Direction de la Sécurité Sociale

Spécifications fonctionnelles

Standard d'interopérabilité entre organismes de la sphère sociale

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

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

Table des mises à jour du document

N° de version	Date	Auteur	Objet de la mise à jour
1.0	07/10/08	Groupe de travail Interops	Version officielle

SOMMAIRE

1. INTRODUCTION

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

Outre la présente introduction :

- 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 :

[organisme client] représente l'organisme de départ dont fait partie l'agent 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 agents appartenant à des organismes clients.

2. CADRE DE DEVELOPPEMENT DU STANDARD

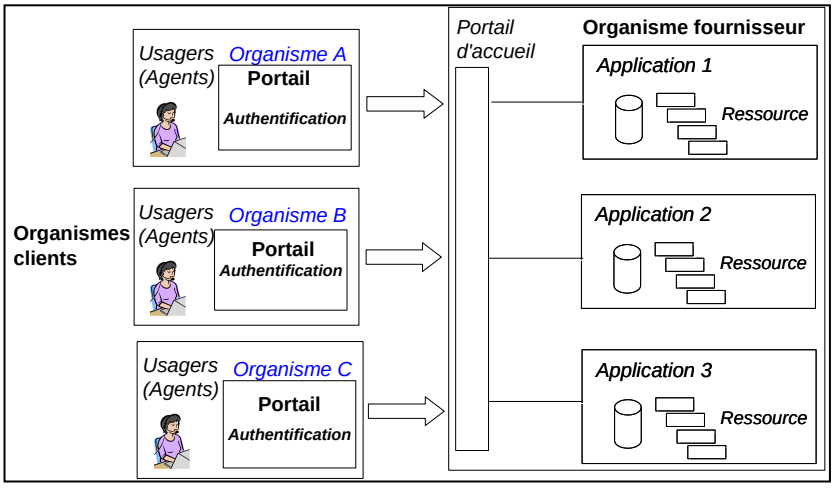
2.1 Objet de la réflexion

2.1.1 Présentation

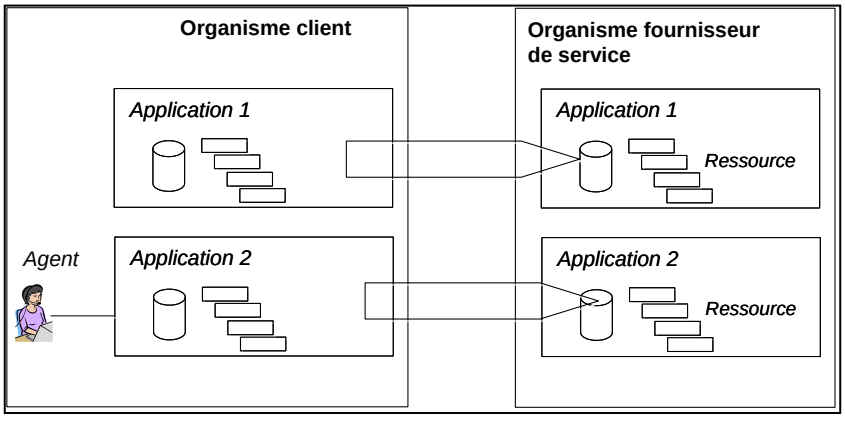
Le standard d'interopérabilité doit permettre l'interconnexion des SI des organismes de la sphère sociale, au travers des 2 modèles d'échanges :

- "portail à portail" : accès d'un agent 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 agent, soit dans un contexte où un agent 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 agents 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.

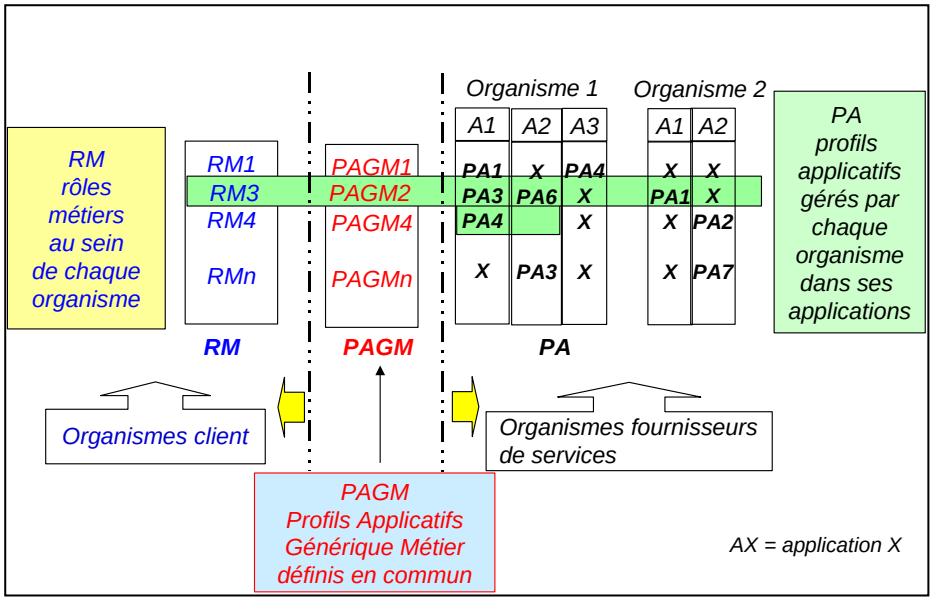
Chaque organisme client met en place une infrastructure qui associe à chaque entité (agent ou application cliente) un ou plusieurs **PAGM** vis à vis d'applications gérées par des organismes fournisseurs de services.

