Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DU BUDGET
DES COMPTES PUBLICS
ET DE LA FONCTION PUBLIQUE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Direction de la Sécurité Sociale

Guide de Mise en Œuvre

Standard d'interopérabilité entre organismes de la sphère sociale

Réf. : Standard Interops1.0_GuideMiseEnOeuvre_v1.0
Version 1.0 du 07/10/2008

Référence :	Standard Interops1.0_GuideMiseEnOeuvre_v1.0
Version :	1.0
Date de dernière mise à jour :	07/10/2008
Niveau de confidentialité :	PUBLIC

Table des mises à jour du document

N° de version	Etat[1]	Date	Auteur	Objet de la mise à jour
0.1	T	20/09/07	F. Zuretti	Création
0.2		08/10/07	Y. Béot	Validation
0.3	T	31/10/07	F. Zuretti	Intégration remarques réunion Interops 09/10/07
0.4	T	07/11/07	F. Zuretti	Ajout accrochage fonctionnel hors-ligne, analyse sécurité et recommandations, gestion des PAGM
0.5	T	19/11/07	F. Zuretti	Correction suite à réunion 09/11/07
0.6	T	26/11/07	F. Zuretti	Ajout démarche Interops-P
0.7	T	28/11/07	F. Zuretti	Compléments démarche Interops-P. Paragraphe Mise en œuvre devient un chapitre
0.8	T	16/01/08	F. Zuretti	Accrochage traces
0.9	T	03/03/08	F. Zuretti	Modification des références
1.0	T	17/09/08	F. Zuretti	Ajout recommandations format des traces applicatives, mise à jour des références

[1] **T** : En cours de modification ; **V** : Validé

SOMMAIRE

1. INTRODUCTION

1.1 Objet du document

Ce document présente la démarche d'accrochage d'une application Interops-A entre un organisme client et un organisme fournisseur.

Le chapitre 2 décrit les étapes nécessaires à la mise en œuvre. Le chapitre 2.9 présente les recommandations relatives à la mise en œuvre.

1.2 Glossaire

CRL	Certificate Revocation List
Interops	Interopérabilité entre les Organismes de Protection Sociale
Interops-A	Interops mode « application à application »
VI	Vecteur d'Identification
WSDL	Web Service Description Language
WSS	Web Service Security

1.3 Références

1.3.1 Documents internes

	Référence	Titre	Auteur	Ver.	Date
[CONV]	Standard Interops1.0_ConventionTechnique	Convention technique	Dictao	1.8	28/07/2008
[WSS]	dictao_DGME_DIP121_lv01	Utilisation de WSS dans le cadre d'IOPS	Dictao	0.5	02/11/2006

1.3.2 Documents externes

	Titre	Auteur	Date
[CRYPTO]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard*	DCSSI	19/12/2006
[PRIS]	Politique de Référencement Intersectorielle de Sécurité v2 - Politiques de Certification Types,	DCSSI	06/11/2006

	Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques		
[WSI]	Basic Profile Version 1.1	Keith Ballinger, David Ehnebuske, Christopher Ferris, Martin Gudgin, Canyang Kevin Liu, Mark Nottingham, Prasacd Yendluri	10/04/2006

2. DEMARCHE D'ACCROCHAGE INTEROPS-A

La mise en œuvre du mode « application à application » du standard Interops porte sur la mise à disposition d'un organisme client par un organisme fournisseur d'un Web Service.

Afin de réaliser l'accrochage des systèmes d'informations clients et fournisseurs, plusieurs étapes ont été identifiées. Les paragraphes qui suivent détaillent ces étapes et l'enchaînement des tâches.

2.1 Gestion des aspects conventionnels

2.1.1 Objectif

L'objectif de cette étape est de mettre en place une « convention technique d'accrochage » permettant de :

- Rassembler les éléments techniques nécessaires à l'accrochage
- Partager ces éléments

Les OPS se baseront sur le document décrivant les conventions techniques du Standard Interops (cf. [CONV]).

2.1.2 Prérequis

Il n'y a pas de prérequis à cette étape.

2.1.3 Déroulement

Les organismes clients et fournisseurs remplissent et s'échangent les documents de convention technique. Les éléments à fournir *a minima* sont :

- Les informations du VI
- Les éléments propres au mode Interops-A
- Les éléments techniques relatifs à la couche de transport

2.2 Accrochage réseau et SSL

2.2.1 Objectif

L'objectif de cet accrochage réseau est de valider les communications entre l'infrastructure de l'organisme client et celle de l'organisme fournisseur, avec activation de la couche SSL. Les éléments impactés sont les suivants :

- Proxy client
- Reverse-proxy fournisseur
- Mécanismes d'authentification mutuelle

2.2.2 Prérequis

Les deux organismes doivent s'être entendus sur les éléments techniques de la couche transports via la « convention d'accrochage ».

Cela implique notamment pour l'accrochage réseau que :

- L'organisme fournisseur doit avoir fourni au client l'URL du Web Service (incluant le nom du serveur et le port utilisé).
- L'organisme fournisseur doit avoir fourni au client les adresses IP du ou des reverse-proxies dans l'espace d'adressage de l'organisme client.
- L'organisme client doit avoir fourni au fournisseur les adresses IP du ou des proxies dans l'espace d'adressage de l'organisme fournisseur.

L'activation de la couche SSL implique que :

- L'organisme fournisseur doit posséder un certificat d'authentification SSL serveur
- L'organisme client doit posséder un certificat d'authentification SSL client
- Chacun des organismes devra obtenir de son partenaire les certificats, les chaînes de certification et les CRL associées : la « convention technique d'accrochage » permet d'échanger le Base64 des certificats d'authentification et des chaines de certification et les URL de téléchargement des CRL.

Chacun des organismes devra s'assurer de l'ouverture des flux réseaux compte tenu des informations ci-dessus.

2.2.3 Déroulement

Les deux organismes configurent leurs équipements réseau (proxy et reverse-proxy) à partir des informations spécifiées par la convention technique d'accrochage :

- Ouverture des flux
- Configuration des adresses IP

A l'issue de ces tâches, l'organisme client pourra tester la communication réseau sans authentification SSL aux adresses spécifiées par le fournisseur via une commande `telnet`.

Les organismes devront configurer le proxy (client) et le reverse-proxy (fournisseur) afin d'activer la couche d'authentification SSL. Le test des communications SSL peut également se faire via une commande `telnet`.

L'organisme fournisseur pourra mettre en place un filtre basé sur le DN (Distinguished Name) ou le CN (Common Name) du certificat d'authentification client afin de n'accepter que les certificats émanant de l'organisme client par exemple et non tout certificat émis par la chaîne de certification.

Conseil : En cas de problème sur la couche SSL, un outil comme `openssl` (via les options `s_client` et `s_server`) permet de réaliser une authentification SSL serveur ou cliente et ainsi détecter les problèmes liés à la reconnaissance des certificats.

2.3 Accrochage fonctionnel hors-ligne

2.3.1 Objectif

Le but de cette étape est de commencer à valider la compatibilité hors standard Interops des implémentations clientes et Web Service.

Cette étape qui trouve son prolongement dans l'accrochage fonctionnel (cf. § 0) n'a pas pour objectif de réaliser la validation complète des composants de la chaine fonctionnelle. Cet accrochage fonctionnel hors-ligne pouvant être réalisé en parallèle de l'accrochage réseau, il permet de gagner du temps sur le planning général de l'accrochage.

Dans la mesure où les échanges sont réalisés sans transmission de VI, le fournisseur devra « bouchonner » son application si celle-ci attend du VI des informations nécessaires à la création du contexte de sécurité (code client, code organisme, attributs optionnels). Le fournisseur devra construire le contexte de sécurité attendu par le service sans avoir recours au VI.

2.3.2 Prérequis

L'organisme fournisseur devra fournir à l'organisme client :

- Le descripteur du Web Service (fichier WSDL)

Note : Le Web Service proposé par l'organisme fournisseur à l'organisme client devrait être conformes aux recommandations du WS-I afin d'offrir les garanties maximales d'interopérabilité. L'organisme fournisseur portera une attention particulière aux problèmes liés à l'encodage des données (jeux de caractères utilisés par l'application cliente, le Web Service, etc.). Le WS-I fourni des outils java (http://www.ws-i.org/Testing/Tools/2005/06/WSI_Test_Java_Final_1.1.zip) ou C# (http://www.ws-i.org/Testing/Tools/2005/06/WSI_Test_CS_Final_1.1.zip) permettant d'analyser un descripteur de Web Service.

- Toutes les documentations nécessaires ou utiles à la mise en œuvre d'un client de ce service :
  - Spécifications fonctionnelles
  - Spécifications techniques des structures de données utilisées dans les échanges
  - Description des cas d'erreurs fonctionnelles
  - Description des tests fonctionnels du WS (cas passants et non-passants) permettant de valider une implémentation cliente. Ces jeux de tests doivent rester strictement fonctionnels (pas de mise en œuvre du standard Interops à ce niveau). Ils ne doivent pas être spécifiques à l'organisme client.

Note : La définition du jeu de test nécessite un gros effort de la part de l'organisme fournisseur. Cependant, compte tenu de la « lourdeur » de mise en œuvre de l'accrochage fonctionnel hors-ligne, l'organisme fournisseur pourra proposer à cette étape un dossier de tests fonctionnels réduit permettant de valider les principaux cas passants et d'erreur.

Par ailleurs, l'accrochage hors-ligne nécessite un outillage spécifique :

- Au niveau de l'organisme client pour récupérer les messages. Les flux SOAP générés par l'implémentation client du Web Service peuvent être récupérés à l'aide d'outils tels que tcpmon (cf. https://tcpmon.dev.java.net/) ou tcpdump (cf. http://www.tcpdump.org/).
- Au niveau de l'organisme fournisseur pour les rejouer. Les flux SOAP peuvent être soumis au Web Service à l'aide d'outils tels que Paros (http://www.parosproxy.org/), wget (http://www.gnu.org/software/wget/wget.html) ou cURL (http://curl.haxx.se/).

2.3.3 Déroulement

L'organisme client développera sa couche d'appel SOAP en fonction du WSDL fourni par l'organisme fournisseur.

Il générera et récupérera les flux SOAP correspondant au dossier de test partiel proposé par l'organisme fournisseur, avant de les lui transmettre par mail.

L'organisme fournisseur soumettra les flux SOAP au Web Service pour validation fonctionnelle.

Le dossier de test partiel doit permettre de remonter les erreurs potentielles suivantes :

- Incompatibilité des couches SOAP cliente et serveur
- Incompatibilité des schémas ou de l'encodage des données

- Etc.

2.4 Accrochage fonctionnel

2.4.1 Objectif

Le but de cette étape est de valider la compatibilité hors standard Interops des différents composants de la chaine fonctionnelle : client Web Service, proxy, reverse-proxy, Web Service.

Dans la mesure où les échanges sont réalisés sans transmission de VI, le fournisseur devra « bouchonner » son application si celle-ci attend du VI des informations nécessaires à la création du contexte de sécurité (code client, code organisme, attributs optionnels). Le fournisseur devra construire le contexte de sécurité attendu par le service sans avoir recours au VI.

Cet accrochage fonctionnel pourra être réalisé avec authentification SSL.

2.4.2 Prérequis

Les prérequis sont ceux de l'accrochage fonctionnel hors-ligne, l'organisme fournisseur devant simplement fournir à l'organisme client le dossier de test fonctionnels complet.

2.4.3 Déroulement

L'organisme client produira les jeux de tests conformes aux spécifications de l'organisme fournisseur permettant de valider son implémentation du client Web Service.

Puis, il lancera les jeux de tests.

