

Direction de la Sécurité Sociale

Standard d'interopérabilité inter-organismes

Version 1.0
en date du 13 juillet 2005

Auteurs du document :

Olivier Chapron – olivier.chapron@edelweb.fr

Peter Sylvester – peter.sylvester@edelweb.fr

Tél : 01 40 99 14 14

TABLE DES MATIERES

1	INTRODUCTION	4
2	CADRE DE DEVELOPPEMENT DU STANDARD	5
2.1	OBJET DE LA REFLEXION	5
2.1.1	<i>Présentation</i>	5
2.1.2	<i>Les deux modèles traités</i>	5
2.2	PORTEE DU STANDARD ET PRINCIPES RETENUS PAR LES ORGANISMES	6
3	CONVENTION PREALABLE	7
3.1	OBJET DE LA CONVENTION	7
3.2	EXEMPLE DE CONVENTION.....	7
4	GESTION D'HABILITATION ET PAGM	9
4.1	PRINCIPES.....	9
4.2	LES PAGM : LE REGROUPEMENT DE PROFILS	9
4.3	CONSTRUCTION DES PAGM.....	10
5	AUTHENTIFICATION ET TRANSFERT D'HABILITATION	11
5.1	PRINCIPES.....	11
5.2	LE VECTEUR D'IDENTIFICATION.....	11
6	LES SOLUTIONS D'UTILISATION D'HABILITATIONS DANS LES ARCHITECTURES APPLICATIVES 13	
6.1	POSITIONNEMENT DE LA PROBLEMATIQUE	13
6.2	LE CADRE "PORTAIL A PORTAIL".....	14
6.2.1	<i>Définition</i>	14
6.2.2	<i>Principe de transmission d'habilitations</i>	14
6.2.3	<i>Cinématique des échanges</i>	15
6.3	LE CADRE "APPLICATION A APPLICATION"	16
6.3.1	<i>Définition</i>	16
6.3.2	<i>Cinématique de transmission d'habilitations</i>	16
7	ELEMENTS FONCTIONNELS ET CONTRAINTES	18
7.1	BLOCS FONCTIONNELS	18
7.2	CONTRAINTES.....	19
7.2.1	<i>Niveau d'authentification</i> :	19
7.2.2	<i>Gestion des PAGM</i>	20
7.2.3	<i>Traces</i>	20
8	ELEMENTS TECHNIQUES	21
8.1	ELEMENTS TRANSMIS EN PREALABLE AUX ECHANGES	21
8.1.1	<i>Constitution du CPP client</i>	22
8.1.2	<i>Constitution du CPP fournisseur</i>	28
8.1.3	<i>Synthèse des deux CPP : le CPA</i>	30
8.1.4	<i>Sécurisation et Echanges des CPP et CPA</i>	32
8.2	FORMAT DU VECTEUR D'IDENTIFICATION	33
8.2.1	<i>Présentation</i>	33
8.2.2	<i>Eléments détaillés</i>	34
8.2.3	<i>Exemple d'assertion SAML pour un échange organisme à organisme</i>	35

8.3	TRANSFERT DE LA REQUETE	37
8.3.1	Transmission d'une requête HTTP	37
8.3.2	Transmission d'une requête SOAP	37
8.4	SECURISATION DU TRANSFERT	38
8.4.1	Protection des canaux et authentification mutuelle	38
8.4.2	Protection des objets SOAP	38
9	ANNEXES.....	39
9.1	LIENS UTILES	39
9.2	ACRONYMES ET GLOSSAIRE	41
9.2.1	Acronymes	41
9.2.2	Glossaire	42
9.3	EXEMPLE D'UNE DECOMPOSITION DES BLOCS FONCTIONNELS	50
9.4	EXEMPLE OASIS-EBXML/CPP POUR WSDL	51

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 authentications 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 développement du standard

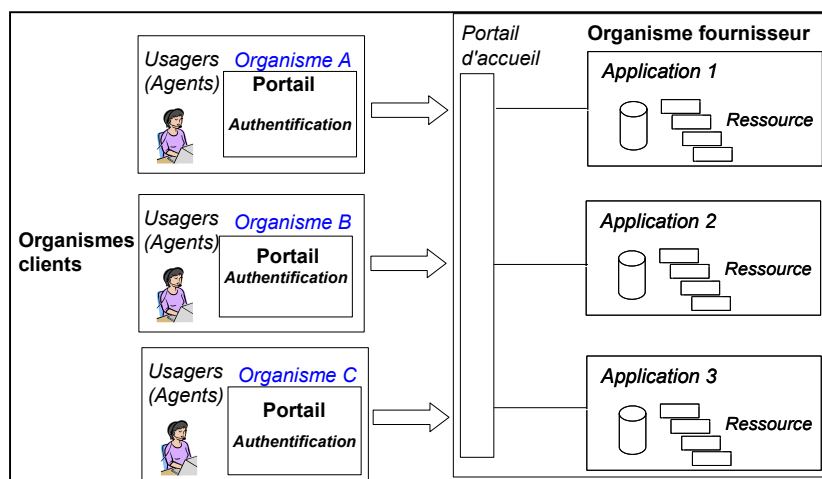
2.1 Objet de la réflexion

2.1.1 Présentation

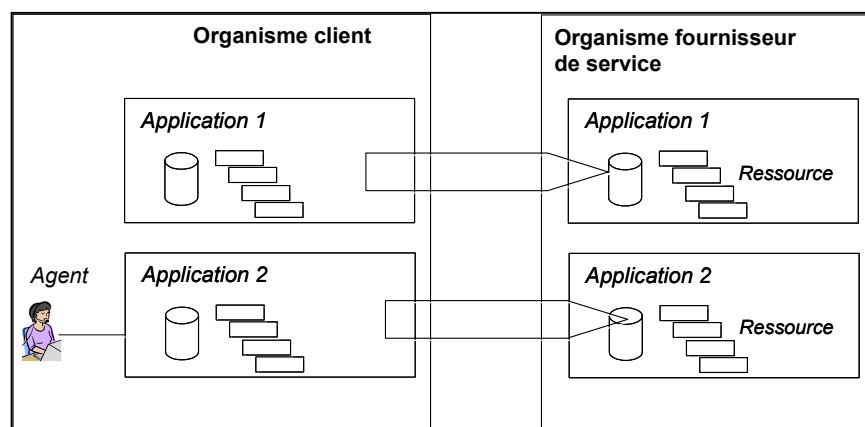
Le standard d'interopérabilité doit permettre l'interconnexion des SI des organismes de la sphère sociale, au travers des 2 modèles d'échanges :

- "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 préalable

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.

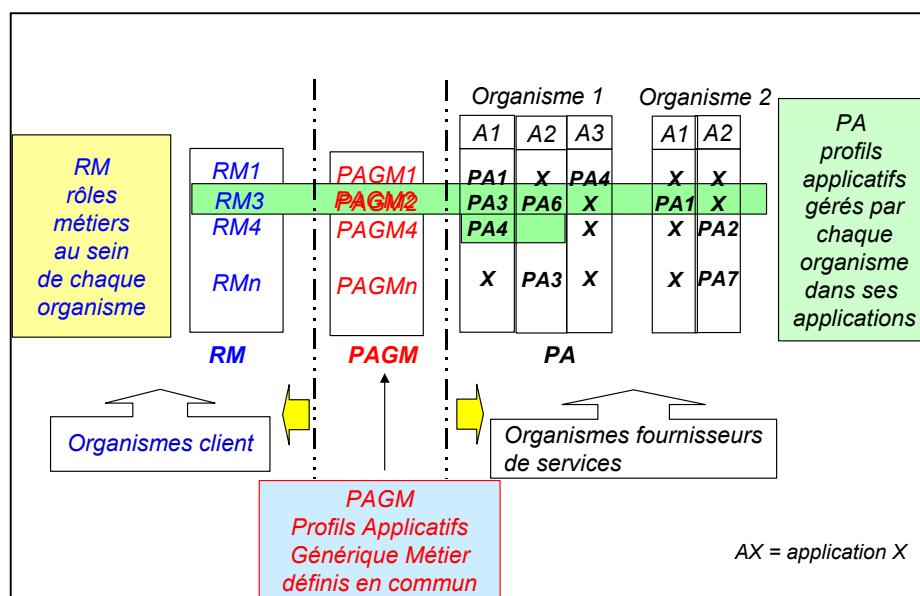
Chaque organisme client met en place une infrastructure qui associe à chaque entité (agent ou application cliente) un ou plusieurs **PAGM** vis à vis d'applications gérées par des organismes fournisseurs de services.

