST_VAL>
</DST_KEY>
</NWS_ROW>
<NWS_ROW>
<NWS_TIT>le titre de la deuxième news</NWS_TIT>
<NWS_DAT>20020325 15:24:14</NWS_DAT>
<NWS_RES>le résumé de la seconde news</NWS_RES>
<NWS_MES>le corps de la seconde news qui peut être
      également au format html</NWS_MES>
<ECH_KEY value="3">
  <ECH_VAL>1</ECH_VAL>
</ECH_KEY>
<DST_KEY value="4">
  <DST_VAL>c_1234</DST_VAL>
</DST_KEY>
</NWS_ROW>
</PPP_NWS>

```

2.3.3 Format d'échange d'un message

Le format XML attendu pour un message est le suivant :

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<PPP_DOC>

```

```

<DOC_ROW>
<!-- =====
        l'identifiant de l'émetteur
        ===== -->
<DOC_EME>aguyon</DOC_EME>
<!-- =====
        le nom du fichier sur disque
        ===== -->
<DOC_NAM>fichier.txt</DOC_NAM>
<!-- =====
        le mime type du fichier, les + courants :
        - text/plain
        - application/msword (extension .doc)
        - application/vnd.ms-excel (extension .xls)
        - application/octet-stream (divers exe, dll, ini...)
        - application/x-zip-compressed (zip)
        - image/jpeg (jpeg, jpg)
        ===== -->
<DOC_MTP>text/plain</DOC_MTP>
<!-- =====
        le titre du document vu par l'utilisateur
        ===== -->
<DOC_TIT>le titre du document vu par
        l'utilisateur connecté</DOC_TIT>
<!-- =====
        date de publication format YYYYMMDD HH24:MI:SS
        ===== -->
<DOC_DAT>20020325 15:24:12</DOC_DAT>
<!-- =====
        Les échéances possibles (calcul du délai d'expiration)
dans ECH_KEY, la valeur dans ECH_VAL
        - 0 : en secondes
        - 1 : en minutes
        - 2 : en heures
        - 3 : en jours
        - 4 : en semaines
        - 5 : en mois
        - 6 : en années

```

```

- dans l'exemple le délai est exprimé en jours et vaut 1
===== -->
<ECH_KEY value="3">
  <ECH_VAL>1</ECH_VAL>
</ECH_KEY>
<!-- =====
      Les destinataires possibles dans DST_KEY, les valeurs
dans DST_VAL
      - 0 : tout le monde
      - 2 : Utilisateurs (le login JCMS)
      - 4 : Groupes (l'identifiant JCMS du groupe)
      - 5 : Applications (le code de l'application)
      - dans l'exemple on cible une liste d'utilisateurs
===== -->
<DST_KEY VALUE="2">
  <DST_VAL>dfleury</DST_VAL>
  <DST_VAL>omercier</DST_VAL>
  <DST_VAL>mtettekpoe</DST_VAL>
</DST_KEY>
</DOC_ROW>
<DOC_ROW>
<DOC_EME>dfleury</DOC_EME>
<DOC_NAM>fichier2.txt</DOC_NAM>
<DOC_MTP>text/plain</DOC_MTP>
<DOC_TIT>le titre du second document vu par
      l'utilisateur connecté</DOC_TIT>
<DOC_DAT>20020325 15:24:12</DOC_DAT>
<ECH_KEY value="3">
  <ECH_VAL>1</ECH_VAL>
</ECH_KEY>
<DST_KEY value="4">
  <DST_VAL>c_1234</DST_VAL>
</DST_KEY>
</DOC_ROW>
</PPP_DOC>

```

3 Le Portail du SIPG et S&A

Le portail est lié à l'application S&A d'une part selon le processus décrit dans la section précédente (S&A étant avant tout une application comme une autre du SIPG), et d'autre part d'une façon plus spécifique pour tout ce qui concerne la gestion des utilisateurs du portail.

Il faut bien noter que ces échanges ne concerne pas l'authentification même des utilisateurs ; la vérification de la concordance login/mot de passe ou du numéro de carte CPS est faite uniquement dans le portail.

3.1 Lien de S&A vers le portail

Le portail demande des informations à S&A à deux moments dans la gestion des utilisateurs :

- Création d'un nouvel utilisateur : lors de la création d'un nouvel utilisateur sur le portail, celui-ci doit déjà être référencé dans S&A via un code Agent. Connaissant ce code Agent, le portail va récupérer depuis S&A un certain nombre d'informations comme le nom, le prénom ou l'email de l'utilisateur.
- Génération du courrier du login ou du mot de passe : deux URL sont disponibles dans le portail pour générer des courriers. Ces courriers récupèrent des informations sur le membre pour leur envoi (nom, adresse...) ; ces informations sont synchronisées depuis S&A pour chaque génération afin d'avoir systématiquement la bonne adresse ou le bon nom.

