Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

MINISTÈRE DU TRAVAIL, DE l'EMPLOI ET DE LA SANTÉ

MINISTÈRE DES SOLIDARITÉ ET DE LA COHÉSION SOCIALE

MINISTÈRE DU BUDGET, DES COMPTES PUBLICS ET DE LA RÉFORME DE L'ÉTAT

Spécifications fonctionnelles

Standard d'interopérabilité entre organismes de la sphère sociale

Réf. : Standard Interops2.0_SpecificationsFonctionnelles
Version 2.0 du 05/04/2012

Référence : **Version :** **Date de dernière mise à jour :**	Standard Interops2.0_SpecificationsFonctionnelles 2.0 05/04/2012
Niveau de confidentialité :	PUBLIC

Table des mises à jour du document

N° de version	Date	Auteur	Objet de la mise à jour
2.0	05/04/12	Groupe de travail Interops	Version pour diffusion

SOMMAIRE

1. INTRODUCTION

1.1 Objet du document

Ce document est la présentation du standard d'interopérabilité des organismes de la sphère sociale.

1.2 Organisation et structure du document

La structure du présent document est, en sus de la présente introduction, organisé comme suit :

- le chapitre 2 constitue une présentation du **cadre de développement de ce standard**,
- le chapitre 3 présente les éléments constitutifs de la **Convention préalable** à la mise en place d'échanges inter-organismes,
- le chapitre 4 traite de la gestion d'habilitation et des Profils Applicatifs Génériques Métiers (**PAGM),**
- le chapitre 5 traite des authentifications et transferts d'habilitation **(Vecteurs d'identification),**
- Le chapitre 6 présente les **solutions d'utilisation d'habilitations** dans les architectures applicatives,
- le chapitre 7 constitue les **spécifications fonctionnelles du standard** et les **contraintes applicables**,
- le chapitre 8 représente **les choix techniques retenus** pour le standard,
- le chapitre 9 est constitué **d'annexes**, dont un glossaire.

Convention de nommage
Dans l'ensemble du document :

[Utilisateur] représente une personne physique appartenant à un organisme de la sphère sociale ou utilisant un poste du système d'information de cet organisme.

[organisme client] représente l'organisme de départ dont fait partie l'utilisateur qui souhaite atteindre une application située hors de son organisme de rattachement,

[organisme fournisseur] représente l'organisme fournisseur de services, qui opère l'application ou le service ouvert(e) à des utilisateurs appartenant à des organismes clients.

1.1 Références

1.1.1 Documents internes

Référence		Titre	Auteur	Ver.	Date
[R1]	Standard Interops2.0_Glossaire	Glossaire du standard Interops	Groupe de travail Interops	2.0	05/04/12
[R2]	Standard Interops2.0_ConventionTechnique	Convention technique	Groupe de travail Interops	2.0	05/04/12

98

1.1.2 Documents externes

	Titre	Auteur	Date
[RGS]	Référentiel Général de Sécurité version 1.0	ANSSI/DGME	06/05/2010
[RGS_A_14]	Référentiel Général de Sécurité version 1.0 Annexe A14 : Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques	ANSSI/DGME	11/02/2010
[RGS_B_1]	Référentiel Général de Sécurité version 1.0 Annexe B1 : Mécanismes cryptographiques	ANSSI/DGME	26/01/2010
[SOAP]	Simple Object Access Protocol (SOAP) 1.1	Andrew, Mendelsohn, Noah, Nielsen, HenrikFrystyk, Winer, Dave, eds.	08/03/2000
[TLS]	RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1	T. Dierks, E. Rescorla	Avril 2006
[XMLDsig]	XML-Signature Syntax and Processing	Eastlake, Donald, Reagle, Joseph, Solo, David, eds.	12/02/2002

2. CADRE DE DEVELOPPEMENT DU STANDARD

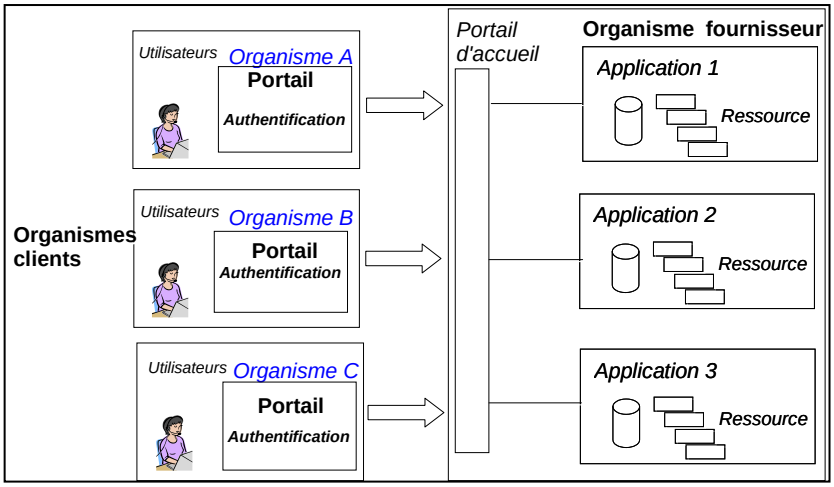
2.1 Objet de la réflexion

2.1.1 Présentation

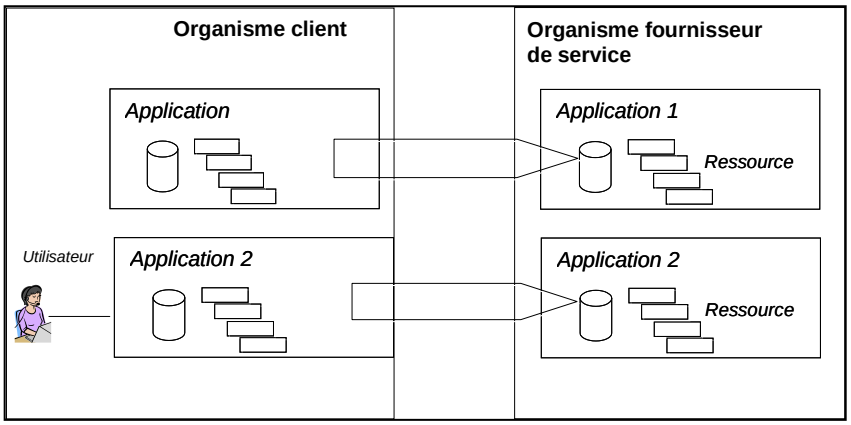
Le standard d'interopérabilité doit permettre l'interconnexion des SI des organismes de la sphère sociale, au travers des 2 modèles d'échanges :

- "portail à portail" : accès d'un utilisateur d'un organisme client à l'application ou au service d'un organisme fournisseur, via les portails web respectifs des 2 organismes,
- "application à application" : échanges, en protocole "Web Services", effectués soit dans un contexte applicatif sans identification d'un utilisateur, soit dans un contexte où un utilisateur d'un organisme client atteint les applications des organismes fournisseurs au travers d'une application locale.