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).

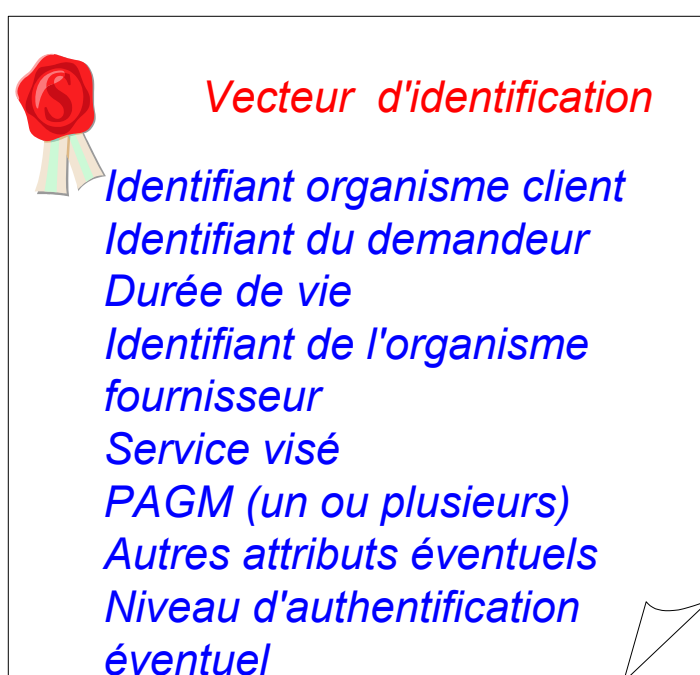
5.2 Le Vecteur d'identification¹

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) :

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.

- ◆ des indications géographiques,
 - ◆ des indications de localisation,
 - ◆ des niveaux de sécurité définis entre organismes,
- Un niveau d'authentification éventuels : implicite ou non, 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.



Le contenu du vecteur d'identification

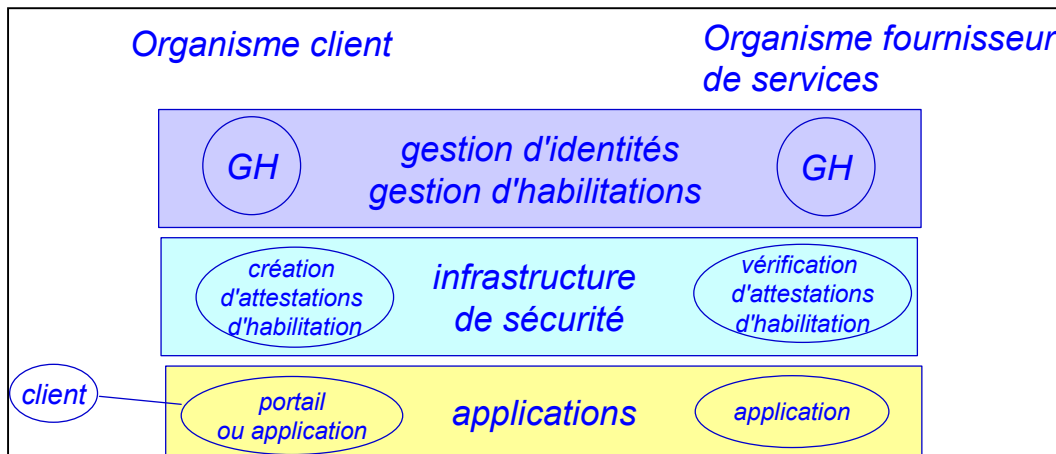
Les moyens de réaliser ce vecteur d'identification sont décrits dans les chapitres suivants.

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 authentications 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

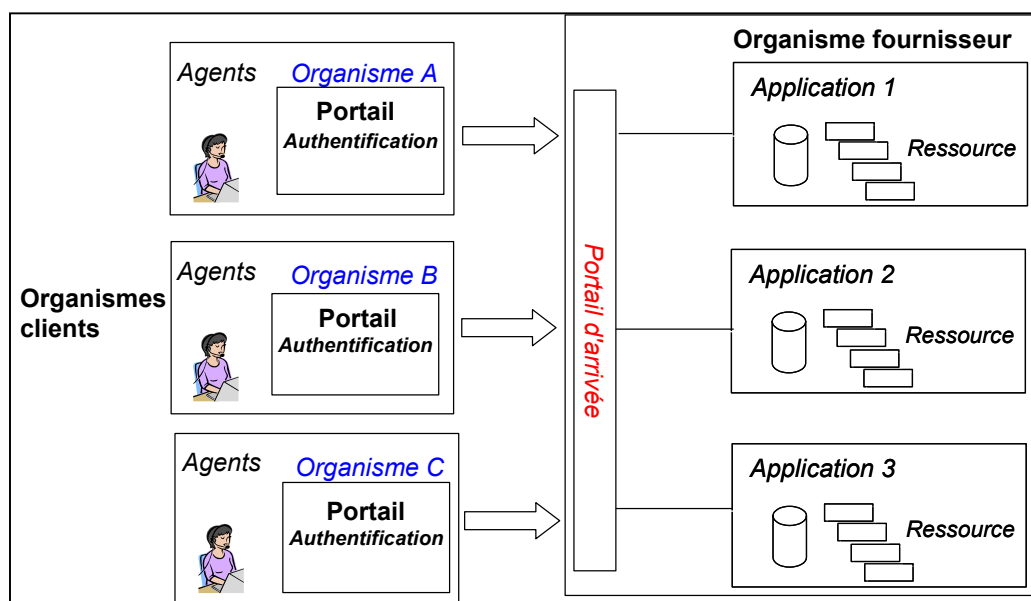
On notera la recommandation d'une séparation entre les 3 niveaux définis ci-dessus.

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

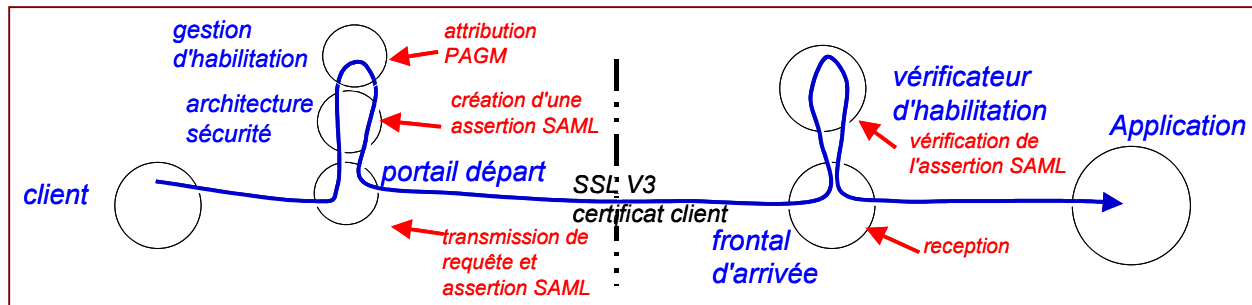
6.2.2 Principe de transmission d'habilitations

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"

