

Référence : à définir	Version : <b>1.0</b>	Date : 05/01/2013
<p><b>Projet AMALFI</b></p> <p><b>TC3.31b.1.15</b></p> <p><b>Spécifications détaillées de la sécurisation des accès pour les utilisateurs externes (IA, SSL...)</b></p>		

Historique des versions			
Version	Création	Description des évolutions	Auteur(s)
1.0	10/10/2008	Création du document	RWI

Historique du processus de validation			
Diffusion	Date de diffusion	Etape de la validation	Date
Version 1.0	10/10/2008		

## **Table des matières**

<b>1. INTRODUCTION</b>	<b>3</b>
1.1. Avant propos	3
1.2. Références documentaires	3
<b>2. GENERALITE SUR LE CHOIX DE MISE EN PLACE DU MECANISME DE CONTROLE D'ACCES</b>	<b>4</b>
<b>3. CONTROLE D'ACCES – IDENTIFICATION UTILISATEUR</b>	<b>5</b>
<b>4. CONTROLE D'ACCES – VALIDATION DE LA CIBLE DEMANDEE</b>	<b>9</b>
<b>5. CONTROLE D'ACCES – COMPLEMENTS DE SECURITE <i>REVERSE PROXY</i></b>	<b>11</b>
<b>6. DETAILS DES OPERATIONS SUR LA GESTION DES UTILISATEURS ET DE LA CONFIGURATION DU CONTROLE D'ACCES</b>	<b>12</b>
6.1. Création des utilisateurs, gestion des Profils	13
<b>7. ELEMENTS D'IMPLEMENTATION ET SCHEMAS DE SYNTHESE</b>	<b>15</b>
7.1. Communication entre les deux composants TAM WebSeal – Policy Server	16
7.2. Communications entre les deux composants TAM WebSeal et LDAP	20
7.3. Communications entre les composants TAM WebSeal, Websphere et LDAP	23
7.4. Communication entre les composants TAM Policy Serveur, Websphere et LDAP	26
<b>8. DISPONIBILITE ET REDONDANCE DES FONCTIONS DU CONTROLE D'ACCES</b>	<b>29</b>
<b>9. CHOIX DU CERTIFICAT SERVEUR DU WEBSEAL SSEE</b>	<b>30</b>
<b>10. ANNEXES- INFORMATIONS SUR LE SCHEMA D'ANNUAIRE</b>	<b>31</b>
10.1. Modèle de données pour AMALFI	32

---

## **1. Introduction**

---

### **1.1. Avant propos**

---

Ce document décrit l'infrastructure de connexion, d'identification et de sécurisation des utilisateurs externes dans le sous-système d'échange avec l'extérieur SSEE.

### **1.2. Références documentaires**

---

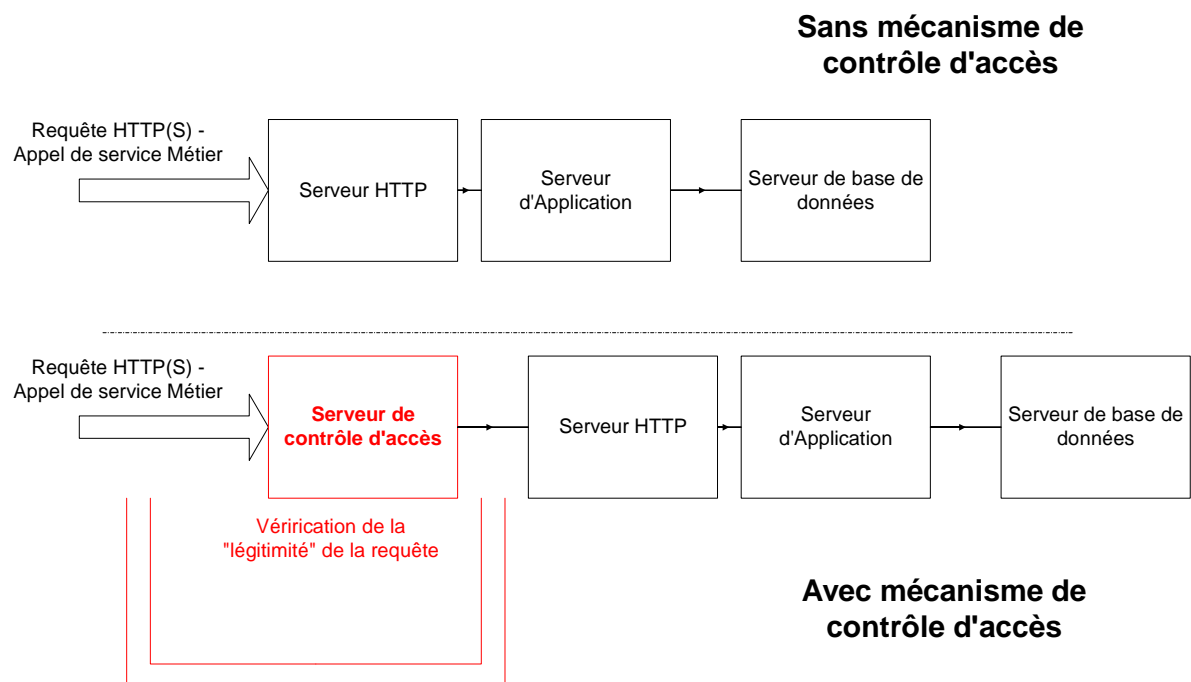
Le tableau ci-après donne la liste des documents de références qui ont permis de traiter la problématique d'architecture. Il indique également les documents qui peuvent être impactés par ce dossier (et cela de façon cohérente par rapport au schéma de la DVSL).

Référence	Date / Version	Resp.	Titre / Sujet / Remarque
TC3.31b.1.3	Version 3.0 Juin 2008	IBM	Spécifications techniques détaillées sous-ensemble fonctionnel
TC3.31b.1.1	Version 2.0 Juillet 2008	IBM	Etude d'Architecture - Conception général
TC3.31b.1.14	Version 3.0 Octobre 2008	IBM	Sécurité - Spécification détaillées - Infrastructure Technique
TC3.31b.1.3 Communication SSEE-SC	Version 2.0 Janvier 2008	IBM	Infrastructure de la communication applicative SSEE-SC
Archi fonctionnelle IAH SSEE	Version 2.0 Octobre 2008	IBM	Architecture fonctionnelle du sous-système IAH pour Identification, Authentification et Habilitation des utilisateurs AMALFI v2 SSEE.

## 2. Généralité sur le choix de mise en place du mécanisme de contrôle d'accès

La délimitation en zones de l'architecture et la possibilité offerte par les technologies choisies pour le projet (système J2EE, N-tiers) permettent d'envisager un renforcement de la sécurité des éléments sensibles de la solution en mettant en place des mécanismes, très amont, de contrôle d'accès.

Dans le cadre d'AMALFI, il a donc été décidé d'implémenter ce type de fonction. L'objectif principal étant de valider, au sein même de la première zone exposée aux accès extérieurs, la légitimité de la requête qui est envoyée au système :



**Figure 1 : Vérification de la légitimité de la requête**

Il est important de noter que le terme **légitimité de la requête** comprend :

- Un contrôle d'identification du client qui émet la requête ;
- Un contrôle sur la cible demandée par l'utilisateur.

En outre, la mise en œuvre d'un frontal d'accès permet également de façon naturelle :

- De déporter les problèmes d'attaques HTTP sur un serveur qui n'est pas Métier ;
- De mettre en place une fonction de **Reverse Proxy**.

Tous ces éléments font partie de la solution cible et sont décrits ci-après.

## 3. Contrôle d'accès – Identification Utilisateur

La première fonction du contrôle d'accès est de vérifier l'identité du demandeur.

Si les éléments réseaux de type **routeur**, **commutateur** et surtout **pare-feu** s'assurent d'un point de vue technique que les seuls flux autorisés arrivent jusqu'au site central (DMZ), le contrôle d'accès gère lui une authentification plus fonctionnelle de la demande.

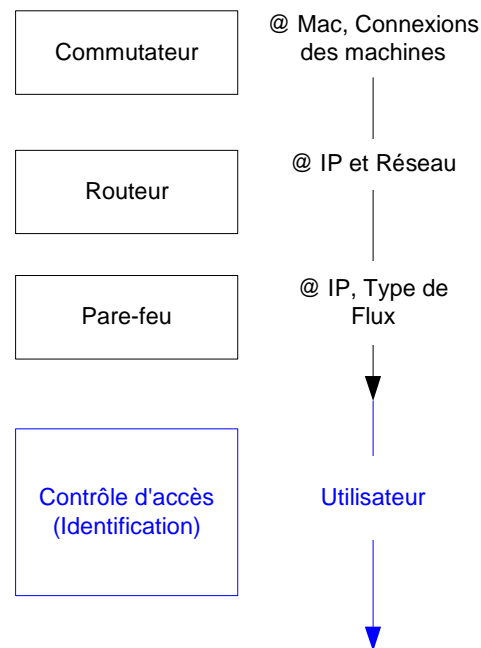


Figure 2 : Principe de sécurisation des accès

L'utilisation de carte à puce pour gérer l'identification des utilisateurs est un principe fort pris sur le projet. On verra plus loin le cas particulier des utilisateurs de type Grand Public qui n'ont pas d'identification.

En outre, il convient également que la solution à mettre en place soit conforme avec :

- Le niveau de sécurité globale ;
- Les principes d'architecture ;
- La volonté de suivre les principaux standards du marché.

De ce fait, le choix a été fait de réaliser cette authentification au travers :

- D'un référentiel de type LDAP ;
- De clés d'authentification inscrites sur la carte à puce ;
- Du standard SSL (HTTPS) ; le contrôle d'accès s'appuyant sur les fonctions d'authentification **Client** natives proposées sur ce protocole.

Le processus de validation de l'accès d'un utilisateur est alors le suivant (hors SSL) :

- Validation de la chaîne de confiance :

# **GILFAM** *Projet AMALFI*

- Validité du certificat de l'AC **filie** signataire du certificat utilisateur (date / révocation sans gestion de cache – accès direct au référentiel LDAP des CRLs) ;
- Validité du certificat de l'AC **root** signataire du certificat de l'AC **filie** (date / révocation sans gestion de cache – accès direct au référentiel LDAP des CRLs) ;
- Etc (jusqu'à la vérification totale de toute la chaîne de liaison).