2.1.2 Les deux modèles traités



Le modèle "portail à portail"



Le modèle "application à application"

2.2 Portée du standard et principes retenus par les organismes

Ce standard est défini pour l'ensemble des organismes de la sphère sociale souhaitant interopérer selon l'un ou l'autre des deux modèles précédents.

Les principes retenus pour la mise en place du standard sont les suivants :

- Le modèle repose sur la confiance entre les organismes,
- L'authentification de l'utilisateur n'est pas effectuée de bout en bout mais est réalisée par l'organisme client,
- L'habilitation est attribuée par l'organisme client à ses utilisateurs en respectant les règles établies avec l'organisme fournisseur (Convention),
- L'habilitation est transmise à l'organisme fournisseur de manière sécurisée (par un Vecteur d'identification),
- Toute création de vecteur d'identification est auditable afin d'en permettre le contrôle "a posteriori".

3. CONVENTION PREALABLE

3.1 Objet de la convention

Les organismes doivent établir une convention visant à définir les modalités d'accès de l'organisme client au SI de l'organisme fournisseur. La convention comprend des annexes techniques permettant la configuration des applications et des infrastructures de contrôle.

L'application du standard entre deux organismes intervient après la signature de cette convention (entre client et fournisseur).

La rédaction des conventions est laissée à l'appréciation des organismes qui peuvent s'inspirer de l'exemple suivant.

3.2 Exemple de Convention

Titre de la convention.

Désignation des parties (dénomination, sigle, siège social, représentant, voire textes relatifs à la représentation).

Article 1 - Objet (définition de l'objet de la convention = détermination d'un standard d'interopérabilité des échanges inter-organismes et des modalités de sa mise en place).

Article 2 - Documents conventionnels (détermination des documents sur lesquels les parties vont s'engager, dits documents conventionnels).

Article 3 - Définition du standard d'interopérabilité inter-organismes et applications ou services visés (voir avec les organismes et groupements s'il est opportun de regrouper ces deux notions au sein d'un même article ou si leur distinction apparaît indispensable pour plus de clarté).

☞ prévoir un renvoi vers la ou les annexes techniques concernées si nécessaire.

Remarque : à cette occasion, les organismes ou groupements concernés pourront s'interroger sur la nécessité d'introduire dans la convention une notion relative à la nature des données à caractère personnel mises à la disposition des parties via ces applications (en conformité avec les autorisations de traitement).

Article 4 - Actions autorisées et gestion des habilitations (voir avec les organismes et groupements s'il est opportun de regrouper ces deux notions au sein d'un même article ou si leur distinction apparaît indispensable pour plus de clarté).

☞ prévoir un renvoi vers la ou les annexes techniques concernées si nécessaire.

Article 5 - Définition du PAGM (profil applicatif générique métier).

☞ prévoir un renvoi vers l'annexe technique concernée.

Article 6 - Authentification et transfert d'habilitation (voir avec les organismes et groupements s'il est opportun de regrouper ces deux notions au sein d'un même article ou si leur distinction apparaît indispensable pour plus de clarté).

☞ prévoir un renvoi vers la ou les annexes techniques concernées si nécessaire.

Article 7 - Sécurité (cet article a pour objet d'engager les parties sur un niveau de sécurité à mettre en place et à maintenir – il peut concerner la sécurité logique, voire physique = à déterminer par les organismes et groupements).

☞ prévoir un renvoi vers la ou les annexes techniques concernées si nécessaire

Article 8 - Obligations des parties (cet article pourra soit regrouper les points particuliers qui ne concernent pas ceux déjà prévus par les articles sus-mentionnés, soit regrouper tous les engagements des organismes et groupements = à déterminer avec ces derniers).

Article 9 - Confidentialité (concerne le rappel des règles relatives au respect du secret professionnel et de l'engagement des parties, de leur personnel et de leurs éventuels sous-traitants).

Article 10 - Propriété intellectuelle (article à insérer si une des parties souhaite faire reconnaître ses droits de propriété sur tel ou tel outil ou logiciel, voire sur des informations qu'elle détient).

Article 11 - Audit (à voir avec les organismes et groupements sur la nécessité de mettre en place une procédure d'audit et de la faire apparaître dans la convention).

Article 12 - Archivage et conservation (cet article abordera la question de la traçabilité des échanges).

Article 13 - Réunion de « bilan » (article à intégrer dans le cas où seront mis en place des réunions inter-organismes – titre à définir).

Article 14 - Conditions financières (article à prévoir si les parties souhaitent faire apparaître cette question dans la convention).

Article 15 - Règlement des litiges (modalités de règlement des litiges = règlement amiable et/ou judiciaire).

Article 16 - Modification de la convention.

Article 17 - Caducité des clauses de la convention (en cas de modifications législatives ou réglementaires qui rendraient les dispositions de la convention contraires à ces dernières).

Article 18 - Dénonciation de la convention (permet à une des parties à la convention de sortir de celle-ci avec toutes les conséquences que cela entraîne).

Article 17 - Adhésion de nouveaux organismes ou groupements (article organisant les modalités d'adhésion d'une nouvelle partie à la convention).

Article 18 - Date d'effet et durée de la convention.

Désignation des parties signataires (sigles et identité des représentants).

ANNEXES (nombre et typologie à déterminer par les parties).

4. GESTION D'HABILITATION ET PAGM

La démarche, a priori dans un premier temps par métier, va consister à définir entre fournisseurs de services des profils communs appelés **PAGM** (Profil Applicatif Générique Métier), et leur relation avec les profils/rôles métiers (côté client) et les profils applicatifs (côté fournisseur).

4.1 Principes

Le concept de PAGM est retenu pour minimiser la matrice rôle/profils applicatifs.

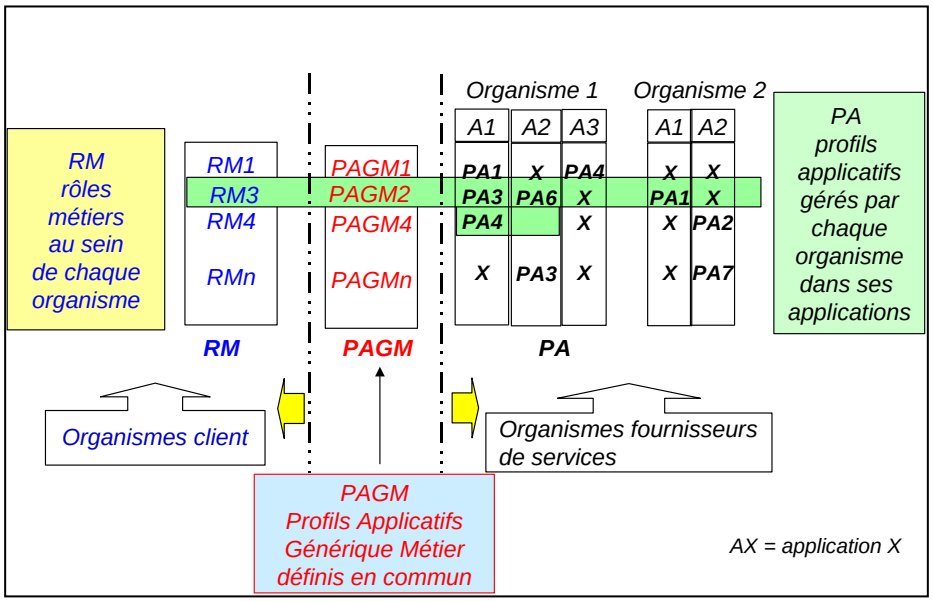
Chaque organisme client met en place une infrastructure qui associe à chaque entité (utilisateur ou application cliente) un ou plusieurs **PAGM** vis à vis d'applications gérées par des organismes fournisseurs de services.