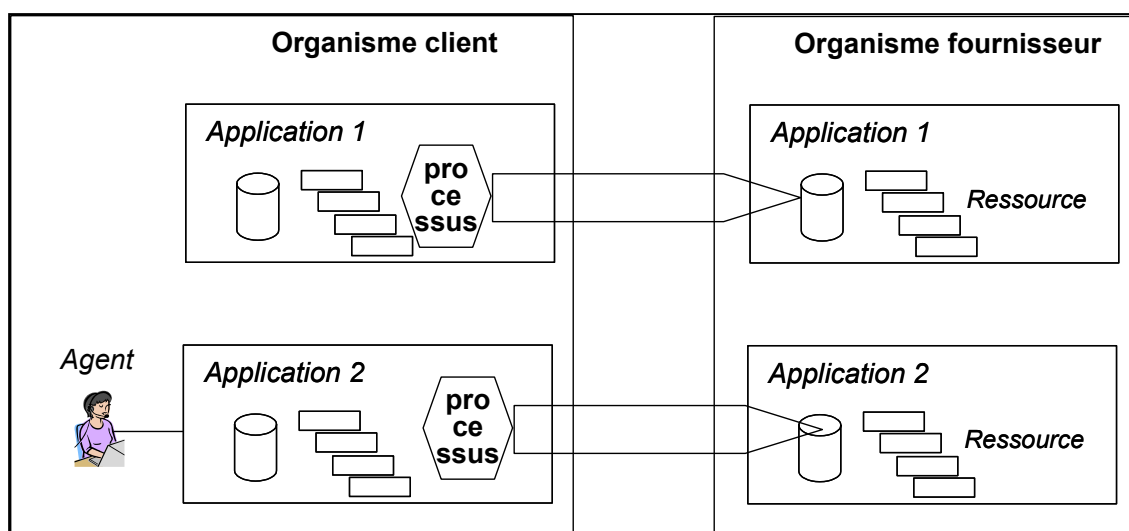
6.3 Le cadre "Application à Application"

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.

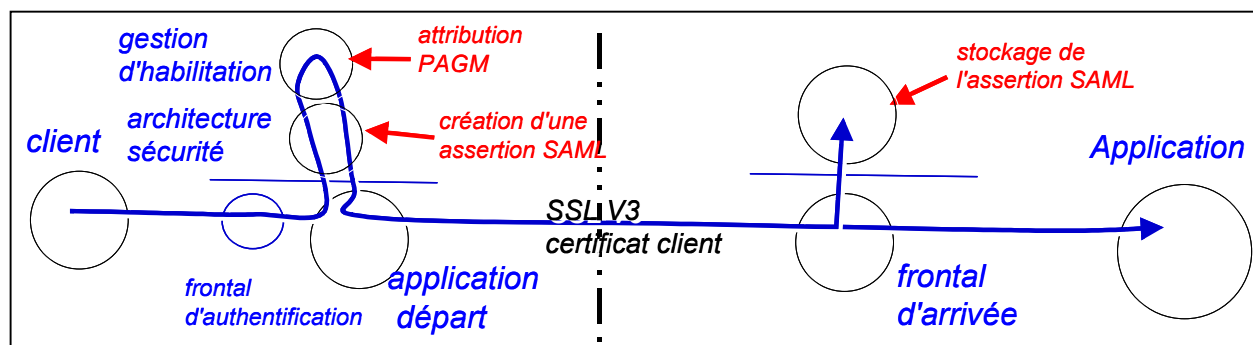


Rappel du modèle des échanges "application à application"

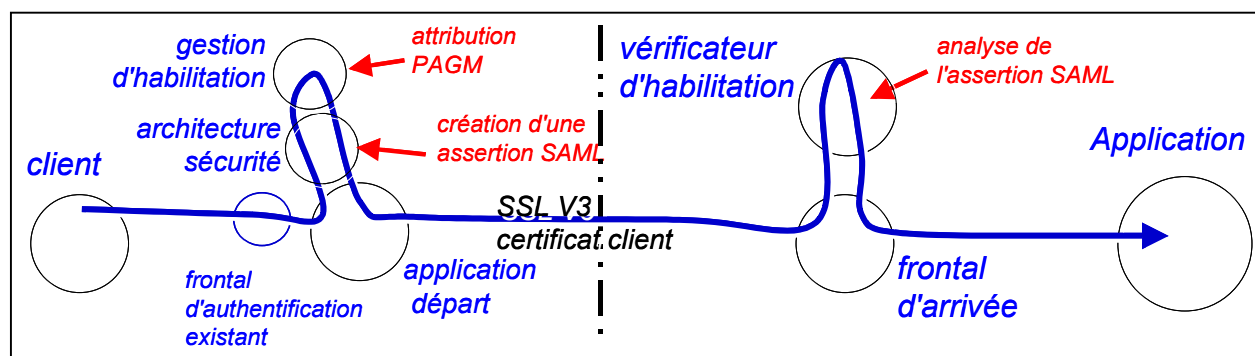
6.3.2 Cinématique de transmission d'habilitations

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 Éléments 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

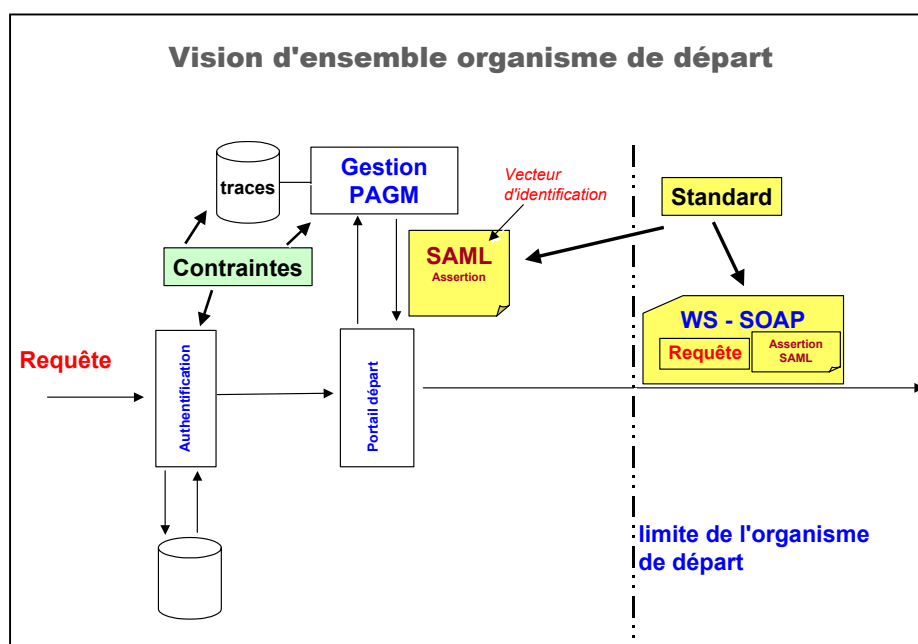
Il s'agit, pour les organismes clients, des blocs fonctionnels suivants :

- 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.



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). Il pourront être transmis de manière implicite.

Ces niveaux pourront être :

- ◆ authentification par login/mot de passe,
- ◆ authentification par bi-clé/certificat "1 étoile" PRIS V2² (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 face³),

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

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).

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


L'organisme client et l'organisme fournisseur sont responsables, chacun en ce qui le concerne, de l'archivage des traces pouvant être utilisées a posteriori en cas de besoins (litige ou contentieux, par exemple).

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

- ❑ 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. (Exemple de traces : l'image de la matrice utilisateurs/PAGM ou rôles/PAGM ou autre/PAGM),
- ❑ les éléments permettant de retrouver l'utilisateur final ayant formulé une requête à un instant donné (exemple de l'archivage sécurisé d'assertions SAML d'authentification utilisées en interne par l'organisme client),
- ❑ les éléments permettant de retrouver pour une requête donnée le couple requête/vecteur d'identification, sous la forme d'un archivage sécurisé de toutes les attestations SAML sortantes (solution simple : archivage complet des requêtes et réponses avec le vecteur d'identification).

L'organismes fournisseur doit être à même de fournir en cas de besoin, sous la forme qu'il choisit :

- ❑ les éléments permettant au fournisseur de démontrer à qui il a donné des informations confidentielles (exemple simple : archivage sécurisé de l'ensemble des requêtes et réponses)
- ❑ les éléments permettant de retrouver un profil applicatif correspondant à une requête (cela peut se faire par exemple par l'archivage d'une assertion d'autorisation SAML qui lie le PAGM à un profil applicatif pour une requête donnée).