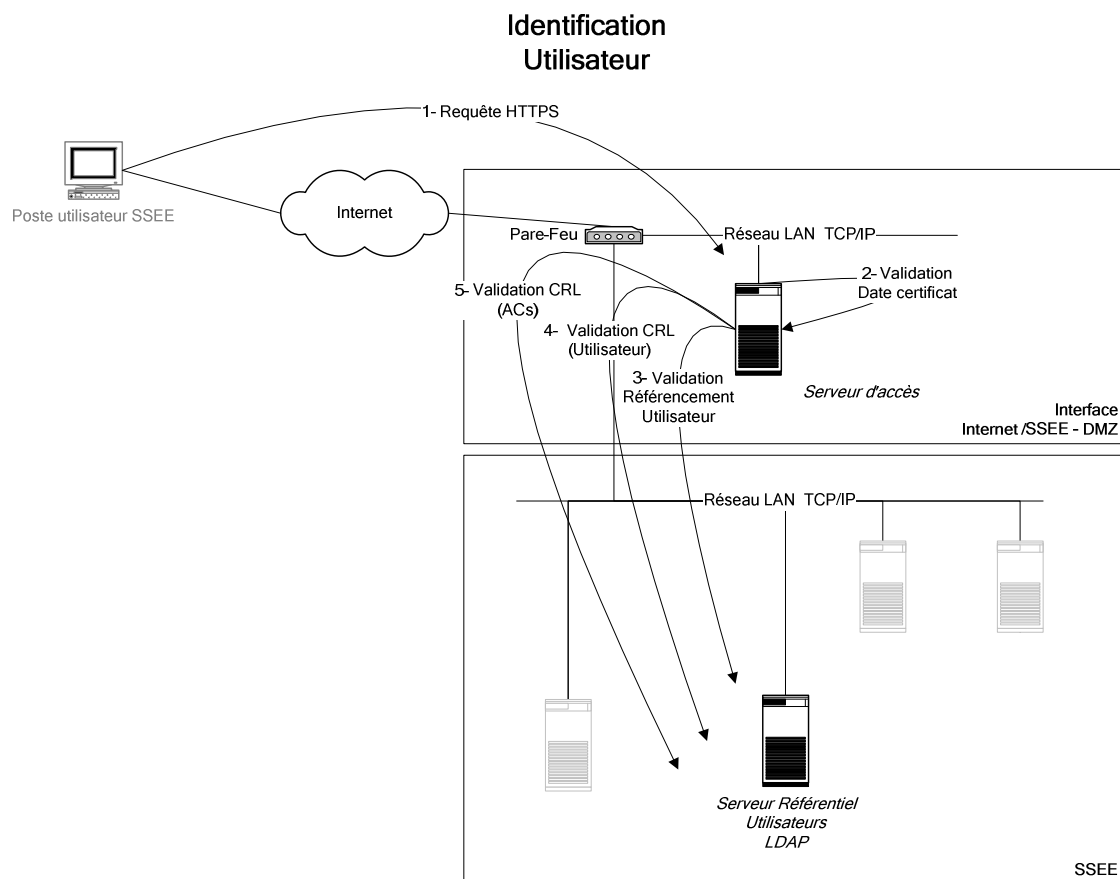
La validation du certificat de l'utilisateur comprend les étapes suivantes :

- Vérification de la date de validité ;
- Vérification que le certificat utilisateur n'est pas révoqué (pas de gestion de cache – accès direct au référentiel LDAP des CRLs) ;
- Validation dans l'annuaire du référencement de l'utilisateur (présence de l'utilisateur dans la partie de l'annuaire réservé au paramétrage du contrôle d'accès) ;

La chaîne de confiance admise par le serveur d'accès est traitée par l'introduction dans un repository d'AC des certificats publics des ACs à vérifier. Dans le cas du contrôle d'accès des utilisateurs pour le SSEE, ces chaînes d'AC sont toutes celles pour lesquels on veut autoriser les certificats des utilisateurs à se connecter au SSEE, par exemple :

- AC root des notaires -> AC des notaires
- AC root des géomètres -> AC des géomètres
- ...

D'un point de vue de l'implémentation il est possible de représenter (flux) ces échanges de la manière suivante.



**Figure 3 : Principe d'identification des utilisateurs**

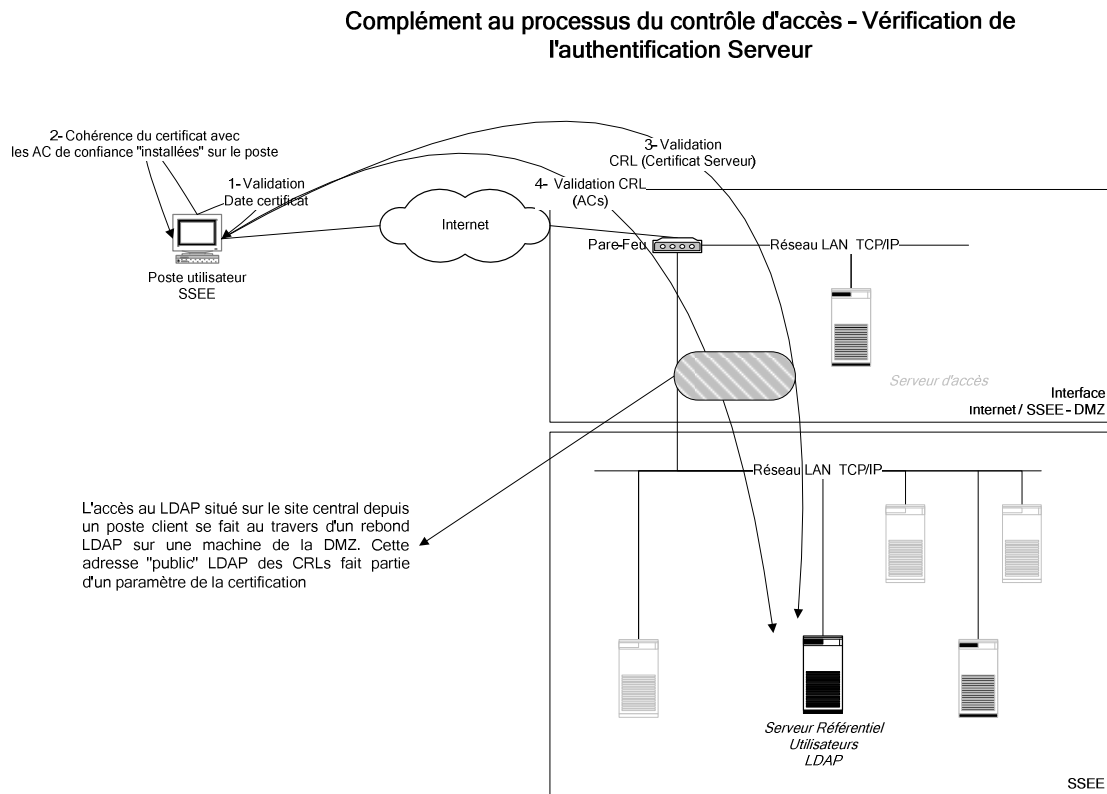
Si cette identification est positive, le système de contrôle d'accès est alors à même de faire le choix de passer à la seconde partie de la vérification de la requête : le choix de la **cible** (URI) visée par la requête. Dans le cas contraire, le système n'autorise pas l'utilisateur à aller plus loin dans les échanges (fourniture d'un message d'erreur HTML mis au format AMALFI fourni directement par le contrôle d'accès).

#### Remarque sur l'authentification de la partie Serveur :

Ce niveau de sécurité permet avant tout de maîtriser les flux arrivant sur le site central. La sécurité reposant le plus souvent sur des principes de confiance mutuelle, il est important de noter que l'authentification serveur a aussi un intérêt et cela afin de fournir à l'utilisateur l'assurance qu'il est bien en train de communiquer avec le système auquel il souhaite se connecter. Cette authentification est réalisée au travers du processus de connexion SSL avec vérification au niveau du navigateur du poste de client de la validité de cette authentification. Ce qui signifie :

- Présence au sein des autorités de certification de confiance (Coffre de certificat) des autorités de certification AMALFI. Ces certificats étant issus du système AMALFI ne sont pas reconnus les magasins de certificat standards des browsers. Une procédure de l'EPELFI (portail) doit donc permettre de télécharger ces certificats de confiance dans les magasins de certificat de confiance des utilisateurs ;

- Accès systématique aux CRLs pour vérification de l'ensemble de la chaîne de certification.



**Figure 4 : Complément au processus du contrôle d'accès - Vérification de l'authentification Serveur**

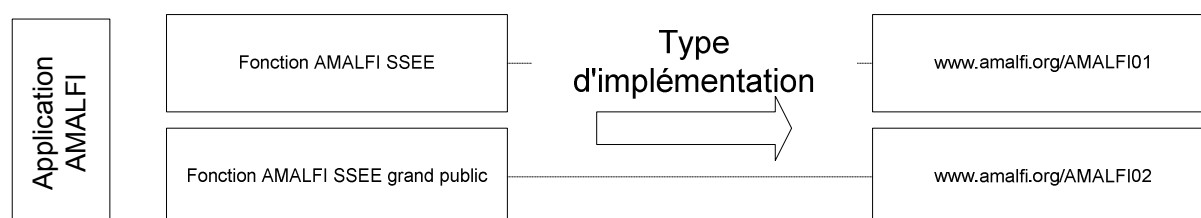
Si l'accès aux CRLs n'est pas possible où si la chaîne de certification présente un certificat non valide, l'accès au système ne peut aboutir.



## 4. Contrôle d'accès – Validation de la cible demandée

Comme indiqué précédemment, le contrôle d'accès doit également assurer un rôle de filtre par rapport à la ressource demandée par la requête. Cette fonction permet en effet d'assurer un niveau fin de contrôle sur l'accès aux fonctions Métiers, ces fonctions étant organisées, dans le cadre du déploiement de l'application, sur des ressources techniques bien définies. Dans le contexte de l'architecture applicative choisie, ces ressources sont en réalité des URIs.