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 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.

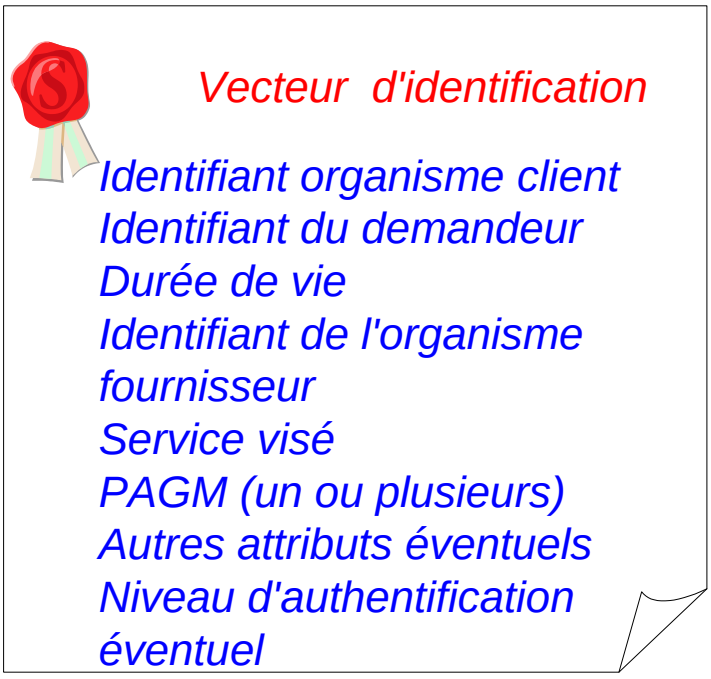
Nota : un **Vecteur d'identification** peut comprendre un ou plusieurs PAGM d'une même application ou famille d'applications (en fonction de l'organisation de l'organisme fournisseur de service).

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 du demandeur 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.*



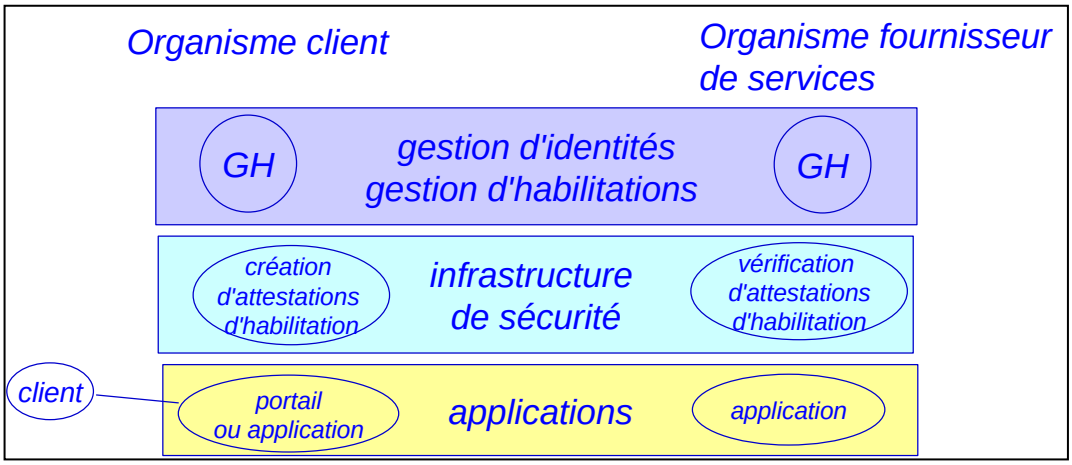
Le contenu du vecteur d'identification

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 agents,
  - gérer les droits des agents 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 agent vers une application,
- un niveau "applicatif", comprenant :
  - des portails (modèle "portail à portail"),
  - ou des applications (modèle "application à application").



Architecture à trois niveaux

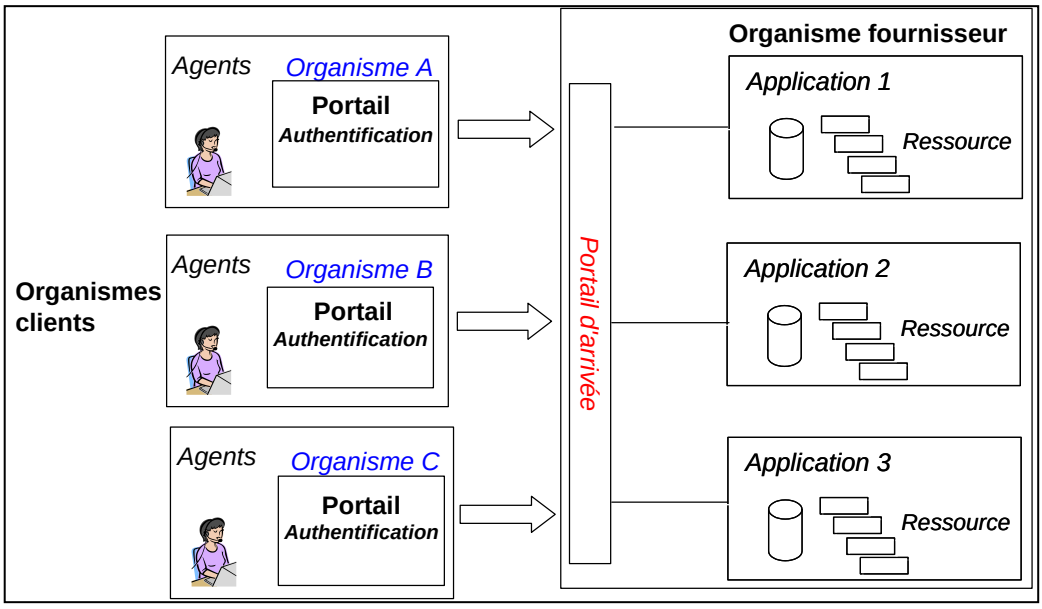
On notera la recommandation d'une séparation entre les 3 niveaux définis ci-dessus.