La réalisation des tests fonctionnels doit permettre de remonter les erreurs potentielles suivantes :

- Mauvaise URL d'accès
- Incompatibilité dans la couche de transport (HTTP)
- Incompatibilité des couches SOAP cliente et serveur
- Incompatibilité des schémas ou de l'encodage des données
- Etc.

En cas d'erreur, l'organisme client se chargera de vérifier qu'il a bien reçu l'acceptation de l'organisme fournisseur et auprès de ses équipes réseaux, que le flux a été ouvert.

2.5 Validation hors-ligne des assertions

2.5.1 Objectif

L'objectif de cette étape est de valider :

- La capacité de l'organisme client à générer un VI conforme au standard Interops et à la convention technique
- La capacité du fournisseur à traiter un VI conforme au standard Interops et à la convention technique

Note : la non-conformité des VI à la convention technique est apparue comme un problème récurrent lors des différentes phases d'expérimentation.

<u>Conseil</u> : Cette étape étant réalisée hors-ligne, elle peut être effectuée en parallèle des accrochages réseau et fonctionnels.

2.5.2 Prérequis

Les éléments de la « convention technique d'accrochage » relatifs au VI doivent avoir été échangés. De même, l'organisme client doit avoir transmis au fournisseur la chaîne de certification permettant de valider la signature du VI pour l'environnement d'accrochage.

L'organisme client doit disposer d'une implémentation de la brique technique de génération des VI conforme au standard Interops-A (par exemple : Serveur de Jeton GIPMDS v3).

L'organisme fournisseur doit disposer d'une implémentation de la brique technique de vérification des VI conforme au standard Interops-A (par exemple : Serveur de Jeton GIPMDS v3).

D'une manière générale, les organismes sont encouragés à mettre en œuvre le maximum de tests en interne permettant de s'assurer de la conformité de leur implémentation de la brique technique de génération/vérification de VI vis-à-vis du standard Interops, et ce afin de limiter le temps perdu en aller-retour entre les organismes.

Parmi les outils permettant de tester rapidement les VI, on notera `XMLSEC` en ligne de commande, qui permet de valider la signature d'un document XML à partir d'une chaine de certification. La commande suivante permet de vérifier la signature d'une Assertion SAML 2.0

```
xmlsec.exe --verify --store-references --trusted-pem [Certificats de la chaîne d'AC] --id-attr:ID Assertion [Fichier XML à vérifier]
```

Parmi les implémentations du standard Interops, on citera le Serveur de Jeton GIPMDS v3 qui a bénéficié de campagnes de tests et de validation étendues lors de l'expérimentation du mode « application à application ».

2.5.3 Déroulement

L'organisme client génère des VI (cas passants uniquement) respectant la « convention technique d'accrochage » puis les envoie par mail au fournisseur, lequel les vérifie.

Les VI générés doivent avoir une durée de vie suffisamment longue pour permettre les tests hors-ligne (une validité de plusieurs jours peut être nécessaire à cette étape).

<u>Attention</u> : une fois signé, le VI doit être transmis sans aucune modification. Tout changement de caractère (même un retour chariot), d'encodage ou de format de fichier (linux/Windows) aura pour conséquence de « casser » la signature. L'organisme client devra donc veiller à transmettre le VI tel qu'il est généré par son implémentation. Des causes fréquentes de signatures invalides sont liées aux « pretty print » des fichiers XML par les outils de visualisation ou les clients mails.

Il est ainsi fortement recommandé à l'organisme client de transmettre le VI sous la forme d'une pièce jointe encodé en Base64.

Afin de faciliter la génération des VI par le client, le fournisseur doit être en mesure d'orienter l'organisme client dans la résolution des problèmes sur les VI générés par ce dernier sont non-conformes.

2.6 Accrochage Interops-A

2.6.1 Objectif

L'objectif de cette étape est de valider l'interopérabilité entre les organismes clients et fournisseurs et la conformité au standard Interops-A.

2.6.2 Prérequis

L'utilisation de WSS pour l'adjonction du vecteur d'identification au message SOAP doit être conforme au document [WSS]. Ainsi, conformément au standard, aucune partie du message SOAP ne sera signé. Le vecteur d'identification sera simplement inclus dans l'entête WSS.

L'organisme fournisseur doit disposer de jeux de test fonctionnels complet (cf. paragraphe 2.3) incluant l'utilisation du VI (code client, code organisme, attributs optionnels, etc.).

L'organisme fournisseur doit disposer de tests exhaustifs permettant de valider sa capacité à traiter les VI et notamment les cas non-passants :

- Vérification du format du VI (tests des éléments ou attributs obligatoires et optionnels de l'assertion SAML)
- Vérification de la conformité du VI à la convention
- Vérification de la validité du jeton SAML (date, signature)

L'organisme fournisseur doit également disposer de jeux de tests permettant de valider le fait que son Web Service se conforme au standard Interops pour la gestion des erreurs. Et qu'il peut traiter (cf. [Interops-A]) :

- Erreurs au niveau assertion (format de jeton ou algorithme de signature non supporté, jeton invalide, serveur de jeton injoignable, signature invalide, jeton non authentifié, pas de jeton de sécurité)
- Erreurs au niveau VI (PAGM invalides, service visé invalide, identifiant de l'organisme client invalide, niveau d'authentification non conventionnel, VI invalide)
- Erreurs au niveau du service fournisseur (service indisponible, injoignable)
- Erreurs au niveau transport (timeout, erreur SSL)

L'organisme client devra tout particulièrement valider le comportement de son application dans le cas d'un problème lié au standard (cf. ci-dessus).

Dans le cadre de l'expérimentation, la synchronisation temporelle ne sera pas aussi stricte qu'en production. Les organismes ont notamment le choix du serveur NTP (interne ou externe). La synchronisation sur une source NTP est cependant obligatoire, pour ainsi éviter tout problème lié à la dérive d'horloge. Pour autant, la durée de vie du vecteur d'identification doit être paramétrable pour effectuer des vérifications du vecteur par l'organisme fournisseur en s'affranchissant des conditions temporelles.

2.6.3 Déroulement

L'organisme fournisseur transmet à l'organisme client la description des jeux de tests à mettre en œuvre. L'organisme client implémente les jeux de tests permettant notamment de valider sa gestion des remontées d'erreurs.

2.7 Accrochage traçabilité

2.7.1 Objectif

L'objectif de cette étape est de valider la capacité des deux organismes à s'échanger des traces sur la base des principes définis par le standard Interops.

2.7.2 Prérequis

La génération des traces d'audit est activée chez chaque organisme.

Lors de la mise en production, les systèmes de traces d'audit sont conformes à la convention des deux cotés (durée de vie, conservation éléments tracés, etc.). En particulier, l'organisme fournisseur devra être capable de générer des traces applicatives conformes aux spécifications conventionnelles en ce qui concerne l'élément « Action ».

Ce n'est pas un prérequis pour l'accrochage.

2.7.3 Déroulement

L'organisme client lance plusieurs requêtes sur le Web Service du fournisseur (valides et invalides).

L'organisme fournisseur génère une déclaration de comportement suspect à partir d'un VI donné (parmi ceux envoyés par le client) au format d'échange des traces. Il envoie cette déclaration par mail au client. Le client doit pouvoir traiter la demande et prouver sa capacité à identifier l'utilisateur local.

L'organisme client génère des demandes de traces à partir d'un VI donné (parmi ceux envoyés) au format d'échange des traces. Il envoi ces demandes par mail au fournisseur. Le fournisseur doit pouvoir traiter les demandes et répondre au client selon le format d'échange des traces. L'organisme client veillera à effectuer des demandes sur des requêtes valides et invalides pour couvrir les différents cas prévus par le standard.

L'organisme client vérifiera en particulier sa capacité à interpréter l'élément « Action » des traces applicatives du fournisseur, dont la présence et les spécifications sont conventionnelles. A cette fin, il générera des demandes de traces concernant des requêtes couvrant toutes les actions possibles.

Ces différentes actions peuvent être réalisées en parallèle.

2.8 Tests de charge

2.8.1 Objectif

L'objectif de cette étape est de valider la capacité du système à tenir la charge telle que précisée par le cahier des charges et/ou les exigences exprimées par les MOA.

Ces tests de charge mettront en œuvre tous les éléments de la chaîne de l'organisme client et de l'organisme fournisseur.

<u>Attention</u> : Cette phase peut avoir un impact fort sur l'utilisation des ressources réseaux et peut donc perturber les services existants. Il convient de limiter les tests de charge au strict nécessaire sans pousser l'architecture de l'organisme fournisseur, qui peut être dimensionnée pour être partagée par plusieurs OPS.

2.8.2 Prérequis

Toutes les autres phases doivent avoir été validées.

L'organisme fournisseur aura au préalable réalisé des tests de charge en interne pour déterminer les seuils de l'infrastructure côté organisme fournisseur.

La MOE côté organisme fournisseur définit les tests de charge à effecuter par l'organisme client et les paramètres associés :

- Nombre de clients simultanés maximum
- Think time ou temps entre chaque requête
- Nombre de tirs/durée du test de charge
- Jeu de test spécifique
- etc.

Afin d'assurer un fonctionnement optimal de la plate-forme en production, il convient d'effectuer *a minima* :

- Des tests de stress de l'application pour observer des dégradations suites à des pics de charge
- Des tests d'endurance pour détecter des dégradations éventuelles au fil du temps

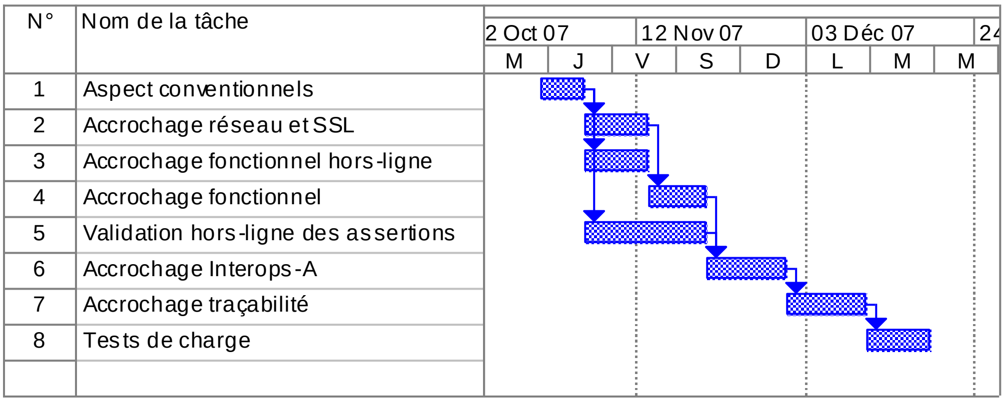
Conseil : Les tests de charge pourront être effectués au niveau du client du Web Service (utilisation d'un framework particulier par exemple), ou au niveau de l'application appelante (application Web effectuant des appels Web Service par exemple).

2.8.3 Déroulement

Les organismes mettent en œuvre le plan de test.

2.9 Enchainement des taches

Le diagramme de Gantt ci-dessous présente l'enchaînement des différentes étapes :



N°	Nom de la tâche
1	Aspect conventionnels
2	Accrochage réseau et SSL
3	Accrochage fonctionnel hors-ligne
4	Accrochage fonctionnel
5	Validation hors-ligne des assertions
6	Accrochage Interops-A
7	Accrochage traçabilité
8	Tests de charge

3. DEMARCHE D’ACCROCHAGE INTEROPS-P

3.1 Gestion des aspects conventionnels

3.1.1 Objectif

L’objectif de cette étape est de mettre en place une « convention technique d’accrochage » permettant de :

- Rassembler les éléments techniques nécessaires à l’accrochage
- Partager ces éléments

Les OPS se baseront sur le document décrivant les conventions techniques du Standard Interops (cf. [CONV]).