Le schéma suivant donne le niveau de décomposition minimale à adopter pour le découpage des ressources par rapports aux besoins fonctionnels connus<sup>1</sup> :



**Figure 5 : Mapping des fonctions sur des URLs**

Il est également important de noter que cette fonction du contrôle d'accès aurait pu être réalisée à un niveau très fin en tenant compte notamment :

- Non plus seulement d'URIs mais de ressources élémentaires comme une page ;
- D'une gestion des droits sur les ressources utilisateur par utilisateur.

Le contexte fonctionnel du projet fait que le niveau de sécurité à appliquer se trouve davantage à un niveau où :

- Le contrôle sur des grands groupes de fonctionnalités est suffisant ;
- La gestion de groupe d'utilisateurs (profil) est suffisante et répond bien à la problématique.

L'implémentation du contrôle sur les ressources, demandées depuis l'extérieur du site central, est réalisée autour des composants de sécurité TIVOLI (IBM TIVOLI ACCESS MANAGER).

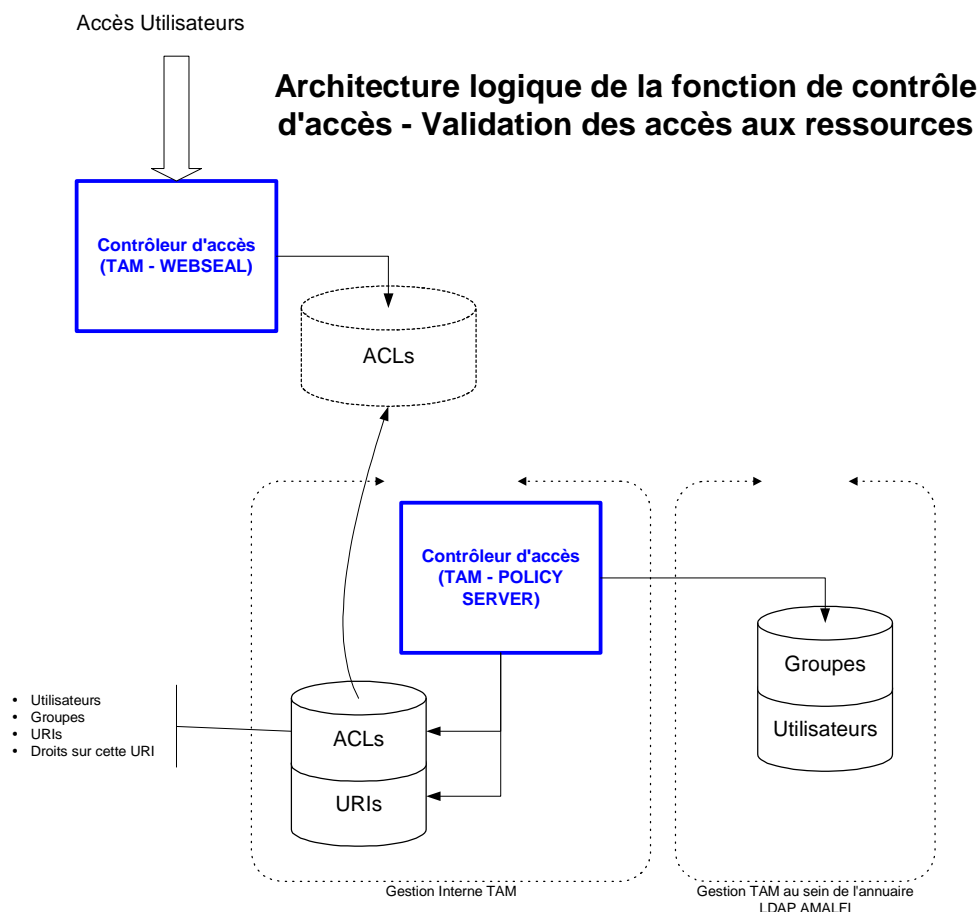
Elle passe en réalité par deux phases :

---

<sup>1</sup> Seul le découpage est important à prendre en compte. Les URIs ([w3.amalfi.org/AMALFIXX](http://w3.amalfi.org/AMALFIXX)) sont données à titre d'exemple.

- Une phase de paramétrage (dynamique et évolutive dans le temps) où :
  - Les utilisateurs sont **créés** dans le système de contrôle d'accès ;
  - Les utilisateurs sont rassemblés dans des groupes ayant des caractéristiques de sécurité identiques (ces groupes correspondent aux profils définis par le système d'habilitation applicative) ;
  - Les URIs sont définis et associés avec des droits à chacun des groupes.
- Une phase de **runtime** où :
  - Cette base de droits est mise à disposition du contrôleur d'accès ;
  - Le contrôleur d'accès vérifie, à partir de l'authentification de l'utilisateur, si ce dernier a effectivement accès à cette ressource ou non.

Ces deux phases sont gérées sur l'architecture logique suivante :



**Figure 6 : Architecture logique de la fonction de contrôle d'accès - Validation des accès aux ressources**

Les mécanismes de création des utilisateurs, des groupes et la gestion des ACLs entre les deux composants TAM sont explicités plus loin dans ce document (cf. § 6 page 12).

## 5. Contrôle d'accès – Compléments de sécurité *Reverse proxy*

De part sa position au sein de la DMZ et du rôle central que ce service apporte au sein de l'architecture globale, le contrôleur d'accès doit également isoler au mieux la zone interne auquel il va accéder suite à une demande utilisateur.

- Le plan d'adressage est foncièrement différent entre la zone du contrôle d'accès et la zone du interne (la zone DMZ contient des adresses sur un réseau TCP/IP qui lui est propre) ;
- Les adresses et URLs visibles et routables sur le RPVJ sont systématiquement transformées (notion de jonction au sein du contrôleur d'accès).

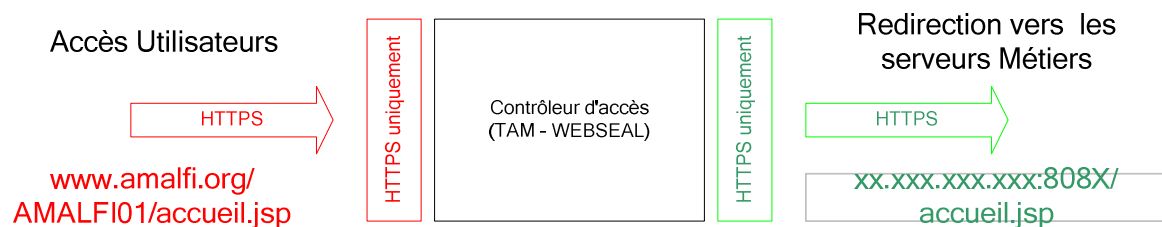


Figure 7 : Fonction de Reverse Proxy

Cette fonction de **Reverse Proxy** est essentielle et représente un élément de sécurité important au niveau de la gestion des accès.

---

## **6. Détails des opérations sur la gestion des utilisateurs et de la configuration du contrôle d'accès**

---

## 6.1. Création des utilisateurs, gestion des Profils

La création des utilisateurs est entièrement pilotée par l'application (Application IAH qui est la même que celle du SC). Cela permet notamment de s'assurer que la mise à jour du référentiel est bien contrôlée par tous les mécanismes de sécurité mis en place autour de l'application ; à savoir :

- Utilisation des fonctions de contrôle d'accès et d'habilitations applicatives pour limiter les droits ;
- Limitation des utilisateurs (administrateurs) de l'annuaire, la plupart des modifications étant faites par un applicatif AMALFI (application IAH) ;
- Cohérence et intégrité du référentiel vis-à-vis de l'ensemble des besoins de manipulations des objets **Utilisateurs**.

De ce fait le processus choisi pour cette gestion des utilisateurs au sein des mécanismes de contrôle est le suivant :

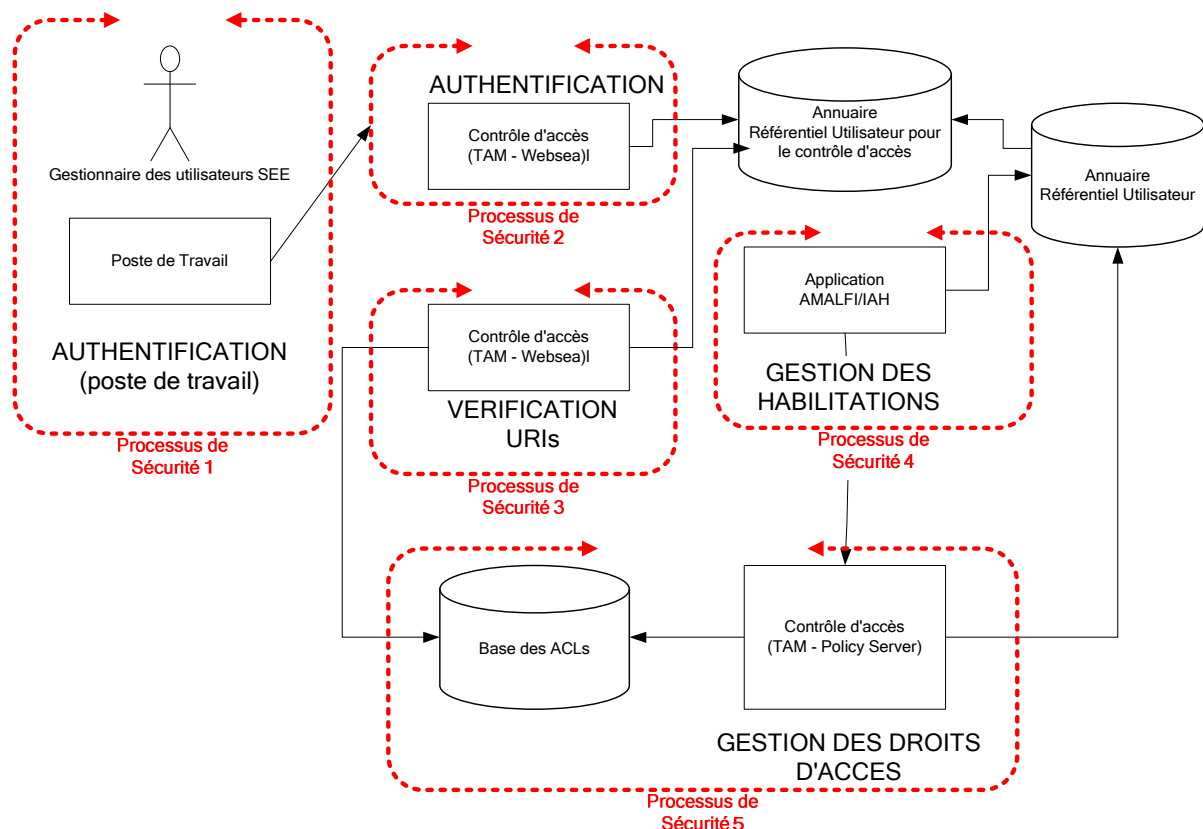


Figure 8 : Procédure de création des utilisateurs, gestion des profils

Processus de Sécurité N°1 : AUTHENTIFICATION au niveau du poste de travail :

- L'utilisateur gestionnaire des utilisateurs du SSEE pour pouvoir se connecter au système doit impérativement se connecter à son poste de travail au travers des

mécanismes d'authentification. Ceci constitue le premier niveau de sécurité sur la gestion des utilisateurs et de ce fait du contrôle d'accès ;

Processus de Sécurité N°2 : AUTHENTIFICATION au niveau du contrôle d'accès lui-même :

- L'utilisateur émet une requête pour accéder à l'application de gestion des utilisateurs. Il passe par le contrôleur d'accès qui sur la base des éléments décrits précédemment procède à un nouveau contrôle d'authentification.