La table de correspondance entre les données S&A (toutes issue de la table SA_ACTEUR) et celles de JCMS est la suivante :

Champ de SA_ACTEUR	Champ JCMS	Commentaire
CODE	Code S&A	Code agence à renseigner pour la création d'un utilisateur
NOM	Nom	
PRENOM	Prénom	
COMP_ADRESSE ADRESSE DISTRIBUTION CODE_POSTAL	Adresse	Ces champs sont regroupés au moyen d'une procédure dédiée (cf. procédure SA_PKG_UTIL.FCSA_ACT_ADRESSE) afin de renseigner le champ « adresse du portail »

NOM_COMMUNE		
COURRIEL	E-mail	
TIT_ID_CIVIL	Civilité	Le code (numérique) présent dans la code est « traduit » à partir de la table SA_TITRE
TIT_ID_TITRE	Fonction	Le code (numérique) présent dans la code est « traduit » à partir de la table SA_TITRE
UPP_ID	Id JCMS	Correspond à l'id JCMS, privé de son préfixe (ou URId). Ex : k_2115 devient 2115
LOGIN	login	
PASSWORD	password	Le mot de passe crypté.
SI_UTI_VALIDE		1 si le membre est activé, 0 s'il est désactivé.

Le champ UPP_ID doit par ailleurs être unique (un seul utilisateur pour un seul identifiant) : dans le cas contraire, une exception SQL sera levée lors d'opérations sur les membres concernés.

3.2 Lien du portail vers S&A

Le portail est amené à mettre les informations de S&A lors de différents processus :

- Changement du mot de passe : lorsque l'administrateur via les interfaces d'administration ou lorsque l'utilisateur change son mot de passe (après expiration ou via le formulaire mis à disposition de tout le monde sur le portail), le nouveau mot de passe est envoyé à S&A.
- Changement d'accès à une application : il est possible dans le portail de donner ou d'enlever à un utilisateur l'accès à une application ; il faut pour cela le rajouter ou l'enlever du groupe de l'application. Cette opération est notifiée à S&A afin que l'application sache exactement à quelles applications un utilisateur donné a accès.
- Désactivation / suppression d'un utilisateur : lorsqu'un utilisateur est désactivé ou supprimé du portail, celui-ci ne doit plus pouvoir s'authentifier aux applications, même en mode dégradé (sans passer par le portail), aussi l'utilisateur est également désactivé dans S&A.

DSI	Portail SIPG	Émetteur :
		Date d'édition : 08/09/2010
	DESCRIPTION DE L'INTEGRATION DU PORTAIL AU SIPG	Version 0.2

Les packages S&A utilisés par le portail sont :

Procédure ou fonction	Utilisation par le portail
FCSA_ACT_ADRESSE	Renvoie l'adresse d'un membre ; cette fonction est utilisée pour vérifier l'adresse de l'acteur avant l'envoi de courriers.
FCSA_ENCRYPT	Crypte un mot de passe en vue de son insertion dans la base.
FCSA_DECRYPT	Décrypte un mot de passe récupéré depuis la base.

Les tables impactées par cette interface sont :

Table	Utilisation par le portail
SA_ACTEUR	Contient les informations concernant les membres du portail. Les colonnes UPP_ID, LOGIN, PASSWORD et SI_UTI_VALIDE sont modifiées par le portail.
SA_TITRE	Permet de réaliser la correspondance entre les titres et les codes numériques leur correspondant, tels qu'ils sont stockés dans la table SA_ACTEUR. Cette table n'est pas modifiée par le portail.
SA_UTI_APP	Contient les autorisations d'accès aux applications. Les autorisations sont stockées sous la forme d'une ligne, les trois colonnes étant APP_ID (l'id de l'application concernée), ETAT (non utilisée) et ACT_ID (l'id de l'acteur, correspondant au champ du même nom de la table SA_ACTEUR et distinct du champ UPP_ID) Lors de l'ajout ou du retrait d'une autorisation, la ligne correspondante est ajoutée ou supprimée.

	Ces lignes doivent par ailleurs être uniques : une exception SQL sera levée dans le cas contraire, dans le cadre d'opérations sur le membre et l'application concernés.
SA_APPLICATION	Contient la liste des applications, avec notamment leur code (information stockée par le portail) et leur id (information utilisée dans la table SA_UTI_APP). Cette table n'est pas modifiée par le portail.