	<p>Nota</p> <p><i>A titre d'exemple, une annexe présente une vue plus détaillée des blocs fonctionnels qui pourraient être mis en place côté client et côté fournisseur.</i></p>
---	---

8 Eléments 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 Eléments transmis en préalable aux échanges

Les détails techniques d'une collaboration entre organismes sont déterminés techniquement par trois documents spécifiés en format XML.

Le modèle utilisé pour cela est le standard OASIS ebXML et en particulier les définitions concernant :

- les profils de protocoles de collaboration (collaboration protocol profile CPP),
- la convention de protocoles de collaboration (collaboration profile agreement CPA).

La version 2.1 du standard OASIS ebXML/ CPP-2.1 utilisée pour cela est au 13/07/2005 en version draft (c'est à dire dans la dernière phase avant la validation formelle) dans le groupe de travail OASIS-ebXML.

L'organisme client prépare un document CPP qui comprend essentiellement :

- ses possibilités d'attribution de PAGM et attributs,
- les moyens d'authentification qu'il utilisera.

L'organisme fournisseur prépare un document CPP comprenant les services/applications qu'il propose, les PAGM associés qu'il permet à l'organisme client, et enfin les contraintes diverses comprenant en particulier le niveau d'authentification requis.

La concaténation des deux documents CPP (client et fournisseur) fait partie de l'annexe de la convention entre ces deux organismes. Ce document est en forme CPA au standard OASIS-ebXML/ CPP.

Nous utilisons dans la suite les spécifications du standard OASIS-ebXML/ CPP qui nous permet d'éviter la création d'un nouveau schéma XML. On notera que la gestion des PAGM et des attributs éventuellement associés seront traités par un point d'extension prévu dans le standard pour ajouter des informations.

Le standard OASIS-ebXML/ CPP décrit en détail (en 218 pages) comment remplir les documents CPP et procéder pour établir un document CPA.

Ayant noté que pour une communication Web (HTTP) la proposition OASIS-ebXML/ CPP intègre beaucoup trop d'éléments de services, le travail a consisté à en extraire les éléments suffisants aux besoins du standard d'interopérabilité.

Ce processus est décrit ci-après sous forme d'exemples qui illustrent l'application de OASIS-ebXML/ CPP au contexte d'interopérabilité inter-organismes. Les éléments de syntaxe sont présentés en commençant par les éléments unitaires les plus simples pour terminer par les descriptions complètes de CPP et CPA.

8.1.1 Constitution du CPP client

L'organisme client doit fournir à l'organisme fournisseur de service un ensemble d'informations concernant le système de départ. Ces informations sont organisées dans un document du type CPP (CollaborationProtocolProfile).

8.1.1.1 Authentification de l'organisme de départ

L'organisme client doit disposer de certificats pour permettre à l'organisme fournisseur de l'authentifier. Il s'agit au minimum de 2 certificats :

- ❑ l'un pour s'authentifier en tant que client dans la communication HTTPS entre le dernier serveur/application de l'organisme client et le premier serveur/application de l'organisme fournisseur,
- ❑ l'autre pour signer les assertions SAML d'autorisation (voir chapitre précédent).

L'élément utilisé est tp:Certificate de OASIS-ebXML/ CPP englobant ds:X509Data de XML-DSIG

Exemple:

```
<tp:Certificate certId="OrganismeA_Client_Cert">
  <ds:X509Data>
    Certificate en forme base 64
  </ds:X509Data>
</tp:Certificate>
<tp:Certificate certId="OrganismeA_SigningCert">
  <ds:X509Data>
    Certificate en forme base 64
  </ds:X509Data>
</tp:Certificate>
```

Au cas où il y a plusieurs portails de départ, ou plusieurs serveurs d'attestation, il convient de transmettre tous les certificats utiles.

En cas de renouvellement ou changement de certificat, une nouvelle communication doit être faite vis à vis de l'organisme fournisseur.

8.1.1.2 Définition des éléments de la partie cliente du canal de communication

L'élément Transport est utilisé pour définir des paramètres des connexion HTTPS entre les deux entités.

Il s'agit de décrire :

- l'identification locale de ce canal de transport,
- le protocole utilisé (http),
- les éléments de sécurité du canal (TLS 1.1),
- la référence au(x) certificat(s) utilisé(s) (ClientCertificateRef.)

Ces informations sont regroupées pour définir la partie cliente (TransPortSender) d'un canal de transport.

```
<tp:Transport transportId="transportA1">
  <tp:TransportSender>
    <tp:TransportProtocol version="1.1">HTTP</tp:TransportProtocol>
    <tp:TransportClientSecurity>
      <tp:TransportSecurityProtocol
        version="1.1">TLS</tp:TransportSecurityProtocol>
      <tp:ClientCertificateRef certId="OrganismeA ClientCert"/>
    </tp:TransportClientSecurity>
  </tp:TransportSender>
</tp:Transport>
```

L'élément ainsi défini peut être ensuite utilisé par référence à son identification (champ transportId).

8.1.1.3 Définition des protections des assertions SAML

Pour définir les informations qui permettent d'authentifier les assertions SAML, l'élément utilisé est le ebXMLSenderBinding qui fait partie d'un élément docExchange.

Il s'agit de décrire:

- une identification locale de l'objet,
- des algorithmes de condensation (hashage) et de signature supportés,
- la référence au(x) certificat(s) utilisé(s) (ClientCertificateRef.)

Ces informations sont regroupées pour définir la partie 'émetteur' (ebXMLSenderBinding) d'un élément d'échange de document. On note que, dans le cas d'un web proxy, il n'y a pas réellement des documents échangés.

```
<tp:DocExchange tp:docExchangeId="docExchangeB1">
```

```

<tp:ebXMLSenderBinding tp:version="2.0">
  <tp:SenderNonRepudiation>
    <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiationProtocol>
    <tp:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</tp:HashFunction>
    <tp:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#dsa
    sha1</tp:SignatureAlgorithm>
    <tp:SigningCertificateRef tp:certId="OrganismeA_SigningCert"/>
  </tp:SenderNonRepudiation>
</tp:ebXMLSenderBinding>
</tp:DocExchange>

```

8.1.1.4 Définition du canal de transmission

Un canal de transport et une spécification d'échange de documents sont ensuite intégrés par référence dans un élément DeliveryChannel, qui permet ainsi de disposer de tous les éléments nécessaires à l'authentification de la partie cliente pour ce qui concerne la connexion HTTPS et des attestations SAML.

```

<tp:DeliveryChannel channelId="ChannelB1" transportId="transportB1"
docExchangeId="docExchangeB1">

```

8.1.1.5 Liste de PAGM, modes d'authentification et attributs

Le schéma CPP-CPA permet d'ajouter certaines extensions. Le point d'extension dans l'élément ActionBinding est utilisé pour ajouter des éléments qui ne peuvent pas être spécifiés autrement.

Pour un organisme client, il est étendu de trois éléments :

- ❑ les PAGM supportés par l'organisme client (qui peuvent n'être qu'une partie de tous les PAGM offerts par l'organisme fournisseur),
- ❑ les attributs supportés par l'organisme client,
- ❑ les modes d'authentification supportés (qui peuvent n'être qu'une partie de tous les modes d'authentification souhaités par l'organisme fournisseur).

Pour les PAGM nous utilisons la syntaxe de l'élément Role qui est défini dans le standard OASIS-ebXML/CPA.

```

<element name="PAGM" type="tp:Role" />

```

Les attributs seront représentés en utilisant la syntaxe du type PartyRef qui permet de référencer une syntaxe externe :

```

<element name="Attribut" type="tp:PartyRef" />

```

En fonction du type d'attribut à ajouter, il est nécessaire de définir un élément et une syntaxe adéquate pour son utilisation dans le vecteur d'identification.