Processus de Sécurité N°3 : VERIFICATION DES DROITS D'ACCES à l'application de gestion des utilisateurs :

- Le contrôleur d'accès (WebSeal) utilise les données du référentiel utilisateur pour identifier les groupes auxquels appartient l'utilisateur authentifié. La base de gestion des droits est ensuite consultée pour valider que la ressource demandée est bien autorisée pour l'un de ces groupes.

Processus de Sécurité N°4 : GESTION DES HABILITATIONS :

- L'application elle-même procède, sur chaque interaction, à une vérification plus fine des droits de l'utilisateur (et cela toujours en fonction du profil). Ainsi, jusqu'à un niveau applicatif assez élémentaire l'accès aux fonctions est vérifiées.

Processus de Sécurité N°5 : GESTION DES DROITS D'ACCES :

- Une fois que la chaîne complète de sécurité est validée, l'utilisateur (opérateur) peut créer, modifier les données relatives à un autre utilisateur (données personnelles mais également données liées à ses habilitations de type Profil). C'est au travers de ces fonctions applicatives que la mise à jour des droits d'accès :
  - L'application modifie le référentiel des utilisateurs ;
  - L'application demande au composant Policy Server, dans le cadre de la création d'un utilisateur, d'importer les informations relatives à cet utilisateur (ce qui a comme conséquence une mise à jour, opérée par le Policy Server, des informations de l'utilisateur au sein du LDAP) ;
  - L'application demande au composant Policy Server, les changements de groupe pour l'utilisateur, dans le cadre d'une modification des habilitations fonctionnelles (ce qui a pour conséquence une modification des de l'utilisateur au sein du LDAP et de la base d'ACLs du contrôle d'accès).

En cas de problème sur l'un de ses composants<sup>2</sup>, les modifications ne sont pas apportées (annulation complète de la transaction).

---

<sup>2</sup> Application, LDAP, Policy Server.

---

## **7. Éléments d'implémentation et schémas de synthèse**

---

Ce chapitre reprend les fonctionnalités décrites précédemment et donne des indications techniques d'implémentation :

- Schématisation des flux principaux entre les composants et les différentes zones ;
- Indication d'éléments de configuration des outils, qui représentent des options de sécurité à préciser dans ce document.

## **7.1. Communication entre les deux composants TAM WebSeal – Policy Server**

---

L'essentiel de ces communications correspond à la mise à disposition du Policy Server des informations relatives aux droits d'accès. Cette mise à disposition peut se faire de plusieurs manières (pushing, pooling, push&pooling). La solution choisie tient compte de deux éléments essentiels :

- La nécessité d'avoir, pour le WebSeal, une base la plus à jour possible ;
- La nécessité également de limiter les flux entre les zones, notamment lorsque ceux-ci créent un flux du type « zone DMZ  $\Rightarrow$  Zone Données » ;
- La volonté de bâtir un système performant répondant aux exigences de qualité transactionnelle demandées par les utilisateurs.

Il a donc été décidé de choisir un mode où le Policy Server informe le serveur WebSeal lorsqu'une modification est apportée à la base de gestion des droits d'accès. Le serveur WebSeal récupère alors immédiatement la nouvelle base de droits et l'utilisent pour gérer le filtrage sur les demandes de ressources par les utilisateurs.

Pour permettre l'authentification des utilisateurs du SSEE par des certificats au travers de la fonctionnalité TAM/WEBSEAL, il est nécessaire de créer ces utilisateurs d'une part dans une base LDAP et d'autre part de les importer dans la base des autorisations TAM. Ces deux bases sont localisées dans le SSEE. Par ailleurs, avant toute connexion au système central, les utilisateurs doivent aussi être enregistrés dans la base AMALFI et leurs habilitations dans l'application AMALFI doivent y être définies.

Afin de respecter les règles de filtrage imposées entre le SC et le SSEE (pas de flux du SSEE vers le SC, donc impossibilité de faire des répliquions TAM entre les deux Systèmes), il est nécessaire de séparer les deux royaumes TAM. Il y a donc un environnement TAM/WEBSEAL/LDAP dans le SSEE distinct de celui du SC.

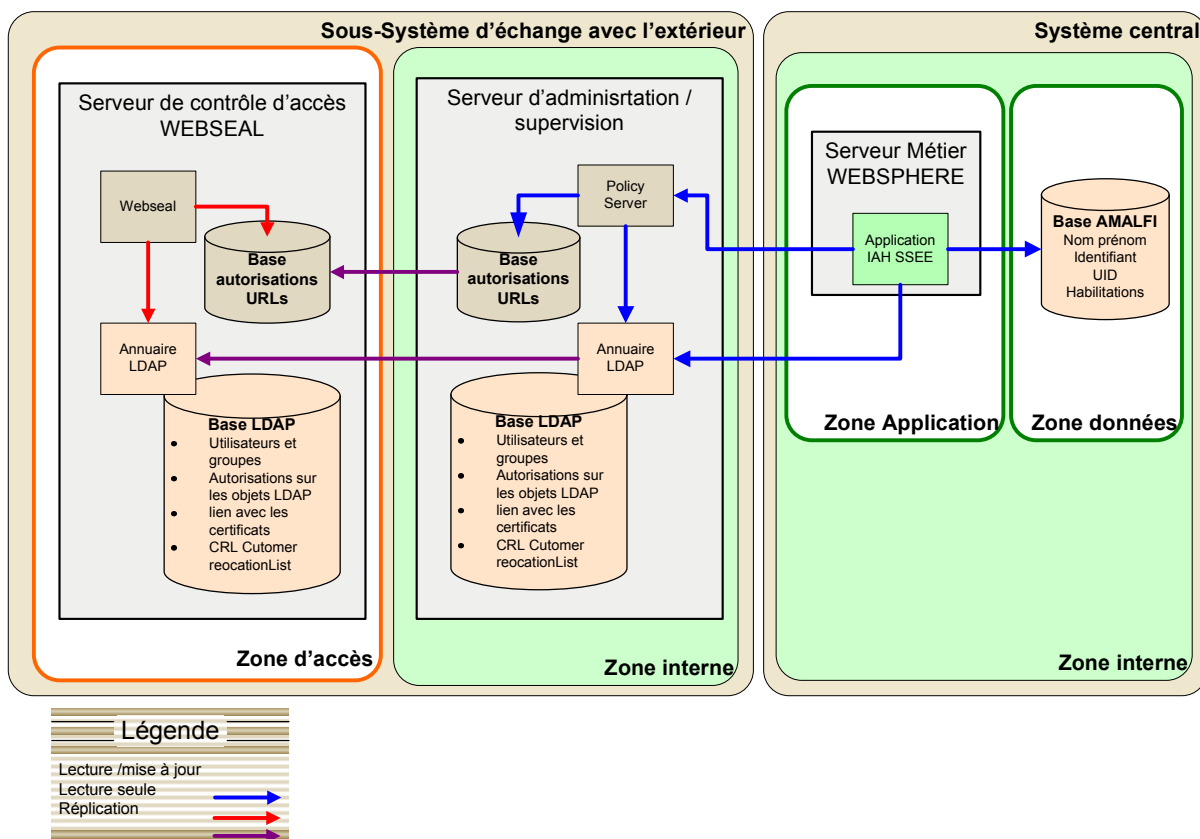
Pour permettre la mise à jour de l'ensemble des bases utilisateurs, l'application IAH SC a été étendue pour permettre aussi de gérer les utilisateurs du SSEE. Cette extension permet la gestion des utilisateurs et de leurs habilitations dans le système AMALFI.

Le schéma ci-dessous présente les différents flux de répliquion et de mise à jour concernant les utilisateurs SSEE gérés dans le système AMALFI (hormis les utilisateurs systèmes et certains utilisateurs d'exploitation).

Cette solution nécessite la mise en œuvre de deux flux de communication entre le SC et le SSEE :

- Flux de mise à jour LDAP sécurisé LDAPs ;
- Flux de mise à jour de TAM de type TCP/SSL.





**Figure 9 : Flux concernant la gestion des autorisations du SSEE**

Dans le cas du SSEE, il n'est pas prévu de zonage réseau dans la zone interne du SSEE. On reste donc dans la configuration standard de synchronisation de la base des autorisations TAM localisée sur le serveur WEBSEAL. Cette synchronisation avec la base maîtresse située dans la zone interne du SSEE (géré par Policy Server) s'effectue à l'initiative du serveur Webseal, après qu'il ait reçu une notification par le Policy Server d'une modification de la base des autorisations TAM du Policy Server. Le serveur Webseal demande alors à TAM de lui envoyer cette base.

La description de la communication entre le SSEE et le SC pour les flux applicatifs est détaillée dans le document [TC3.31b.1.3 Communications applicatives entre le SC et le SSEE](#).

Ces communications sont réalisées via SSL<sup>3</sup>.

### Remarques complémentaires sur la notion de Réseau TAM :

Il est à noter que les communications sécurisées (et surtout les clés utilisées pour ces communications) sont aujourd’hui gérées par le produit. Les clés SSL ne peuvent donc pas être des clés provenant de l’IGC AMALFI. Les processus et règles de gestion de ce réseau et par la même de gestion des différentes clés est présentée ci-après :

<sup>3</sup> Avec authentification des deux parties (chiffrement et authentification SSL implémentés).

