Pour

Application des Spécifications détaillées pour la Retraite, architecture portail à portail

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	2005-1001-005
Version	1.0
Date	03/04/06
Nombre de pages	20
Interlocuteur	Olivier Chapron – Directeur du projet – Consultant Manager 01 40 99 14 14 – olivier.chapron@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
03/01/06	PVS	0.1	Création du document, version préliminaire
08/03/06	PVS	0.4	Révision interne
20/03/06	PVS	0.8	Révision interne
21/03/06	OCN	0.9	Validation avant diffusion aux organismes de la version pré-finale
03/04/06	OCN+PSR +PVS	1.0	Version finale approuvée formellement

Références

Identifiant	Titre
R1	Standard d'interopérabilité inter-organismes – *Olivier CHAPRON, Peter SYLVESTER – version 1.0 (13 juillet 2005)*
R2	Spécifications détaillées et de mise en œuvre – *Patrick Vigneras*

Sommaire

1. Introduction

1.1. Objet du document

Ce document étend le document [R2] de spécifications détaillées de l'interopérabilité en décrivant les éléments spécifiques du standard d'interopérabilité pour son application **au service RNIAM pour le mode Portail-à-portail.**

1.2. Relation avec d'autres documents

Ce document complète le document [R2] pour les besoins spécifiques du RNIAM dans le contexte Portail à Portail.

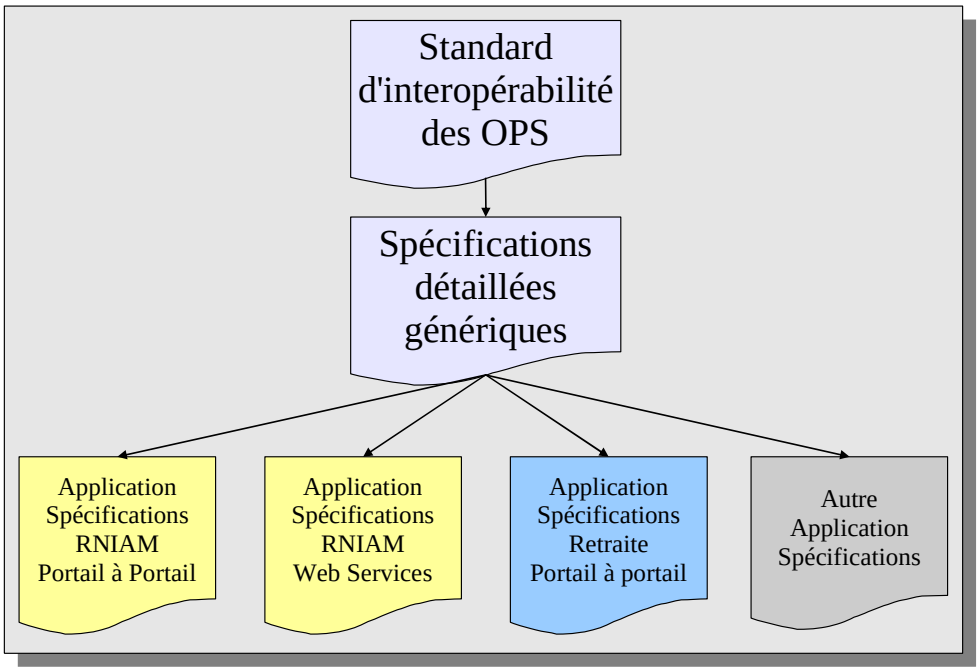


Figure 1 : relation avec d'autres documents

1.3. Organisation et structure du document

La structure du présent document reprend celle du document de Spécifications Détaillées [R2] :

- Le chapitre *2 Eléments d'architecture* : décrit le service Retraite, comment les organismes interagissent à travers Retraite et quels sont les parties du standard spécifiquement impactées par le service Retraite,

- Le chapitre *3 Module de transcription du vecteur d'identification* : décrit comment le standard doit être appliqué dans le cadre spécifique du service Retraite.

Dans la suite du document, les remarques et commentaires ON-X ne relevant pas des spécifications mais servant à éclairer ou étendre certains propos seront présentés dans le formatage texte courant : texte italique encadré de bleu.

2. Eléments d'architecture

2.1. Les Organismes

L'Organisme Fournisseur est la CNAVTS et les Organismes Clients sont la MSA et l'ORGANIC/CANCAVA.

2.2. Le service

Il s'agit de mettre à disposition des Organisme Clients le service Retraite sous forme de deux services distincts :

- Le service de Notification,
- Le service d'Actualités.

Dans le cadre du service Retraite, il y a potentiellement deux profils applicatifs d'accès aux données : le profil applicatif standard (qui représente 99% des utilisateurs) et le profil applicatif webmestre qui est une extension du profil standard avec la possibilité d'accéder aux données statistiques. Ce profil a uniquement un intérêt interne à la CNAVTS.