Exemple d'une définition d'un type géographique pour une indication de départements.

```
<element name="Zone" type="frdss:zonefr.type" />
<simpleType name="departmentfr.type">
  <restriction base="NMTOKEN">
    <enumeration value="01">
      <!--liste de valeurs pour chaque zone, ici numéro de département -->
    <enumeration value=" 99"> <!-- pour les étrangers -->
  </restriction>
</simpleType>
```

Pour indiquer les niveaux d'authentification, les types d'assertions SAML sont utilisés.

```
<element name="AuthnClass" type="saml:AuthnContextClassRef" />
```

L'exemple suivant montre la disponibilité de deux PAGM, un attribut de zone géographique et un niveau d'authentification par mot de passe associé à un canal de communication.

```
<tp:ThisPartyActionBinding id="OrganismeAversOrganismeB">
  <tp:ChannelId>channelB</tp:ChannelId>
  <frdss:PAGM name="PAGM1">
  <frdss:PAGM name="PAGM2">
  <frdss:Attribute name="ZoneFR"
    schemaLocation="http://www.frdss.org/schemasdss#zonefr" />
  <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
  </frdss:AuthnClass>
</tp:ThisPartyActionBinding>
```

8.1.1.6 Définition des modes de communication possibles

Le standard OASIS-ebXML/ CPP permet d'indiquer le type du service dans un élément tp:ProcessSpecification. Dans le cas présent, deux types de service sont définis : WebProxy (portail à portail) et WebService (application à application). Ces définitions sont faites par référence à des documents XML qui spécifient les processus de collaboration.

Exemple pour Web Service :

Pour l'utilisation de WebService deux rôles sont définis: WebClient et WebServer.

```
<tp:ProcessSpecification version="1.0" name="WebService" xlink:type="simple"
  xlink:href="WSDLBPSS.xml" uuid="urn:webservice"/>
```

Exemple pour Web Proxy :

Pour les besoins de portail http, il est défini un Process "WebProxy" qui sera référencé comme suit. Les mêmes indications de rôle que dans le WebService (WebClient et WebServer) sont utilisées.

```
<tp:ProcessSpecification version="1.0" name="WebProxy" xlink:type="simple"
  xlink:href="DSSWEBPROXY.xml" uuid="urn:webproxy"/>
```

8.1.1.7 Définition des caractéristiques de l'application ou du portail client

Plusieurs éléments sont utilisés pour décrire ces caractéristiques :

- le type d'échanges,
- les PAGM supportés par l'organisme client,
- le canal de transmission utilisé.

Exemple:

```
<tp:CollaborationRole>
  <tp:ProcessSpecification version="1.0" name="WebProxy"
    xlink:type="simple" xlink:href="" />
  <tp:Role name="WebClient" xlink:type="simple" xlink:href="" />
  <tp:ServiceBinding>
    <tp:Service>urn:webproxy</tp:Service>
    <tp:CanSend>
      <tp:ThisPartyActionBinding id="OrganismeAversOrganismeB">
        <tp:ChannelId>channelB1</tp:ChannelId>
        <frdss:PAGM name="PAGM1">
        <frdss:PAGM name="PAGM2">
        <frdss:Attribute name="ZoneFR"
          schemaLocation="http://www.frdss.org/schemasdss#zonefr" />
        <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        </frdss:AuthnClass>
      </tp:ThisPartyActionBinding>
    </tp:ThisPartyActionBinding>
  </tp:CanSend>
</tp:ServiceBinding>
</tp:CollaborationRole>
```

8.1.1.8 Identification du document CPP envoyé par le client

Pour permettre d'identifier le cadre d'utilisation, il convient d'utiliser le format d'échange d'une CPP (Cooperation Protocol Profile) des spécifications OASIS-ebXML/ CPP. Ce format est conçu pour établir une convention technique concernant la coopération entre organismes s'appuyant sur l'échange de documents.

```
<?xml version="1.0"?>
<tp:CollaborationProtocolProfile xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2_x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:frdss="http://www.frdss.org/2005/XMLSchema"
  xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-
cppa/schema/cpp-cpa-2_x.xsd /Schemas/cpp-cpa-2_x.xsd" cppid="uri:OrganismeA-
cpp" version="2_x">
  <tp:PartyInfo partyName="OrganismeA">
    <tp:PartyId type=" urn:oasis:names:tc:SAML:1.1:nameid-
format:X509Subject" O=CNAMTS, C=FR </tp:PartyId>

<!-- Informations CollaborationProfile -->
<!-- Informations Transport DeliveryChannel -->
<!-- Informations Certificat -->
  </tp:PartyInfo>
</tp:CollaborationProtocolProfile>
```

8.1.1.9 Exemple de contenu complet d'un CPP client

```

<?xml version="1.0"?>
<tp:CollaborationProtocolProfile xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2 x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:frdss="http://www.frdss.org/2005/XMLSchema"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-
cpa-2 x.xsd /Schemas/cpp-cpa-2 x.xsd" cppid="uri:OrganismeA-cpp"
version="2_x">
  <tp:PartyInfo partyName="OrganismeA">
    <tp:PartyId type=" urn:oasis:names:tc:SAML:1.1:nameid-
format:X509Subject" O=CNAMTS, C=FR </tp:PartyId>
    <tp:CollaborationRole>
      <tp:ProcessSpecification version="1.0" name="WebProxy"
        xlink:type="simple" xlink:href="" />
      <tp:Role name="WebClient" xlink:type="simple" xlink:href="" />
      <tp:ServiceBinding>
        <tp:Service>urn:webproxy</tp:Service>
        <tp:CanSend>
          <tp:ThisPartyActionBinding id="OrganismeA">
            <tp:ChannelId>channelB1</tp:ChannelId>
            <frdss:PAGM name="PAGM1">
            <frdss:PAGM name="PAGM2">
            <frdss:Attribute name="ZoneFR"
              schemaLocation="http://www.frdss.org/schemasdss#zonefr" />
            <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
            </frdss:AuthnClass>
          </tp:ThisPartyActionBinding>
        </tp:ThisPartyActionBinding>
      </tp:CanSend>
    </tp:Service>
  </tp:ServiceBinding>
</tp:CollaborationRole>
<tp:DeliveryChannel channelId="webproxyB1" transportId="transportA"
  docExchangeId="docExchange" />
  <tp:Certificate certId="OrganismeA_Client_Cert">
    <ds:X509Data>
      Certificate en forme base 64
    </ds:X509Data>
  </tp:Certificate>
  <tp:Certificate certId="OrganismeA_SigningCert">
    <ds:X509Data>
      Certificate en forme base 64
    </ds:X509Data>
  </tp:Certificate>
  <tp:DocExchange tp:docExchangeId="docExchange">
    <tp:ebXMLSenderBinding tp:version="2.0">
      <tp:SenderNonRepudiation>
        <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiatio
nProtocol>
        <tp:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</tp:HashFunction>
        <tp:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#dsa
        sha1</tp:SignatureAlgorithm>
        <tp:SigningCertificateRef tp:certId="OrganismeA_SigningCert"/>
      </tp:SenderNonRepudiation>
    </tp:ebXMLSenderBinding>
  </tp:DocExchange>

  <tp:Transport transportId="transportA">
    <tp:TransportSender>
      <tp:TransportProtocol version="1.1">HTTP</tp:TransportProtocol>
      <tp:TransportClientSecurity>
        <tp:TransportSecurityProtocol
          version="1.1">TLS</tp:TransportSecurityProtocol>
        <tp:ClientCertificateRef certId="OrganismeA_ClientCert"/>
      </tp:TransportClientSecurity>
    </tp:TransportSender>
  </tp:Transport>
</tp:PartyInfo>
</tp:CollaborationProtocolProfile>

```

8.1.2 Constitution du CPP fournisseur

L'organisme fournisseur prépare également un profil de protocole de coopération qui comprend son offre de services et ses besoins de sécurité, tels que les détails d'accès.

Contenu du CPP fournisseur

Le CPP de l'organisme fournisseur contient des éléments syntaxiques équivalents au CPP client. L'élément CanReceive et son contenu forment la partie fournisseur du Service.