# **GILFAM** *Projet AMALFI*

- Lors de l'installation du Policy Serveur, celui-ci crée un Token contenant une bi-clé d'AC et un certificat serveur certifié par cette AC. Ce Token est un fichier sécurisé chiffré qu'il n'est pas possible de manipuler autrement qu'au travers des fonctions (API ou commande TAM), uniquement accessibles par l'administrateur du produit ;
- Le processus d'enregistrement et de certification d'un serveur dans le réseau TAM (serveur Webseal par exemple) est géré de la manière suivante :
  - Le produit est installé et les éléments fondamentaux, comme le DN du serveur, sont renseignés ;
  - En dehors des heures d'ouvertures du service, et par mesure de sécurité, la liaison entre SSEE et internet est logiquement stoppé ;
  - La configuration du serveur TAM est modifiée pour autoriser un échange de clés automatisés (et cela pour éviter des processus plus complexes de transferts de clé par copie de fichiers) ;
  - La procédure d'enregistrement du serveur dans le réseau TAM est alors lancée :
    - Connexion au serveur TAM ;
    - Saisie du login et du mot de passe de l'administrateur du serveur principal TAM (Policy Serveur) ;
    - Enregistrement dans le LDAP du DN du nouveau serveur ;
    - Traitement d'une demande de certification par le serveur principal et transmission d'un token sécurisé contenant la clé d'authentification du nouveau serveur (certifiée par l'AC TAM).
  - La configuration du serveur TAM est modifiée pour ne plus autoriser la diffusion automatique des clés ;
  - Eventuellement, le mot de passe administrateur de TAM est modifié ;
  - Le RSSI vérifie au sein du LDAP que seul le nouveau serveur a été enregistré ;
  - La liaison entre site central et RPVJ est rétablie.

Dans le cas d'un problème sur un serveur (volonté de ne plus l'intégrer dans le réseau TAM), le produit n'offre pas de solution de révocation simple. Les procédures suivantes s'appliquent :

- Evaluation par le RSSI du type de problématique de sécurité (compromission des clés ou plus simplement suppression du serveur et donc de son identifiant DN par exemple)
- Choix d'une **stratégie** de suppression du serveur au sein du réseau TAM :
  - Problème de sécurité non critique : celui-ci peut être traité par la suppression (déréférencement du serveur) au sein de l'annuaire LDAP – le serveur, même lorsqu'il présente sa clé d'authentification qui reste valide d'un point de vue stricte de l'IGC, ne peut plus se connecter au serveur principal TAM ;
  - Problème de sécurité plus critique : le traitement de ce problème passe par la création d'un nouveau réseau TAM :

# ***GILFAM*** *Projet AMALFI*

- Changement du mot de passe administrateur de TAM
- Demande de renouvellement des clés au niveau du serveur principal ;
- Procédure de réenregistrement des serveurs autorisés à participer au réseau.

## **7.2. Communications entre les deux composants TAM WebSeal et LDAP**

---

Certains utilisateurs du SSEE se connectent en SSLV3. Il est donc nécessaire de vérifier la validité des certificats présentés au serveur ou à l'utilisateur. Cette validité est vérifiée par un accès du serveur WEBSEAL au serveur LDAP à la chaîne d'ACs relative au certificat de l'utilisateur présenté à Webseal.

Les communications entre Webseal et LDAP concernent principalement la recherche des CRLs pour contrôler les certificats **Utilisateurs** et **Autorités de certification** ainsi que l'identification de l'utilisateur (référencement au sein des mécanismes de contrôle d'accès).

### **7.2.1. Recherche de la validité des certificats**

La recherche de la validité des CRLs est fortement liée au processus de connexion SSL entre le poste client et le serveur WebSeal. La vérification des CRLs est effectuée par un composant adossé au serveur WebSeal (GSK – Global Security Kit). Ce composant interroge le serveur LDAP d'une manière similaire à ce que pourrait faire un navigateur. C'est-à-dire :

- Qu'il communique en LDAP avec l'annuaire (pas de SSL) ;
- Qu'il utilise l'utilisateur **Anonymous** pour récupérer les informations (CRLs).

Une fois cette vérification faite, la connexion SSL est établie et le serveur WebSeal peut traiter la deuxième phase de la recherche d'informations sur l'utilisateur.

### **7.2.2. Mise à disposition des CRLs**

Au niveau du serveur de contrôle d'accès WEBSEAL du SSEE, la solution utilisée dépend des différents types de certificats utilisateurs. Actuellement seul le type de connexion des notaires est connu. Les autres types de connexion ne sont pas définis.

#### **7.2.2.1. Vérification des CRLs pour les notaires**

Les notaires ont des certificats qui sont émis par REAL. Les certificats sont uniquement disponibles en http en dehors du réseau intranet des notaires. De plus, les certificats utilisateurs des différentes ACs ne possèdent pas l'attribut `crlDistributionPoint`. Dans ce cas, Webseal prend le DN de l'Issuer du certificat et récupère la CRL dans un annuaire LDAP définis par paramétrage. Suivant le type de certificat utilisateur ou ACs ( extension `isCA=true`), Webseal lit la CRL soit dans l'attribut `certificateRevocationList` soit dans l'attribut `AuthorityRevocationList` dans l'entrée LDAP correspondant à l'Issuer du certificat.

Il a donc été décidé de récupérer automatiquement ces CRLs pour les stocker dans LDAP. Un programme batch exécuté sur le serveur d'administration/supervision du SSEE récupère à intervalle régulier les CRLs en http et les stocke sur le serveur LDAP localisé sur le serveur d'administration/supervision du SSEE.

Les paramètres de ce batch pour chaque CRL à récupérer sont donc :

1. l'adresse http où la CRL peut être récupérée
2. Le serveur LDAP et l'entrée dans laquelle il faut stocker les CRLs
3. l'attribut dans lequel il faut stocker les CRLs

Ces CRLs sont ensuite mises à disposition de Webseal lors de la réplication LDAP vers les serveurs LDAP de la DMZ.

Il faut donc positionner les droits d'accès aux URLs de téléchargement des CRLs dans les pare-feu du SSEE (internet/Zone d'accès et Zone d'accès/Zone interne).

### **Remarques :**

Les différentes versions des ACs ont toutes le même Subject Name, la distinction entre les différentes versions des certificats se faisant avec le serial number. Les champs Subject Key Identifier et Authority Key Identifier permettent de retrouver les certificats signataires.

Ce mode de gestion entraîne qu'une seule CRL est gérée pour l'ensemble des différents certificats d'une même AC. Le paramétrage du batch de récupération des CRLs n'est pas modifié lorsqu'un nouveau certificat est créé.

Par contre, pour permettre la connexion des utilisateurs de type notaire, il faut que l'ensemble des certificats des ACs des notaires soit dans le magasin des clés de WEBSEAL. Il reste à définir le processus par lequel le GILFAM est averti de l'existence d'un nouveau certificat afin de le récupérer et de le stocker dans le magasin de clé de WEBSEAL.

## **7.2.3. Recherche des informations utilisateurs vis-à-vis du contrôle d'accès**

Le serveur WebSeal récupère le DN du certificat qui a été validé au travers de la connexion SSL. Il utilise ce DN pour récupérer des données du LDAP gérées par le contrôle d'accès (association du DN avec un Id TAM, appartenance aux groupes).

Ces informations sont recueillies au travers d'une connexion LDAP :

- Sécurisée (SSL)<sup>4</sup> ;
- En utilisant un User/Mot de passe WebSeal.

Cette combinaison **utilisateur / Mot de passe** est stockée dans un fichier de configuration et donne des droits de lecture uniquement sur :

- Les branches utilisateurs (pas plus qu' **Anonymous**) ;
- Les branches TAM (plus qu' **Anonymous**).

### **Remarques sur la sécurisation du fichier de configuration et du processus WebSeal :**

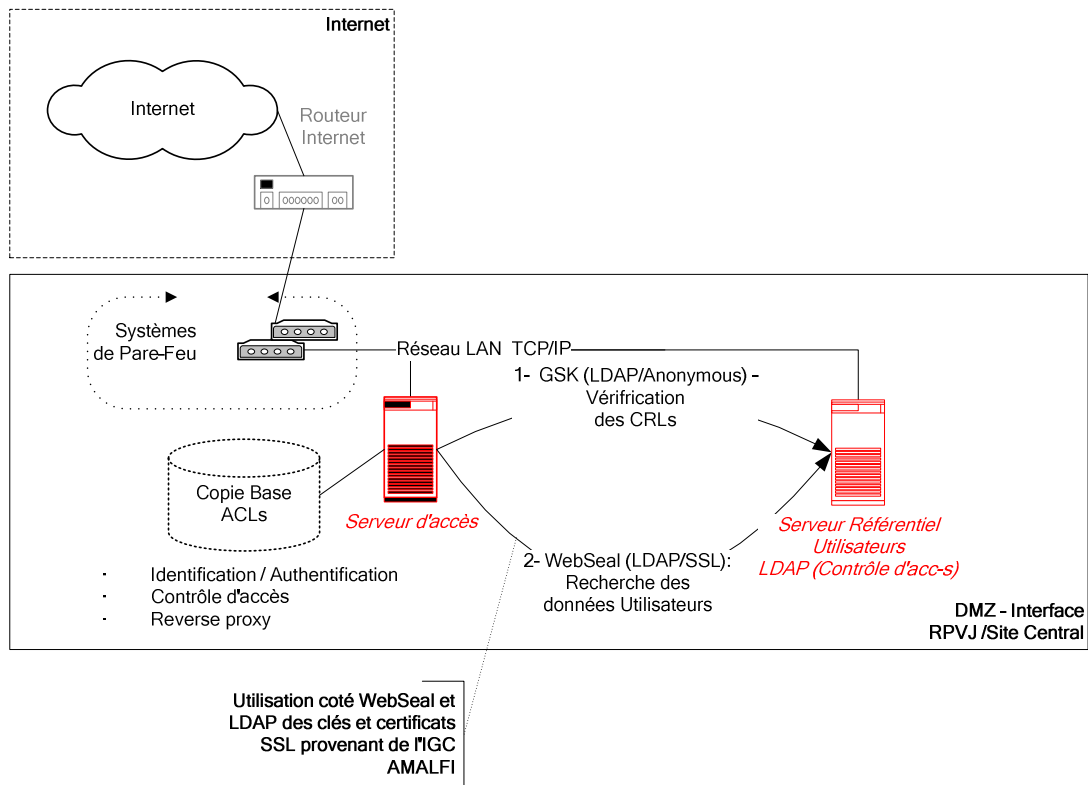
Ces informations de connexions sont inscrites non chiffrées dans un fichier de configuration présent sur les serveurs WebSeal (WebSeal.conf). Les droits sur ce fichier sont traités au travers du système d'exploitation (AIX).