En date du 1er mars 2006 le service Retraite est prévu pour le mode Portail-à-Portail uniquement.

2.3. Attribution de PAGM

Il n'est pas du ressort de ce document de proposer les PAGM pour les échanges Retraite entre organismes. Par contre, il est rappelé les points suivants :

- A l'heure actuelle les Organismes Clients devraient transmettre, dans les requêtes à destination du service Retraite, tous les PAGM attribués à l'utilisateur pour le service Retraite,
- Les règles d'attribution de PAGM (contraintes) doivent être exprimées dans la convention.

2.4. Présentation de service

La présentation des services Retraite, c'est à dire la façon dont l'Organisme Fournisseur va adapter les menus contextuels ainsi que la mise en forme peut être considéré comme un service.

Si, à l'heure actuelle, la CNAVTS ne prévoit pas, dans le cadre du service Retraite, de différencier les données en fonction des organismes il est prévu de différencier la présentation en fonction des PAGM transmis. C'est pourquoi il est recommandé de transmettre tous les PAGM valides lors de chaque requête.

2.5. Eléments spécifiques

Le document [R2] ayant défini les éléments génériques.

Le présent document défini les éléments non génériques, c'est à dire nécessitant une spécification particulière liée au service.

Il s'agit dans le cas présent du module de transcription du vecteur d'identification qui provient de l'Organisme Fournisseur. Dans le cadre Retraite il doit reposer sur le système existant : le SSO Oracle combiné avec la base SAS pour la récupération des éléments d'habilitation à l'accès au service Retraite.

3. Module de transcription du vecteur d'identification

C'est l'élément spécifique au service Retraite (c'est à dire le service de Notification et le service d'Actualités) pour le mode Portail-à-portail. Il repose sur le mécanisme d'identification et d'habilitation SAS mis en œuvre par la CNAVTS.

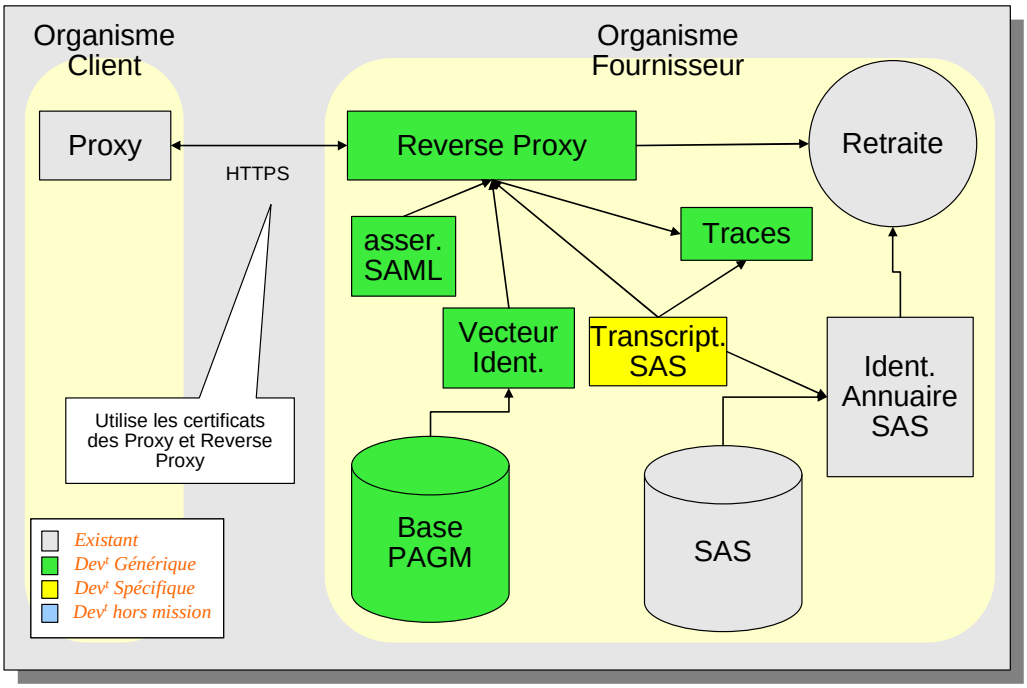


Figure 2 : Module Transcription SAS

Les éléments Retraite Identification Annuaire SAS et Base SAS sont les éléments que le module de Transcription SAS va utiliser : ils sont intégrés au SSO Oracle selon le mécanisme décrit dans ce chapitre.

Ce chapitre décrit aussi comment le module de transcription peut utiliser ces éléments.