L'organisme client est responsable de la sécurité du mécanisme de gestion des **PAGM**.

Les modalités d'attribution des PAGM (par exemple association de rôles métiers interne à l'organisme client avec certains PAGM) ne font pas partie du standard et sont spécifiques à chaque organisme.

4.2 Les PAGM : le regroupement de profils

Les droits accordés par les organismes fournisseurs de services aux organismes clients sont représentés par des **PAGM** (Profil Applicatif Générique Métier). La liste des PAGM disponibles pour une application ou un ensemble d'applications est déterminée par les organismes propriétaires d'applications et rendus disponibles aux organismes clients en fonction du contenu de la convention bi-partite.



Construction des PAGM

Cette définition permet de rendre la transmission d'une habilitation indépendante des profils applicatifs et de l'organisation des applications des organismes fournisseurs de services.

Dans l'exemple ci-dessus, le PAGM2 :

- va correspondre avec le rôle métier 3 de l'organisme client,
- correspond parfaitement avec le profil applicatif PA6 de l'application A2 de l'organisme fournisseur 1 et avec le profil applicatif PA1 de l'application A1 de l'organisme fournisseur 2,
- correspond à des droits représentés par les 2 profils applicatifs PA3 et PA4 de l'application A1 de l'organisme fournisseur 1.

4.3 Construction des PAGM

La granularité des PAGM est 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 de services et organismes clients.**

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

5. AUTHENTIFICATION ET TRANSFERT D'HABILITATION

5.1 Principes

Les principes retenus pour l'authentification et les transferts d'habilitations sont les suivants :

- L'authentification initiale de l'utilisateur est réalisée par l'organisme client,
- En fonction de la destination un **Vecteur d'identification** est fabriqué puis transmis avec les requêtes,
- L'association entre identifiant de départ et vecteur d'identification est tracée et donc auditable.
- Il y a une **authentification mutuelle** des organismes clients et fournisseurs de services.
- L'authenticité de chaque vecteur d'identification peut être vérifiée par l'organisme fournisseur de service,
- L'organisme fournisseur de services détermine les droits sur les applications en fonction des contenus d'habilitations transmis par l'intermédiaire du PAGM au sein du Vecteur d'identification.

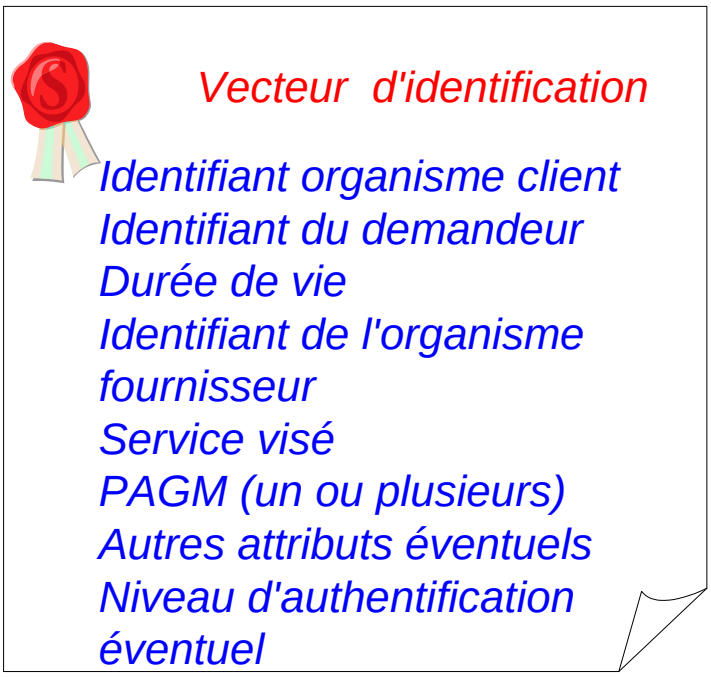
Nota : un **Vecteur d'identification** peut comprendre un ou plusieurs PAGM d'une même application ou famille d'applications (en fonction de l'organisation de l'organisme fournisseur de service).

5.2 Le vecteur d'identification[1]

Un vecteur d'identification est une attestation de l'organisme de départ comprenant :

- L'identifiant de l'organisme client d'origine,
- L'identifiant de l'utilisateur du service ou de l'application de départ : cette identité n'est pas nécessairement nominative, elle peut être représentée par un identifiant dépersonnalisé permettant ultérieurement une opposabilité (traçabilité),
- La durée de vie de l'habilitation,
- L'identifiant de l'organisme fournisseur de services,
- Le service visé en forme d'URI (Universal Ressource Information),
- Le ou les profils selon lequel l'utilisateur (ou l'application cliente) souhaite et doit travailler (par l'intermédiaire du ou des PAGM définis en commun et autorisé(s) pour cet utilisateur/cette application),
- D'autres attributs éventuels, parmi lesquels on pourrait trouver (à titre d'exemple) :
  - o des indications géographiques,
  - o des indications de localisation,
  - o des niveaux de sécurité définis entre organismes,
- Un niveau d'authentification : il peut par exemple représenter le moyen ou le niveau du moyen avec laquelle l'authentification est réalisée,
- Une signature numérique délivrée par l'organisme client qui permet de valider l'authenticité des éléments décrits ci-dessus.