---

<sup>4</sup> Les clés et certificats utilisés pour cette connexion sont des clés provenant de l'IGC AMALFI.

En dehors de **Root**, seul l'utilisateur **WebSeal** est habilité à lire/écrire/exécuter ce fichier.

Il est en de même pour le processus **WebSeal** qui fonctionne toujours sous cet utilisateur **WebSeal**. Cet utilisateur n'ayant par ailleurs aucun droit particulier (en dehors du traitement du processus **WebSeal** ) sur le reste de l'arborescence du système.



**Figure 10 : Connexion du serveur TAM à LDAP**

## **7.3. Communications entre les composants TAM WebSeal, Websphere et LDAP**

---

Les processus décrits précédemment dans l'ensemble du chapitre sur le contrôle d'accès ne font état que des fonctions d'authentification et de **Reverse Proxy** au niveau du serveur WebSeal. Il est évident que l'intérêt d'avoir un frontal d'authentification réside principalement dans la faculté à propager de façon sécurisée cette authentification (par ailleurs lourde à réaliser) sur les autres composants de l'architecture.

De ce fait, il y a donc bien des communications entre le serveur WebSeal et le serveur Websphere (WAS).

Il existe plusieurs méthodes pour faire transiter (propager) de façon sécurisée les données d'authentification du serveur WebSeal au serveur WAS :

- L'utilisation d'une Trust Association Interceptors Junction (TAI Junction) ;
- La fourniture d'un cookie LTPA chiffrée.

Ces deux techniques utilisent le fait que le WebSeal est utilisé comme **Reverse proxy** et donc qu'il assure le transfert des requêtes HTTP jusqu'aux serveurs WAS. La différence majeure entre ces deux techniques est cependant la suivante :

- TAI : Utilise une transformation de Header HTTP pour transmettre les données d'identification ;
- LTAP : utilise la notion de Jeton et de cookie pour transmettre les données d'identification.

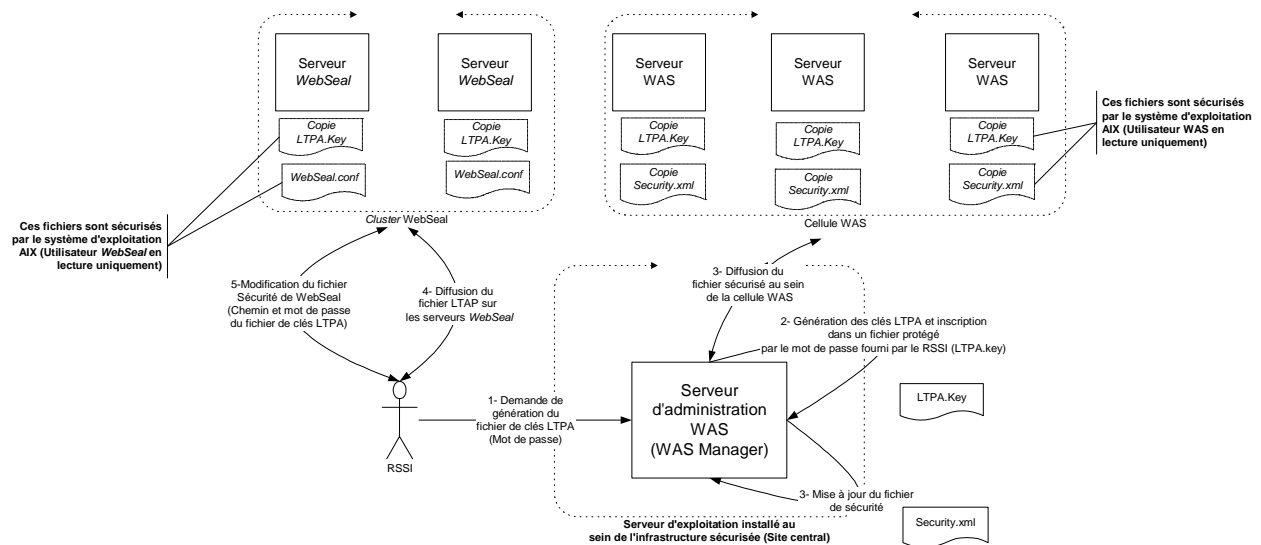
L'option LTPA est celle présentant le plus de sécurité et par conséquent celle qui a été choisie.

### **7.3.1. Fonctionnement d'une Jonction de type LTPA, Avantages et Inconvénients**

Une jonction de type LTPA fonctionne sur la base de la transmission d'un cookie d'authentification chiffré. Le chiffrement de ce cookie est traité par des clés de chiffrement produites pour l'infrastructure WAS et mises à disposition du serveur WebSeal.

Le schéma ci-après décrit la procédure :

- De création et de diffusion de ces clés au sein d'un fichier sécurisé ;
- D'utilisation de ce fichier.



**Figure 11 : Création du cookie de sécurité LTPA**

Les éléments important à noter sur ces procédures sont les suivants :

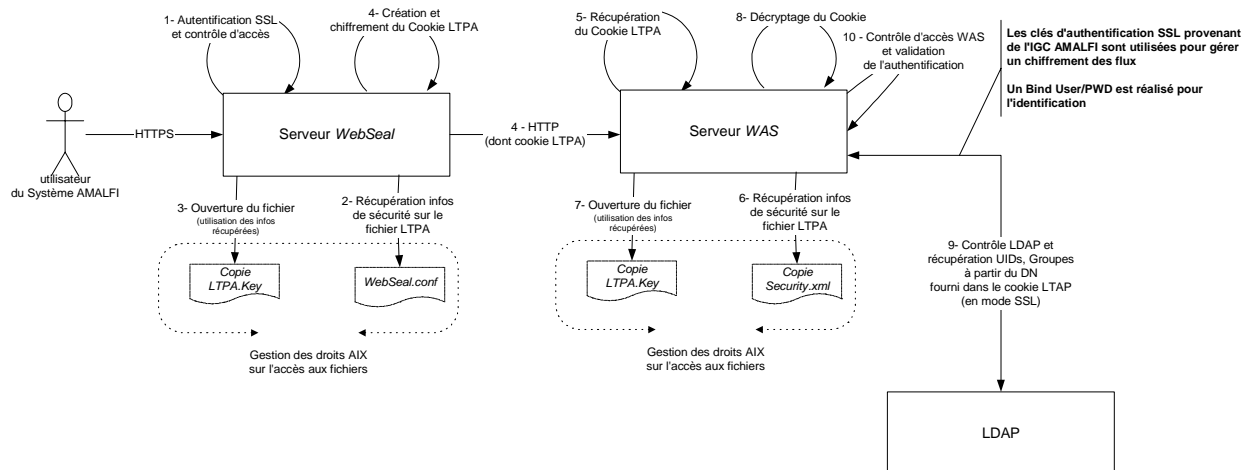
- Seul le RSSI est habilité à créer de nouvelles clés LTPA et à préciser le mot de passe sécurisant ce fichier de clés ;
- Les mots de passe inscrits dans les fichiers de sécurité des cellules WAS et du cluster WebSeal sont chiffrés avec un algorithme simple (XOR). La protection du mot de passe est donc davantage garantie par les droits AIX positionnés sur ces fichiers de sécurité (en lecture uniquement - les utilisateurs WAS pour les serveur WAS et utilisateur WebSeal pour le contrôle d'accès)

En fonctionnement nominal, le WebSeal après avoir réalisé l'authentification et le filtrage sur les URIs produits pour chaque nouvel utilisateur un cookie chiffré avec les clés contenus dans le fichier qui lui a été fourni par le RSSI. Ce cookie contient toutes les informations nécessaires à l'identification de l'utilisateur. Il est décrypté par le WAS et les informations qu'il contient sont vérifiées par le WAS en fonction de la politique de sécurité appliqué sur les serveurs d'application (connexion LDAP). La chaîne de confiance WebSeal / WAS est assurée par le fait que chacun des deux parties est en possession :

- Du fichier de clés ;
- Du mot de passe sécurisant ce fichier.



# GILFAM *Projet AMALFI*



**Figure 12 : Procédure de transmission de l'identité d'un utilisateur entre Webseal et WAS en utilisant LTPA**

L'application est alors à même de récupérer directement l'UID de l'utilisateur.

Les éléments important à noter sur cette procédure de connexion sont les suivants :

- Le cookie LTPA ne transite qu'entre le contrôle d'accès et le serveur WAS. Il n'est jamais mis à disposition de l'utilisateur limitant ainsi le risque :
  - D'analyse du cookie par un utilisateur externe ;
  - De capture réseaux (ou poste de travail) qui pourrait éventuellement permettre de rejouer les transactions d'authentification ;
- La nécessité de passer en SSL n'existe pas du fait du chiffrement du cookie. Ce chiffrement (et le décryptage associé) comporte un overhead sur le temps machine consommé à chaque transaction. (dans une moindre mesure que le chiffrement SSL). La mise en œuvre de la fonction de **cache** du cookie LTPA au niveau du serveur WebSeal et de validation des habilitations au niveau WAS permet de réduire considérablement cet overhead. Il ne comporte pas en outre de risque majeur de sécurité. Une modification des droits des utilisateurs (que cela soit au niveau de la certification comme au niveau des habilitations fonctionnelles) est dans tous les cas :
  - Prises en comptes à chaque nouvelle session de l'utilisateur par l'ensemble de composants ;
  - En temps réels et de façon applicative sur des fonctions très spécifiques à surveiller comme la signature par exemple.
- La sécurité est fortement basée sur la sécurité d'accès à certains fichiers. La gestion AIX de ces droits est fondamentale pour que la solution soit fiable.