> *Il est rappelé que le module de transcription ne vérifie pas la validité du vecteur d'identification, c'est-à-dire le fait qu'un Organisme Client a le droit d'émettre une requête pour un service donné et avec la liste de PAGM fournie. Cela est fait dans le module Vecteur d'Identification. Ainsi, si d'un point de vue réalisation logicielle, les deux fonctions peuvent être confondues dans les mêmes éléments logiciels, ce document ne s'attache qu'à décrire la fonction de transcription du vecteur d'identification.*

3.1. Identification et habilitation avec SSO Oracle et SAS

3.1.1. Principe

La CNAVTS utilise le système SSO Oracle dans le cadre des accès portail-à-portail pour gérer l'authentification et la session d'un utilisateur distant. L'identification et l'authentification à la base s'effectue à l'aide d'un dispositif de type login, password. Le SSO Oracle permet d'incruster un module (le

TPAM – Third Party Access Manager) au SSO pour récupérer et vérifier les données de sécurité. Dans le système de la CNAVTS le TPAM permet l'accès à la base SAS.

Actuellement le système de la base SAS permet d'enregistrer des utilisateurs externes à la CNAVTS pour leur autoriser l'accès aux services internes, en fonction d'accords de service passés entre la CNAVTS et des organismes partenaires d'où sont issus ces utilisateurs.

Le schéma suivant décrit la cinématique d'une requête lors de l'établissement d'une session :

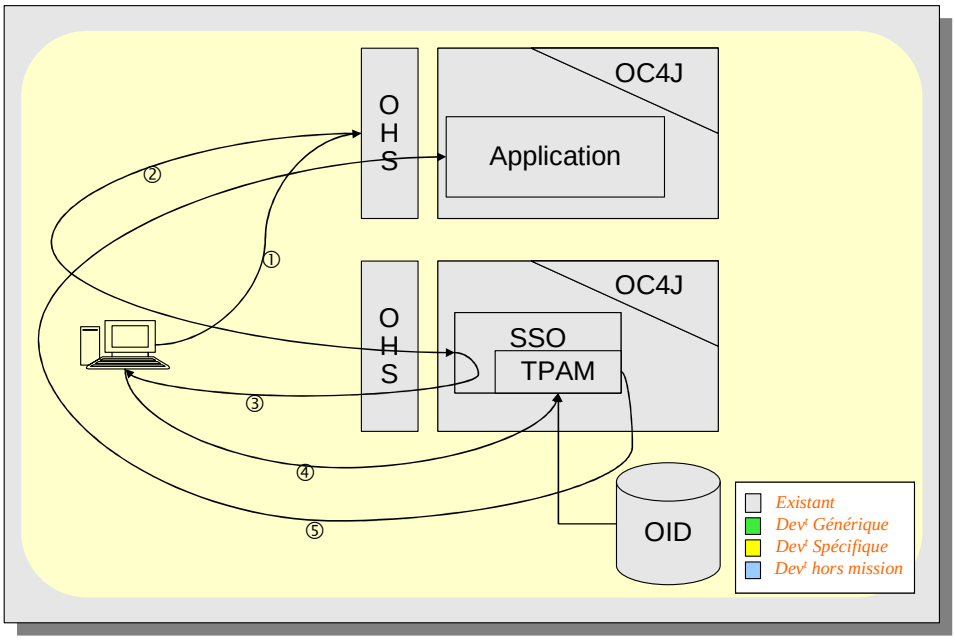


Figure 3 : Cinématique d'une requête

L'OHS (Oracle HTTP Server), l'OC4J (Oracle Container For Java), le TPAM (Third-Party Access Manager) et l'OID (Oracle Internet Directory) sont des éléments du SSO Oracle.

Le schéma présente cinq flux. Ils sont décrits plus finement ci-dessous, en se basant sur l'analyse fournie par la CNAVTS :

3.1.1.1. Flux 1 : la requête cliente

L'application cliente effectue une requête sur une URL, il s'agit d'une première connexion, il n'y a donc pas de cookie contenant les éléments d'identification et d'habilitation de l'utilisateur.

Requête client vers l'OHS primaire : **GET** http://**serveur-appli**/page-originale-visée, pas de cookie identifiant, pas de cookie SSO

Réponse OHS : 302 Redirection vers le système SSO

3.1.1.2. Flux 2 : Redirection vers le SSO

L'OHS détecte qu'il s'agit d'une première connexion, il redirige le client vers l'adresse du SSO. Noter que les paramètres de la requête originelle sont perdus.

Requête client vers le système SSO : **GET** http://**serveur-sso**/admin-login, pas de cookie identifiant

Réponse SSO : 302 Redirection vers la page de saisie

3.1.1.3. Flux 3 : Page de saisie de mot de passe

Le système SSO Oracle renvoie vers le client une page permettant la saisie d'un login et mot de passe.

Requête client vers le système SSO : **GET** http://**serveur-sso**/login

Réponse SSO : la page de saisie de login et mot de passe

3.1.1.4. Flux 4 : Vérification par le TPAM

Le client renvoie les login et mot de passe et le SSO vérifie ces informations via l'OID. Le module TPAM dans le cadre de Retraite accède à la base SAS pour permettre cette vérification. Si la vérification est réussie un token Oracle est généré.

