



Date de rédaction :	20/01/2017	Projet : Annexes CCTP Sous projet : Gestion des identités et des habilitations
Auteur :	B.Bérard	
Référence :	SSI\17\0015\BB\VB	

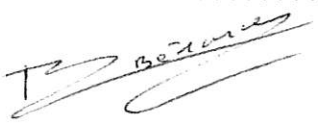

Direction du Système d'Information  
Et de l'Informatique

Annexes CCTP  
Gestion des identités et des habilitations  
V 1.0

Commentaires :

Diffusion :  
Leaders DSII

SIGNATURES

Rédacteur B. BERARD	Validation	Visa Directeur DSII PH. CASTETS
		

## GESTION DES IDENTITES ET DES HABILITATIONS

### VERSION 1.0

#### 1. CONTEXTE

Au sein d'un système d'information, un acteur peut avoir besoin d'utiliser différents identifiants en fonction des contraintes locales.

Afin de réduire les risques de doublons, de maîtriser les processus d'entrée et sortie et de gestion des habilitations, les Hospices Civils de Lyon ont déployé un annuaire central d'identités adossé à l'annuaire des ressources humaines.

Les objectifs sont la mise en conformité avec les réglementations, la protection et la traçabilité des attributions d'accès aux applications critiques, en réduisant les coûts de gestion de la sécurité.

Le présent document a pour objet de décrire les mécanismes en place et faciliter l'intégration de nouvelles applications.

La description (paragraphe 2), sous forme d'annexe à destination des fournisseurs est à intégrer aux CCTP. L'expression de besoin générique (paragraphe 3) est à adapter en fonction du cahier des charges.

#### 2. GESTION DES IDENTITES ET DES HABILITATIONS

Se reporter à l'ANNEXE – Mécanismes de gestion des identités et des habilitations

#### 3. EXPRESSION DE BESOIN GNERIQUE

Le candidat décrira avec précision les moyens, adaptés à l'environnement HCL, qu'il mettra en œuvre afin d'automatiser la gestion des habilitations dans son application.

L'ensemble des actions réalisées, de façon manuelle ou automatique devront faire l'objet de la production de journaux horodatés permettant d'identifier l'origine du mouvement, les modifications apportées (état avant/après) et le compte utilisé.

Le candidat intégrera à son offre :

- une solution opérationnelle d'alimentation automatique des comptes et des habilitations, intégrée aux outils de gestion des identités des HCL ;
- les prestations d'assistance à la mise en œuvre :
  - o l'installation ;
  - o le transfert de compétence auprès des équipes HCL ;
  - o l'assistance au paramétrage des composants ;
  - o le développement des composants spécifiques éventuellement nécessaires (dans la cas par exemple d'une interface d'alimentation qui n'utiliserait pas Active Directory) ;
- les documentations d'installation, d'administration et d'exploitation de sa solution.

## ANNEXE

### Mécanismes de gestion des identités et des habilitations

Au sein d'un Système d'Information, un acteur peut avoir besoin d'utiliser différents identifiants en fonction des contraintes locales.

Afin de réduire les risques de doublons, de maîtriser les processus d'entrée et sortie et de gestion des habilitations, les Hospices Civils de Lyon ont déployé un annuaire central d'identité adossé à l'annuaire des ressources humaines.

Les objectifs sont la mise en conformité avec les réglementations, la protection et la traçabilité des attributions d'accès aux applications critiques, en réduisant les coûts de gestion de la sécurité.

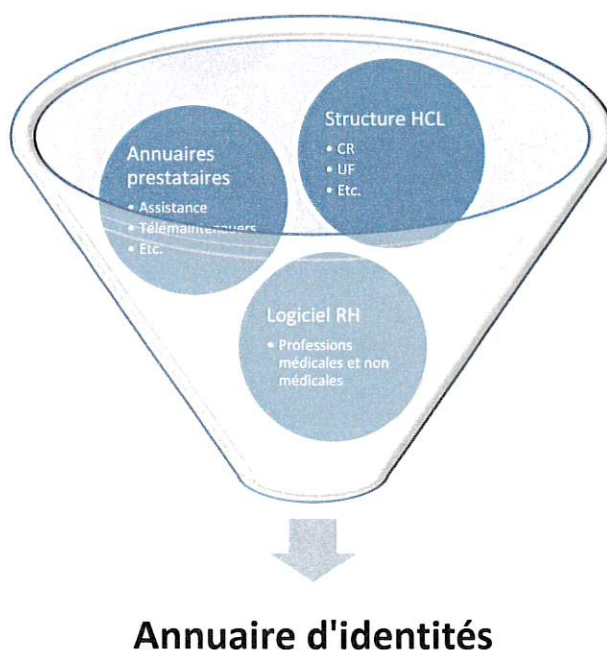
L'outillage mis en œuvre est constitué :

- d'un annuaire central d'identités;
- d'une solution de synchronisation des différents référentiels (alimentation 'amont') ;
- d'un moteur d'habilitations (alimentation 'aval').

L'annuaire d'identités centralise :

- les données d'identités des personnes (professionnels salariés, prestataires, étudiants, etc.) qu'ils soient employés ou non par l'établissement ;
- les données de structure organisationnelle des HCL : établissements, centres de responsabilités, unités fonctionnelles, etc ;
- les composantes applicatives du Système d'Information ;
- les habilitations primaires des personnes : accès aux applications (et le cas échéant des droits fins dans ces applications si une gestion centralisée est possible).

Les connecteurs d'alimentation amont mettent à jour les identités et structures contenues dans l'annuaire à partir des informations contenues dans les référentiels d'identités, de structures, d'emploi, etc.



Les connecteurs d'alimentation aval alimentent les applications du SIH à partir :

- de matrices de droits applicatifs basés sur les rôles et affectations ;
- de droits discrétionnaires.

Ils propagent :

- les comptes applicatifs, par création, modification, désactivation ou suppression de comptes applicatifs, de paramètres de comptes, d'identifiants et de mots de passe ;
- les habilitations par l'affectation ou le retrait de droits et profils applicatifs.

Les cibles sont :

- MS Active Directory ;
- les applications du système d'information (bases d'habilitations locales).

Les interfaces techniques d'alimentation utilisent :

- des connecteurs de type LDAP (Active Directory, AD LDS, OpenLDAP ...) ;
- des appels à des webservices ;
- des connecteurs bases de données (SQL Server, Oracle ...) ;
- des fichiers pivots d'alimentation ;
- des appels à des scripts d'alimentation.

Les méthodes minimales requises au niveau des applications sont:

- lister l'ensemble des comptes applicatifs (avec les propriétés des comptes et les droits/habilitations des comptes) ;
- créer les comptes applicatifs et leurs associer des droits/habilitations ;
- modifier les comptes applicatifs et les droits/habilitations associés ;
- supprimer/désactiver les comptes applicatifs.



Les HCL ont retenu la solution de gestions des identités et des habilitations de l'éditeur Avencis.