6.2 Le cadre "Portail à Portail"

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

6.2.1 Définition

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



Rappel du modèle des échanges portail à portail

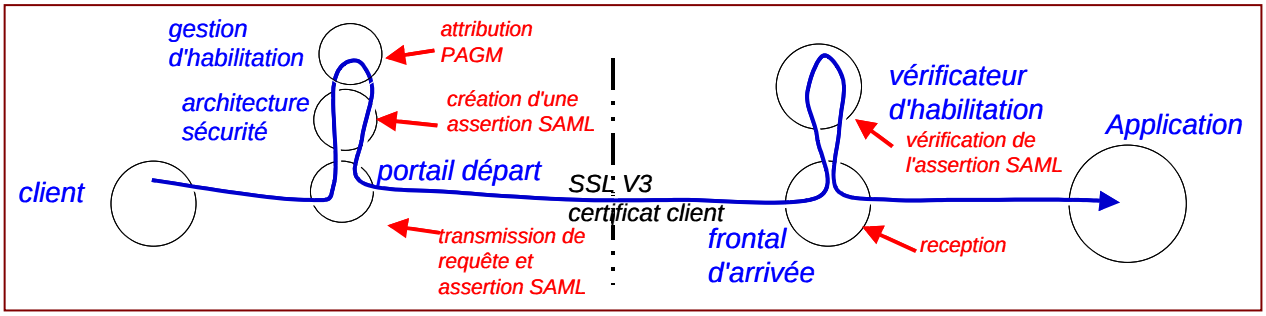
6.2.2 Principe de transmission d'habilitations

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'agent de l'organisme client.



Cinématique des échanges "portail à portail"

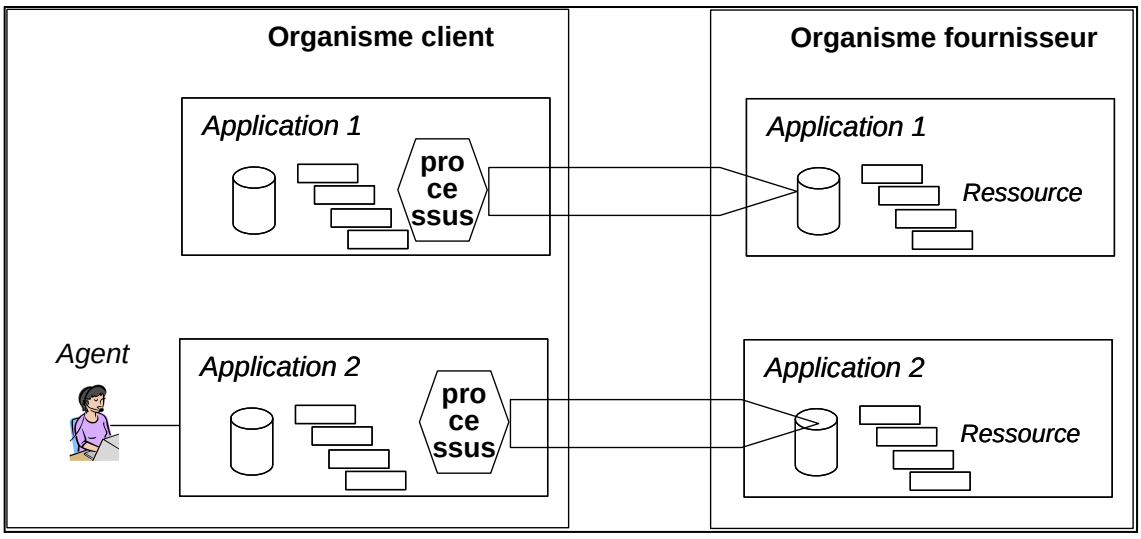
6.3 Le cadre "Application à Application"

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 agent de l'organisme client à des données d'une application de l'organisme fournisseur au travers d'une application locale.

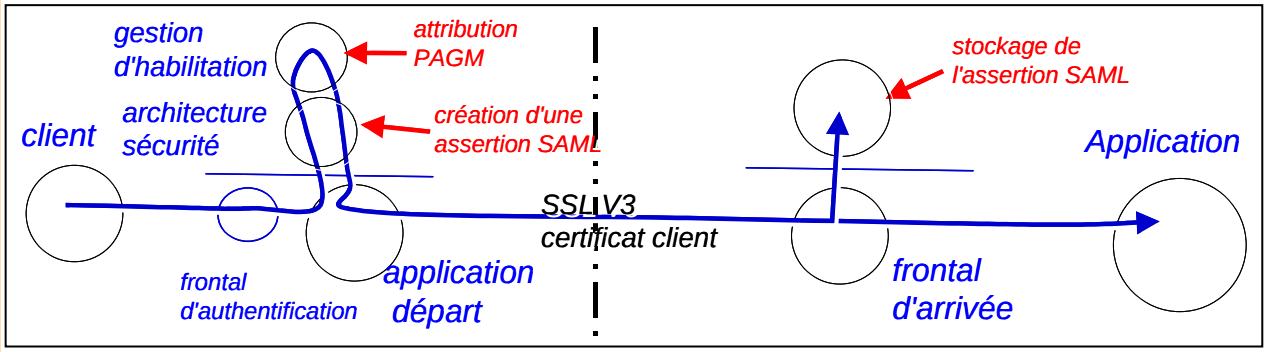


Rappel du modèle des échanges "application à application"