Une extension du type ActionBinding permet au fournisseur d'indiquer les URL accessibles et des commentaires de présentation par le portail. Il s'agit d'inclure un élément du type Body du langage HTML.

```
<element name="Application" type="html:body" />
```

Les liens doivent être spécifiés en forme relative.

Exemple:

```
<tp:Service>
  <tp:CanReceive>
    <tp:ThisPartyActionBinding id="OrganismeAversOrganismeB">
      <tp:ChannelId>channelB1</tp:ChannelId>
      <frdss:PAGM name="PAGM1">
        <frdss:Attribute name="ZoneFR"
          schemaLocation=http://www.frdss.org/schemasdss#zonefr />
      <frdss:AuthnClass urn:oasis:names:tc:SAML:2.0:ac:classes:Password
      </frdss:AuthnClass>
        <frdss:Application>
          <h1><a href="/.abc.html">Application ABC</a></h1>
          <h1><a href="/.xyz.html">Application XYZ</a></h1>
        </frdss:Application>
      </tp:ThisPartyActionBinding>
    </tp:CanReceive>
  </tp:Service>
```

L'URL de base se trouve dans l'élément EndPoint du canal de Transport. Dans cette description on trouve aussi la référence du certificat d'authentification du serveur du fournisseur.

```
<tp:Transport transportId="transportB1">
  <tp:TransportReceiver>
    <tp:TransportProtocol version="1.1">HTTP</tp:TransportProtocol>
    <tp:EndPoint uri="https://www.xxx.fr/application1/">
    <tp:AccessAuthentication>PAGM/tp:AccessAuthentication>
  <tp:TransportServerSecurity>
    <tp:TransportSecurityProtocol
      version="1.1">TLS</tp:TransportSecurityProtocol>
    <tp:ServerCertificateRef certId="OrganismeB_ServerCert"/>
  </tp:TransportServerSecurity>
  </tp:TransportReceiver>
</tp:Transport>
```

8.1.2.1 CPP fournisseur complet

Voici un exemple complet d'un CPP fournisseur.

```
<?xml version="1.0"?>
<tp:CollaborationProtocolProfile xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2_x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-
cpa-2_x.xsd /Schemas/cpp-cpa-2_x.xsd" cppid="uri:OrganismeB-cpp"
version="2_x">
  <tp:PartyInfo partyName="OrganismeA">
    <tp:PartyId type=" urn:oasis:names:tc:SAML:1.1:nameid-format:X509Subject">
O=XXX, C=FR </tp:PartyId>
    <tp:CollaborationRole>
      <tp:ProcessSpecification version="1.0" name="WebProxy"
xlink:type="simple" xlink:href="webproxy.xml" uuid="urn:webproxy"/>
      <tp:Role name="WebServer xlink:type="simple" xlink:href="" />
      <tp:ServiceBinding>
        <tp:Service>
          <tp:CanReceive>
            <tp:ThisPartyActionBinding id="OrganismeB1">
              <tp:ChannelId>channelB1</tp:ChannelId>
              <frdss:PAGM name="PAGM1">
                <frdss:Attribute name="ZoneFR"
schemaLocation=http://www.frdss.org/schemasdss#zonefr />
              <frdss:AuthnClass urn:oasis:names:tc:SAML:2.0:ac:classes:Password
/>
              <frdss:AuthnClass>
                <frdss:Application>
<h1><a href=" ./abc.html">Application ABC</a></h1>
<h1><a href=" ./xyz.html">Application XYZ</a></h1>
                </frdss:Application>
              </tp:ThisPartyActionBinding>
            </tp:CanReceive>
          </tp:Service>
        </tp:ServiceBinding>
      </tp:CollaborationRole>
      <tp:DeliveryChannel channelId="channelB1" transportId="transportB" />
      <tp:Certificate certId="OrganismeB_Server_Cert">
        <ds:X509Data>
          Certificate en forme base 64
        </ds:X509Data>
      </tp:Certificate>
      <tp:Transport transportId="transportB">
        <tp:TransportReceiver>
          <tp:TransportProtocol version="1.1">HTTP</tp:TransportProtocol>
          <tp:EndPoint uri="https://rniam.partenaires.cnaf.fr"
          <tp:AccessAuthentication>PAGM/tp:AccessAuthentication>
        <tp:TransportServerSecurity>
          <tp:TransportSecurityProtocol
version="1.1">TLS</tp:TransportSecurityProtocol>
          <tp:ServerCertificateRef certId="OrganismeB_ServerCert"/>
        </tp:TransportServerSecurity>
        </tp:TransportReceiver>
      </tp:Transport>
    </tp:PartyInfo>
  </tp:CollaborationProtocolProfile>
```

8.1.3 Synthèse des deux CPP : le CPA

Le profil de l'organisme fournisseur (organisme B dans l'exemple) est intégré avec le profil de l'organisme client (organisme A dans l'exemple) pour faire une synthèse en forme de document CPA (Cooperation Profile Agreement). Le CPA est produit par l'organisme fournisseur et envoyé à l'organisme client.

```
<?xml version="1.0"?>
<tp:CollaborationProtocolAgreement xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2 x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-
cpa-2 x.xsd /Schemas/cpp-cpa-2 x-sep23.xsd " cpaid="urn:companyA-CompanyB-
cpa:wsdl:sayHello" version="2 x">
  <tp:Status value="agreed"/>
  <tp:Start>2005-05-20T07:21:00Z</tp:Start>
  <tp:End>2010-05-20T07:21:00Z</tp:End>
  <tp:PartyInfo partyName="OrganismeA">
    <tp:PartyId type=" urn:oasis:names:tc:SAML:1.1:nameid-
format:X509Subject"> O=CNAMTS, C=FR </tp:PartyId>
    <tp:CollaborationRole>
      <tp:ProcessSpecification version="1.0" name="WebProxy"
        xlink:type="simple" xlink:href="" />
      <tp:Role name="WebClient" xlink:type="simple" xlink:href=""/>
    <tp:ServiceBinding>
      <tp:Service>urn:webproxy</tp:Service>
      <tp:CanSend>
        <tp:ThisPartyActionBinding id="OrganismeA">
          <tp:ChannelId>channel1</tp:ChannelId>
          <frdss:PAGM name="PAGM1">
            <frdss:Attribute name="ZoneFR"
              schemaLocation="http://www.frdss.org/schemasdss#zonefr" />
          <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
          </frdss:AuthnClass>
        </tp:ThisPartyActionBinding>
        <tp:OtherPartyActionBinding>OrganismeB</tp:OtherPartyActionBinding>
      </tp:CanSend>
    </tp:Service>
  </tp:ServiceBinding>
  </tp:CollaborationRole>
  <tp:DeliveryChannel channelId="channel1" transportId="transportA"
docExchangeId="docExchange">/>
    <tp:Certificate certId="OrganismeA_Client_Cert">
      <ds:X509Data>
        Certificate en forme base 64
      </ds:X509Data>
    </tp:Certificate>
    <tp:Certificate certId="OrganismeA_SigningCert">
      <ds:X509Data>
        Certificate en forme base 64
      </ds:X509Data>
    </tp:Certificate>
    <tp:DocExchange tp:docExchangeId="docExchange">
      <tp:ebXMLSenderBinding tp:version="2.0">
        <tp:SenderNonRepudiation>
          <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiatio
nProtocol>
          <tp:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</tp:HashFunction>
          <tp:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#dsa
          sha1</tp:SignatureAlgorithm>
          <tp:SigningCertificateRef tp:certId="OrganismeA_SigningCert"/>
        </tp:SenderNonRepudiation>
      </tp:DocExchange>
  </tp:DeliveryChannel>

