Intégration dans le contexte client

Version 1.0

ON-X S.A. *est une société du* ***Groupe ON-X***
15, quai Dion Bouton – 92816 PUTEAUX cedex. Tél : 01 40 99 14 14 – Fax : 01 40 99 99 58.
SA au capital de 3 752 000 Euros. RCS Nanterre B 391 176 971. Siret 00037. Code APE 721 Z.
www.on-x.com

Identification et historique

Identification client

Référence client	CCTP 0592110
Interlocuteur	Thierry LAHALLE – thierry.lahalle@sante.gouv.fr
Interlocuteur	Michel JANIN – michel.janin@cnav.fr

Identification ON-X

Référence ON-X	2005-1001-008
Version	1.0
Date	06/04/2006
Nombre de pages	17
Interlocuteur	Olivier Chapron – Directeur du projet – Consultant Manager 01 40 99 14 14 – olivier.chapron@edelweb.fr
Interlocuteur	Peter Sylvester – Expert 01 40 99 14 14 – peter.sylvester@edelweb.fr
Interlocuteur	Patrick Vigneras – Chef de projet 01 40 99 14 14 – pvigneras@on-x.com

Visa

Fonction	Nom
Rédaction	Patrick VIGNERAS
Vérification	Peter SYLVESTER
Approbation	Olivier CHAPRON

Historique

Date	Auteur	Version	Objet
04/04/06	PVS	0.1	Création du document, version préliminaire
05/04/06	PSR	0.3	Révision interne
06/04/06	OCN	1.0	Validation avant diffusion

Références

Identifiant	Titre
R1	Standard d'interopérabilité inter-organismes – *Olivier CHAPRON, Peter SYLVESTER – version 1.0 (13 juillet 2005)*
R2	http://www.ssi.gouv.fr/fr/
R3	Spécifications détaillées et de mise en œuvre (Réf. 2005-1001-001) – *Patrick Vigneras*
R4	Application des Spécifications détaillées pour le RNIAM, architecture WebService (Réf. 2005-1001-003) – *Patrick Vigneras*
R5	Application des Spécifications détaillées pour le RNIAM, architecture Portail à Portail (Réf. 2005-1001-004) – *Patrick Vigneras*
R6	Application des Spécifications détaillées pour la Retraite, architecture Portail à Portail (Réf. 2005-1001-005) – *Patrick Vigneras*
R7	Plan d'Intégration (Réf. 2005-1001-007) – *Olivier Chapron*

TABLE DES MATIERES

1. Introduction

1.1. Objet du document

Ce document présente une vision synthétique de notre compréhention des Systèmes d'Information des Organismes Clients ainsi que des propositions d'intégration des composants du standard correspondant au Lot 2 (*Lot 2 Vecteur et Proxy Organisme Client*, voir le document [R3]) discutées avec chacun. Ce document n'impose en rien des solutions de réalisation, il est essentiellement une synthèse des informations échangées pendant des réunions avec les Organismes Clients concernant des approches et des possibilités techniques pour la réalisation du standard par chacun de ces organismes.

Ce document ne porte que sur les Organismes Clients ayant pu échanger sur les aspects de la réalisation du standard, à savoir : CNAMTS, CNAF et MSA.

1.2. Organisation et structure du document

Pour chaque organisme on retrouvera dans le document :

- une brève description des systèmes d'identification et d'habilitation autour desquels viennent s'intégrer les composants nécessaires à la réalisation du standard,
- une proposition d'intégration de ces composants.

Ces descriptions font l'effet d'un chapitre par organisme et de renvois vers une annexe comprenant les compte rendus des réunions.

Outre la présente introduction, le document est structuré comme suit :

- Chapitre 2 : CNAMTS,
- Chapitre 3 : CNAF,
- Chapitre 4 : MSA,
- Les annexes.

2. CNAMTS

2.1. Description du système existant

Le système d'identification, d'authentification et d'habilitation de la CNAMTS est basé sur la combinaison de :

- Certificats numériques sous forme de cartes, pour l'identification des utilisateurs,
- AccessMaster pour l'authentification et la gestion des habilitations des utilisateurs,
- Un annuaire LDAP pour l'export d'information d'habilitation à des applications,

Il a été exposé également un exemple d'application avec un Proxy Squid qui utilise l'authentification des utilisateurs lors des accès externes par l'Internet.