Requête client vers le système SSO : **POST** http://**serveur-sso**/authentification

Réponse SSO : 302 Redirection vers l'OHS primaire avec création de cookie identifiant

3.1.1.5. Flux 5 : Création de cookie de session

Le token est transmis par redirection au premier OHS lequel génère un cookie SSO pour le client et contenant les informations d'identification et d'authentification pour session.

Le module de transcription peut donc se reposer sur ces deux systèmes : le SSO Oracle et la base SAS, pour réaliser l'autorisation d'accès avec le vecteur d'identification.

Requête client vers l'OHS primaire : **GET** http://**serveur-appli**/login-ok avec cookie identifiant, pas de cookie SSO

Réponse OHS : 302 Redirection vers le système SSO

Requête client vers le système SSO : **GET** http://**serveur-sso**/admin-login avec cookie identifiant

Réponse SSO : 302 Redirection vers l'OHS primaire avec mise à jour du cookie identifiant

Requête client vers l'OHS primaire : **GET** http://**serveur-appli**/login-ok avec cookie identifiant, pas de cookie SSO

Réponse OHS : 302 Redirection vers la page originale visée avec création du cookie SSO

3.1.2. Identification SAS

Hors du cadre du standard d'interopérabilité la base SAS est utilisée pour permettre à des utilisateurs externes précisément identifiés d'accéder aux services de la CNAVTS. L'identification avec le SSO Oracle et la base SAS est une paire {login, password}, telle que définie par l'administrateur qui enregistre chaque utilisateur dans la base SAS.

Dans le cadre de l'interopérabilité il n'y a pas d'authentification de bout en bout. Pour autoriser l'accès au service il faut prévoir des identifiants dans la base SAS et faire correspondre les vecteurs d'identification reçus à ces identifiants. Il n'est pas nécessaire d'enregistrer ces identifiants de façon dynamique : une possibilité d'identifiant dans la base SAS est la liste des combinaisons PAGM – Organisme Client.

3.1.3. Délégation d'administration SAS

Hors du cadre du standard d'opérabilité : la base SAS est accessible en externe par des administrateurs désignés et appartenant à un organisme autre que la CNAVTS pour permettre l'ajout d'utilisateurs du même organisme que l'administrateur.

Il n'est pas prévu d'utiliser ce mécanisme dans le cadre de l'interopérabilité.

3.1.4. Session

Le système SSO Oracle utilise, grâce au cookie contenant les informations d'identification et d'habilitation, un mécanisme de session avec une fonction de terminaison de session (logout) permettant d'invalider le cookie. Le standard ne prévoit pas l'utilisation de session : le vecteur d'identification accompagnant chaque requête est suffisant en soi pour permettre l'accès (ou l'interdire) à un service donné. En conséquence, il est fortement suggéré de ne pas proposer un lien vers cette fonction.

Il nous semble dangereux de transmettre le cookie de session à l'Organisme Client pour plusieurs raisons. Le Reverse Proxy frontal CNAVTS doit assurer que :

- Un utilisateur dûment habilité ait accès au service demandé, avec une session créée de manière transparente par le SSO Oracle,
- Tout autre utilisateur ne peut pas utiliser cette même session pour accéder au service,
- Un cookie ne doit pas être en conflit avec un système d'authentification local du client,
- L'environnement Organisme Client filtre des cookies, en particulier, si la passerelle « client » utilise un système de maintient de session similaire (ou identique).

En principe, il est possible de générer le cookie de session Oracle pour chaque requête à partir du vecteur d'identification. Puisque l'utilisateur n'intervient pas, le seul impact est la performance interne entre le Reverse Proxy et le système SSO Oracle. Pour améliorer la performance il suffit que le Reverse Proxy maintienne un cache de cookie et vecteur d'identification.

Pour illustrer la problématique, il suffit de regarder la CNAVTS comme étant un fournisseur pour elle-même à travers une passerelle portail de création de vecteur d'identification, où l'authentification locale client se fait également avec le SSO Oracle.

3.2. Organisation du module de transcription

La transcription utilise le mécanisme de cookie du SSO Oracle ainsi que le lien entre le système SSO avec la base SAS à l'aide d'un TPAM.

La transcription du vecteur d'identification peut donc être réalisée en intégrant deux éléments dans l'architecture de la CNAVTS :

- Un module TPAM permettant de faire le lien avec la base SAS pour la vérification des éléments contenus dans le vecteur d'identification,

- Un module de gestion lié au Reverse Proxy et gérant la transcription vis-à-vis du système SSO Oracle.

Ceci peut se décliner de deux manières : si le module TPAM est nécessairement intégré au système SSO, le module de gestion peut être intégré soit au premier OHS soit directement au Reverse Proxy.

3.3. Module de vérification TPAM

Le module de vérification TPAM s'intègre au niveau du système SSO Oracle.