```

certificat de l'organisme client
qui servira à l'authentification
mutuelle

certificat de l'organisme client
qui servira à la signature
SAML

```

</tp:AuthnClass>
</tp:DocExchange>

<tp:Transport transportId="transportA">
  <tp:TransportSender>
    <tp:TransportProtocol version="1.1">HTTP</tp:TransportProtocol>
    <tp:TransportClientSecurity>
      <tp:TransportSecurityProtocol
        version="1.1">TLS</tp:TransportSecurityProtocol>
      <tp:ClientCertificateRef certId="OrganismeA_ClientCert"/>
    </tp:TransportClientSecurity>
  </tp:TransportSender>
</tp:Transport>
</tp:PartyInfo>
<tp:PartyInfo partyName="OrganismeA">
  <tp:PartyId type=" urn:oasis:names:tc:SAML:1.1:nameid-format:X509Subject">
O=XXX, C=FR </tp:PartyId>
  <tp:CollaborationRole>
    <tp:ProcessSpecification version="1.0" name="WebProxy"
xlink:type="simple" xlink:href="webproxy.xml" uuid="urn:webproxy"/>
    <tp:Role name="WebServer xlink:type="simple" xlink:href="" />
    <tp:ServiceBinding>
      <tp:Service>
        <tp:CanReceive>
          <tp:ThisPartyActionBinding id="OrganismeB">
            <tp:ChannelId>channelB1</tp:ChannelId>
            <frdss:PAGM name="PAGM1">
              <frdss:Attribute name="ZoneFR"
                schemaLocation=http://www.frdss.org/schemasdss#zonefr />
            </frdss:PAGM>
            <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
            </frdss:AuthnClass>
            <frdss:Application>
              <h1><a href="./abc.html">Application ABC</a></h1>
              <h1><a href="./xyz.html">Application XYZ</a></h1>
            </frdss:Application>
          </tp:ThisPartyActionBinding>
          <tp:OtherPartyActionBinding>OrganismeA</tp:OtherPartyActionBinding>
        </tp:CanReceive>
      </tp:Service>
    </tp:ServiceBinding>
  </tp:CollaborationRole>
  <tp:DeliveryChannel channelId="webproxy1" transportId="transportB" />
  <tp:Certificate certId="OrganismeB Server Cert">
    <ds:X509Data>
      Certificate en forme base 64
    </ds:X509Data>
  </tp:Certificate>
  <tp:Transport transportId="transportB">
    <tp:TransportReceiver>
      <tp:TransportProtocol version="1.1">HTTP</tp:TransportProtocol>
      <tp:EndPoint uri="https://rniam.partenaires.cnnav.fr">
        <tp:AccessAuthentication>PAGM/tp:AccessAuthentication>
      </tp:EndPoint>
      <tp:TransportServerSecurity>
        <tp:TransportSecurityProtocol
          version="1.1">TLS</tp:TransportSecurityProtocol>
        <tp:ServerCertificateRef certId="OrganismeB ServerCert"/>
      </tp:TransportServerSecurity>
    </tp:TransportReceiver>
  </tp:Transport>
</tp:PartyInfo>
</tp:CollaborationProtocolAgreement>

```

Attribut souhaité en lien avec le PAGM1

Si une exigence explicite de niveau d'authentification est nécessaire, elle est mentionnée ici

URL de l'application

8.1.4 Sécurisation et Echanges des CPP et CPA

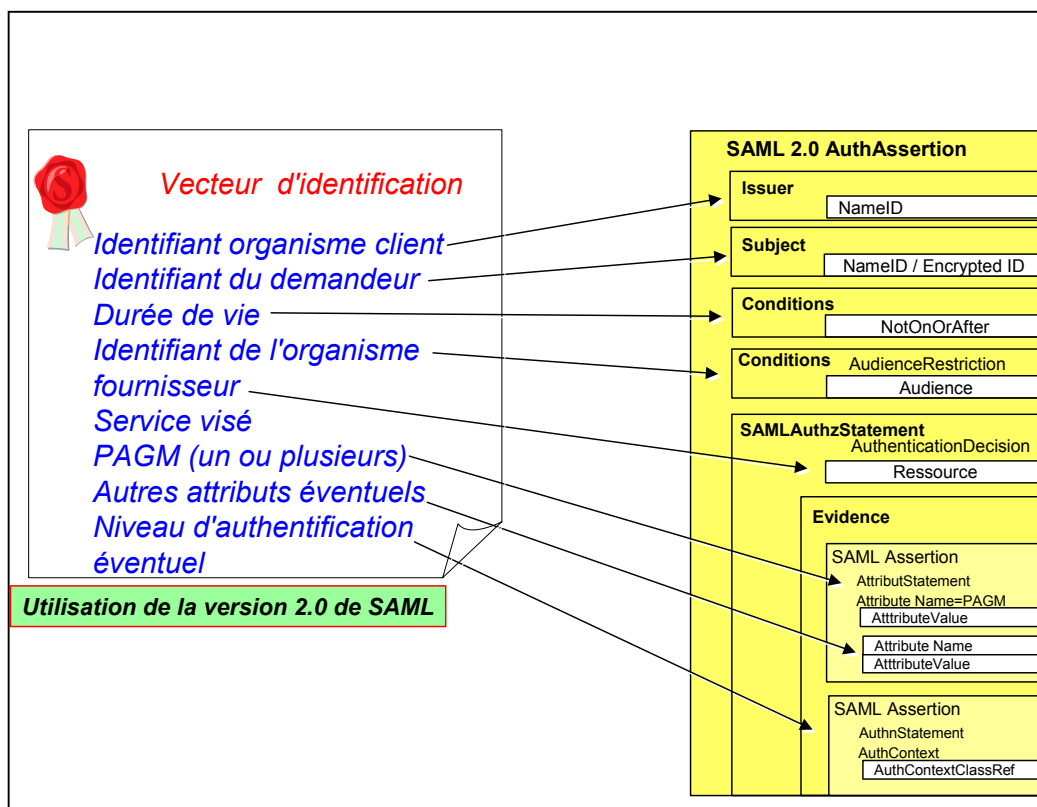
Les clients et fournisseurs doivent être sûr de l'intégrité et de l'authenticité des CPP et CPA.

Il convient d'utiliser des méthodes de signature des fichiers CPP et CPA afin d'être capable de les échanger de manière électronique.

8.2 Format du vecteur d'identification


8.2.1 Présentation

Le vecteur d'identification est représenté par une assertion d'autorisation SAML, donc une attestation qui comprend un élément **AuthzStatement** incluant une assertion avec un **AttributeStatement** et une assertion avec un **AuthnStatement** dans l'élément **Evidence**



La version 2.0 de SAML sera utilisée, cela est indiqué par l'attribut `Version="2.0"` de l'élément **Assertion**.

Correspondance entre le vecteur d'identification et l'assertion SAML

	<p>Nota</p> <p>Dans le cas HTTP, l'URL est celle visée dans l'organisme fournisseur. Elle peut ou non avoir une relation avec la requête d'origine. En général (proxy simple), 2 cas peuvent exister : le portail de départ utilise un DNS modifié pour permettre les mêmes URL qu'un utilisateur local à l'application d'arrivée, dans un autre cas le portail de départ a ses propres URL et doit "mapper" la partie host vers la partie host du système à distance.</p> <p>Dans le cas Web-Service, le champ contient l'URL de destination (l'application visée) renseigné par l'application de départ en fonction de ce que veut faire l'utilisateur.</p>
---	--

8.2.2 Eléments détaillés

Dans ce paragraphe nous décrivons le profil d'une assertion SAML utilisée pour véhiculer le vecteur d'identification. Il s'agit d'indiquer les éléments dans la hiérarchie de l'assertion SAML.

Indication de l'organisme Client

L'organisme fournisseur est indiqué par l'élément **Issuer**.

Indication de l'identité

L'identité de l'utilisateur est indiquée par l'élément **Subject** dans **NameID** ou **EncryptedID** avec libre choix du format des identifiants.

Indication de la durée de vie

La durée de vie est indiquée dans un élément **Conditions->NotBefore** et **Condition->NotAfter** ou dans l'élément **Conditions->NotOnOrAfter**.

Indication de l'organisme fournisseur

L'organisme fournisseur de service est indiqué par l'élément **Conditions->AudienceRestriction->Audience**.

Indication de l'application visée

L'attribut **Ressource** de l'élément **AuthzDecisionStatement** indique la ressource (L'URL).