3.1.2 Prérequis

Il n’y a pas de prérequis à cette étape.

3.1.3 Déroulement

Les organismes clients et fournisseurs remplissent et s’échangent les documents de convention technique. Les éléments à fournir *a minima* sont :

- Les informations du VI
- Les éléments propres au mode Interops-P
- Les éléments techniques relatifs à la couche de transport

3.2 Accrochage réseau et SSL

3.2.1 Objectif

L’objectif de cet accrochage réseau est de valider les communications entre l’infrastructure de l’organisme client et celle de l’organisme fournisseur, avec activation de la couche SSL. Les éléments impactés sont les suivants :

- Proxy client
- Reverse-proxy fournisseur
- Mécanismes d’authentification mutuelle

3.2.2 Prérequis

Les deux organismes doivent s’être entendus sur les éléments techniques de la couche transports via la « convention d’accrochage ».

Cela implique notamment pour l’accrochage réseau que :

- L’organisme fournisseur doit avoir fourni au client l’URL du Service Web (incluant le nom du serveur et le port utilisé).
- L’organisme fournisseur doit avoir fourni au client les adresses IP du ou des reverse-proxies dans l’espace d’adressage de l’organisme client.

- L'organisme client doit avoir fourni au fournisseur les adresses IP du ou des proxies dans l'espace d'adressage de l'organisme fournisseur.

L'activation de la couche SSL implique que :

- L'organisme fournisseur doit posséder un certificat d'authentification SSL serveur
- L'organisme client doit posséder un certificat d'authentification SSL client
- Chacun des organismes devra obtenir de son partenaire les certificats, les chaînes de certification et les CRL associées : la « convention technique d'accrochage » permet d'échanger le Base64 des certificats d'authentification et des chaines de certification et les URL de téléchargement des CRL.

Chacun des organismes devra s'assurer de l'ouverture des flux réseaux compte tenu des informations ci-dessus.

Conseil : L'organisme fournisseur pourra mettre en place une page web statique de test indiquant que la page a été atteinte avec un protocole donné.

3.2.3 Déroulement

Les deux organismes configurent leurs équipements réseau (proxy et reverse-proxy) à partir des informations spécifiées par la convention technique d'accrochage :

- Ouverture des flux
- Configuration des adresses IP

A l'issue de ces tâches, l'organisme client pourra tester la communication réseau sans authentification SSL aux adresses spécifiées par le fournisseur via une commande *`telnet`*.

Les organismes devront configurer le proxy (client) et le reverse-proxy (fournisseur) afin d'activer la couche d'authentification SSL. Le test des communications SSL peut également se faire via une commande *`telnet`*.

L'organisme fournisseur pourra mettre en place un filtre basé sur le DN (Distinguished Name) ou le CN (Common Name) du certificat d'authentification client afin de n'accepter que les certificats émanant de l'organisme client par exemple et non tout certificat émis par la chaîne de certification.

Conseil : En cas de problème sur la couche SSL, un outil comme `openssl` (via les options `s_client` et `s_server`) permet de réaliser une authentification SSL serveur ou cliente et ainsi détecter les problèmes liés à la reconnaissance des certificats.

A l'issue des tests effectués par le client à l'aide des commandes *`telnet`* et *`openssl`*, ce dernier pourra réaliser une connexion depuis un navigateur web via le proxy et le reverse-proxy et vérifier l'accès à la page web de test.

3.3 Validation hors-ligne des jetons SAML

3.3.1 Objectif

L'objectif de cette étape est de valider :

- La capacité de l'organisme client à générer un VI conforme au standard Interops et à la convention technique
- La capacité du fournisseur à traiter un VI conforme au standard Interops et à la convention technique

Note : la non-conformité des VI à la convention technique est apparue comme un problème récurrent lors des différentes phases d'expérimentation.

Conseil : Cette étape étant réalisée hors-ligne, elle peut être effectuée en parallèle des accrochages réseau et fonctionnels.

3.3.2 Prérequis

Les éléments de la « convention technique d'accrochage » relatifs au VI doivent avoir été échangés. De même, l'organisme client doit avoir transmis au fournisseur la chaîne de certification permettant de valider la signature du VI pour l'environnement d'accrochage.

L'organisme client doit disposer d'une implémentation de la brique technique de génération des VI conforme au standard Interops-P (par exemple : Serveur de Jeton GIPMDS v3).

L'organisme fournisseur doit disposer d'une implémentation de la brique technique de vérification des VI conforme au standard Interops-P (par exemple : Serveur de Jeton GIPMDS v3).

L'organisme fournisseur doit disposer de tests exhaustifs permettant de valider sa capacité à traiter les VI et notamment les cas non-passants :

- Vérification du format du VI (tests des éléments ou attributs obligatoires et optionnels du jeton SAML)
- Vérification de la conformité du VI à la convention
- Vérification de la validité du jeton SAML (date, signature)

D'une manière générale, les organismes sont encouragés à mettre en œuvre le maximum de tests en interne permettant de s'assurer de la conformité de leur implémentation de la brique technique de génération/vérification de VI vis-à-vis du standard Interops, et ce afin de limiter le temps perdu en aller-retour entre les organismes.

Parmi les outils permettant de tester rapidement les VI, on notera `XMLSEC` en ligne de commande, qui permet de valider la signature d'un document XML à partir d'une chaine de certification. La commande suivante permet de vérifier la signature d'une Assertion SAML 2.0 contenue dans une Response SAML 2.0.

```
xmlsec.exe --verify --store-references --trusted-pem [Certificats de la chaîne d'AC] --id-attr:ID Assertion [Fichier XML à vérifier]
```

Conseil : Parmi les implémentations du standard Interops, on citera le Serveur de Jeton GIPMDS v3 qui a bénéficié de campagnes de tests et de validation étendues lors de l'expérimentation du mode « portail à portail ».

3.3.3 Déroulement

L'organisme client génère des VI (cas passants uniquement) respectant la « convention technique d'accrochage » puis les envoie par mail au fournisseur, lequel les vérifie.

Les VI générés doivent avoir une durée de vie suffisamment longue pour permettre les tests hors-ligne (une validité de plusieurs jours peut être nécessaire à cette étape).

Attention : une fois signé, le VI doit être transmis sans aucune modification. Tout changement de caractère (même un retour chariot), d'encodage ou de format de fichier (linux/Windows) aura pour conséquence de « casser » la signature. L'organisme client devra donc veiller à transmettre le VI tel qu'il est généré par son implémentation. Des causes fréquentes de signatures invalides sont liées aux « pretty print » des fichiers XML par les outils de visualisation ou les clients mails.

Il est ainsi fortement recommandé à l'organisme client de transmettre le VI sous la forme d'une pièce jointe encodé en Base64.

Afin de faciliter la génération des VI par le client, le fournisseur doit être en mesure d'orienter l'organisme client dans la résolution des problèmes sur les VI générés par ce dernier sont non-conformes.

3.4 Accrochage Interops-P sans application

3.4.1 Objectif

L'objectif de cette étape est de valider l'interopérabilité entre les organismes clients et fournisseurs et la conformité au standard Interops-P.

Cette étape devra permettre de :

- Valider les réécritures mise en place côté proxy client (modification de l'espace de nommage et gestion des cookies)
- Valider le Service de transfert Inter-sites mis en place par le client
- Valider l'intégration et la transmission du jeton SAML (SAML Response 2.0)

Cette étape est réalisée sans application, ce qui signifie que l'application visée peut être une application « bouchon » facilitant la validation du standard Interops-P.

3.4.2 Prérequis

Les éléments de la « convention technique d'accrochage » relatifs au VI et à la couche transport doivent avoir été échangés. De même, l'organisme client doit avoir transmis au fournisseur la chaîne de certification permettant de valider la signature du VI pour l'environnement d'accrochage.

Le client devra avoir mis en place son service de transfert inter-sites, ainsi que les mécanismes de réécriture des cookies et des URL sur son ou ses proxies.

En particulier, il devra s'assurer de sa capacité à générer des requêtes HTTP contenant un champ relayState précisant le service visé extrait des données conventionnelles.

Le fournisseur devra avoir mis en place une application « bouchon » et son service de consommation d'assertion.

Conseil : L'application « bouchon » proposée par le fournisseur peut afficher le VI extrait du jeton SAML et les cookies reçus. En cas d'échec de vérification du jeton SAML, l'application peut en afficher la cause pour faciliter l'accrochage du client.

L'organisme fournisseur doit également disposer de jeux de tests permettant de valider le fait que son infrastructure peut traiter les cas d'erreur liés au VI :

- Erreurs au niveau Assertion ou Response (format de jeton ou algorithme de signature non supporté, jeton invalide, serveur de jeton injoignable, signature invalide, jeton non authentifié, pas de jeton de sécurité)
- Erreurs au niveau VI (PAGM invalides, service visé invalide, identifiant de l'organisme client invalide, niveau d'authentification non conventionnel, VI invalide)

Conseil : D'une manière générale, les organismes devraient personnaliser les erreurs renvoyées par chacun des éléments de la chaine fonctionnelle (proxy client, reverse-proxy fournisseur, application). Ceci afin de faciliter le diagnostique en cas de problèmes.

Note : Le niveau de détail de cette personnalisation doit être un compromis entre la facilitation du diagnostique et la non-divulgation d'informations sensibles (statut de vérification des VI non-passant notamment).

L'organisme fournisseur devra en outre vérifier la capacité de son service de consommation d'assertion à rediriger l'utilisateur vers le service visé :

- En utilisant le champ « relayState » si ce dernier est présent.
- En utilisant une URL par défaut fonction de l'identifiant du service visé précisé par le VI si la requête ne contient pas de « relayState ».

Dans le cadre de l'expérimentation, la synchronisation temporelle ne sera pas aussi stricte qu'en production. Les organismes ont notamment le choix du serveur NTP (interne ou externe). La synchronisation sur une source NTP est cependant obligatoire en production, pour ainsi éviter tout problème lié à la dérive d'horloge. Pour autant, la durée de vie du vecteur d'identification doit être paramétrable pour effectuer des vérifications du vecteur par l'organisme fournisseur en s'affranchissant des conditions temporelles.

3.4.3 Déroulement

Le client tentera d'accéder à la page de l'application « bouchon ».

Pour tester la bonne gestion des cookies, il faudra accéder au moins 2 fois à la page dans une session navigateur.

Des cas d'erreurs fonctionnels liés au VI pourront être testés pour tester les vérifications et le comportement de la chaîne :

- Absence de vecteur d'identification
- Assertion expirée
- Mauvais PAGM
- Mauvais identifiant de l'émetteur de l'assertion
- Mauvais nom de l'attribut PAGM
- Mauvaise signature
- Etc.

3.5 Accrochage Interops-P avec application

3.5.1 Objectifs

L'objectif de cette étape est de vérifier l'accès par le client à l'application web du fournisseur au travers des mécanismes d'interopérabilité.

Cette étape prolonge la phase précédente en mettant en œuvre l'application cible plutôt qu'une application « bouchon ».

3.5.2 Prérequis

L'organisme fournisseur doit fournir au client des jeux de test fonctionnels complets pour naviguer dans l'application.

3.5.3 Déroulement

Le client joue les jeux de tests proposés par le fournisseur.

3.6 Accrochage traçabilité

3.6.1 Objectif

L'objectif de cette étape est de valider la capacité des deux organismes à s'échanger des traces sur la base des principes définis par le standard Interops.

3.6.2 Prérequis

La génération des traces d'audit est activée chez chaque organisme.