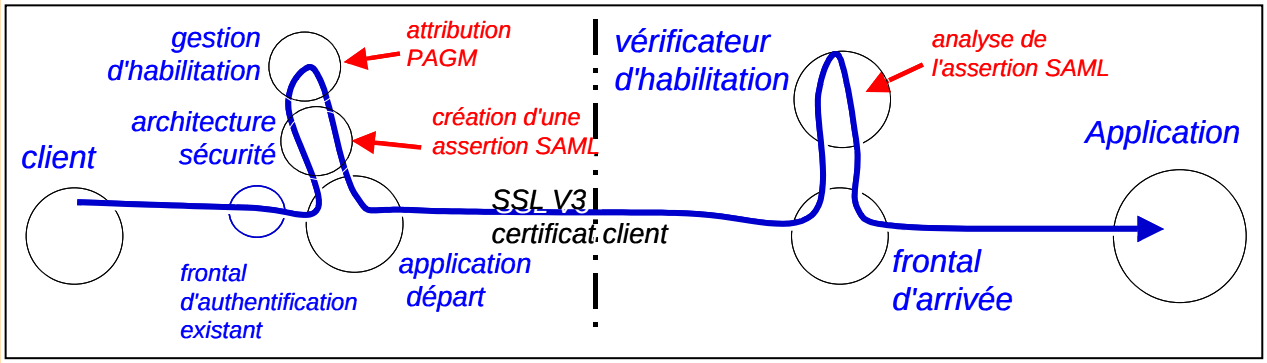
6.3.2 Cinématique de transmission d'habilitations

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

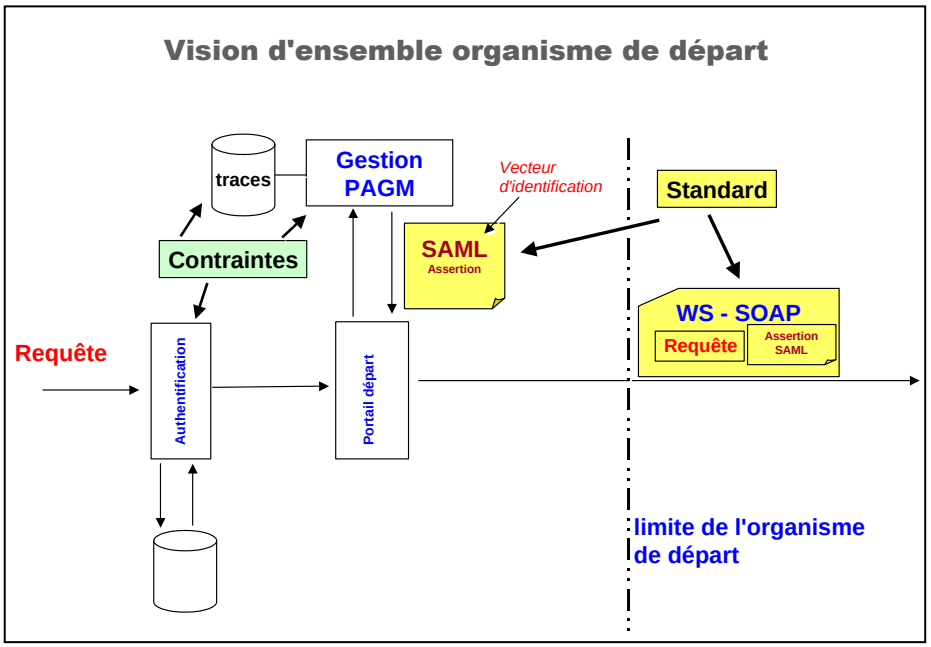
Il s'agit, pour les organismes clients, des blocs fonctionnels suivants :

- 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 agents 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 "1 étoile" PRIS V2[2] (correspondant en l'état de la PRIS au 21/04/2005 à un bi-clé/certificat logiciel remis sans face à face),
- authentification par bi-clé/certificat "2 étoiles" PRIS V2 (correspond en l'état de la PRIS au 21/04/2005 à un bi-clé/certificat sur support matériel individuel dont l'enregistrement / remise comprend un face à face),
- authentification par bi-clé/certificat "3 étoiles" PRIS V2 (correspond en l'état de la PRIS au 21/04/2005 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).

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

---

2 *Selon les références disponibles au 26/04/2005 PRIS version 2.05 en date du 04/10/2004 publiée sur le site de l'ADAE pour appel à commentaires.*

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).*

- 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

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 finale
- 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 (format Word) annexée à la convention juridique et une convention technique au format XML.

Le document (Word) de convention technique permet de rappeler de manière exhaustive et documenté 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 : Interops1.0_ConventionTechnique_v1.2.

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 listes de certificats révoqués
- Certificat SSL client , chaîne de certification et listes de certificats révoqués
- Certificat SSL fournisseur, chaîne de certification et 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. Le document (Word) de conventions 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 utilise le protocole HTTPS avec TLS.

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

Le protocole TLS (SSL) est utilisé entre les deux portails et/ou applications des organismes client et fournisseur[4].