L'*ANNEXE 1 : la fiche CNAMTS* page 9 décrit les interactions entre les différents composants du système existant de la CNAMTS.

2.2. Proposition d'intégration

Les interfaces aux composants du système existant permettent au standard de s'appliquer immédiatement en utilisant les composants génériques du Lot 2, à savoir l'interface LDAP.

En ce qui concerne le proxy : ainsi qu'il est précisé dans l'annexe, un enchainement en cascade de proxys n'est pas en contradiction avec le standard.

De façon similaire à Squid, un proxy sortant peut utiliser LDAP pour les habilitations d'accès à l'Internet, donc un serveur Apache quasiment standard en mode reverse proxy peut utiliser la gestion des habilitations LDAP d'une manière similaire.

L'attribution de PAGM peut être explicite dans LDAP ou être réalisés par une matrice d'associations de rôles métier à des PAGM sous forme d'un fichier (ou table dans LDAP). Il s'agit par exemple d'une table de correspondances d'un attribut existant LDAP avec un PAGM.

La CNAM devra étudier si l'on peut partir sur la base du proxy Squid (qui gère aussi un cache d'information), ou s'il est préférable de prendre un serveur Apache et d'utiliser un des modes d'authentification avec LDAP pour intégrer cela avec un module générique du Lot 2.

Compte tenu de l'existence d'un mode d'authentification forte sans gestion des sessions avec des certificats d'agent, il nous semble possible de développer cette solution d'une façon totalement générique, ce qui pourrait par la suite faire partie d'une implémentation de référence, du fait de la simplicité de mise en place de quelques certificats et d'un annuaire LDAP.

3. CNAF

3.1. Description du système en cours de mise en œuvre

Le système en cours de mise en œuvre au sein de la CNAF repose sur :

- un serveur J2ee,
- un annuaire LDAP Domino,
- une Base de traces BSA.

L'*ANNEXE 2 : la fiche CNAF* page 11 décrit l'ensemble des composants et les méthodes d'habilitation en cours de mise en œuvre au sein de la CNAF.

La CNAF a présenté une architecture logique de point de remplissage pour le vecteur d'identification dans leur contexte. La solution envisagée est basée sur JAVA.

3.2. Proposition d'intégration

La proposition d'intégration des composants du Lot 2 du standard est décrite dans l'annexe.

Il s'agit de :

- Bénéficier des flux XML de description de service pour distribuer les PAGM nécessaires à une requête,
- Utiliser la construction du jeton SAML pour y intégrer les éléments du vecteur d'identification.

Dans ce cadre, la CNAF pourra :

- soit utiliser les éléments génériques du Lot 2 du standard pour créer l'assertion SAML en utilisant directement l'interface LDAP,
- soit utiliser les interfaces internes des composants de sureté décrits dans l'annexe pour compléter le jeton SAML en en faisant le vecteur d'identification requis par le standard.

Remarque additionnelle ON-X

Nous avons mis en avant le fait que l'architecture proposée nous semble quelque peu monolithique du fait du paradigme d'utilisation d'API dans le contexte JAVA. Cependant, il nous semble aisé d'ajouter les couches de communication nécessaires pour séparer physiquement certaines fonctions, comme par exemple le traçage.

4. MSA

4.1. Description du système existant

Le système d'information de la MSA repose sur une gestion décentralisée des habilitations.

Il utilise :

- une Identification par annuaire LDAP national répliqué,
- une Habilitation par base régionale,
- un Serveur d'applications régional WebLogic.

L'*ANNEXE 3 : la fiche MSA* page 14 décrit l'organisation du système d'information de la MSA.

4.2. Proposition d'intégration

La solution mise en avant dans les réflexions avec la MSA met en avant une solution Apache reverse proxy avec LDAP.

L'annexe MSA présente deux scénarios d'intégration des composants du Lot 2 du standard au sein du système d'information de la MSA.