Lors de la mise en production, les systèmes de traces d'audit sont conformes à la convention des deux cotés (durée de vie, conservation éléments tracés…). En particulier, l'organisme fournisseur devra être capable de générer des traces applicatives conformes aux spécifications conventionnelles en ce qui concerne l'élément « Action ».

Ce n'est pas un prérequis pour l'accrochage.

3.6.3 Déroulement

L'organisme client tente plusieurs accès à l'application du fournisseur (avec des jetons valides et invalides).

L'organisme fournisseur génère une déclaration de comportement suspect à partir d'un VI donné (parmi ceux envoyés par le client) au format d'échange des traces. Il envoie cette déclaration par mail au client. Le client doit pouvoir traiter la demande et prouver sa capacité à identifier l'utilisateur local.

L'organisme client génère des demandes de traces à partir d'un VI donné (parmi ceux envoyés) au format d'échange des traces. Il envoi ces demandes par mail au fournisseur. Le fournisseur doit pouvoir traiter les demandes et répondre au client selon le format d'échange des traces. L'organisme client veillera à effectuer des demandes sur des requêtes valides et invalides pour couvrir les différents cas prévus par le standard.

L'organisme client vérifiera en particulier sa capacité à interpréter l'élément « Action » des traces applicatives du fournisseur, dont la présence et les spécifications sont conventionnelles. A cette fin, il générera des demandes de traces concernant des requêtes couvrant toutes les actions possibles.

Ces différentes actions peuvent être réalisées en parallèle.

3.7 Tests de charge

3.7.1 Objectif

L'objectif de cette étape est de valider la capacité du système à tenir la charge telle que précisée par le cahier des charges et/ou les exigences exprimées par les MOA.

Ces tests de charge mettront en œuvre tous les éléments de la chaîne de l'organisme client et de l'organisme fournisseur.

Attention : Cette phase peut avoir un impact fort sur l'utilisation des ressources réseaux et peut donc perturber les services existants. Il convient de limiter les tests de charge au stricte nécessaire sans pousser l'architecture de l'organisme fournisseur, qui peut être dimensionnée pour être partagée par plusieurs OPS.

3.7.2 Prérequis

Toutes les autres phases doivent avoir été validées.

L'organisme fournisseur aura au préalable réalisé des tests de charge en interne pour déterminer les seuils de l'infrastructure côté organisme fournisseur.

La MOE côté organisme fournisseur définit les tests de charge à effecuter par l'organisme client et les paramètres associés :

- Nombre de clients simultanés maximum
- Think time ou temps entre chaque requête
- Nombre de tirs/durée du test de charge
- Jeu de test spécifique
- etc.

Afin d'assurer un fonctionnement optimal de la plate-forme en production, il convient d'effectuer *a minima* :

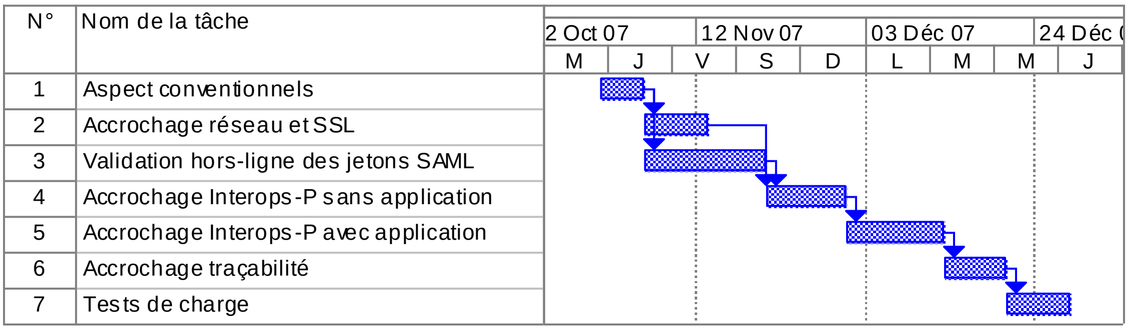
- Des tests de stress de l'application pour observer des dégradations suites à des pics de charge
- Des tests d'endurance pour détecter des dégradations éventuelles au fil du temps

3.7.3 Déroulement

Les organismes mettent en œuvre le plan de test.

3.8 Enchainement des taches

Le diagramme de Gantt ci-dessous présente l'enchaînement des différentes étapes :



N°	Nom de la tâche
1	Aspect conventionnels
2	Accrochage réseau et SSL
3	Validation hors-ligne des jetons SAML
4	Accrochage Interops-P sans application
5	Accrochage Interops-P avec application
6	Accrochage traçabilité
7	Tests de charge

4. ANALYSE DE SECURITE

4.1 Analyse de risque pour l'organisme client

La présente analyse est effectuée pour une architecture de l'organisme client composée des éléments présenté à la Figure 1. Cette analyse est à adapter en fonction de l'architecture effectivement mise en place par l'organisme client.

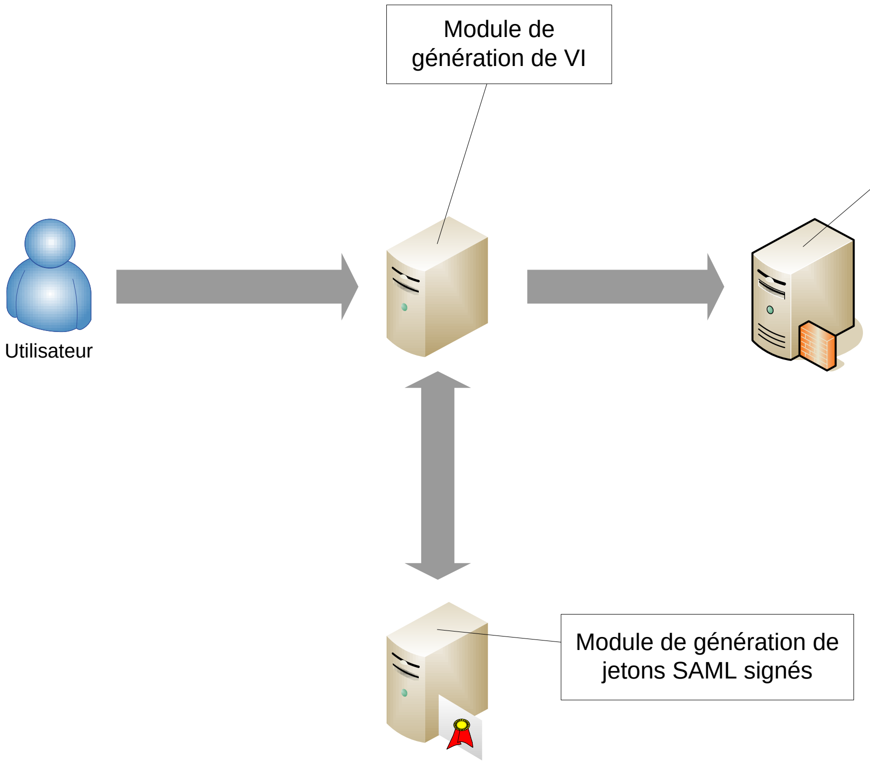


Figure 1 : Architecture de l'organisme client.

Les éléments de l'organisme client sont donc les suivants :

- Service client (poste de travail ou application)
- Module de génération du VI :
    - Authentification de l'utilisateur.
    - Regroupe ou construit les éléments du VI.
    - Client du module de génération des jetons SAML signés.
- Module de génération des jetons SAML signés :
    - Certifie le VI
- Proxy :
    - Authentification SSL avec le reverse-proxy de l'organisme fournisseur
- Réseau interne reliant les différents éléments et notamment :
    - Le client au module de génération du VI et au proxy
    - Le module de génération du VI au module de génération des jetons SAML et au proxy
- Réseau externe permettant de transmettre le jeton SAML signé à l'organisme fournisseur

Les éléments suivant sont donc à protéger :

- Fonction de génération des VI
- Fonction de génération et de signature des jetons SAML
- Clefs privée de signature
- Le jeton SAML signé
- Les traces
- Clefs privée d'authentification SSL

4.1.1 Besoins de sécurité

Les évènements redoutés sont :

- L'usurpation de l'identité d'un porteur vis-à-vis de l'organisme fournisseur
- La certification de mauvais attributs dans le jeton.

4.1.1.1 Fonction de génération des VI

➢ **Intégrité**

Il faut garantir que les éléments fournis par le client lors de son authentification sont intègres. Il faut également garantir que les informations récupérées pour la génération du VI (auprès du référentiel d'habilitation par exemple) sont intègres. Une modification de ces éléments conduirait à générer un VI contenant des attributs du porteur invalides.

➢ **Confidentialité et contrôle d'accès**

Il faut vérifier que la demande de génération du VI porte bien sur le client autorisé.

Il faut assurer la confidentialité des informations d'authentification du client (ex : login / mot de passe).

Remarque : les informations disponibles dans le jeton n'ont pas de caractère confidentiel vis-à-vis de l'organisme fournisseur puisqu'elle lui sont destinées.

Note : En revanche, l'article 6 de la convention juridique rappelle que « les données échangées dans le cadre du standard INTEROPS, quelle soient ou non à caractère personnel, sont des données confidentielles ».

➢ **Disponibilité**

La disponibilité du service est fonction des besoins définis conjointement par les organismes clients et fournisseurs.

4.1.1.2 Fonction de génération des jetons SAML signés

➢ **Intégrité**

Il faut garantir que les informations à signer sont intègres et n'ont pas été modifiées entre la génération du VI et la signature.

➢ **Confidentialité et contrôle d'accès**

Il faut vérifier que la demande de signature provient bien du module de génération du VI. Il faut éviter que quelqu'un puisse lancer une requête de génération de jeton SAML signé à la place du module de génération du VI.

➢ **Disponibilité**

La disponibilité du service est fonction des besoins définis conjointement par les organismes clients et fournisseurs.

4.1.1.3 Clef privée de signature

- **Intégrité**

Il faut garantir que la clef privée signant le jeton est bien celle qui est prévue par la convention technique passée entre les deux organismes.

Il faut garantir que l'on peut réinstaller la clé privée sur le serveur de signature en cas de perte de cette dernière. La destruction ou la perte de la clé de signature a un coût (mise à jour de la convention technique, exploitation, etc.).

- **Confidentialité et contrôle d'accès**

Il faut s'assurer que l'on ne peut pas signer à la place du module de signature. La divulgation et l'utilisation de la clé privée de signature sont inacceptables.

- **Disponibilité**

Il faut s'assurer que l'on ne peut pas rendre les clefs indisponibles.

4.1.1.4 Jeton SAML signé

- **Intégrité**

Les besoins d'intégrité sont garantis par la signature. Une altération du jeton n'aurait pas d'impact.

- **Confidentialité et contrôle d'accès**

Il faut garantir que l'on ne peut pas intercepter et utiliser le jeton (n'ayant pas encore été transmis) pour usurper l'identité du porteur.

Il faut s'assurer que l'on ne peut pas rejouer le jeton à la place du client pour usurper son identité.

- **Disponibilité**

La disponibilité du service est fonction des besoins définis conjointement par les organismes clients et fournisseurs.

4.1.1.5 Traces

- **Intégrité**

Il faut garantir la conservation intègre de la trace de génération des jetons signés.

- **Confidentialité et contrôle d'accès**

Les traces de génération des jetons contiennent des informations confidentielles vis-à-vis du fournisseur notamment telles que l'identité du client. Il faut s'assurer que ces traces ne sont accessibles qu'aux personnes autorisées.

- **Disponibilité**

Les traces doivent être disponibles pendant la durée de conservation décidée conjointement par les organismes clients et fournisseurs.