[1] *On notera que la terminologie Vecteur d'Identification est conservée pour l'homogénéité avec les travaux ADAE sur le même sujet, alors qu'en réalité ce Vecteur transporte simultanément identifiant et habilitation.*



273

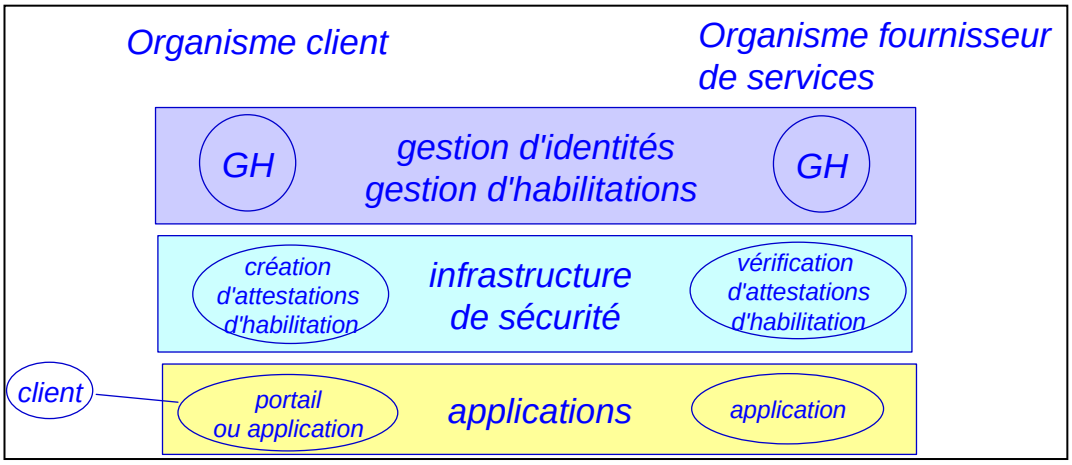
274 ***Le contenu du vecteur d'identification***

6. LES SOLUTIONS D'UTILISATION D'HABILITATIONS DANS LES ARCHITECTURES APPLICATIVES

6.1 Positionnement de la problématique

Compte-tenu du contexte de déploiement du standard, les organismes mettent en place une infrastructure avec une architecture qui peut se décomposer fonctionnellement en 3 niveaux :

- un niveau haut comprenant "gestion d'identités" et "gestion d'habilitations", consistant à :
  - gérer les identités et les authentifications des utilisateurs,
  - gérer les droits des utilisateurs ou des applications clientes par rapport aux droits métiers qui leurs sont accordés, représentés par les PAGM,
- un niveau "infrastructure de sécurité", consistant, selon la situation, à créer ou analyser des attestations d'habilitations dans le contexte d'une requête faite par un utilisateur ou une application cliente vers une application,
- un niveau "applicatif", comprenant :
  - des portails (modèle "portail à portail"),
  - ou des applications (modèle "application à application").



Architecture à trois niveaux

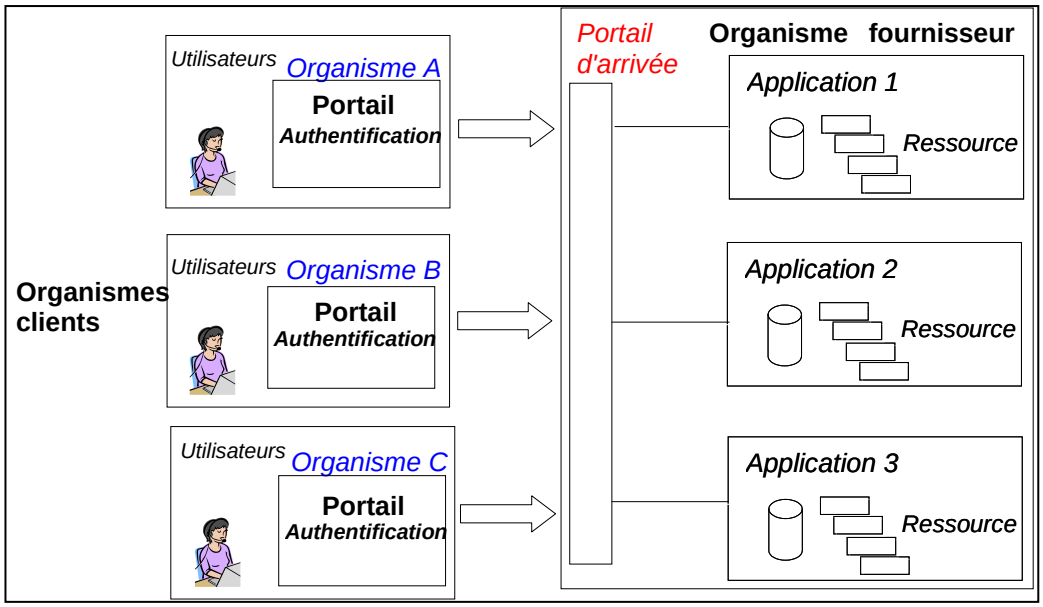
On notera la recommandation d'une séparation entre les 3 niveaux définis ci-dessus.

6.2 Le cadre "Portail à Portail"

Plusieurs formes d'échanges de l'attestation ont été discutées, et la solution suivante avec Reverse Proxy a été retenue.

6.2.1 Définition

Le cadre "portail à portail" concerne l'accès par un utilisateur à une application située dans un organisme distant.



Rappel du modèle des échanges portail à portail

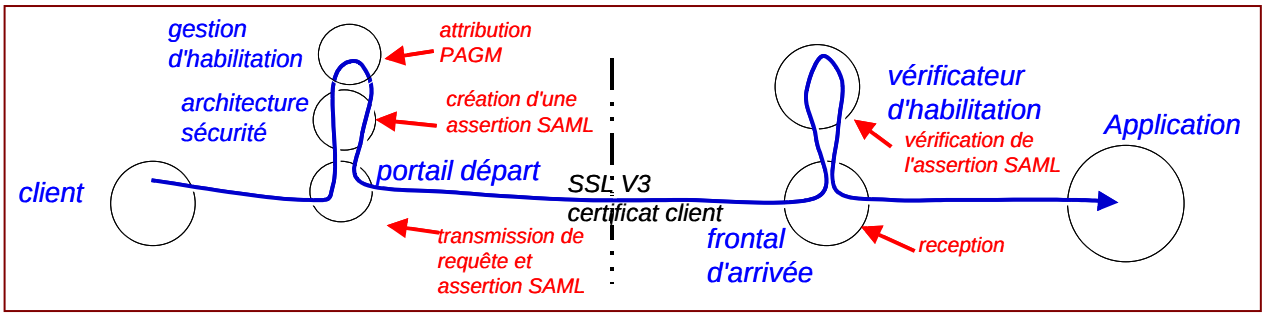
6.2.2 Principe de transmission d'habilitations

Le mode de transmission d'habilitations retenu est celui du "proxy applicatif", dans lequel :

- les éléments nécessaires à la création du vecteur d'identification sont créés dans l'organisme départ,
- le portail de départ se comporte comme un relais entre le client et l'application distante,
- l'habilitation (Vecteur d'identification) est représentée par une assertion SAML.

6.2.3 Cinématique des échanges

Pour le modèle "**portail à portail**", les attestations SAML sont utilisées à l'arrivée pour déterminer les droits de l'utilisateur de l'organisme client.