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).*

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

Ce glossaire est **un extrait du glossaire utilisé par l'ADAE** dans le cadre du projet ADELE 121 qui peut être utile à la compréhension du standard.

Terme	Définition
A – B	
Agent	Personne physique agissant au sein de la sphère publique de façon permanente ou temporaire et ayant l'un des statuts suivants : fonctionnaire, contractuel, partenaire institutionnel, prestataire, intérimaire ou stagiaire.
Annuaire	Service distribué permettant de localiser les ressources d'un système d'information/une personne et de leur affecter des propriétés/des droits (CTA). Interface donnant accès à des données de références. Ces données représentent des informations techniques ou structurelles auxquelles on accède plus fréquemment en lecture qu'en écriture (PYC).
Annuaire de sécurité ou annuaire d'identité	Annuaire du SI dédié au stockage des paramètres de sécurité des différents utilisateurs. Ces paramètres représentent pour ces derniers leurs éléments d'identification, d'authentification et de gestion de droits.
Approche métier	La gestion des habilitations peut s'appuyer sur un modèle dit « d'approche métiers » qui consiste en une approche collective issue de l'analyse des métiers exercés. Les droits d'une personne sont ceux du métier qu'elle exerce et sont identiques à ceux des personnes ayant le même métier.
Architecture logique	Description du système sous forme : ❑ d'une organisation structurée et hiérarchique des fonctions internes du système (fonctions, sous fonctions, composants logiques) et du couplage entre ces fonctions et l'environnement (vue statique) ❑ des flux de données et de contrôle entre ces entités logiques définissant le séquencement de leur exécution (vue dynamique). Cette description réalise les exigences fonctionnelles et les exigences de performances.
Architecture physique	Description d'un système, sous forme d'un ensemble d'organes matériels et de leurs interactions, constituant la solution traduisant l'architecture fonctionnelle et satisfaisant les exigences [IEEE1220]
Attribut	Qualificateur d'un individu, d'un rôle ou d'un objet (par exemple : adresse, âge, profession, fonction d'une organisation, etc.).
Autorisation	Mécanisme qui, à partir du vecteur d'autorisation, accorde ou non, à un utilisateur, l'accès à des applications, fonctions ou données spécifiques, en s'intéressant à des couples « objet, actions, conditions »

Terme	Définition
Authentification	Terme informatique pour l'opération d'identification réalisée par un processus informatique. Les principaux moyens d'authentification sont : ❑ mot de passe ❑ clé symétrique ❑ certificat ❑ biométrie
C-D	
Certificat	Fonctionnellement, un certificat se définit comme un objet informatique logique lié à une entité. Fonctionnellement, il s'agit d'une clé publique signée par une Autorité de Certification. L'ensemble bi-clé/certificat permet d'utiliser des fonctions cryptographique (cryptographie assymétique) permettant des opérations d'authentification et de signature numérique. ,
Client réseau banalisé	Application logicielle de consultation et de traitement du contenu des pages Web accessibles à l'utilisateur. Par exemple : un navigateur Web tel que Netscape ou Internet Explorer ou une interface WAP.
Composant	Module logiciel ou matériel participant à la cohérence d'un dispositif plus vaste (services socle, services applicatifs, services réseaux, par exemple) Par exemple : ❑ un serveur web, un serveur d'application, un annuaire LDAP, une base de données sont des composants techniques logiciels ❑ un poste de travail, une machine serveur, un PC sont des composants techniques matériels certains composants tels qu'un pare-feu, un routeur, un Proxy, un antivirus ou un antispam peuvent être des composants logiciels ou matériels.
Contrôle d'accès	Principe ou dispositif de sécurité vérifiant l'identité et les droits associés à une entité en termes d'usage des services du système d'information.
Cookie	Petit fichier implanté sur le poste client et utilisé comme marqueur pour suivre le cheminement d'un utilisateur sur un site Web. Lorsque l'internaute retournera visiter ce même site, le serveur pourra alors récupérer les informations contenues dans ce fichier. Les cookies sont surtout utilisés à des fins statistiques et pour conserver le profil d'un internaute.
Droit	Un droit correspond à l'habilitation d'un métier dans une application et se compose d'un ou plusieurs groupes d'actions unitaires.
E – F	
Entité	Elément accédant aux ressources d'une application : exemple : personne ou application