Dans les deux cas les modules génériques du Lot 2 sont utilisés mais :

- soit ils devront être modifiés pour intégrer les données du jeton transmis du niveau régional au niveau national,
- soit une interface entre le jeton transmis et le module de Construction du Vecteur d'Identification doit être installée.

Remarque additionnelle ON-X

Cette solution doit gérer localement des cookies de session. Il s'agit du travail le plus important à réaliser.

5. ANNEXE 1 : la fiche CNAMTS

5.1. Présentation

Cette fiche est le résultat validé par la CNAMTS de la réunion du 09 février 2006.

5.2. Fiche CNAMTS

Présentation du standard

Rappel des éléments du standard tels que définis par la prestation précédente : PAGM, vecteur d'identification, assertion SAML, proxy et reverse proxy, problématiques de sécurisations de proche en proche et de bout en bout.

Rappel des travaux en cours sur les spécifications détaillées du standard en particulier en termes de découpage par modules, de gestion des accords d'interopérabilité, de performance et de la non corrélation entre le standard et les données d'échange purement applicatives (en particulier la présentation des services par les portails fournisseurs).

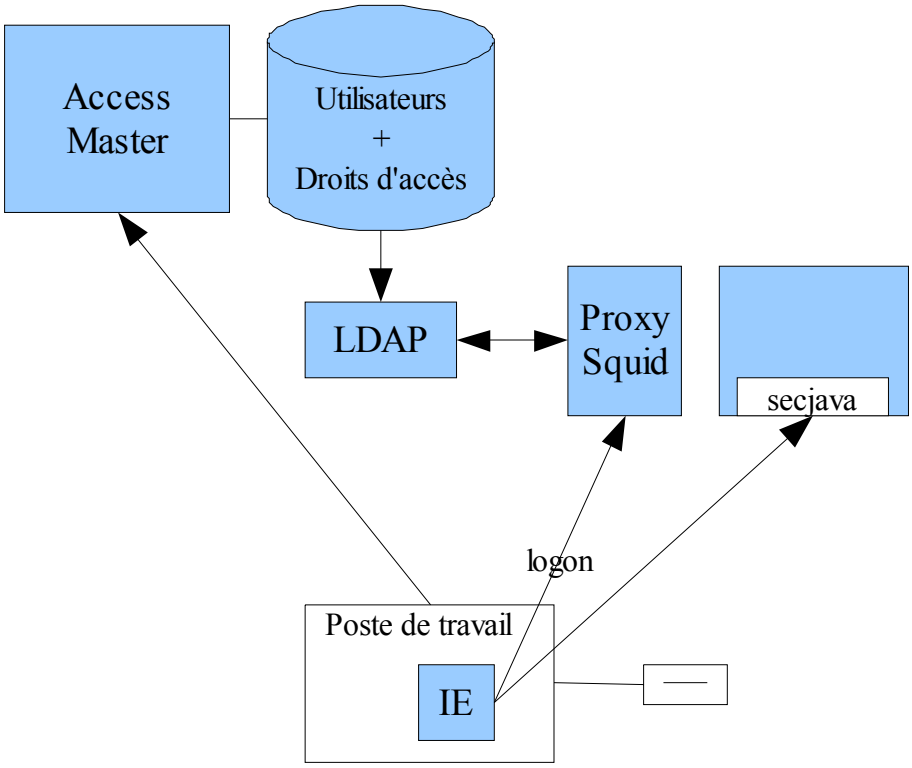
Mise en avant des éléments de l'interopérabilité à prendre en charge par les Organismes Client : la confidentialité des communications avec le fournisseur, la création d'un vecteur d'identification à insérer dans les requêtes sortantes, le besoin d'identification utilisateur et la récupération des autorisations associées, la corrélation entre les autorisations utilisateurs et les autorisations définies dans les accords, le traçage des vecteurs d'identification.

L'important est de faire remplir ces fonctions par le système local, en particulier en ce qui concerne les autorisations. Il est noté toutefois que, en l'absence d'une fonction équivalente, l'essentiel des fonctions sont supportées par des produits existant, notamment open source.

Shibboleth est évoqué à ce propos.