Cinématique des échanges "portail à portail"

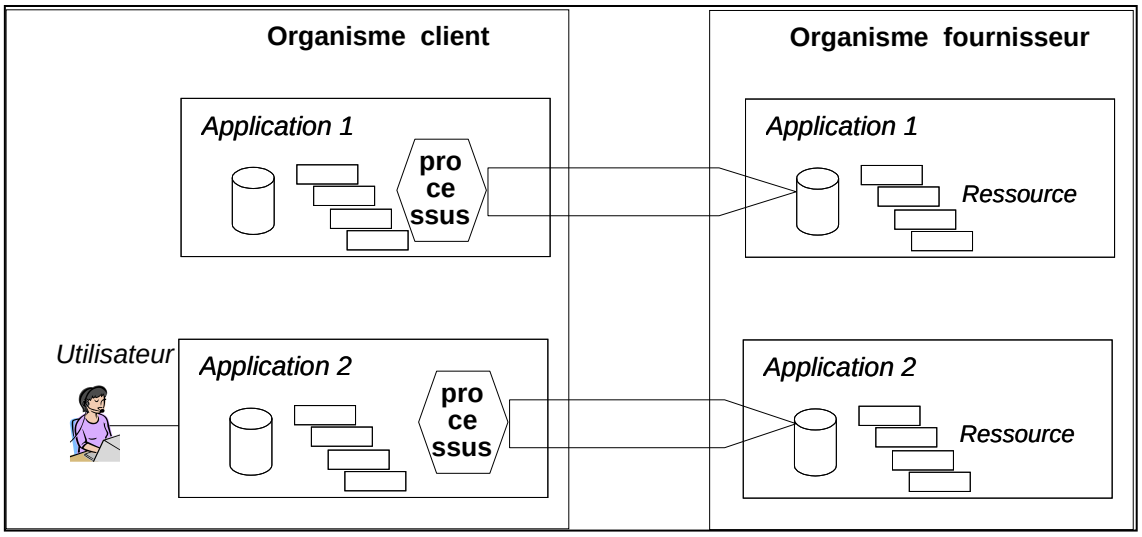
6.3 Le cadre "Application à Application"

Il s'agit du cas d'une application d'un organisme client qui communique avec une application située chez un organisme fournisseur en utilisant des techniques Web Services.

6.3.1 Définition

Le cadre "application à application" concerne :

- soit un Web-Service entre des applications situées respectivement dans l'organisme client et l'organisme fournisseur,
- soit l'accès d'un utilisateur de l'organisme client à des données d'une application de l'organisme fournisseur au travers d'une application locale.

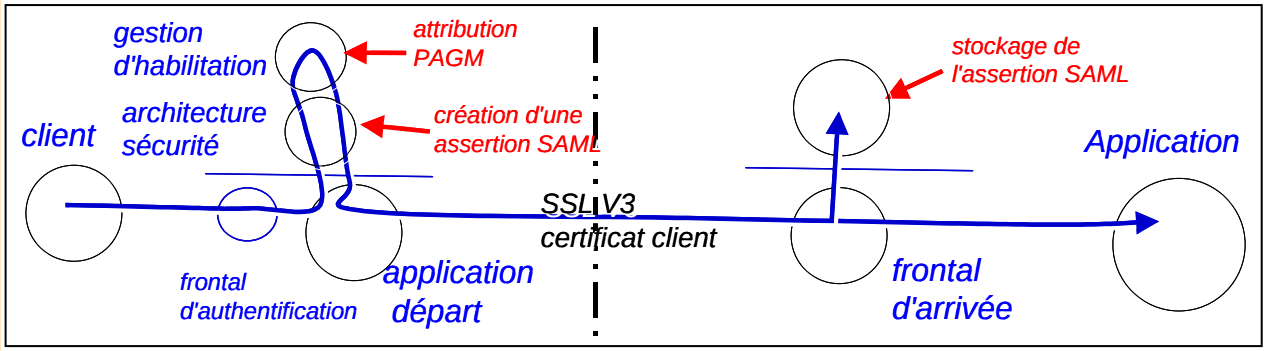


Rappel du modèle des échanges "application à application"

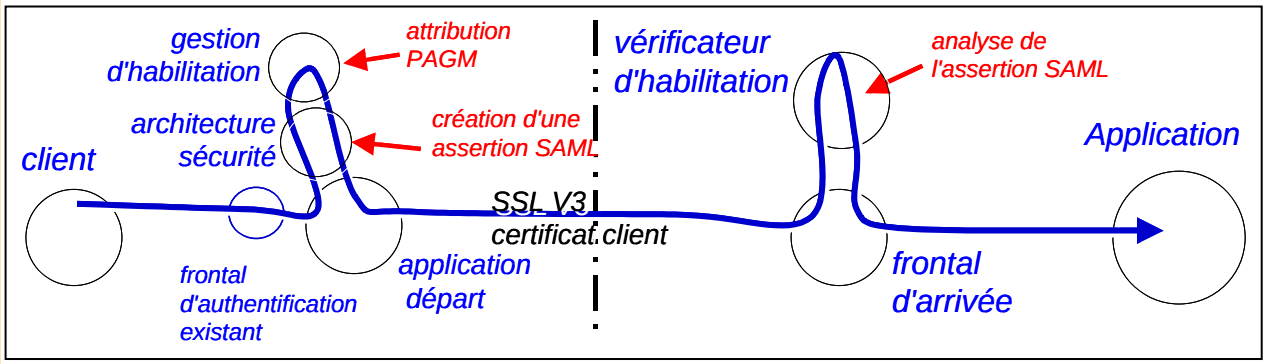
6.3.2 Cinématique de transmission d'habilitations

Pour **le modèle "application à application",** il a été décidé de conserver le principe du transfert d'habilitations par attestation SAML. Les attestations SAML sont créées au sein de l'organisme client et peuvent alors :

- soit être simplement archivées, si l'authentification de l'application de départ (SSLV3 mode client) est suffisante en terme de confiance pour l'organisme d'arrivée,
- soit servir à des contrôles supplémentaires.



Cinématique des échanges "application à application" sans vérification de l'attestation SAML



Cinématique des échanges "application à application" avec vérification de l'attestation SAML

7. ELEMENTS FONCTIONNELS ET CONTRAINTES

Les choix de l'architecture et de l'implémentation des blocs fonctionnels sont considérés comme de la responsabilité des organismes. Ils ne font pas partie du standard.