## **7.4. Communication entre les composants TAM Policy Serveur, Websphere et LDAP**

---

Ces communications correspondent à la mise en œuvre de la gestion des utilisateurs au sein de l'application AMALFI/IAH. Les processus à traiter sont les suivants :

- Gestion des utilisateurs (Création/Modification/Suppression) ;
- Gestion des habilitations des utilisateurs (Création/Modification/Suppression des habilitations fonctionnelles et géographiques) ;
- Récupération applicative des informations utilisateurs pour :
  - La gestion des contrôles ou des comportements applicatifs ;
  - L'affichage et le traitement des données utilisateurs dans les processus AMALFI ou IAH.

### **7.4.1. Gestion des utilisateurs et des habilitations - Création/Modification/Suppression**

Le choix a été fait de traiter ce processus au travers d'une application s'intégrant dans l'architecture AMALFI. En outre, et pour garantir une complète cohérence entre le référentiel des utilisateurs et la gestion au travers de TAM du contrôle d'accès, cette application AMALFI/IAH intègre également le pilotage du composant TAM Policy Serveur.

Le processus de traitement des utilisateurs est donc le suivant :

- Création/modification/suppression<sup>5</sup> des utilisateurs au sein du référentiel LDAP ;
- Pilotage du serveur TAM (Policy Server) pour gérer l'import et/ou les modifications d'attributs des utilisateurs.

Les composants étant au sein d'une même zone de Sécurité, il ne paraît pas nécessaire (compte tenu également de l'intégration de ces processus au sein de l'ensemble de la chaîne d'authentification et de contrôle AMALFI) que ces échanges soient sécurisés. Les choix structurants sont donc les suivants :

- Pas de connexion SSL a priori sur l'ensemble de ces échanges ;
- Pas d'authentification forte à prévoir mais une gestion sécurisée des utilisateurs se connectant aux différents systèmes.

Sur la base de ces postulats, il est important de noter que l'architecture TAM n'autorise pas de pilotage sans liaison sécurisée par SSL (cf. paragraphe sur les échanges entre WebSeal et TAM Policy Server) et impose en outre sur les différents canaux de communication la gestion des clés d'authentification SSL suivante :

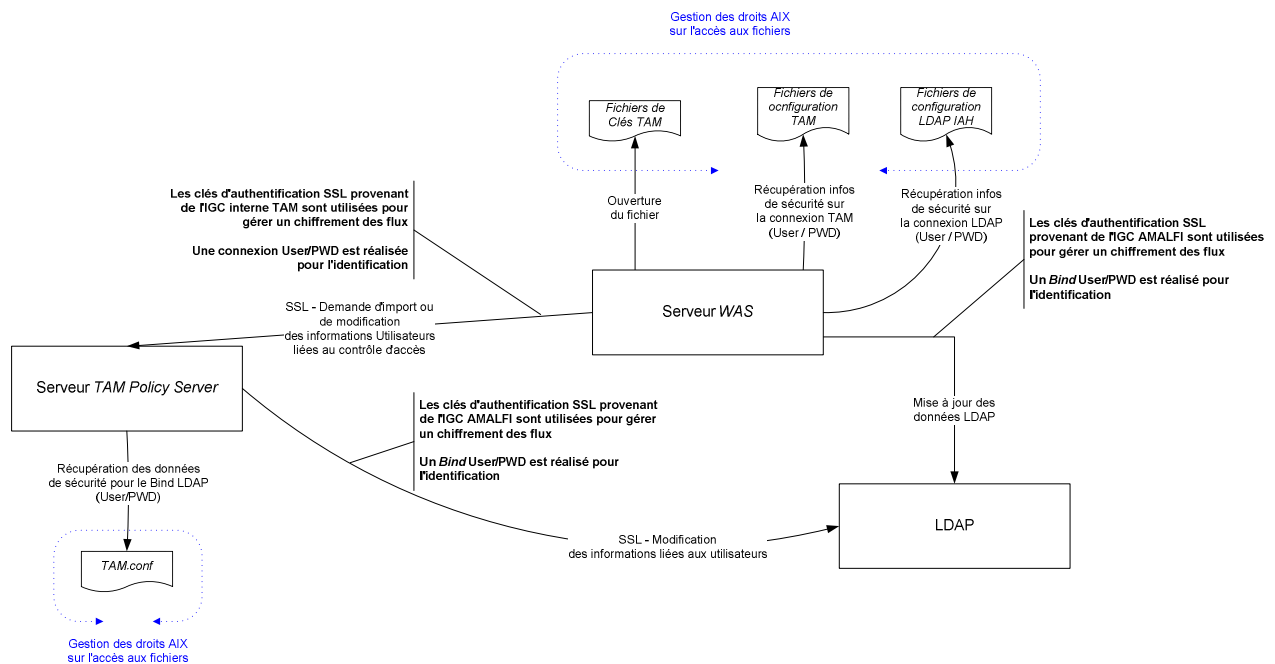
---

<sup>5</sup> La suppression n'est qu'une suppression logique. Aucune entrée **Utilisateur** n'est supprimée de l'annuaire.

# GILFAM *Projet AMALFI*

- Pilotage du TAM Policy Server par WAS – communications internes au **Réseau TAM** - échanges SSL avec des clés d'authentification provenant d'une IGC intégrée à TAM ;
- Communications entre TAM Policy Server et le LDAP (suite aux demandes du WAS) – échanges SSL avec choix des clés d'authentification (dans le cas d'AMALFI, IGC interne AMALFI).
- Utilisation des éléments SSL comme des éléments de chiffrement – l'identification est faite systématiquement au travers de la fourniture d'un couple utilisateur/ mot de passe.

Le schéma ci-après reprend, en synthèse les différentes interactions, les **Utilisateurs / Mots de passe** utilisés et leurs méthodes de sécurisation au sien de l'architecture de sécurité proposée.



**Figure 13 : Description des connexions de l'application IAH avec TAM et LDAP**

Remarques :

1. La sécurité des fichiers contenant les informations d'identification et de connexion est gérée par le système UNIX.
2. Il existe bien un identifiant IAH spécifique pour la connexion LDAP avec des droits permettant des modifications sur les arborescences dites **fonctionnelles**: Utilisateurs, Cartes, ACs, BFs. Il est à noter que toutes les fonctions liées à l'IGC et pour lesquelles l'application IAH à en charge de mettre à jour l'annuaire utilise cet identifiant.

3. L'application IAH est localisée dans le SC et les serveur LDAP et TAM sont localisées dans le SSEE.

## **7.4.2. Récupération et Utilisation des informations utilisateurs par l'application AMALFI**

L'application AMALFI accède directement aux données des utilisateurs stockées dans la base applicative et n'utilise pas les données LDAP et TAM

---

## **8. Disponibilité et redondance des fonctions du contrôle d'accès**

---

L'infrastructure mise en œuvre pour assurer la disponibilité et la redondance des fonctions du contrôle d'accès est décrite dans le livrable [TC3.31b.1.3](#).

---

## **9. Choix du certificat serveur du Webseal SSEE**

---

Le certificat serveur utilisé pour Webseal SSEE est un certificat signé par l'AC SE de l'IGC AMALFI V2. La vérification des certificats serveurs est possible par un accès au serveur LDAP<sup>6</sup> (localisé sur les serveurs WEBSEAL du SSEE) où les CRLs sont stockées.

---

<sup>6</sup> Sous réserve que le nom DNS dans le champ "crlDistributionPoint" du certificat serveur puisse être résolu par le poste de travail de l'utilisateur se connectant à AMALFI.

---

## **10. Annexes- Informations sur le schéma d'annuaire**

---

## **10.1.     Modèle de données pour AMALFI**

---

L'annuaire héberge à la fois des données dites fonctionnelles et des données techniques. Des liens existent entre ces différents types de données mais leurs utilisations sont différentes.

Le modèle de données fonctionnelles dans le cas du SSEE est lié essentiellement aux modèles définis par les PKIs des certificats qui sont autorisés à se connecter au SSEE

Le modèle de données technique est lié quasi essentiellement à des fonctions de sécurité et sert principalement à la gestion du contrôle d'accès et des habilitations :

- Passage entre zone d'accès et Zone interne (rôle du contrôle d'accès) ;
- Sécurité des ressources du serveur d'application ;
- Administration de certains composants (comme le serveur d'application lui-même).

Le modèle fonctionnel est défini par les PCs des différentes PKIs reconnues par AMALFI

Le modèle technique est lié (par contrainte) à l'utilisation de certains progiciels comme TAM. Les impacts de leur utilisation sont décrits également ci-après.

### **10.1.1. Modèle Technique – impact TAM V6**

#### **10.1.1.1. Classes d'objets « TAM »**

Tivoli Access Manager 6 impose une extension de schéma pour l'annuaire LDAP, c'est-à-dire un ajout de classes et d'attributs par rapport aux classes normalisées.