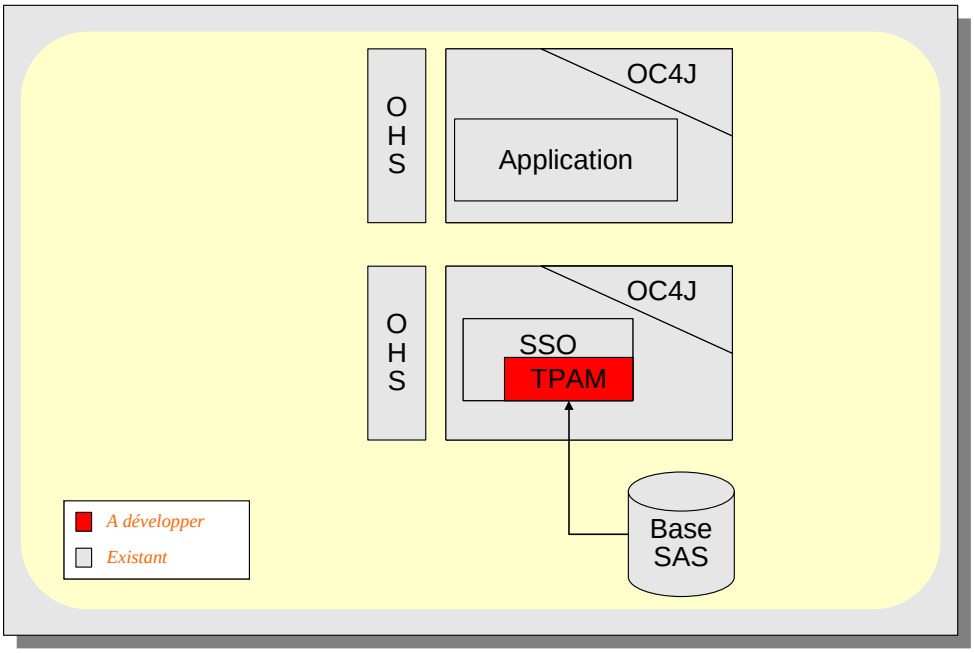


Figure 4 : module de vérification TPAM

3.3.1. Rôle du module

Le rôle de ce module est, dans le cadre du module de transcription du vecteur d'identification, de finaliser l'identification vis-à-vis de la base SAS, de permettre la génération du token Oracle qui autorise l'ouverture locale d'une session et, éventuellement, d'insérer dans la base SAS les informations d'identification de l'utilisateur.

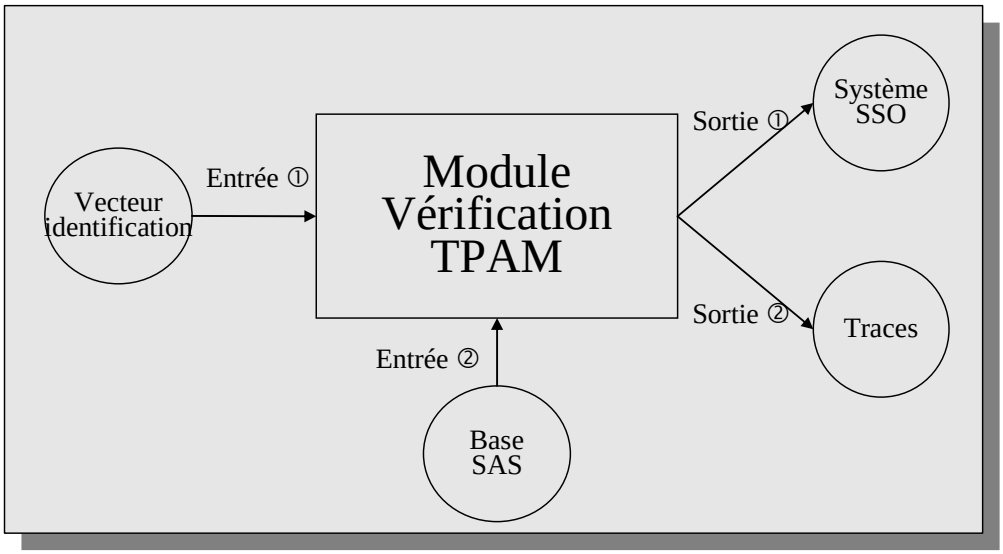


Figure 5 : Module de vérification TPAM

3.3.2. Interface d'entrée

3.3.2.1. Flux numéro 1 : le vecteur d'identification par le système SSO

Le système SSO reçoit une requête http contenant le vecteur d'identification sous forme d'assertion SAML, lors de la redirection. Il le transmet au module de vérification TPAM. Cette transmission s'effectue selon l'interface définie pour un module TPAM par le système SSO Oracle.

3.3.2.2. Flux numéro 2 : la base SAS

Le module de vérification TPAM récupère auprès de la base SAS les éléments d'identification qui seront utilisés pour la génération d'un token Oracle par le système SSO d'une part et pour identification par les applications d'autre part, en fonction de la liste des PAGM présente dans le vecteur d'identification.