Présentation du système d'habilitation CNAMTS

Le système d'habilitation repose sur l'utilisation d'AccessMaster. La figure ci-dessous représente le fonctionne général du système d'identification, authentification et habilitation :



126 L'authentification des utilisateurs s'effectue par carte avec certificat. AccessMaster envoie les droits des
127 utilisateurs au poste de travail.

128 L'organisation représente environ 150 AccessMaster installés. Il n'y a pas d'incidence sur l'application du
129 standard

130 Le proxy utilisé par la CNAMTS est Squid. Lors d'un accès vers l'extérieur, un utilisateur (de IE) accède au
131 proxy, un identifiant/mot de passe est demandé. Le proxy accède à un répertoire LDAP pour autoriser ou
132 non l'accès.

133 Il est noté que l'utilisation de Squid n'est pas en contradiction avec le standard. Il est aussi noté que, si le
134 cas se présentait, un enchaînement en cascade de proxys n'empêche pas le standard d'être applicable.

135 Il est rappelé que les choix effectués par les organismes en matière de sécurité interne ne relève pas de
136 l'interopérabilité.

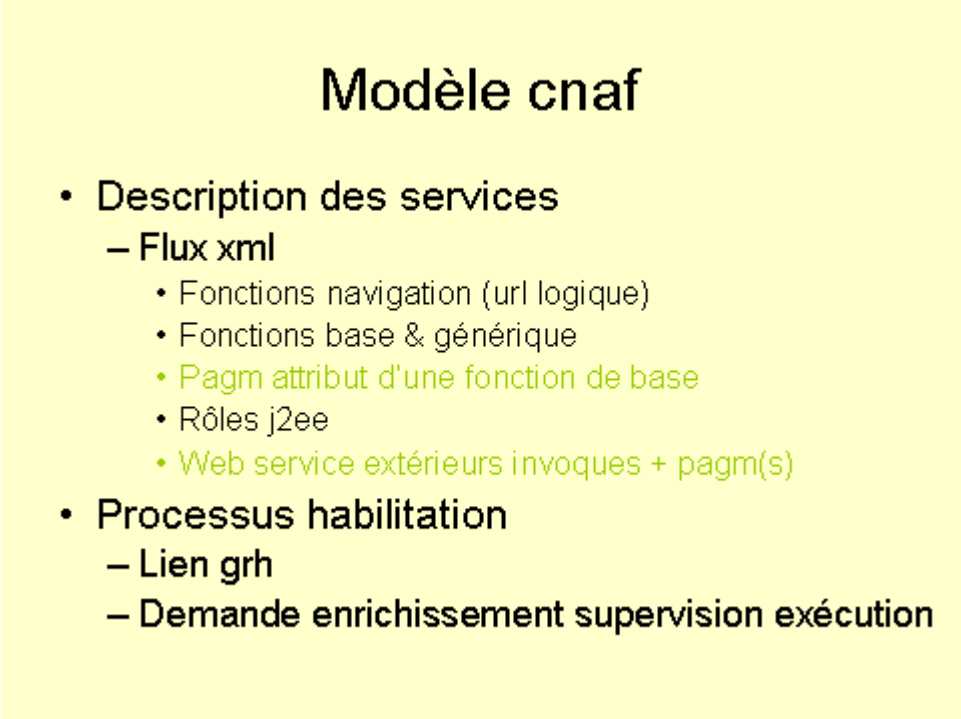
137 # 6. ANNEXE 2 : la fiche CNAF

138 ## 6.1. Présentation

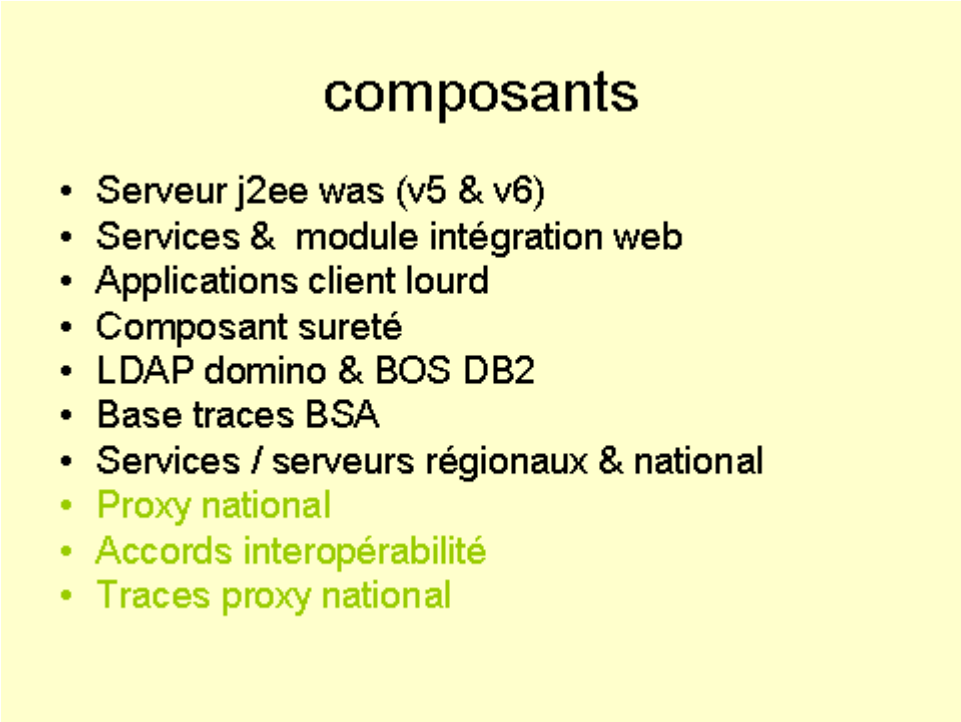
139 Cette fiche est la présentation réalisée par la CNAF lors de la réunion du 15 février 2006.

140 ## 6.2. Fiche CNAF

141 *Page 1 : Modèle cnaf*

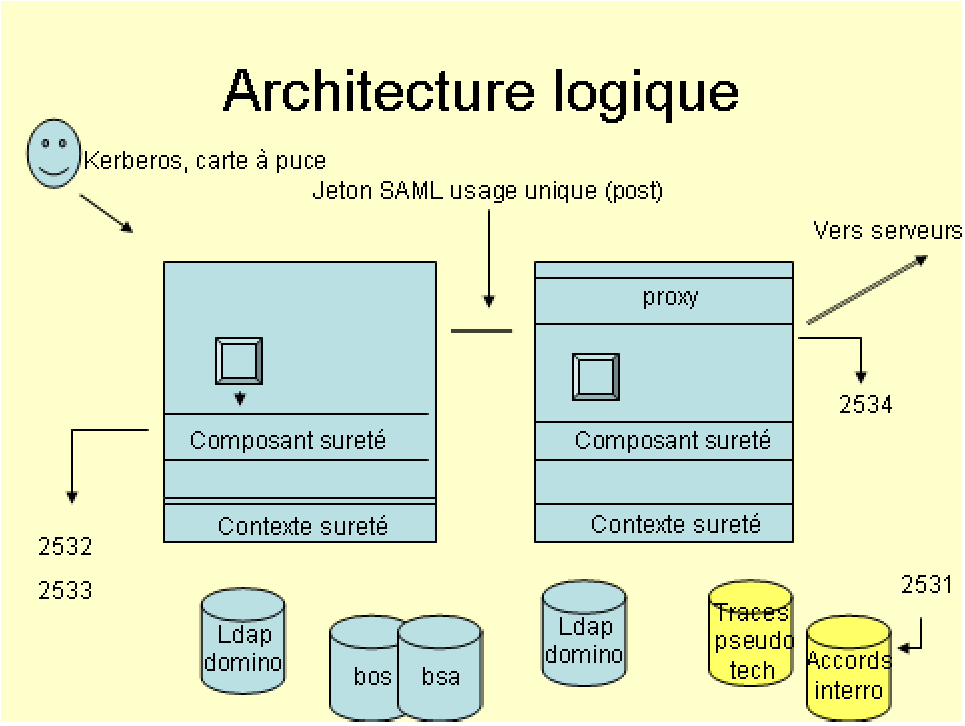


142 *Page 2 : Composants*



143 *Page 3 : Architecture logicielle*

144 *Dans cette page les numéros 2531, 2532, 2533 et 2534 font référence à des éléments du vecteur*
145 *d'identification. Selon le document de spécification [R1], lire respectivement 2531, 2532, 2533 et 2534*
146 *comme étant respectivement les éléments 1, 2, 3 et 4 du vecteur d'identification décrit au paragraphe*
147 *2.6.1, à savoir : numéro de version, identifiant de vecteur, identifiant de l'organisme client et identifiant du*
148 *demandeur.*