4.1.1.6 Clef privée d'authentification SSL

- **Intégrité**

Le proxy héberge une clef privée (d'authentification SSL client) dont il faut garantir l'intégrité.

Il faut garantir que la clef privée d'authentification SSL est bien celle qui est prévue par la convention technique passée entre les deux organismes.

Il faut garantir que l'on peut réinstaller la clef privée d'authentification SSL sur le proxy en cas de perte de cette dernière. La destruction ou la perte de la clef a un coût (mise à jour de la convention technique, exploitation, etc.).

- **Confidentialité et contrôle d'accès**

Il faut s'assurer que l'on ne peut pas s'authentifier au reverse-proxy fournisseur à la place du proxy client. La divulgation et l'utilisation de la clé privée d'authentification SSL sont inacceptables.

- **Disponibilité**

La disponibilité du service est fonction des besoins définis conjointement par les organismes clients et fournisseurs.

4.1.2 Menaces

4.1.2.1 Service client (poste de travail ou serveur)

Les vulnérabilités des clients sont hors scope de l'analyse.

4.1.2.2 Module de génération du VI

Les menaces pesant sur le module de génération des jetons sont :

- Sinistre conduisant à une destruction de la machine et donc à la perte des traces conservées.
- Intrusion sur le système ou abus des droits de l'administrateur conduisant à une divulgation d'informations confidentielles (traces) ou une altération du fonctionnement du module.
- Panne de la machine conduisant à l'impossibilité de générer les jetons.
- Parasitage continu du serveur.
- Attaque du dispositif d'authentification conduisant à une usurpation de l'identité du porteur dans le but de transmission par un client non autorisé de mauvais attributs au module de génération de VI conduisant à la certification de ces attributs invalides.
- Transmission par un client autorisé de mauvais attributs (comme par exemple la modification de son identité ou de l'identité cible ou source ou de la méthode d'authentification) conduisant à la certification de ces attributs invalides.
- Erreur de paramétrage du module conduisant à produire des jetons malformés.

4.1.2.3 Module de génération des jetons SAML signés

Les menaces pesant sur le module de signature des jetons sont :

- Sinistre conduisant à une destruction de la machine et donc à la perte des traces conservées et de la clé privée.
- Intrusion sur le système ou abus des droits de l'administrateur conduisant à une divulgation d'informations confidentielles (traces, clef privée de signature) ou une altération du fonctionnement du module.
- Panne de la machine conduisant à l'impossibilité de signer les jetons.
- Vol du support contenant la clé privée (disque, sauvegarde, etc.) conduisant à créer de vrai/faux jetons.
- Divulgation de la clé privée par négligence conduisant à créer de vrai/faux jetons.
- Cheval de Troie permettant de récupérer à distance le jeton et de le jouer à la place du client.

- Accès direct sans passer par le module de génération de VI pour faire signer un faux jeton.
- Erreur de paramétrage conduisant à produire de mauvaises signatures.

4.1.2.4 Proxy

Les menaces pesant sur le proxy sont :

- Sinistre conduisant à une destruction de la machine et donc à la perte de la clé privée d’authentification SSL.
- Intrusion sur le système ou abus des droits de l’administrateur conduisant à une divulgation d’informations confidentielles (clef privée d’authentification SSL) ou une altération du fonctionnement du module.
- Panne de la machine conduisant à l’impossibilité de se connecter à l’organisme fournisseur.
- Parasitage continu du serveur.
- Erreur de paramétrage.
- Vol du support contenant la clé privée d’authentification SSL conduisant à une usurpation de l’identité du proxy.
- Divulgation de la clé privée d’authentification SSL par négligence conduisant à une usurpation de l’identité du proxy.
- Accès direct sans passer par le module de génération de VI pour faire signer un faux jeton.

4.1.2.5 Le réseau interne

Les menaces pesant sur le réseau interne de l’organisme client sont :

- Ecoute du réseau pour voler les moyens d’authentification au serveur de génération du VI et se faire passer pour un client autorisé.
- Usurpation de l’identité du porteur par une attaque de type « man in the middle ».
- Requêtes de génération de jetons SAML signés n’émanant pas du module de génération du VI ou ne contenant pas la bonne information (« man in the middle »).
- Interception d’un jeton SAML signé (« man in the middle »).

4.1.2.6 Le réseau externe

Les menaces pesant sur le réseau externe sont :

- Ecoute du réseau pour voler le jeton SAML et le rejouer dans une requête auprès de l’organisme fournisseur.
- Usurpation de l’identité du serveur de jeton pour tenter de faire reconnaître par l’organisme fournisseur un faux jeton signé par une autre autorité.
- Usurpation de l’identité du proxy client ou du reverse-proxy fournisseur.

4.1.3 Recommandations

4.1.3.1 Service client (poste de travail ou serveur)

Hors scope de l’analyse.

4.1.3.2 Module de génération de VI

Les recommandations en vue de sécuriser le module de génération du VI sont :

- Mettre en œuvre un niveau d'authentification de l'utilisateur suffisant.

4.1.3.3 Module de génération des jetons SAML signés

Les recommandations en vue de sécuriser le module de signature des jetons sont :

- Protection des bi-clefs logiciels par mot de passe, voir utilisation de HSM
- Mise en place et respect de procédures organisationnelles de génération et de distribution des clefs (gestion des habilitations, informations des acteurs, etc.)
- Mise en place et respect de procédure de sauvegarde des clefs.
- Différencier les clefs de signature et les clefs d'authentification SSL.
- Stockage externalisé des traces avec protection de leur intégrité.

4.1.3.4 Proxy

Les recommandations en vue de sécuriser le proxy sont :

- Protection des bi-clefs logiciels par mot de passe, voir utilisation de HSM
- Mise en place et respect de procédures organisationnelles de génération et de distribution des clefs (gestion des habilitations, informations des acteurs, etc.)
- Mise en place et respect de procédure de sauvegarde des clefs
- Différencier les clefs de signature et les clefs d'authentification SSL.

4.1.3.5 Le réseau interne

Les recommandations en vue de sécuriser le réseau interne de l'organisme client sont :

- Authentification mutuelle entre les différents composants de l'architecture (en particulier entre le module de génération de VI et le module de génération des jetons SAML signés).

4.1.3.6 Le réseau externe

Les recommandations en vue de sécuriser le réseau externe de l'organisme client sont :

- Authentification mutuelle entre le proxy client et le reverse-proxy fournisseur.

4.2 Analyse de risque pour l'organisme fournisseur

La présente analyse est effectuée pour une architecture de l'organisme fournisseur composée des éléments présenté à la Figure 2. Cette analyse est à adapter en fonction de l'architecture effectivement mise en place par l'organisme fournisseur.

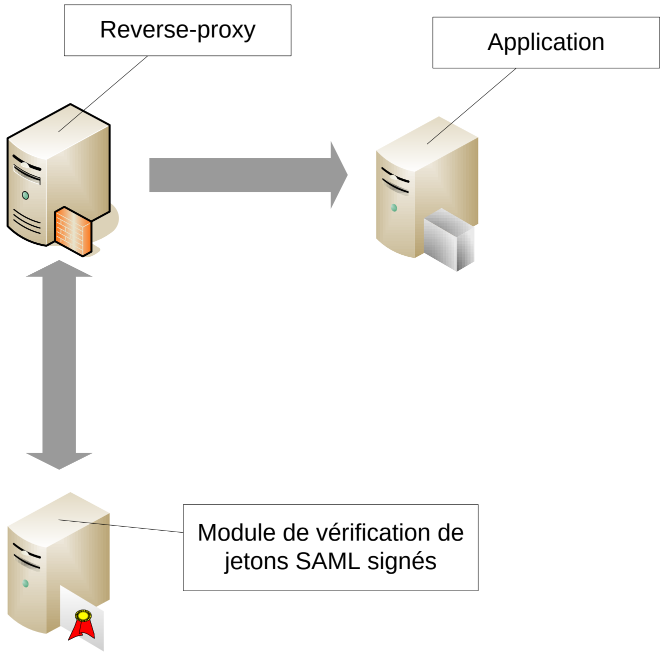


Figure 2 : Architecture de l'organisme fournisseur.

Les éléments de l'organisme fournisseur sont donc les suivants :

- Reverse-proxy :
  - Authentification SSL avec le proxy de l'organisme client
- Module de vérification des jetons SAML signés
  - Vérifie la validité du jeton SAML
  - Extrait les informations du VI
- Application cible
- Réseau interne reliant les différents éléments et notamment :
  - Le reverse-proxy au module de vérification des jetons SAML et à l'application
- Réseau externe permettant de recevoir le jeton SAML signé de l'organisme client

Les éléments suivant sont donc à protéger :

- Fonction de vérification des jetons SAML
- Les traces
- Clef privée d'authentification SSL

4.2.1 Besoins de sécurité

Les évènements redoutés :

- La validation d'un jeton SAML invalide

4.2.1.1 Fonction de vérification des jetons SAML

➢ **Intégrité**

Il faut garantir que les informations extraites du jeton SAML sont intègres et n'ont pas été modifiées entre la réception du jeton et l'extraction du VI.

➢ **Confidentialité et contrôle d'accès**

Il faut vérifier que la demande de vérification du jeton signé provient bien du reverse-proxy.

- **Disponibilité**

La disponibilité du service est fonction des besoins définis conjointement par les organismes clients et fournisseurs.

4.2.1.2 Traces

- **Intégrité**

Il faut garantir la conservation intègre de la trace de vérification des jetons signés.

- **Confidentialité et contrôle d'accès**

Les traces de vérification des jetons ne contiennent pas d'informations confidentielles vis-à-vis du client. Il reste cependant souhaitable de s'assurer que ces traces ne sont accessibles qu'aux personnes autorisées.

- **Disponibilité**

Les traces doivent être disponibles pendant la durée de conservation décidée conjointement par les organismes clients et fournisseurs.

4.2.1.3 Clef privée d'authentification SSL

- **Intégrité**

Le reverse-proxy héberge une clef privée (d'authentification SSL serveur) dont il faut garantir l'intégrité.

Il faut garantir que la clef privée d'authentification SSL est bien celle qui est prévue par la convention technique passée entre les deux organismes.

Il faut garantir que l'on peut réinstaller la clef privée d'authentification SSL sur le reverse-proxy en cas de perte de cette dernière. La destruction ou la perte de la clef a un coût (mise à jour de la convention technique, exploitation, etc.).

- **Confidentialité et contrôle d'accès**

Il faut s'assurer que l'on ne peut pas s'authentifier au proxy client à la place du reverse-proxy fournisseur. La divulgation et l'utilisation de la clé privée d'authentification SSL sont inacceptables.

- **Disponibilité**

La disponibilité du service est fonction des besoins définis conjointement par les organismes clients et fournisseurs.

4.2.2 Menaces

4.2.2.1 Application cible

Les vulnérabilités de l'application cible sont hors scope de l'analyse.

4.2.2.2 Module de vérification des jetons SAML signés

Les menaces pesant sur le module de vérification des jetons sont :

- Sinistre conduisant à une destruction de la machine et donc à la perte des traces conservées.

- Intrusion sur le système ou abus des droits de l'administrateur conduisant à une divulgation d'informations confidentielles (traces) ou une altération du fonctionnement du module.
- Panne de la machine conduisant à l'impossibilité de vérifier les jetons.
- Cheval de Troie permettant de valider le jeton quelque soit sa validité.
- Accès direct sans passer par le reverse-proxy pour faire valider un faux jeton.
- Rejeu d'un jeton conduisant à un déni de service.
- Erreur de paramétrage conduisant à produire des résultats de vérification erronés.