3.3.3. Interface de sortie

3.3.3.1. Flux numéro 1 : la validation à travers le système SSO

Le module de vérification TPAM transmet, selon l'interface définie pour un module TPAM par le système SSO Oracle, les éléments de validation de l'identification permettant notamment au système SSO de générer le token Oracle.

3.3.3.2. Flux numéro 2 : les traces

Ce lien est recommandé dans la mesure où c'est dans ce module qu'est fait le lien entre un identifiant de la base SAS et le vecteur d'identification. La trace est donc le vecteur d'identification ainsi que l'identifiant SAS.

3.4. Module de gestion intégré au Reverse Proxy

Intégrer le module de gestion au Reverse Proxy oblige à prendre en compte les ordres de redirection donnés par le premier OHS. Par contre cela évite de modifier l'OHS lui-même ainsi que de gérer les éventuels distributions sur plusieurs hôtes de l'OHS secondaire auquel est attaché le système SSO.

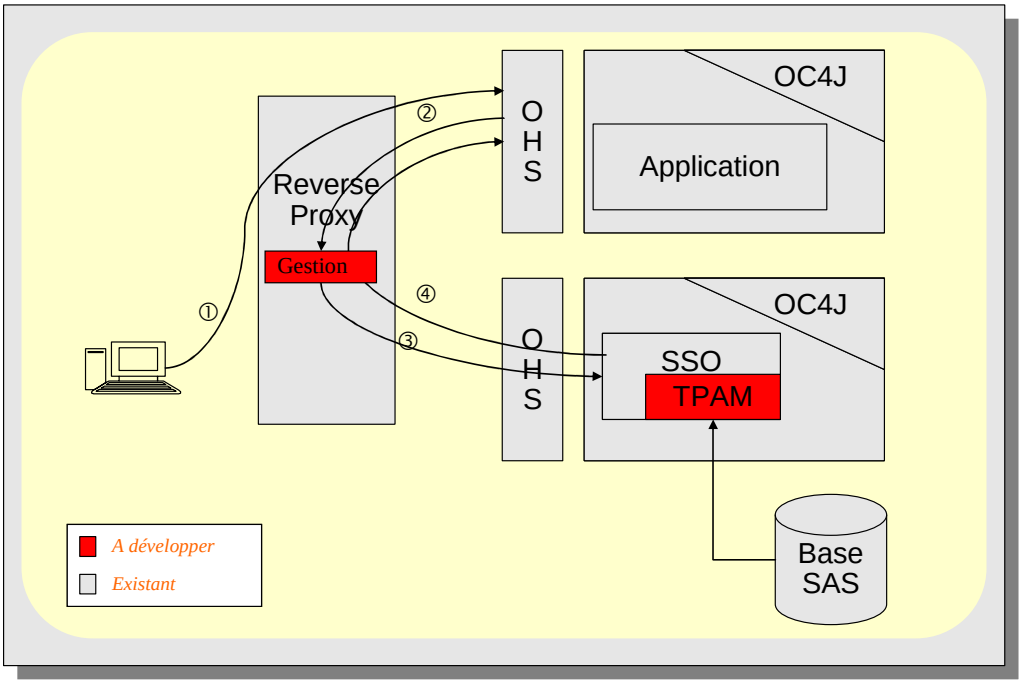


Figure 6 : Module de gestion intégré au Reverse Proxy

Le schéma ci-dessus est organisé selon les quatre flux décrits dans les paragraphes suivants.

3.4.1.1. Flux numéro 1 : la requête avec le vecteur d'identification

La requête, traitée par le système de l'Organisme Client contient un vecteur d'identification.

3.4.1.2. Flux numéro 2 : Redirection vers le SSO

L'OHS détecte qu'il s'agit d'une première connexion, il redirige le client vers l'adresse du SSO. Noter que les paramètres de la requête originelle sont perdus. Cette demande de redirection est captée par le module de gestion.

3.4.1.3. Flux numéro 3 : Redirection avec vecteur d'identification

Le module de gestion applique la redirection vers le système SSO en joignant le vecteur d'identification.

3.4.1.4. Flux numéro 4 : Création de cookie de session

Après validation par le système SSO et le module de vérification TPAM intégré, le module de gestion reçoit la dernière redirection vers l'URL d'origine avec le token Oracle et insère à nouveau le vecteur d'identification. La requête est envoyée au premier OHS qui peut dès lors créer le bon cookie de session.

3.4.2. Rôle du module

Ce module a pour rôle de capter les requêtes de redirections émises par le SSO Oracle lors du démarrage de session et de s'assurer de la bonne transmission à chaque requête de redirection du vecteur d'identification.