7.1 Blocs fonctionnels

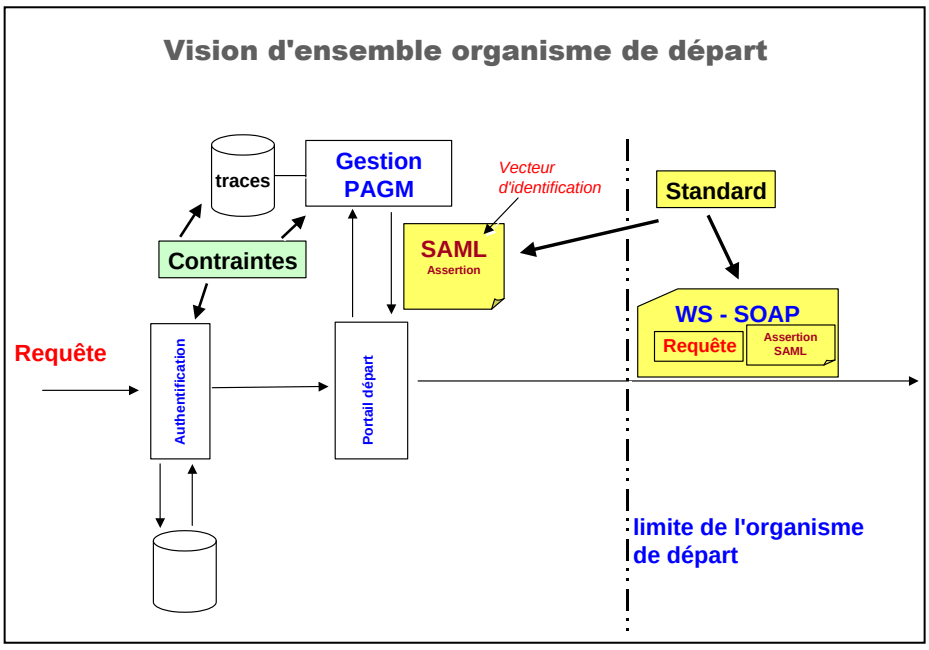
Il s'agit, pour les organismes clients, des blocs fonctionnels suivants :

- gestion des identités,
- gestion des authentifications,
- gestion des PAGM (association avec utilisateurs et/ou rôles),
- gestion de la preuve (gestion de traces).

Il s'agit pour les organismes fournisseurs des blocs suivants :

- gestion des PAGM (association avec les profils applicatifs),
- gestion de la preuve (gestion de traces).

Néanmoins, des contraintes et/ou exigences porteront sur ces blocs fonctionnels, à charge pour les organismes de les respecter (il s'agit d'une logique de résultat et non d'une logique de moyens). Ces contraintes et exigences sont définies précisément dans les annexes de la convention signée entre organisme client et organisme fournisseur.



Vision d'ensemble

7.2 Contraintes

Les contraintes portent principalement sur :

- la sécurité de certains mécanismes,
- les traces qui doivent être conservées par l'organisme client et l'organisme fournisseur.

7.2.1 Niveau d'authentification :

L'organisme client est responsable de l'authentification des utilisateurs ou applications clientes souhaitant aller vers des services opérés par l'organisme fournisseur.

Les niveaux d'authentification nécessaires seront mentionnés dans les conventions entre organismes (et en particulier dans leurs annexes techniques). Ils pourront être transmis de manière implicite.

Ces niveaux pourront être :

- authentification par login/mot de passe,
- authentification par bi-clé/certificat RGS[2] "1 étoile" (correspondant à un bi-clé/certificat logiciel remis sans face à face),
- authentification par bi-clé/certificat RGS "2 étoiles" (correspond à un bi-clé/certificat sur support matériel individuel dont l'enregistrement / remise comprend un face à face),
- authentification par bi-clé/certificat RGS "3 étoiles" (correspond à un bi-clé/certificat qualifié sur support matériel individuel dont l'enregistrement / remise comprend un face à face[3]),

Nota : ces niveaux sont donnés à titre indicatif, ils peuvent être différents et sont décrits dans l'annexe technique correspondante de la convention.

7.2.2 Gestion des PAGM

L'infrastructure qui associe à chaque identifiant un ou plusieurs PAGM, appelée "Gestion des PAGM", est du ressort de l'organisme client.

Ce dernier est responsable de la sécurité du mécanisme d'attribution des PAGM.

7.2.3 Traces

La complétude des traces est assurée par une consolidation des traces de l'organisme client et de l'organisme fournisseur.

Chacun des organismes est responsable des traces des éléments qui leur incombent et de leurs archivages pouvant être utilisées a posteriori en cas de besoins (litige ou contentieux, par exemple). La convention établie entre les organismes permet d'établir le format d'échanges des traces InterOPS.

L'organisme client a la responsabilité d'être à même de fournir en cas de besoin, sous la forme qu'il choisit :

- Les éléments liés à l'authentification de l'utilisateur final
- Les éléments permettant de retrouver l'association à un instant donné entre un utilisateur ou un type d'utilisateur (exemple rôle ou profil métier) et les PAGM autorisés
- les éléments permettant de retrouver l'utilisateur final ayant effectué une requête d'accès à un organisme fournisseur donnée

---

2 *Selon les références disponibles au 26/04/2011 RGS version 1.0 en date du 06/05/2010*

3 *Les différences entre 2 étoiles et 3 étoiles ne sont pas apparentes pour le porteur. La différence réside principalement dans le niveau plus élevé pour les exigences portant en particulier sur l'administration de l'IGC, le niveau d'évaluation et certification du boîtier cryptographique de l'AC (boîtier HSM au sein duquel sont signés les certificats des titulaires), les modalités de remise (exemple l'acceptation du certificat par le titulaire doit être faite sous la forme d'un accord signé dans le cas 3 étoiles, et peut être tacite dans le cas 2 étoiles).*

De même, l'organisme fournisseur a la responsabilité d'être à même de fournir en cas de besoin, sous la forme qu'il choisit :

- Les éléments de vérification du vecteur d'identification par le fournisseur et de création du contexte de sécurité pour l'utilisateur final
- Les éléments permettant de retrouver à qui il a donné des informations
- Les éléments permettant de retrouver un profil applicatif correspondant à une requête

8. ELEMENTS TECHNIQUES

Dans ce chapitre nous décrivons des éléments techniques qui sont utilisables dans ce standard.

Il s'agit :

- d'un format de description de l'annexe technique de la convention, incluant les détails permettant la configuration des systèmes, décrit dans le chapitre comme « Eléments transmis au préalable des échanges »,
- d'un format de description du Vecteur d'Identification,
- du protocole d'échange des requêtes,
- de la sécurisation des transferts entre organismes.

8.1 Éléments transmis en préalable aux échanges

L'accord passé entre les organismes est matérialisé par trois documents : une convention juridique, une convention technique annexée à la convention juridique et une convention technique au format XML.

Le document de convention technique permet de rappeler de manière exhaustive et documentée les éléments d'une convention. Le document au format XML permet de formaliser les informations et de faciliter l'échange des conventions techniques.

Aucun des trois standards existant pour la formalisation et l'échange des conventions techniques (ebXML, SAML 2.0 Metadata, WS-Policy) ne permet de couvrir complètement les besoins d'Interops.

Le schéma des conventions XML est donc spécifique à Interops. En outre, il ne dérive pas des standards cités précédemment pour éviter les adhérences aux évolutions de ces derniers. Par contre, il reprend la structuration et la nomenclature des standards précités (SAML 2.0 Metadata en particulier) afin de bénéficier du travail déjà effectué.

Le schéma XML des conventions Interops est décrit dans un document spécifique [R2].