4.2.2.3 Reverse-proxy

Les menaces pesant sur le reverse-proxy sont :

- Sinistre conduisant à une destruction de la machine et donc à la perte de la clé privée d'authentification SSL.
- Intrusion sur le système ou abus des droits de l'administrateur conduisant à une divulgation d'informations confidentielles (clef privée d'authentification SSL) ou une altération du fonctionnement du module.
- Panne de la machine conduisant à l'impossibilité de se connecter à l'organisme client.
- Parasitage continu du serveur.
- Erreur de paramétrage.
- Vol du support contenant la clé privée d'authentification SSL conduisant à une usurpation de l'identité du reverse-proxy.
- Divulgation de la clé privée d'authentification SSL par négligence conduisant à une usurpation de l'identité du reverse-proxy.

4.2.2.4 Le réseau interne

Les menaces pesant sur le réseau interne de l'organisme fournisseur sont :

- Requêtes de vérification de jetons SAML signés n'émanant pas du reverse-proxy ou ne contenant pas la bonne information (« man in the middle »).
- Interception d'un VI entre le reverse-proxy et le module de vérification des jetons après vérification du jeton SAML signé (« man in the middle »).
- Interception des informations transmise à l'application par le reverse-proxy.

4.2.2.5 Le réseau externe

Les menaces pesant sur le réseau externe sont :

- Usurpation de l'identité du proxy client pour tenter de faire reconnaître par l'organisme fournisseur un faux jeton signé par une autre autorité.
- Déni de service (par rejeu d'un jeton intercepté par exemple).

4.2.3 Recommandations

4.2.3.1 Application cible

Hors scope de l'analyse.

4.2.3.2 Module de vérification des jetons

Les recommandations en vue de sécuriser le module de vérification des jetons sont :

- Mise en place et respect de procédures organisationnelles de génération et de distribution des clefs publiques (gestion des habilitations, informations des acteurs, etc.)
- Mise en place et respect de procédure de sauvegarde des clefs.
- Stockage externalisé des traces avec protection de leur intégrité.
- Vérifier la période de validité du jeton SAML.
- Vérifier au moyen de l'identifiant unique que le jeton SAML n'a pas déjà été présenté.

4.2.3.3 Reverse-proxy

Les recommandations en vue de sécuriser le reverse-proxy sont :

- Protection des bi-clefs logiciels par mot de passe, voir utilisation de HSM
- Mise en place et respect de procédures organisationnelles de génération et de distribution des clefs (gestion des habilitations, informations des acteurs, etc.)
- Mise en place et respect de procédure de sauvegarde des clefs

4.2.3.4 Le réseau interne

Les recommandations en vue de sécuriser le réseau interne de l'organisme fournisseur sont :

- Authentification mutuelle entre le module de vérification des jetons et le reverse-proxy.
- Authentification mutuelle entre reverse-proxy et l'application.

4.2.3.5 Le réseau externe

Les recommandations en vue de sécuriser le réseau externe de l'organisme fournisseur sont :

- Authentification mutuelle entre le proxy client et le reverse-proxy fournisseur.
- Filtrage des certificats présentés par le proxy client.

5. MISE EN ŒUVRE

5.1 Distinction des environnements

Le standard Interops propose de mettre en œuvre plusieurs conventions techniques pour distinguer les différents environnements (accrochage, production, etc.). En effet, certains des éléments techniques (certificats ou configuration réseau notamment) sont susceptibles d'évoluer entre la phase d'accrochage et la mise en production.

Deux approches sont possibles pour mettre en œuvre ces conventions techniques multiples :

- Différencier les conventions par les identifiants utilisés ou les versions de l'accord. Dans le cas de l'utilisation du Serveur de Jeton GIPMDS, cela permet de faire cohabiter ces différentes conventions sur une même machine.
- Conserver les identifiants et versions d'accord entre les différents environnements tout en utilisant une PKI différente pour l'accrochage que pour la production. Dans le cas de l'utilisation du Serveur de Jeton GIPMDS, cela nécessite d'instancier des serveurs de jeton propre à chaque environnement. C'est le choix de la CNAV et de l'AGIRC-ARCCO.

5.2 Profils des certificats

La mise en œuvre du standard Interops et des recommandations émises aux paragraphes précédents repose *a minima* sur l'utilisation de trois profils de certificats :

- Certificat SSL serveur pour l'authentification du reverse-proxy fournisseur par le proxy client.
- Certificat SSL client pour l'authentification du proxy client par le reverse-proxy fournisseur.
- Certificat de signature pour la signature des jetons SAML par le module dédié de l'organisme client.

Note : L'article 7 de la convention juridique du standard Interops précise que « *les parties s'engagent sur un niveau de sécurité conformément à ce qui a été défini dans le référentiel général de sécurité (RGS) ou dans la politique de référencement inter-sectoriel (PRIS)* ».

Les recommandations émise dans ce document seront donc conformes à celle de la PRIS v2.1, mais tiendront compte également des contraintes techniques liées aux implémentations existantes notamment.

Si l'IGC retenue dans la convention en particulier ne supporte pas la PRIS, on suivra les exigences de la politique de certification de l'IGC.

5.2.1 Certificats SSL serveur

5.2.1.1 Algorithmes et tailles de clefs

La PRIS v2.1 (cf. [PRIS]) émet les recommandations suivante concernant les algorithmes et les tailles de clefs utilisées pour l'authentification SSL :

	*	**
RSA	1024 bits ou 2048 bits	1024 bits ou 2048 bits

Hachage - SHA	SHA-1 (160 bits)	SHA-1 (160 bits)

La DCSSI émet les recommandations suivantes concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard* (cf. [CRYPTO]) :

- Fonction de hachage : SHA-1 n'atteint pas le niveau de sécurité standard en raison des attaques dont il a fait récemment l'objet. L'algorithme SHA-256 est recommandé.
- La taille minimale du module pour les clefs RSA est de :
  - 1536 bits pour une utilisation ne devant pas dépasser l'année 2010.
  - 2048 bits, pour une utilisation ne devant pas dépasser l'année 2020.
  - 4096 bits au-delà de 2020.

Cependant, les clés RSA de 2048 bits et l'algorithme SHA-256 sont peu pris en charge par les implémentations actuelles :

- Parmi les OS Microsoft, seul Windows Server 2003 peut gérer nativement le SHA-256.
- Openssl ne gère SHA-256 qu'à partir de la version 0.9.8.

Compte tenu de ces éléments, les bi-clés SSL serveur utilisés dans le cadre du standard Interops devraient utiliser l'algorithme SHA-1 et des tailles de clés RSA de 1024 bits.

Cette recommandation pourra être révisée et passer à SHA-256 et des clés RSA de 2048 bits lorsque les implémentations le permettront.

5.2.1.2 Gabarits

Les gabarits des certificats doit correspondre à la version X.509v3. Il n'y a pas d'exigence supplémentaire concernant le gabarit.

5.2.1.3 Extensions

La PRIS v2.1 stipule que les extensions suivantes sont obligatoires : *Authority Key Identifier, Subject Key Identifier, Key Usage, Certificate Policies, CRL Distribution Points, Freshest CRL, Authority Information Access, Extended Key Usage*.

Cette obligation sera gardée. En outre, elle précise le statut du *Key Usage* et du *Extended Key Usage*.

- *Key Usage :* Cette extension doit être présente et être marquée comme "critique". Les bits "digitalSignature" et "keyAgreement" doivent être à "1", tous les autres bits à "0".
- *Extended Key Usage :* Cette extension doit être présente et marquée "non critique". Elle ne doit contenir que la valeur "id-kp-serverAuth[1]" à l'exclusion de toute autre.

Les certificats d'authentification SSL serveur utilisés dans le cadre du standard Interops doivent respecter ces obligations.

5.2.1.4 Identification des certificats (DN)

Le `Distinguished Name` des certificats d'authentification SSL serveur doit contenir a minima les éléments suivants :

---

[1] *L'extension Extended Key Usage est définie par la RFC 3280 (cf. http://www.ietf.org/rfc/rfc3280.txt).*

- L'attribut `commonName` doit être utilisé et ne doit comporter que le FQDN (Fully Qualified Domain Name) du serveur. Les attributs `givenName` et `surname` ne doivent pas être utilisés. Une identification de l'entité à laquelle le serveur est rattaché est obligatoire.
- L'attribut `countryName` doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, …).
- L'attribut `organizationName` doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes.
- Une instance de l'attribut `organizationalUnitName` doit être présente et doit contenir l'identification de cette entité. Pour cela, cette instance de l'attribut `organizationalUnitName` doit être structurée conformément à la norme ISO 6523. Le format retenu est :

  `ICD Identification de l'organisation`

  - L'ICD (International Code Designator) est sur 4 caractères. Pour les entités de droit français, l'identification doit être le n° SIREN ou le n° SIRET.
  - L'identification de l'organisation sur 35 caractères. L'ICD du n° SIREN / SIRET est 0002.
  - Le séparateur entre les deux chaînes est un espace.
- Si d'autres instances de l'attribut `organizationalUnitName` sont présentes, elles ne doivent pas commencer par 4 chiffres.

Exemple :

`DN = {C=FR, O= CNAV, OU= 0002 123456789, CN=www.cnav.fr}.`

5.2.2 Certificats SSL client

Les recommandations concernant les certificats d'authentification SSL client sont identiques à celles des certifications serveur sauf éléments mentionnés ci-dessous.

5.2.2.1 Extensions

- *Extended Key Usage :* Cette extension doit être présente et marquée "non critique". Elle ne doit contenir que la valeur "id-kp-clientAuth[2]" à l'exclusion de toute autre.

5.2.3 Certificats de signature

Les recommandations concernant les certificats de signature sont identiques à celles des certifications serveur sauf éléments mentionnés ci-dessous.

5.2.3.1 Extensions

- *Key Usage :* Cette extension doit être présente et être marquée comme "critique". Le bit "digitalSignature" doit être à "1", tous les autres bits à "0".
- *Extended Key Usage :* Cette extension ne doit pas être présente.

---

[2] *L'extension Extended Key Usage est définie par la RFC 3280 (cf. http://www.ietf.org/rfc/rfc3280.txt).*

5.2.3.2 Identification des certificats (DN)

- L'attribut `commonName` doit être utilisé. Les attributs `givenName` et `surname` ne doivent pas être utilisés. Une identification de l'entité à laquelle le serveur est rattaché est obligatoire. Il n'y a pas de recommandations particulières sur l'attribut. Le DN du certificat devra permettre de différencier les environnements (accrochage, production, etc.).

Exemple :

```
DN = {C=FR, O= CNAV, OU= 0002 123456789, CN=Signataire CNAV Accrochage}.
```

5.3 Filtrage des certificats

Les recommandations émises dans les paragraphes précédents préconisent la mise en place d'authentification SSL mutuelle entre les différents éléments internes aux architectures des organismes clients et fournisseurs, ainsi qu'entre le proxy client et le reverse-proxy fournisseur.

Les serveurs web généralement utilisés (Apache *httpd*) permettent aisément de mettre en œuvre cette authentification. Les paragraphe suivants ont pour objet de présenter ces techniques.

5.3.1 Authentification serveur

5.3.1.1 Principe

Lors d'une authentification SSL serveur, le serveur présente un certificat au client. Si celui-ci l'accepte, la communication est établie et chiffrée.

Ce type d'authentification nécessite la mise en œuvre d'une clef privée d'authentification SSL sur le serveur (cf. 5.2.1) et de la chaine des certificats publics des autorités de certification de cette clef sur le client.

Note : Ce type d'authentification ne protège pas contre l'usurpation de l'identité du client.