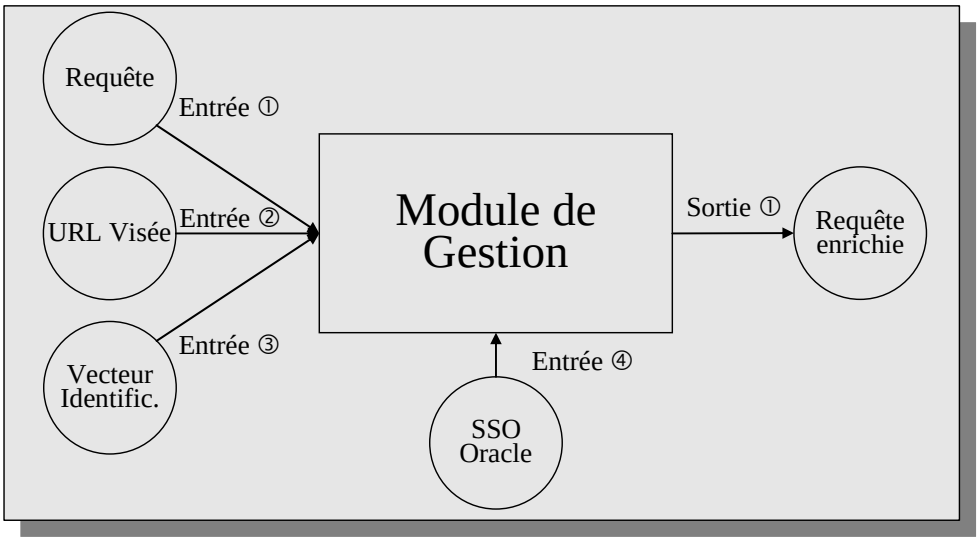


Figure 7 : Module de gestion

3.4.3. Interface d'entrée

3.4.3.1. Flux numéro 1 : la requête

S'il s'agit de la requête d'origine le module enregistre le vecteur d'identification. S'il s'agit d'une requête de redirection (en réponse à la requête d'origine), le module applique la redirection en transmettant aussi le vecteur d'identification.

3.4.3.2. Flux numéro 2 : l'URL Visée

Permet de déterminer le comportement du module concernant la requête et le vecteur d'identification.

3.4.3.3. Flux numéro 3 : le vecteur d'identification

Le module doit connaître le vecteur pour permettre sa transmission au module de vérification TPAM lequel fera la transcription effective vers le système d'identification/autorisation local.

3.4.3.4. Flux numéro 4 : le SSO Oracle

Le module intercepte les requêtes de redirection provenant du SSO Oracle et les applique en transmettant toujours le vecteur d'identification. Il relaie toutefois les deux requêtes de redirection qui contiennent les instructions de création de cookie.

3.4.4. Interface de sortie

3.4.4.1. Flux numéro 1 : la requête enrichie

La requête enrichie est soit à destination du service visé soit à destination du SSO.

- Vers le SSO, le module retransmet la requête reçue telle qu'elle s'il s'agit de la requête d'origine. Si la requête reçue est une requête de redirection, le module applique la redirection en insérant le vecteur d'identification enregistré,

- Vers le service visé le module transmet la requête en incluant le cookie de session s'il est disponible et valide.

Il est recommandé que le module ne transmette pas le cookie de session au client d'origine. Cela veut dire que la requête contenant la directive *SetCookie* est supprimée.

3.5. Module de gestion intégré au premier OHS

Intégrer le module de gestion au premier OHS permet d'éviter les différentes redirections dues à la nécessité d'ouvrir une session. En revanche cela impose de modifier l'OHS (qui est un serveur HTTP Apache modifié). Cette solution basée sur le produit OHS ayant potentiellement des répercussions en termes juridiques –par exemple la garantie– autant qu'en termes technique, ne peut être retenue à ce stade car elle doit faire l'objet d'études sous la responsabilité de la CNAVTS.

Il y a au moins deux façons d'implémenter ce module :

- Intégrer la fonctionnalité nécessaire directement dans le module Apache mod_osso,

- Ajouter un module Apache qui sera utilisé avant le mod_osso avec une interface par variable d'environnement.