L'accord rassemble les informations suivantes :

➢ **Description générale**

- Description de l'application
- Description des acteurs
- Contacts

➢ **Description du VI**

- Numéro de version de la convention
- Mode Interops de l'application
- Version SAML
- Identifiant des organismes
- Identifiant du service visé
- Format de l'identifiant de l'utilisateur
- Niveaux d'authentification requis
- PAGM et attributs complémentaires
- Durée de validité du VI
- Décalage d'horloge autorisé
- Paramètres de la signature
- URL du web-service (Interops-A) ou base URL du service (Interops-P)

- URL du consommateur d'assertions (Interops-P)
- Adresses IP du ou des reverse-proxy
- Description des cookies (Interops-P)

➢ **Éléments de la couche de transport**

- Protocole de transport et version, algorithmes SSL utilisés
- Certificat de signature, chaîne de certification et le point de distribution des listes de certificats révoqués
- Certificat SSL client, chaîne de certification et le point de distribution des listes de certificats révoqués
- Certificat SSL fournisseur, chaîne de certification et le point de distribution des listes de certificats révoqués
- Adresses IP du ou des proxy
- Méthodes de synchronisation temporelle des serveurs

➢ **Traces**

- Durée de conservation
- Version du format d'échange
- Spécifications de l'élément « Action »

La modification de certaines des informations contenues dans la convention techniques donne lieu à une re-signature de la convention juridique. La convention technique définit plus précisément les modifications qui peuvent être apportées au document nécessitant une re-signature ou non du document.

8.2 Transfert de la requête

La communication entre les organismes doit être sécurisée.

8.2.1 Transmission d'une requête HTTP

Dans le mode portail à portail, les accès se font conformément au profil de Web Browser SSO/POST, initié au niveau du fournisseur d'identité. Ce profil est décrit dans le document « Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 » de S. Cantor et al.

Le vecteur d'identification est généré par l'organisme client. Il est transmis uniquement à la première connexion dans un formulaire auto-soumis à l'utilisateur final qui le relaie à l'organisme fournisseur.

L'organisme fournisseur vérifie une fois le vecteur d'identification et crée un contexte de sécurité pour l'utilisateur final.

8.2.2 Transmission d'une requête SOAP

Ce cas concerne le mode application à application en Web Service.

L'assertion SAML devient le SecurityToken de la requête SOAP.

8.3 Sécurisation du transfert

8.3.1 Protection des canaux et authentification mutuelle

Afin de sécuriser les échanges entre organismes client et fournisseur[4], il est possible d'utiliser le protocole TLS (SSL).

Dans ce cas, les deux partenaires d'une communication TLS s'authentifient mutuellement en utilisant la technique asymétrique de clé publique et privée et des certificats d'identité X.509 des deux serveurs. Toute communication est protégée par chiffrement avec algorithme AES à l'intérieur de TLS.

SSL V3 est la version qui permet techniquement l'utilisation de certificats clients. Par abus de langage, on dit utiliser SSLV3 pour indiquer une authentification mutuelle. La version TLS est préconisée, étant la plus avancée et normalisée. En outre, elle est techniquement implémentée par la grande majorité des technologies du marché. Néanmoins, ces techniques n'imposent pas l'utilisation de certificats clients. C'est pourquoi ce point est précisé dans ce chapitre.

La protection de l'accès aux clés privées est de la responsabilité respective des 2 organismes.

- *L'utilisation d'une protection des canaux est nécessaire.*

  La méthode de protection décrite ci-dessus n'est cependant pas obligatoire, les organismes restant libres de décider la mettre en place ou non pour leurs échanges (si la confidentialité des échanges est assurée par ailleurs).

- ***Dans le cas où les échanges devront être sécurisés en utilisant des mécanismes conformes au Référentiel Général de Sécurité, les moyens cryptographiques utilisés devront suivre les préconisations contenues dans le [RGS]. En particulier, les tailles de clés et algorithmes utilisés devront respecter [RGS_B_1] et les profils de certificats devront s'appuyer sur [RGS_A_14].***

8.3.2 Protection des objets SOAP

Si la convention entre les organismes le précise, les objets SOAP sont protégés par une signature XML DSIG de l'organisme client.

Exemple : si les objets sont traités par des fonctions de back office qui doivent vérifier l'authenticité de l'émetteur, il est souhaitable d'utiliser cette protection en sus de la protection du canal.

---

[4] *Afin de garantir la plus grande indépendance entre le code applicatif et le système d'exploitation et pour la simplicité de l'implémentation.*

Nota : avec l'utilisation de IPSEC seul (sans TLS), il est difficile pour l'application de déterminer et contrôler le niveau de protection du canal.

9. ANNEXES

9.1 Liens utiles

OASIS : http://www.oasis-open.org

Spécifications OASIS : http://www.oasis-open.org/specs/index.php

Spécifications SAML : http://www.oasis-open.org/specs/index.php#samlv2.0

OASIS-ebXML/CPP : http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa

[ccOVER] ebXML Core Components Overview, http://www.ebxml.org/specs/ccOVER.pdf.

[ebBPSS] ebXML Business Process Specification Schema, http://www.ebxml.org/specs/ebBPSS.pdf.

[ebBPSS2] OASIS ebXML Business Process,

[ebMS] ebXML Message Service Specification, http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf.

[ebRS] ebXML Registry Services Specification, http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebrs.pdf.

[HTTP] Hypertext Transfer Protocol, Internet Engineering Task Force RFC 2616, http://www.rfc-editor.org/rfc/rfc2616.txt.

[RFC2119] Key Words for use in RFCs to Indicate Requirement Levels, Internet Engineering Task Force RFC 2119, http://www.ietf.org/rfc/rfc2119.txt.

[RFC2396] Uniform Resource Identifiers (URI): Generic Syntax, Internet Engineering Task Force RFC 2396, http://www.ietf.org/rfc/rfc2396.txt.

[RFC2246] The TLS Protocol, Internet Engineering Task Force RFC 2246, http://www.ietf.org/rfc/rfc2246.txt.

[SAML] Security Assertion Markup Language, http://www.oasis-open.org/committees/security/ -documents.

[XML] Extensible Markup Language (XML), World Wide Web Consortium,

http://www.w3.org/XML.

[XMLC14N] Canonical XML, Ver. 1.0, Worldwide Web Consortium, http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

[XMLDSIG] XML Signature Syntax and Processing, Worldwide Web Consortium, http://www.w3.org/TR/xmldsig-core/.

[XMLENC] XML Encryption Syntax and Processing, Worldwide Web Consortium, http://www.w3.org/TR/2002/CR-xmlenc-core-20020304/.

[XMLNS] Namespaces in XML, Worldwide Web Consortium, http://www.w3.org/TR/REC-xml-names/.

[XMLSCHEMA-1] XML Schema Part 1: Structures, Worldwide Web Consortium, http://www.w3.org/TR/xmlschema-1/.

[XMLSCHEMA-2] XML Schema Part 2: Datatypes, Worldwide Web Consortium, http://www.w3.org/TR/xmlschema-2/.