5.3.1.2 Mise en œuvre dans Apache

Le module `mod_ssl` d'Apache *httpd* propose une interface vers la bibliothèque *openssl* qui propose des mécanismes d'authentification forte et de sécurisation de la couche de transport.

La mise en œuvre de ce module se fait via la configuration d'Apache.

Il faut en premier lieu s'assurer que le module mod_ssl est bien chargé, la ligne suivante du fichier `httpd.conf` doit être dé-commentée :

```
LoadModule ssl_module modules/libmodssl.so
```

La directive `SSLEngine` permet de spécifier l'utilisation de SSL :

```
SSLEngine on
```

La directive SSLCertificateFile permet de spécifier le fichier du certificat serveur encodé en PEM et éventuellement la clef privée associée (dans le même fichier) :

```
SSLCertificateFile /usr/local/apache2/conf/ssl.crt/server.crt
```

Si la clef privée n'est pas incluse dans le fichier certificat serveur, on peut référencer le fichier (au format PEM) avec la directive SSLCertificateKeyFile :

```
SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/server.key
```

5.3.2 Authentification mutuelle

5.3.2.1 Principe

Lors d'une authentification SSL mutuelle, le serveur présente un certificat au client et lui demande le sien. Si le client accepte le certificat serveur, il lui présente le sien. Si le serveur l'accepte, la communication est établie et chiffrée.

Ce type d'authentification nécessite la mise en œuvre d'une clef privée d'authentification SSL sur le serveur (cf. 5.2.1) et sur le client (cf. 5.2.2) et des chaines des certificats publics des autorités de certification de ces clefs sur le client et le serveur respectivement.

5.3.2.2 Mise en œuvre dans Apache

La mise en œuvre de l'authentification mutuelle est identique à celle de l'authentification serveur avec en plus : la configuration de la chaine de certification du certificat client et les directives concernant le niveau d'authentification requis.

Pour référencer l'emplacement de la chaine de certification du client sur le serveur, deux directives peuvent être utilisées : SSLCACertificateFile et SSLCACertificatePath.

La directive SSLCACertificateFile permet de préciser un fichier contenant la concaténation des certificats des AC du client au format PEM :

```
SSLCACertificateFile /usr/local/apache2/conf/ssl.crt/ca-client.crt
```

La directive SSLCACertificatePath permet de spécifier le répertoire contenant les certificats d'AC (au format PEM) du client :

```
SSLCACertificatePath /usr/local/apache2/conf/ssl.crt/
```

Les listes de révocations peuvent être précisées selon les mêmes modalités avec les directives SSLCARevocationFile et SSLCARevocationPath.

```
SSLCARevocationFile /usr/local/apache2/conf/ssl.crl/ca-client.crl

SSLCARevocationPath /usr/local/apache2/conf/ssl.crl/
```

Attention, dans le cas où les directives SSLCACertificatePath ou SSLCARevocationPath sont utilisées, Apache recherche des fichiers avec des noms correspondant au hash des certificats. Ces valeurs peuvent être obtenues avec la commande `` `openssl x509 -noout -hash' ``. Il faut donc créer des liens symboliques avec la valeur obtenue pour chaque certificat d'AC ou CRL.

La directive SSLVerifyDepth permet de préciser le nombre de certificats à vérifier dans la chaine de certification :

```
SSLVerifyDepth 10
```

Les directives précédentes permettent au serveur de retrouver et vérifier la chaine de certification du certificat client, il faut également préciser au client le niveau d'authentification requis. Cela est réalisé par la directive SSLVerifyClient. Cette directive peut prendre plusieurs valeurs, mais dans la pratique seule la valeur `require` est utilisée pour demander l'authentification cliente (la valeur par défaut est `none` auquel cas aucune authentification client n'est requise).

```
SSLVerifyClient require
```

5.3.3 Filtrage des certificats

5.3.3.1 Principe

L'authentification mutuelle mise en œuvre aux paragraphes précédents permet de vérifier la chaine de certification du certificat client, mais n'assure pas forcément un filtrage suffisant. Par exemple, dans le cadre d'Interops, l'organisme fournisseur voudra s'assurer que le certificat présenté est bien celui du ou des proxies de l'organisme client en plus de savoir qu'il a bien été émis par une autorité reconnue.

On peut donc envisager un filtrage fin des certificats sur le DN, le Serial Number, voir le base64 du certificat lui-même. Le paragraphe suivant propose des exemples de mise en œuvre dans Apache.

5.3.3.2 Mise en œuvre dans Apache

Le module `mod_ssl` propose la directive `SSLRequire` permettant d'effectuer un contrôle d'accès à partir d'expressions booléennes complexes.

Le module `mod_ssl` propose en outre une large gamme de variables d'environnement permettant de récupérer les informations liées aux certificats mis en jeu. La liste suivante n'est pas exhaustive :

- `SSL_CLIENT_S_DN` est une chaine contenant le DN du sujet du certificat client.
- `SSL_CLIENT_S_DN_`*`x509`* est une chaine contenant l'attribut *`x509`* du DN du sujet du certificat client. Par exemple `SSL_CLIENT_S_DN_OU` représente l'OU du DN.
- `SSL_CLIENT_M_SERIAL` est une chaine contenant le Serial Number du certificat client.

5.3.3.3 Filtrage sur le DN

En combinant ceux deux mécanismes, il est possible d'effectuer un filtrage sur le DN du sujet du certificat :

```
SSLRequire ( %{SSL_CLIENT_S_DN_O} eq "CNAV" and %{SSL_CLIENT_S_DN_OU}
in {"0002 123456789"} and %{SSL_CLIENT_S_DN_CN} in {"proxy1.cnav.fr",
"proxy2.cnav.fr"} )
```

5.3.3.4 Filtrage sur le Serial

Il est également possible d'effectuer un filtrage sur le Serial Number du sujet du certificat.

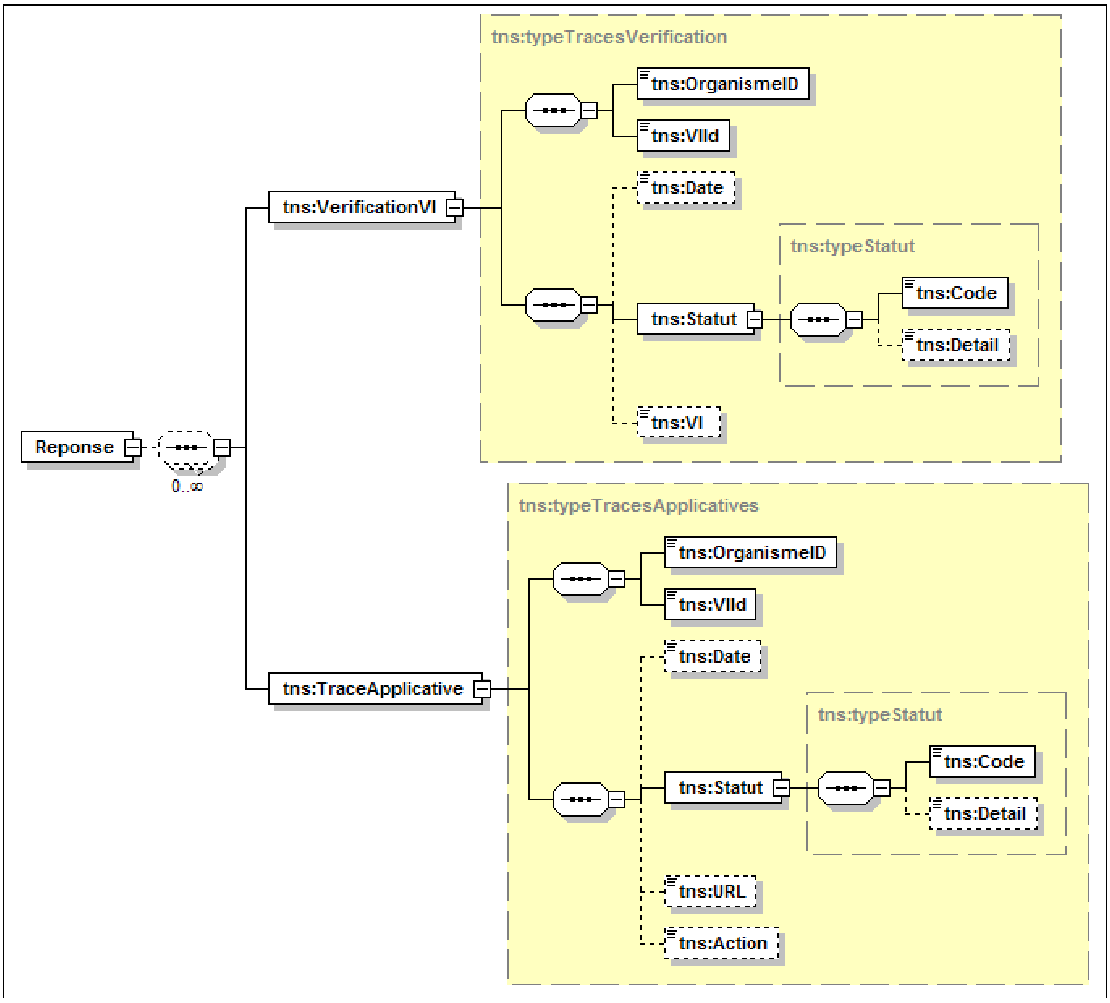
```
SSLRequire ( %{SSL_CLIENT_M_SERIAL} in {"01", "02"} )
```

5.4 Gestion des traces applicatives

Le format des traces applicatives dans le cadre de la mise en œuvre du standard Interops n'a pas été normalisé. Les paragraphes qui suivent présentent néanmoins un exemple d'implémentation ayant valeur de recommandation.

5.4.1 Rappel sur le format d'échange des traces

Le standard INTEROPS définit un format d'échange des traces dont le schéma est décrit dans la figure suivante :



- **URL et Action**

URL	URL de la page accédée durant la transaction
Action	Description de l'action effectuée par l'agent

- **Statut**

Champs disponibles pour préciser le résultat d'appel à une méthode (structure « Statut ») :

Code	Code de retour
Detail	Contient des détails, notamment en cas d'échec

Cette structure permet de spécifier si le service concerné par la trace applicative a été rendu ; elle est constituée d'un champ « Code » et d'un champ « Detail » (texte libre).

Le format pivot INTEROPS d'échange des traces applicatives définit les valeurs suivantes pour le champ « Code » :

Success	Le service a été rendu (quelque soit le résultat fonctionnel)
Failed	Le service n'a pas pu être rendu (généralement associé à une erreur technique)

- NotFound Le VI n'a pas été trouvé
- Undetermined Autres cas

5.4.2 Normalisation de l'élément Statut

➢ Cas 1 – Réponse fonctionnelle OK ou KO

La valeur du champ « Code » doit être « Success ».

Le champ « Detail » doit contenir des précisions sur le résultat fonctionnel, conformément aux SFD associées au service.

Dans l'exemple suivant, on essaie d'accéder à un document :

Résultat fonctionnel	Statut	
	Code	Detail
Le document a été retourné	Success	0 – Pas d'erreur
Le document n'a pas été retourné	Success	8 – Problème de lecture du document…

➢ Cas 2 – Le service n'a pu être rendu

La valeur du champ « Code » doit être « Failed ».

Il n'est pas nécessaire d'alimenter le champ « Detail », le besoin étant de préciser uniquement si le service a été rendu et non pas pourquoi il n'a pas été rendu.

➢ Cas 3 – Pas de traces applicatives associées à un VI

La valeur du champ « Code » doit être « NotFound », le champ « Detail » restant vide.