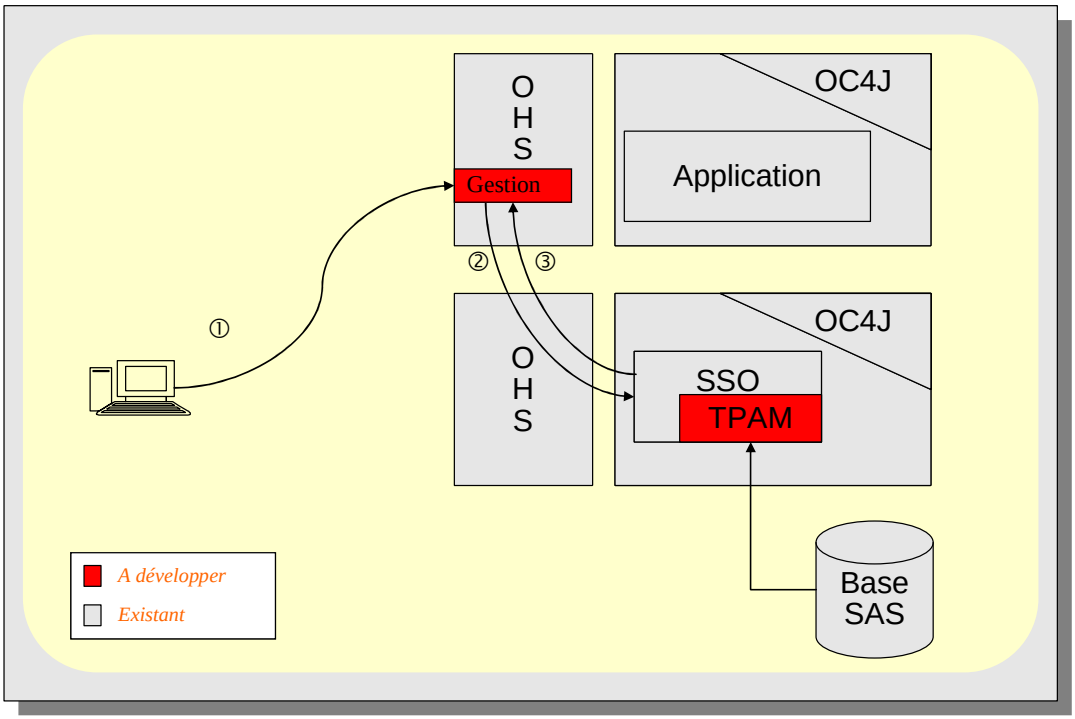


Figure 8 : Module de gestion intégré au Reverse Proxy

Le schéma ci-dessus est organisé selon les trois flux décrits dans les paragraphes suivants.

3.5.1.1. Flux numéro 1 : la requête avec le vecteur d'identification

La requête, traitée par le système de l'Organisme Client contient un vecteur d'identification, aucun cookie valide pour l'identification du SSO Oracle n'accompagne la requête.

3.5.1.2. Flux numéro 2 : Requête vers le SSO

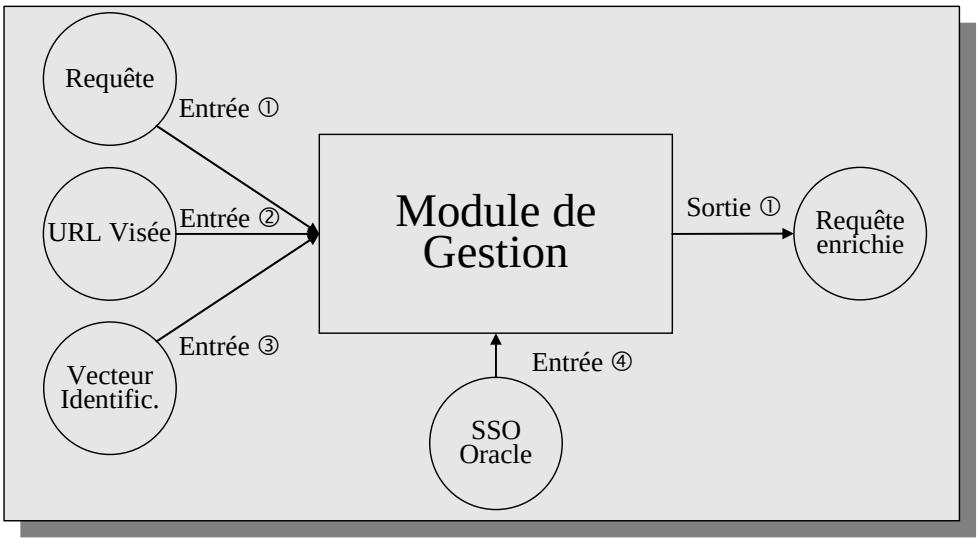
Le module de gestion capte la requête, détecte la nécessité d'ouvrir une session (car soit le cookie présent n'est pas compatible avec le vecteur d'identification soit il n'y a pas de cookie pour la session) et envoie une requête au système SSO avec le vecteur d'identification pour permettre l'ouverture de la session.

3.5.1.3. Flux numéro 3 : Création de cookie de session

Après validation par le système SSO et le module de vérification TPAM intégré, le module de gestion reçoit la réponse du système SSO avec le token Oracle et permet à l'OHS de créer le cookie de session.

3.5.2. Rôle du module

Ce module a pour rôle de capter les requêtes de redirections émises par le SSO Oracle lors du démarrage de session et de s'assurer de la bonne transmission à chaque requête de redirection du vecteur d'identification.



265 **Figure 9 : Module de gestion**

266 Les interfaces d'entrée et de sortie dans ce cas de figure sont identiques à celles du cas de figure
267 présenté au paragraphe *3.4 Module de gestion intégré au Reverse Proxy*. Dans les deux cas le module
268 doit intercepter les requêtes de redirection, la différence étant ici que le module applique la redirection
269 depuis l'OHS lui même, ce qui implique un gain de performance.

270 **FIN DU DOCUMENT**