Terme	Définition
Espace de confiance	Ensemble de composants fonctionnels et techniques permettant de fournir à une personne les outils et les ressources nécessaires pour effectuer des opérations et des transactions électroniques. Un espace est dit de confiance quand il répond à des critères de sécurité considérés comme suffisants par la Maîtrise d'Ouvrage concernée.
Espace de travail	Ensemble d'interfaces, d'outils et de données permettant à l'utilisateur de réaliser des opérations et des transactions sur des applications mis à disposition au travers un portail. Dans le cadre de services Web, cet espace pourra être, par exemple, représenté par une ou plusieurs fenêtres de navigateur web dans le cas de client réseau banalisés de type PC ou Mac.
Fédération d'identités	Principe de partage d'informations relatives à un utilisateur entre plusieurs applications ou plusieurs domaines de confiance. La relation établie entre chaque service ou entité peut permettre de reconnaître l'identité d'un individu ou, au contraire, de garantir son anonymat.
Fonction	Action attendue d'un composant technique (ou réalisée par lui) pour répondre à tout ou partie d'un besoin d'un utilisateur ou d'un service du système d'information. Par exemple, l'authentification, l'identification et l'autorisation sont des fonctions s'appuyant sur des composants logiciels tels que un annuaire LDAP et un serveur web.
Fournisseur d'identité	Composante de l'espace de confiance chargée de créer, maintenir et gérer des informations relatives à l'identité d'un utilisateur ou d'une entité au sens large. Le fournisseur d'identité est également en charge de la fonction d'authentification des utilisateurs et, si nécessaire, de l'enrichissement du vecteur d'identification (par exemple : ajout d'attribut caractérisation sa localisation ou son statut).
Fournisseur de service	Composante de l'espace de confiance mettant à disposition des utilisateurs et des organisations autorisées des services applicatifs et des ressources. Elle est également chargée de gérer l'autorisation d'accès aux ressources et aux applications. Le fournisseur de service peut s'appuyer sur le fournisseur d'identité pour les fonctions d'identification et d'authentification.
G – O	
Habilitation	Les habilitations permettent à un utilisateur d'accéder à un ensemble de procédures informatiques.
Identifiant	Information permettant d'identifier une entité (exemple : une personne ou une application) (par exemple : NIR, NUMEN, n° matricule, RNE, n° de passeport, etc.).
Identifiant unique	Identifiant destiné à être utilisé par un ensemble d'applications indépendamment de leur hétérogénéité.
Identification	L'identification consiste à associer un identifiant à une entité.

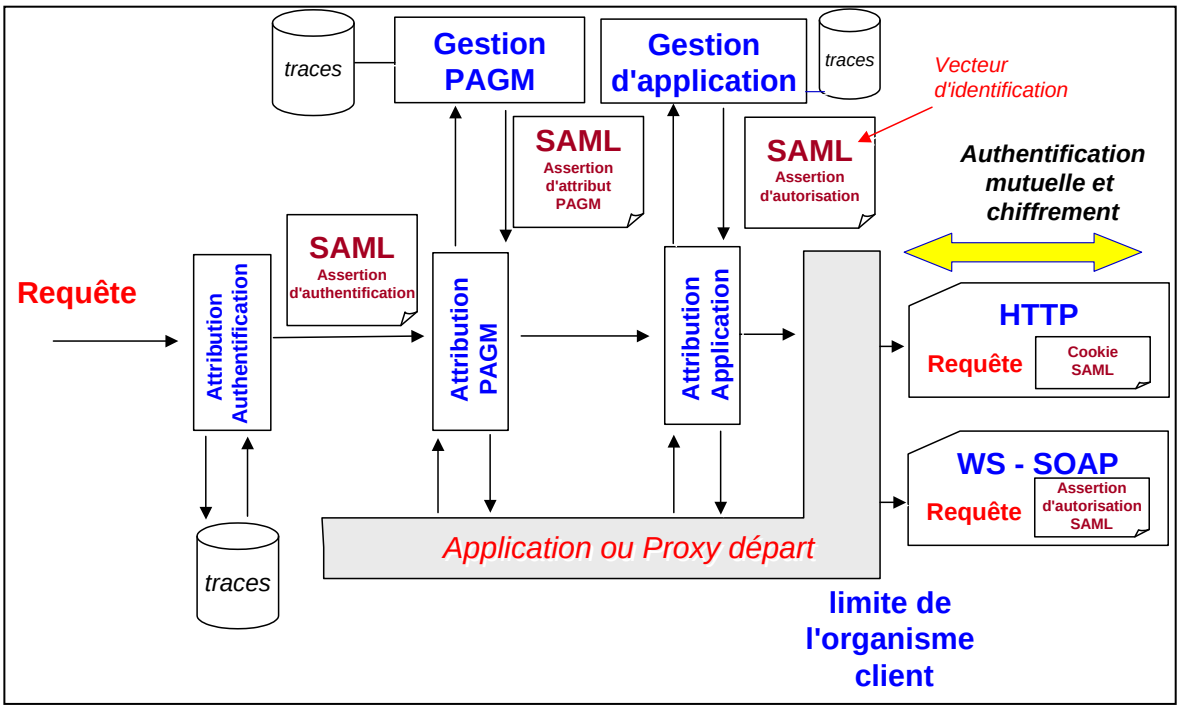
Terme	Définition
Infrastructure de gestion de clés (aussi appelée Infrastructure à clés publiques)	Ensemble de personnel, politique, procédures, composants et facilités qui lient l'identité de l'individu à deux clés cryptographiques asymétriques. Architecture et organisation permettant de demander, générer puis remettre des bi-clés/certificats.
Interopérabilité	Faculté que possèdent des services ou des composants hétérogènes de fonctionner conjointement. L'une des conditions fondamentales permettant la communication entre ces services et ces composants est l'utilisation de langages et de protocoles communs. Par exemple, les protocoles SOAP ou XML sont normalisés et permettent aux différents services web d'échanger des informations selon les mêmes règles et les mêmes méthodes.
Load balancing (répartition de charge)	Technique consistant à distribuer le travail à effectuer sur plusieurs machines, en particulier sur plusieurs serveurs. Cela permet de faire face plus efficacement aux grosses variations d'activité.
Métier	Ensemble d'opérations à réaliser répondant à un noyau commun pour une activité donnée au sein de l'organisme. Le métier se situe à un niveau plus élevé que les droits au sein des applications informatiques. Il couvre l'ensemble des droits accès de toutes les applications.
Objet métier	Unité structurée et limitée conçue pour représenter les processus et les connaissances d'un métier en particulier (souvent dans une application).
Organisme	Entité organisationnelle pouvant correspondre à une mairie, une entreprise, un ministère, etc.
P – R	
Personnalisée (diffusion)	Les éléments de personnalisation tels que l'accès aux services et la présentation de l'espace de travail sont définis par des règles s'appuyant sur les informations des utilisateurs (son profil notamment). Ces éléments ne sont pas modifiables par l'utilisateur.
Personnalisable (diffusion)	L'utilisateur peut modeler (par l'intermédiaire du service de personnalisation) le contenu et sa présentation en choisissant explicitement parmi une sélection d'option ses services et ses préférences.
Profil	On ne retiendra pas cette notion qui : ❑ Recopie le rôle ou l'ensemble (rôle + attributs) ❑ Peut définir un profil applicatif ❑ Pourrait correspondre au terme anglais « role »
Profil applicatif (PA)	Identifiant permettant d'attribuer des droits dans le cadre de l'accès aux ressources d'une application
PAGM Profil Applicatif générique métier	Profil défini en commun par les fournisseurs d'applications qui caractérise de manière générique un groupe de permissions représentant des actions sur une ressource applicative.Un PAGP pourra être mis en relation d'un ou plusieurs profils applicatifs d'une application.
Prestataire de service de certification	*Acteur offrant des services de certification.*
Propagation des identités et des droits	Transfert, échange des informations relatives au profil entre applications, services et autres entités (utilisation de carte de vie quotidienne, inter-administration, identités accord-Education, liaison