Architecture logique
Kerberos, carte à puce
Jeton SAML usage unique (post)
Vers serveurs
proxy
2534
Composant sureté
Contexte sureté
Composant sureté
Contexte sureté
2532
2533
2531
Ldap domino
bos
bsa
Ldap domino
Traces pseudo tech
Accords interro

149

7. ANNEXE 3 : la fiche MSA

7.1. Présentation

Cette fiche est le résultat validé par la MSA de la réunion du 07 mars 2006.

7.2. Fiche MSA

Présentation générale de la structure du SI de la MSA

Il s'agit, potentiellement, de plusieurs systèmes d'habilitation, la gestion y est décentralisée : il y a 3 niveaux de gestion :

1. Niveau départemental : ce sont les différentes caisses, là où sont les applications de type bureautique,
2. Niveau régional : il y a 5 centres, c'est la gestion des applications,
3. Niveau national : le centre gérant les applications nationales, les relations avec les autres organismes.

Présentation du standard

Rappel des éléments du standard tels que définis par la prestation précédente : PAGM, vecteur d'identification, assertion SAML, proxy et reverse proxy, problématiques de sécurisations de proche en proche et de bout en bout.

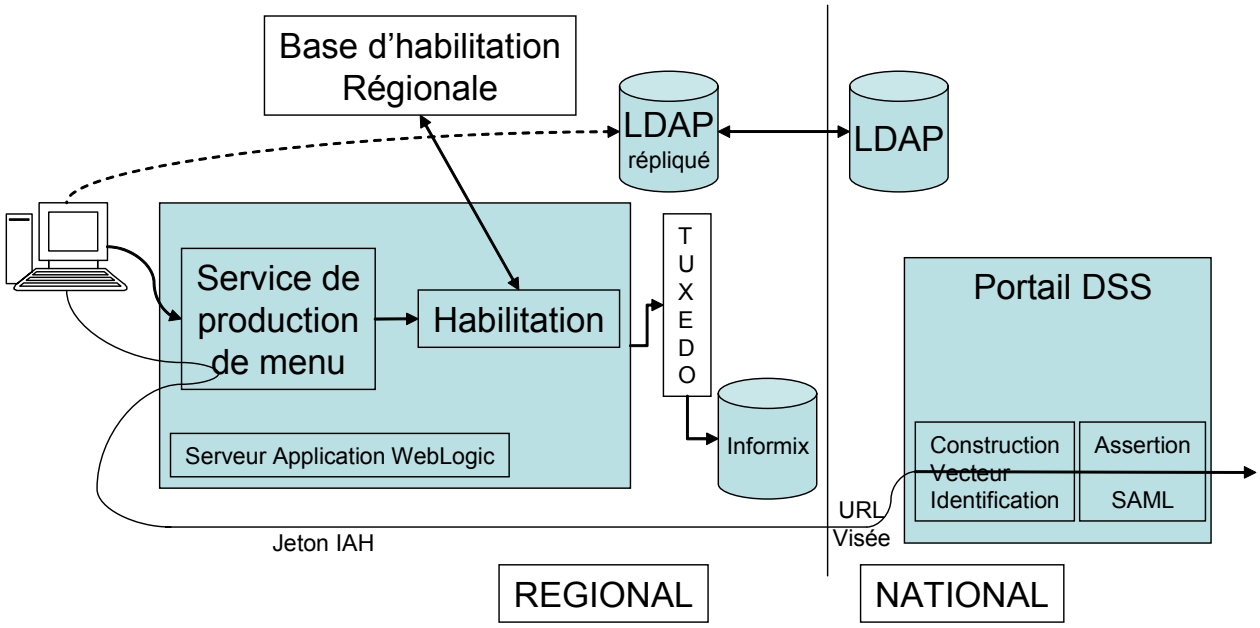
Rappel des différentes problématiques liées à l'adressage des services, en particulier la notion même de service du point de vue du standard ne doit pas être confondue avec un service tel qu'il peut être défini par un organisme fournisseur.