5.4.3 Normalisation des champs URL et Action

5.4.3.1 Standard Interops-A

➢ URL

Format : URN-Vversion.nomMéthode

URN	URN du service visé tel que défini dans la convention technique
version	Version du webservice
nomMéthode	Nom de la méthode appelée

Exemple :

```
urn:interops:gip-info-retraite:archives-retours-V2.donner_archives
```

➢ Action

Liste des données applicatives séparées par un point-virgule, chaque donnée applicative étant représentée par un couple « code donnée/valeur ».

Exemple :

```
CR=0068;NIR=1650433243088;NOM=DUPONT
```

5.4.3.2 Standard Interops-P

Dans le cas du standard Interops-P, il est recommandé de ne générer des traces applicatives que pour les actions effectuées (pas de trace pour les accès à des ressources par exemple). Dans le cas d'un portail basé sur un Framework web avec un modèle MVC (Struts, etc.), cela revient à faire générer les traces par les classes d'action.

- **URL**

Format :	URN-Vversion/URIAction
URN	URN du service visé tel que défini dans la convention technique
version	Version du service offert
URIAction	URI identifiant de manière unique l'action réalisée

Exemple :

```
urn:interops:gip-info-retraite:archives-retours-V2/donner_archives
```

- **Action**

Liste des données applicatives séparées par un point-virgule, chaque donnée applicative étant représentée par un couple « code donnée/valeur ».

Exemple :

```
CR=0068;NIR=1650433243088;NOM=DUPONT
```

6. GESTION DES PAGM

6.1 Rappel de définitions issues du standard

Les PAGM doivent être définis entre les deux organismes, et ce dès l'expression du besoin, étape à laquelle a lieu la définition des rôles de la population cible.

Il est particulièrement important de ne pas rejeter cette problématique à la fin de la démarche ou d'en faire porter les conséquences sur l'organisme client seulement.

Il faut donc très en amont du projet définir les rapprochements possibles entre les profils applicatifs et les rôles métier. Ces décisions ont en effet un impact sur l'organisme client qui doit différencier sa population avec une granularité suffisante (définition des rôles métier) et éventuellement consolider ses différents référentiels d'habilitation en conséquence. Elles ont également un impact sur l'organisme fournisseur qui doit adapter sa gestion des droits pour les applications proposées.

La granularité des PAGM est donc choisie d'un commun accord entre les organismes. Elle varie en fonction des sujets et domaines métiers traités, et résulte d'une discussion entre organismes fournisseurs et organismes clients.

La réflexion sur les PAGM doit intégrer la plupart des organismes potentiellement concernés (clients et fournisseurs) pour une meilleure pérennité des définitions retenues pour ces profils.

6.2 Modèle d'utilisation

On peut envisager plusieurs cas d'usage des PAGM dans le cadre d'Interops. Nous en distinguerons ici trois : les PAGM « cumulatifs », les PAGM « par rôle » et les PAGM « poupées russes ».

6.2.1 PAGM « cumulatifs »

Le principe des PAGM « cumulatifs » est représenté à la [CONV].

Figure 3 : Schéma de principe des PAGM « cumulatifs ».

On peut imaginer une application prévoyant des droits applicatifs suivants :

- Consultation de la donnée A
- Administration de la donnée A
- Consultation de la donnée B
- Administration de la donnée B

Le client ayant défini les rôles métier suivants :

- Lecteur
- Expert

Les PAGM qu'on en déduirait dans le modèle cumulatif seraient calqués sur ces droits :

- PAGM1 : Consultation de la donnée A

- PAGM2 : Administration de la donnée A
- PAGM3 : Consultation de la donnée B
- PAGM4 : Administration de la donnée B

Le VI d'un Lecteur pourrait donc contenir les PAGM1 et PAGM3, celui d'un Expert pourrait contenir tous les PAGM.

Dans ce modèle, correspondant à un découpage par droit, les PAGM s'ajoutent donc les uns aux autres. La combinatoire des droits peut conduire à définir un nombre important de PAGM.

Ce modèle est régit par les règles de gestion suivantes :

- On peut transmettre dans le VI plusieurs PAGM
- Si aucun PAGM n'est transmis, le VI doit être rejeté

Ce modèle ne permet pas donc d'avoir des règles de gestion simple. En effet, l'application peut nécessiter une combinaison de PAGM ou au contraire, des combinaisons peuvent être interdites.

Les PAGM correspondants à des droits applicatifs plus qu'à des rôles métiers, l'organisme client aura en outre la charge de créer ces droits applicatifs dans son référentiel et de faire correspondre ces droits à chacun de ses rôles. Ce modèle a donc un impact potentiellement fort sur le SI de l'organisme client.

Note : Compte tenu des éléments ci-dessus, ce modèle d'utilisation est à proscrire autant que faire se peut dans le cadre d'Interops.

Le standard Interops (cf. Convention technique [CONV]) a défini plusieurs politiques d'acceptation des PAGM. Le modèle des PAGM « cumulatifs » peut être implémenté en suivant la politique « MatchAny » identifiée par l'URN suivant :

`urn:interops:1.0:attr-policy:matchAny`

6.2.2 PAGM « par rôles »

Le principe des PAGM « par rôles » est représenté à la Figure 4.

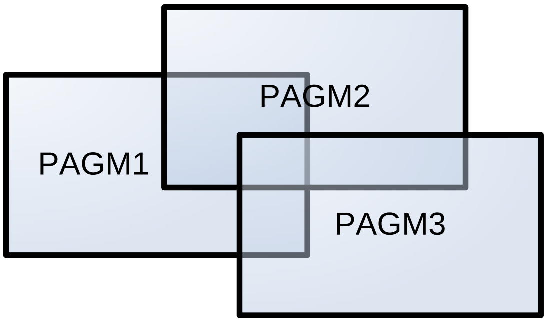


Figure 4 : Schéma de principe des PAGM « par rôles ».

Si on décidait d'adapter les PAGM prévus dans le cadre de l'application définie précédemment à ce modèle, on pourrait définir les PAGM suivants :

- PAGM1 correspondant à un agent Lecteur et rassemblant les droits applicatifs Consultation de la donnée A et Consultation de la donnée B.
- PAGM2 correspondant à un agent Expert et rassemblant tous les droits applicatifs prévus par l'application.

Dans ce modèle correspondant à un découpage par rôle métier donnant accès à des droits, un PAGM peut correspondre à plusieurs profils applicatifs.

La combinatoire est réduite et le principe initial des PAGM est respecté : il s'agit bien de faire le lien entre les profils applicatifs et les rôles métier. Ce modèle permet de limiter et répartir les impacts sur les SI des organismes.

Les règles de gestion associées à ce modèle sont les suivantes :

- On doit transmettre dans le VI un et un seul PAGM correspondant au rôle de l'utilisateur.
- Si aucun ou plusieurs PAGM sont transmis, le VI doit être rejeté.

Le standard Interops (cf. Convention technique [CONV]) a défini plusieurs politiques d'acceptation des PAGM. Le modèle des PAGM « par rôle » peut être implémenté en suivant la politique « OnlyOne » identifiée par l'URN suivant :

`urn:interops:1.0:attr-policy:onlyOne`

6.2.3 PAGM « poupées russes »

Le principe des PAGM « poupées russes » est représenté à la Figure 5.

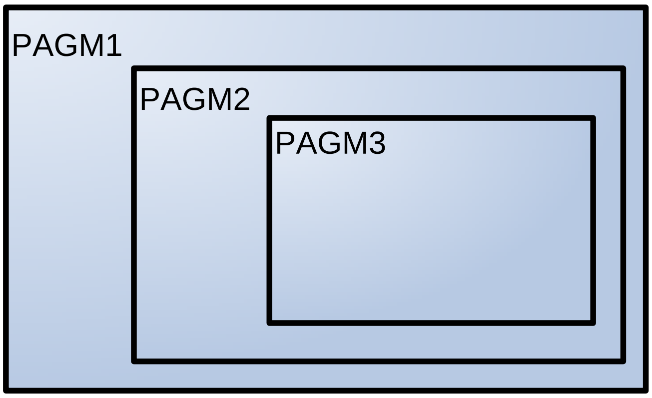


Figure 5 : Schéma de principe des PAGM « poupées russes ».

Les PAGM utilisées pour accéder à l'application IDENT de la CNAV illustrent ce modèle : deux PAGM sont prévus, `CNAV_IDENT_STANDARD` et `CNAV_IDENT_EXPERT`, le second englobant les droits du premier.

Dans ce modèle, les profils applicatifs liés aux PAGM sont donc inclus les uns dans les autres. Il en découle que les PAGM sont exclusifs et que la transmission d'un seul de ces PAGM est nécessaire et suffisante. C'est un sous-ensemble du modèle « par rôle ».

On peut donc en tirer les règles de gestion suivante :

- On doit transmettre dans le VI un et un seul PAGM
- Si aucun ou plusieurs PAGM sont transmis, le VI doit être rejeté.

Ce modèle s'applique particulièrement au mode « application à application » et « portail à service ».

Le standard Interops (cf. Convention technique [CONV]) a défini plusieurs politiques d'acceptation des PAGM. Le modèle des PAGM « par rôle » peut être implémenté en suivant la politique « OnlyOne » identifiée par l'URN suivant :

`urn:interops:1.0:attr-policy:onlyOne`

6.3 Cas d’usage

6.3.1 Principes généraux

On peut imposer que

- L'organisme client doit transmettre un ensemble minimal de PAGM
- L'organisme client doit transmettre uniquement des PAGM conventionnels
- L'organisme fournisseur peut rejeter une requête si un PAGM est non conventionnel

Note : Cette notion d’ensemble minimal reste problématique dans le cas du modèle « cumulatif » et les règles de gestion sont à régler au cas par cas. On notera que les modèles « par rôle » ou « poupée russe » définissent clairement l’ensemble minimal comme étant le PAGM correspondant au rôle métier de l’utilisateur concerné par le VI.

6.3.2 Interops-A : application à application

6.3.2.1 Notion de profil applicatif

On appellera par la suite **profil applicatif** un niveau de fonctionnalité rendu par une application.

Par exemple, le service « ident » de la CNAV a deux profils applicatifs : niveau « standard » et niveau « expert ».

Il est à noter qu’une convention technique par Web Service (profil applicatif) sera nécessaire. Dans l’exemple ci-dessus, deux conventions sont donc nécessaires.

6.3.2.2 Utilisation des PAGM

Dans Interops-A, **des PAGM pourront donner accès à un service**, c’est-à-dire à un profil applicatif. Ils ne sont pas interprétables fonctionnellement pour limiter le résultat. Les attributs complémentaires seront utilisés à cet effet.

Il peut exister un risque si un organisme client envoie tous les PAGM d'un agent (concernant des applications différentes). Il pourrait apparaître des problèmes d'homonymie, de collision, etc. **L'organisme client doit donc transmettre uniquement le ou les PAGM déclarés dans la convention technique.**

6.3.3 Interops-P : portail à portail

Si un portail présente des services distincts ayant des PAGM différents, il est nécessaire de transmettre les PAGM de chacun des services. La convention technique du portail contient donc les PAGM de tous les services. Une seule convention technique est nécessaire.

On associe un PAGM à un service ou un bouquet de service auquel cas la sélection du PAGM se fait au niveau de l'organisme client.

Un portail pouvant présenter plusieurs services ou bouquets de service, plusieurs PAGM sont transmis. Le portail de l’organisme client devient alors un portail d’authentification.

Le portail de l’organisme fournisseur devra gérer le cas où des PAGM sont exclusifs.

6.3.4 Interops-P : portail à service

Comme pour Interops-A, un seul PAGM doit être nécessaire pour personnaliser le comportement du service. Un retour au portail de l'organisme client pourra donc être nécessaire pour changer de PAGM.