9.2 Acronymes et Glossaire

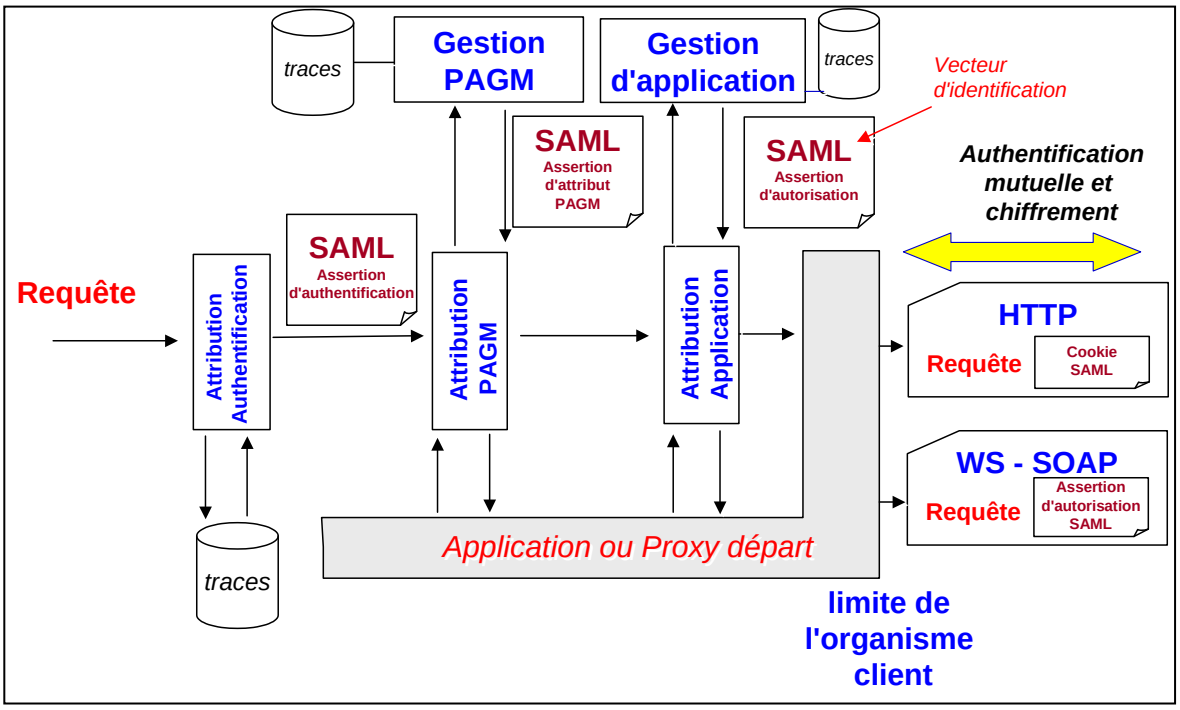
9.2.1 Acronymes

Sigles - abréviations	Définition
AAS	Authentification-Autorisation-SSO
ADAE	Agence pour le développement de l'administration électronique
CNIL	Commission Nationale de l'Informatique et des Libertés
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
MSP	Mon Service Public
PDA	Personal Digital Assistant
SAML	Security Assertion Markup Language
SI	Système d'Information
SOAP	Simple Object Access Protocol
SSO	Single Sign-On (équivalent français : authentification unique)
URI	Universal Ressource Information
URL	Universal Ressource Location
WAP	Wireless Application Protocol
X.509	Norme relative aux certificats à clé publique
XML	eXtented Markup Language

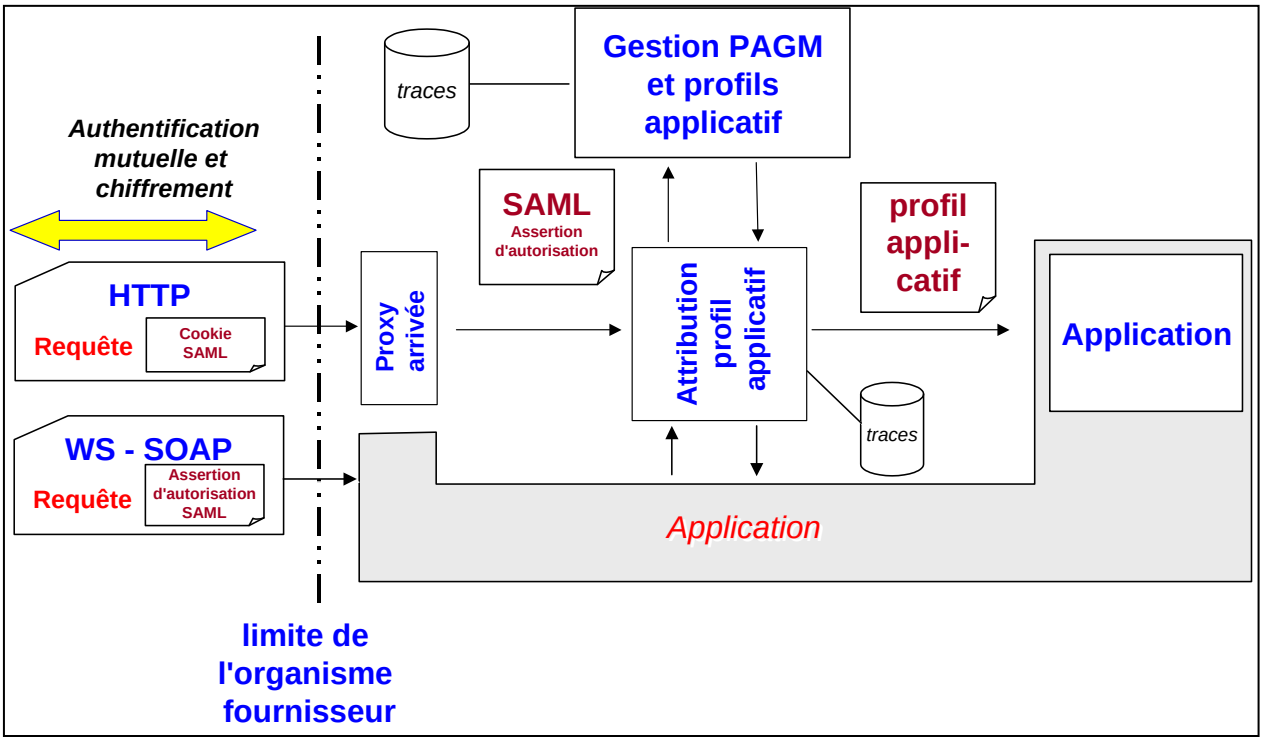
9.2.2 Glossaire

Le glossaire est contenu dans le document intitulé ***Glossaire du standard « interops »*** sous la référence ***[R1]***

9.3 Exemple d'une décomposition des blocs fonctionnels



Représentation d'un exemple au niveau d'un organisme client



Représentation d'un exemple au niveau d'un organisme fournisseur