Ainsi, du point de vue du standard, un service existe s'il est publié dans la convention et il peut être tout ou partie de l'ensemble des fonctionnalités d'une application mises à disposition de clients par un organisme fournisseur, aussi bien que la combinaison de fonctionnalités de plusieurs applications mises à disposition de clients par un organisme fournisseur.

Deux scénarios d'intégration du standard dans les systèmes MSA

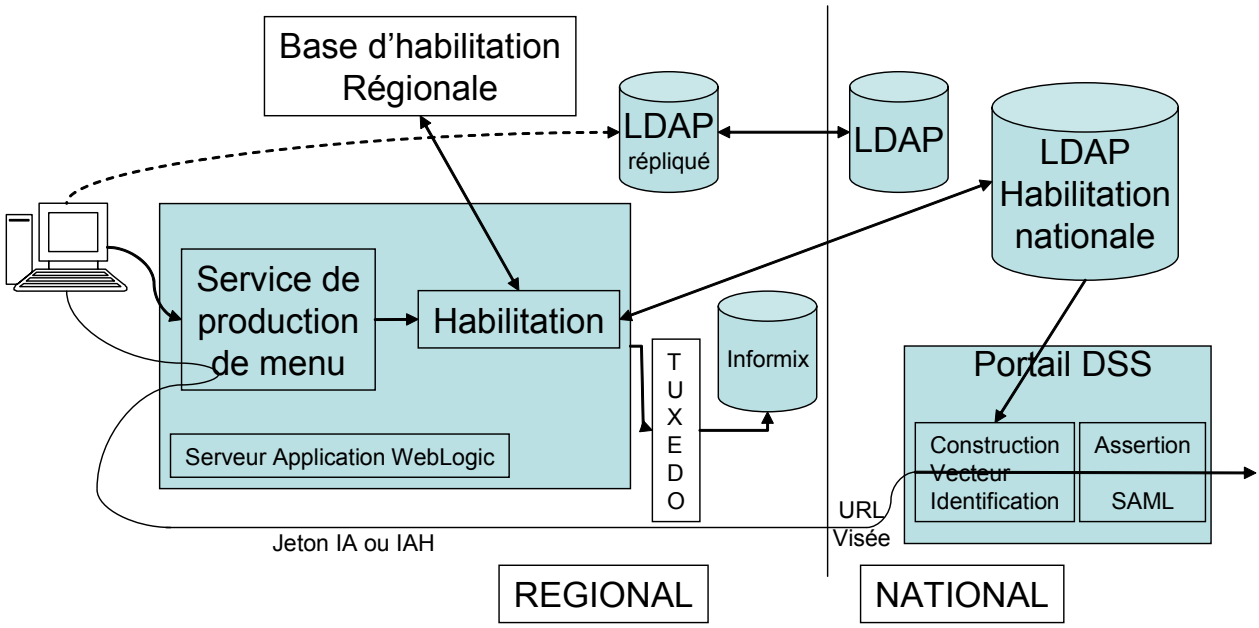
Deux scénarios sont discutés permettant de valider les pistes travaillées en interne par la MSA.

Scénario 1 :



176 Ce scénario montre que la présentation de menu est gérée en fonction des habilitations gérées
177 régionalement. Le vecteur d'identification est géré uniquement au niveau national. Les Actions
178 Elémentaires sont transformées par le module de construction du vecteur d'identification en PAGM.

179 Scénario 2 :



180 Par rapport au scénario précédent les attributs permettant de gérer les PAGM ne sont plus transmis du
181 niveau régional vers le niveau national mais sont récupérés auprès d'une base nationale d'habilitation.

La proposition de laisser au serveur d'application le soin de gérer la construction de vecteur d'identification n'est pas retenue pour un problème de performance.

De manière générale, un autre problème est évoqué : comme il n'y a pas de session avec le standard, la MSA doit mettre en place un mécanisme permettant de terminer la session locale avec le jeton IA/IAH

186 .

FIN DU DOCUMENT