Terme	Définition
	sco-sup ...).
Proxy	Dispositif informatique associé à un serveur et réalisant, pour des applications autorisées, des fonctions de médiation, telle que le stockage des documents les plus fréquemment demandés ou l'établissement de passerelles. Il a généralement un rôle de sécurité et de filtrage, et d'antémémoire / mémoire cache (optimise les performances d'accès à des pages Internet fréquemment consultées).
Référentiel	Ensemble structuré d'informations, utilisé pour l'exécution d'un logiciel, et constituant un cadre commun à plusieurs applications. On associe généralement le référentiel à l'annuaire LDAP de référence pour les fonctions de contrôle d'accès.
Ressource	Données ou fonction gérée par une application auquel on accède, - équivalent "d'objet" dans certains modèles.
Rôle métier (RM)	*Fonction associée à une entité. Une entité peut avoir plusieurs rôles métiers (exemples : directeur, maire professeur, parent, citoyen, etc.).*
S	
Sauvegarde	Copie de sécurité destinée à protéger de tout incident un ensemble de données mises en mémoire, ou sur support numérique. "Faire une sauvegarde". [*Petit Robert*]
Service	Regroupement cohérent de fonctions visant à répondre à un élément du besoin d'un utilisateur ou d'entités fonctionnelles du système. [DCSSI]
Services AAS	Les services AAS (Authentification-Autorisation-SSO) assurent les fonctions suivantes : ❑ Contrôle d'accès (identification, authentification, autorisation) ❑ Gestion d'identité et des habilitations (gestion des rôles et des profils, gestion de la politique d'habilitation) ❑ Propagation des identités et des droits à l'intérieur d'un espace de confiance et/ou entre plusieurs espaces.
Services applicatifs	*(encore appelés « briques » ou « briques applicatives »)* Ensemble des services numériques spécifiques à une activité ou un secteur. En l'occurrence, ces services sont mis à disposition de la communauté éducative. Conformément au SDET, les principaux services applicatifs sont : ❑ Services pédagogiques (construction des ressources pédagogiques, cahier de texte) ❑ Services de vie d'établissement (aide à la publication Web, publication de brèves, …) ❑ Services scolaires (gestion des absences, gestion des notes, emploi du temps, tableau d'affichage) ❑ Services documentaires (ressources personnelles de l'élève ou de l'enseignant, ressources du CDI, …) ❑ Services de communication (services avancés de messagerie, chat, Forum de discussion, liste de distribution, …) ❑ Bureau numérique (carnet d'adresses, espace de stockage, outils bureautiques, …) Ces services font appel aux services socle.
Service applicatif distant	Un service distant est un service qui ne peut pas être intégré au portail via des connecteurs applicatifs. Il doit donc communiquer avec le portail via HTTP et des protocoles de type Web Services (SOAP