En particulier, les nouvelles classes suivantes sont à ajouter<sup>7</sup> (elles sont déjà intégrées dans la Version 6 de IBM Directory Server) :

- SecUser
- SecMap
- SecGroup
- SecPolicy
- SecAuthorityInfo
- SecPolicyData
- SecResource

---

<sup>7</sup> Le détail des extensions de schéma est disponible à l'adresse suivante, dans le fichier secschema.def à extraire du fichier tar :

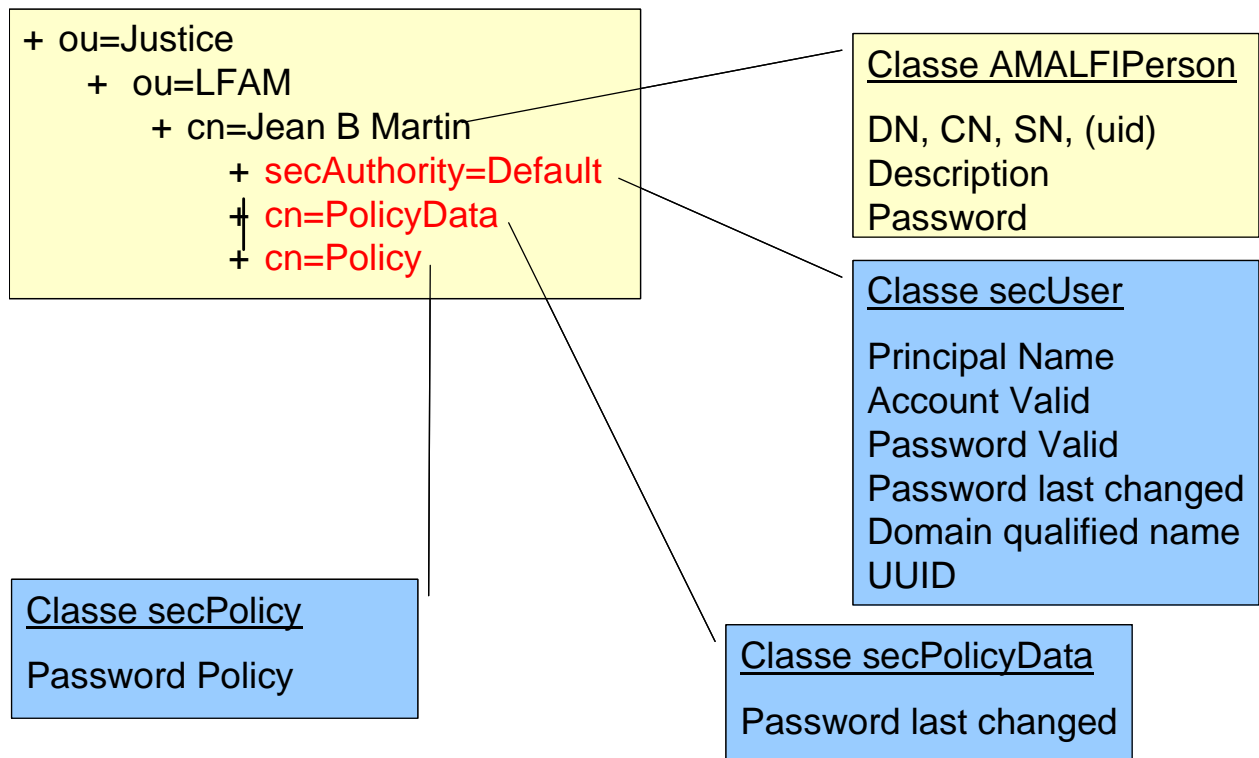
[http://www3.software.ibm.com/ibmdl/pub/software/tivoli\\_support/misc/Security/AMeB/am6.0/tuning\\_guide\\_scripts\\_60.tar](http://www3.software.ibm.com/ibmdl/pub/software/tivoli_support/misc/Security/AMeB/am6.0/tuning_guide_scripts_60.tar)



- SecResGroups
- SecResCreds

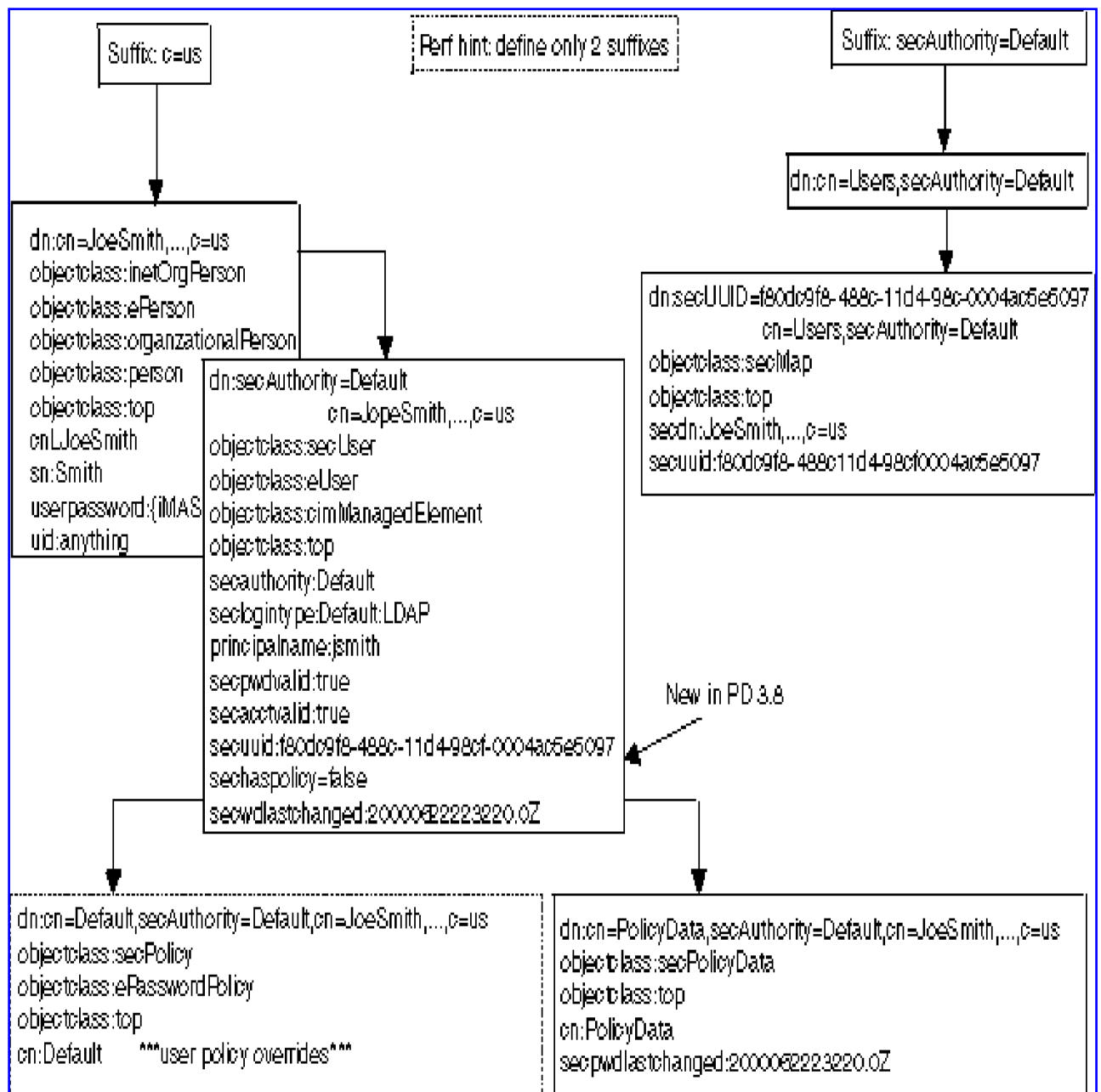
## **10.1.1.2. Arborescence de l'annuaire - TAM**

L'arborescence des données de l'annuaire LDAP imposée par le composant TAM version 6.0 peut-être représentée sur le schéma suivant.



**Figure 14 : Ajout de classes TAM pour la gestion des users dans LDAP**

Ainsi, sur un exemple plus détaillé, l'arborescence LDAP type est :



A un utilisateur (ou un compte) correspond, dans l'annuaire LDAP, un minimum de 4 entrées :

- Une première partie de l'arborescence des données doit être obligatoirement **à plat**. Les entrées de la classe `secMAP` sont **toutes** situées dans l'arborescence LDAP **directement** sous l'entrée `cn=Users,secAuthority=Default` (voir ci-dessus)... Cette partie de l'arborescence comprend donc les objets de la classe `secMap`
- La seconde partie de l'annuaire comprendra les objets des 3 classes `inetOrgPerson`, `secUser` et `secPolicyData` (les entrées de la classe `secPolicy` qui servent à remplacer pour un utilisateur la politique de gestion des mots de passe par défaut ne seront pas utilisées)

## **10.1.1.3. Les Groupes**

L'annuaire LDAP comportera également des groupes d'utilisateurs, puisqu'il est prévu de mettre en œuvre un premier niveau d'habilitation au niveau du composant WebSeal. Des droits sur certaines ressources seront positionnés en fonction de l'appartenance d'un utilisateur à un groupe.

## **10.1.1.4. Les droits sur les données de l'annuaire - TAM**

L'annuaire LDAP définit les droits sur ses propres données (ACL). Les droits sur les données de l'annuaire sont gérés à partir des principes suivants :

- L'utilisateur root (Au sens LDAP) aura, par nature, accès en lecture et écriture à toutes les informations de l'annuaire.
- Les utilisateurs n'auront pas le droit de mise à jour sur l'annuaire.

## **10.1.2. Modèle de données – Impacts IGC**

Concernant le SSEE, les ACs et les CRLs RAC et SE AMALFI sont publiées dans le serveur LDAP.

## **10.1.3. DIT Spécifique Exploitation de la solution**

Un certain nombre d'outils d'administration et d'exploitation utilise également l'annuaire LDAP. Une branche spéciale est gérée pour ces besoins. Cette branche est administrée par un utilisateur spécifique créé dans cette branche. Cet utilisateur a tous les droits sur cette branche de l'annuaire.

Cette arborescence a comme racine l'entrée ayant pour dn :

cn=amalfi\_Infra, ou=Livre Foncier Alsace/Moselle, ou=justice, o=gouv, c=fr.

Cette entrée est de la classe container.

Les entrées sous cette racine ne sont pas répliquées sur les serveurs LDAP en DMZ.

L'organisation de cette branche est laissée libre à l'exploitation. Les éléments du système AMALFI pour lesquels les utilisateurs sont gérés dans cette branche LDAP sont :

- ▶ Websphere
- ▶ AIX
- ▶ TAM

### **10.1.3.1. Websphere / TAM**

Cette branche LDAP comporte :

- Une définition des groupes d'exploitation ;
- La liste des cn associés que l'administrateur a choisi de positionner dans ces groupes.

Les utilisateurs sont créés avec des classes ePerson et les groupes sous forme de groupOfNames. L'organisation de cette arborescence est laissée libre.

WebSphere accède à l'annuaire LDAP avec un user de cette branche.

WebSphere ne fait pas de mises à jour de l'annuaire LDAP.

## **10.1.3.2. Impacts Users AIX**

L'ensemble des utilisateurs nominatifs pour les accès au serveur AIX sont gérés dans ce LDAP. Afin de gérer les utilisateurs AIX dans LDAP, il faut créer les entrées suivantes dans le serveur LDAP :

- ▶ Tous les groupes unix auxquels sont rattachés les users AIX gérés dans LDAP. Ces groupes font partie de la classe AIXaccessGroup
- ▶ Tous les utilisateurs gérés dans LDAP. Ces entrées font partie de la classe AIXaccount.