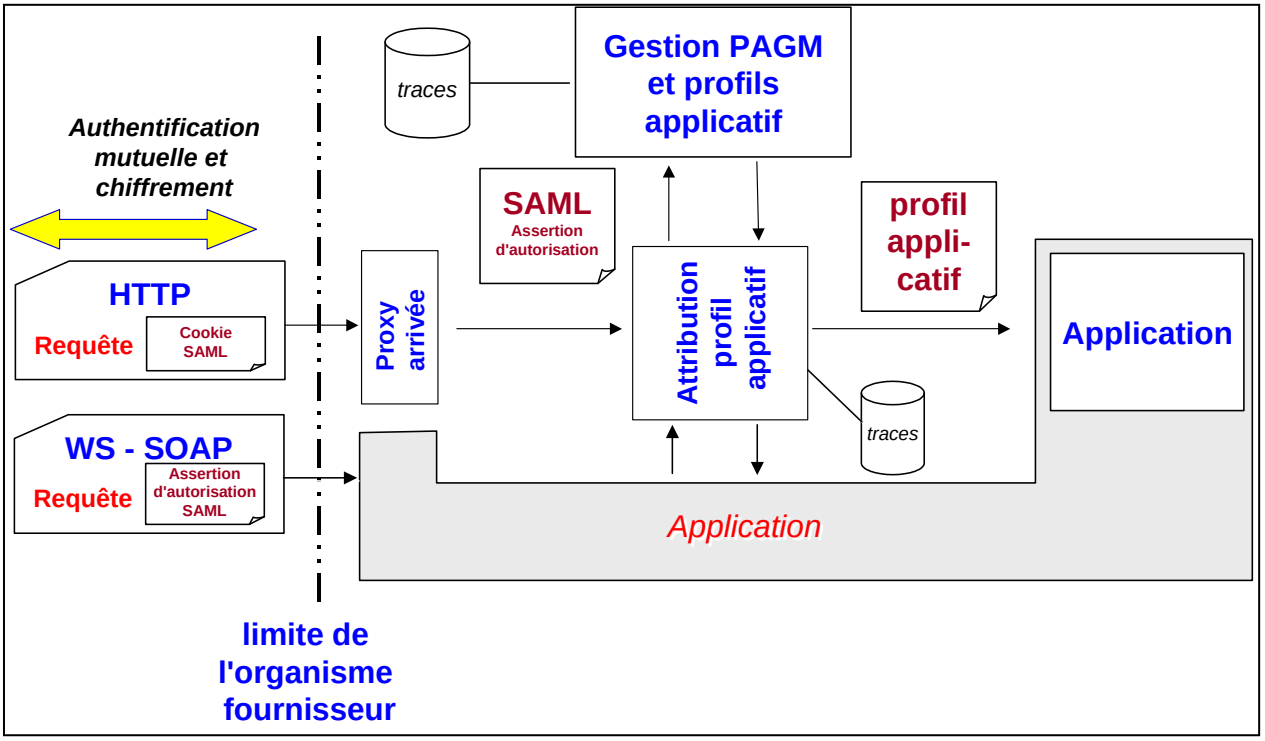
Terme	Définition
	notamment).
Service applicatif intégré	Le service installé sur le portail lui-même ou sur une extension de celui-ci.
Services d'administration	Les services d'administration représentent : ❑ Outils d'exploitation ❑ Gestion de la configuration ❑ Gestion des alertes et des incidents ❑ Outils de suivi et de pilotage ❑ Statistiques de flux
Services d'aide en ligne	Les services d'aide en ligne pour les services socle, utilisables par les applications permettent d'assurer les fonctions suivantes : ❑ Publication de guides de formation ❑ Mise en place et maintien d'un FAQ ❑ Forum de discussion ❑ Help desk en ligne ❑ Interface de communication entre les applications et l'aide en ligne
Services d'annuaire	Les services d'annuaire assurent notamment les fonctions suivantes : ❑ Alimentation de l'annuaire (ou Provisionning) ❑ Synchronisation des données assurée par des connecteurs ❑ Mise à jour des informations (réplication synchrone/asynchrone, partielle/complète)
Services d'échanges	Les services d'échanges entre le socle et les services applicatifs désignent : ❑ Interfaces applicatives (« web services ») ❑ Fonctions d'interopérabilité (protocoles associés) ❑ Annuaire d'objets techniques (UDDI) Ces services sont placés dans le socle.
Service de gestion des identités et des accès	Les services de gestion des identités et des accès désignent : ❑ Les services d'annuaire qui contiennent les informations des acteurs (identités et habilitations) ❑ Les services AAS
Service de gestion des transactions	Gère les échanges entre les services applicatifs et le client réseau.
Service en ligne	Service mis à disposition des usagers sous un format électronique et accessible depuis un client réseau.
Service multi-canal	En relation avec le service de présentation, ce service permet de diffuser les informations au format requis par le client réseau (navigateur web, PDA, téléphonique mobile).
Services réseaux	Il s'agit des composants sur lesquels s'appuient les composants de l'espace de confiance pour communiquer entre eux et avec l'environnement extérieur : ❑ Protocoles (HTTP, WAP, …) ❑ Supports de communication (Lignes spécialisées, RTC, …)

Terme	Définition
	Les services réseaux assurent également les premières fonctions de contrôle d'accès (pare-feu, proxy) et de contrôle de contenu (anti-spam, antivirus).
Single Sign-On (ou authentification unique)	Concept consistant à permettre à un utilisateur d'accéder à des services numériques différents en ne devant s'authentifier qu'une seule et unique fois. On parle par exemple de propagation de l'identité entre le portail et une application qui permet de ne pas redemander l'identifiant et le mot de passe. (cf. propagation des identités et des droits).
Socle technique	Terme utilisé pour définir les éléments techniques du socle de services minimum. Typiquement, les serveurs, les logiciels sont des éléments techniques.
Stockage	Action d'enregistrer sur un support numérique en vue d'une utilisation ultérieure. [*Petit Robert*]
Système d'information	Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.
Usager	Personne physique ou morale, y compris de droit public, dans ses relations avec une administration
Vecteur d'autorisation	Définit les habilitations (ou les droits) d'un utilisateur sur une ressource ou définit les actions possibles sur un objet et, si nécessaire, les conditions à remplir ou les permissions nécessaires pour lancer l'action sur l'objet concerné. Le vecteur d'autorisation pourrait être représenté de la façon suivante : Compte fiscal, consultation, déclaration TVA, mise à jour, …
Vecteur d'identification	Ensemble d'éléments caractéristiques d'une entité. Est composé de l'identifiant et l'authentifiant de l'utilisateur ainsi que d'attributs le caractérisant
W	
Web services (SOAP, XML)	Les services web sont des services applicatifs, accessibles via des protocoles standardisés du web par des entités distantes (applications ou utilisateurs).

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

603