PAGM et autres attributs

Chaque PAGM utilisable par l'utilisateur est indiqué par un élément **Attribute** spécifique à ce standard, indiqué dans l'élément **AttributeStatement**. L'attribut est indiqué par une valeur PAGM pour l'élément **Name** ; les valeurs sont indiquées par une représentation textuelle d'un Object Identifier.

D'autres attributs sont indiqués d'une façon similaires.

Indication du niveau de l'authentification

Le niveau de sécurité est indiqué par l'attribut **AuthnContextClassRef** de l'élément **AuthnStatement**

8.2.3 Exemple d'assertion SAML pour un échange organisme à organisme

Le vecteur d'identification:

Organisme Client : **X509Subject O=CNAMTS, C=FR**

Organisme Fournisseur : **X509Subject O=CNAVTS, C=FR**

Durée de vie : pas après **2005-04-01T11:57.11.367Z**

Application: **https://rniam.partenaires.cnav/**

PAGM: **1.2.3.4.5.6** (ceci représente un OID – Object Identifier - associé au PAGM "Consultation pour identification")

Attribut nom **GeoZone** valeur **75**

Identité **a123@cnamts.fr**


Niveau d'authentification : **Password**

```
<Assertion ID="1174efac03" IssueInstant="2005-04-01T11:47.11.367Z"
  Version="2.0">
  <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509Subject"
    O=CNAMTS, C=FR
  </Issuer>
  <Subject
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
      a123@cnamts.fr
    </NameID>
  </Subject>
  <Conditions NotOnOrAfter="2005-04-01T11:57.11.367Z"/>
  <Condition>
  <AudienceRestriction>
    <Audience>
      <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509Subject"
        O=CNAVTS, C=FR
      </NameID>
    </Audience>
  </AudienceRestriction>
  </Conditions>
  <AuthzStatement>
    <AuthenticationDecision Resource="https://rniam.partenaires.cnav/"
      Decision="Permit" />
  <Evidence>
  <Assertion ID="1174efac02" IssueInstant="2005-04-01T11:47.11.367Z"
    Version="2.0">
  <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509Subject"
    O=CNAMTS, C=FR
  </Issuer>
  <Subject
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
      a123@cnamts.fr
    </NameID>
  </Subject>
  <AttributeStatement>
    <Attribute Name="PAGM">
      <AttributeValue>1.2.3.4.5.6</AttributeValue>
    </Attribute>
    <Attribute Name="GeoZone">
      <AttributeValue>75</AttributeValue>
    </Attribute>
  </AttributeStatement>
  </Assertion>
```

```
</AttributeStatement>
</Assertion>
<Assertion ID="1174efac01" IssueInstant="2005-04-01T11:47:11.367Z"
  Version="2.0">
  <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509Subject"
    O=CNAMTS, C=FR
  </Issuer>
  <Subject
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
      a123@cnamts.fr
    </NameID>
  </Subject>
  <AuthnStatement AuthnInstant="2001-05-31T13:21:00-05:00">
    <AuthnContext>
      <AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:Password
      </AuthnContextClassRef>
    </AuthnContext>
  </AuthnStatement>
</Assertion>
</Evidence>
<AuthzStatement>
<Signature>
  Signature xml dsig
</Signature>
</Assertion>
```

8.3 Transfert de la requête

La communication entre les organismes utilise le protocole HTTPS avec TLS.


	<p>Nota</p> <p><i>Il faut distinguer</i></p> <ul style="list-style-type: none">- les identifiants du vecteur d'identification (qui a pris la décision de la requête),- l'authenticité des assertions SAML (la signature sur l'assertion SAML),- la protection des connexions entre entreprises (par SSL avec authentification mutuelle avec certificat serveur et certificat client)
---	---

8.3.1 Transmission d'une requête HTTP

Ce cas concerne le relayage des pages Web dans le mode portail à portail (ou portail à application).

L'assertion SAML sera codée en forme BASE64 et transformée en Cookie. L'identifiant du Cookie sera l'identifiant du portail de départ.

Le système d'arrivée peut ainsi traiter la requête sans développement supplémentaire.

	<p>Nota</p> <p><i>Il s'agit de transmettre entre le dernier serveur de départ et le premier serveur d'arrivée le vecteur d'identification dans l'hypothèse où l'on souhaite relayer une requête http d'origine sans trop de modifications.</i></p> <p><i>Le cookie est généré par le dernier serveur de départ (le relais portail), puis il est utilisé par le système d'arrivée (en fonction des besoins de sécurité : simplement stocké ou également vérifié par un frontal d'autorisation pour traduire le PAGM vers des profils applicatifs).</i></p> <p><i>Ce cookie n'existe qu'entre les deux serveurs et n'est jamais transmis, ni a fortiori stocké, sur un poste de travail.</i></p>
---	---

8.3.2 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.

8.4 Sécurisation du transfert


8.4.1 Protection des canaux et authentification mutuelle

Le protocole TLS (SSL) est utilisé entre les deux portails et/ou applications des organismes client et fournisseur⁴.

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.

	<p>Nota</p> <p><i>L'utilisation d'une protection des canaux est nécessaire.</i></p> <p><i>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).</i></p>
---	--

8.4.2 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>
- Spécification SAML : <http://www.oasis-open.org/specs/index.php#samlv2.0>
- OASIS-ebXML/ CPP : <http://www.oasis-open.org/committees/download.php/12208/ebcpp-2.1-april-5-2005-draft.doc>

[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/xmlsig-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 structurelle 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 : <ul style="list-style-type: none"> ❑ 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 séquençement de leur exécution (vue dynamique). <p>Cette description réalise les exigences fonctionnelles et les exigences de performances.</p>
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	<p>Terme informatique pour l'opération d'identification réalisée par un processus informatique.</p> <p>Les principaux moyens d'authentification sont :</p> <ul style="list-style-type: none"> <input type="checkbox"/> mot de passe <input type="checkbox"/> clé symétrique <input type="checkbox"/> certificat <input type="checkbox"/> biométrie
C-D	
Certificat	<p>Fonctionnellement, un certificat se définit comme un objet informatique logique lié à une entité.</p> <p>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 asymétrique) permettant des opérations d'authentification et de signature numérique. ,</p>
Client réseau banalisé	<p>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.</p>
Composant	<p>Module logiciel ou matériel participant à la cohérence d'un dispositif plus vaste (services socle, services applicatifs, services réseaux, par exemple)</p> <p>Par exemple :</p> <ul style="list-style-type: none"> <input type="checkbox"/> un serveur web, un serveur d'application, un annuaire LDAP, une base de données sont des composants techniques logiciels <input type="checkbox"/> un poste de travail, une machine serveur, un PC sont des composants techniques matériels <p>certaines composants tels qu'un pare-feu, un routeur, un Proxy, un antivirus ou un antispam peuvent être des composants logiciels ou matériels.</p>
Contrôle d'accès	<p>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.</p>
Cookie	<p>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.</p>
Droit	<p>Un droit correspond à l'habilitation d'un métier dans une application et se compose d'un ou plusieurs groupes d'actions unitaires.</p>
E - F	
Entité	<p>Élément accédant aux ressources d'une application : exemple : personne ou application</p>

Terme	Définition
Espace de confiance	<p>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.</p> <p>Un espace est dit de confiance quand il répond à des critères de sécurité considérés comme suffisants par la Maîtrise d'Ouvrage concernée.</p>
Espace de travail	<p>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.</p> <p>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.</p>
Fédération d'identités	<p>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.</p>
Fonction	<p>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.</p> <p>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.</p>
Fournisseur d'identité	<p>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.</p> <p>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).</p>
Fournisseur de service	<p>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.</p> <p>Le fournisseur de service peut s'appuyer sur le fournisseur d'identité pour les fonctions d'identification et d'authentification.</p>
G – O	
Habilitation	<p>Les habilitations permettent à un utilisateur d'accéder à un ensemble de procédures informatiques.</p>

Terme	Définition
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.
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 applications).
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.

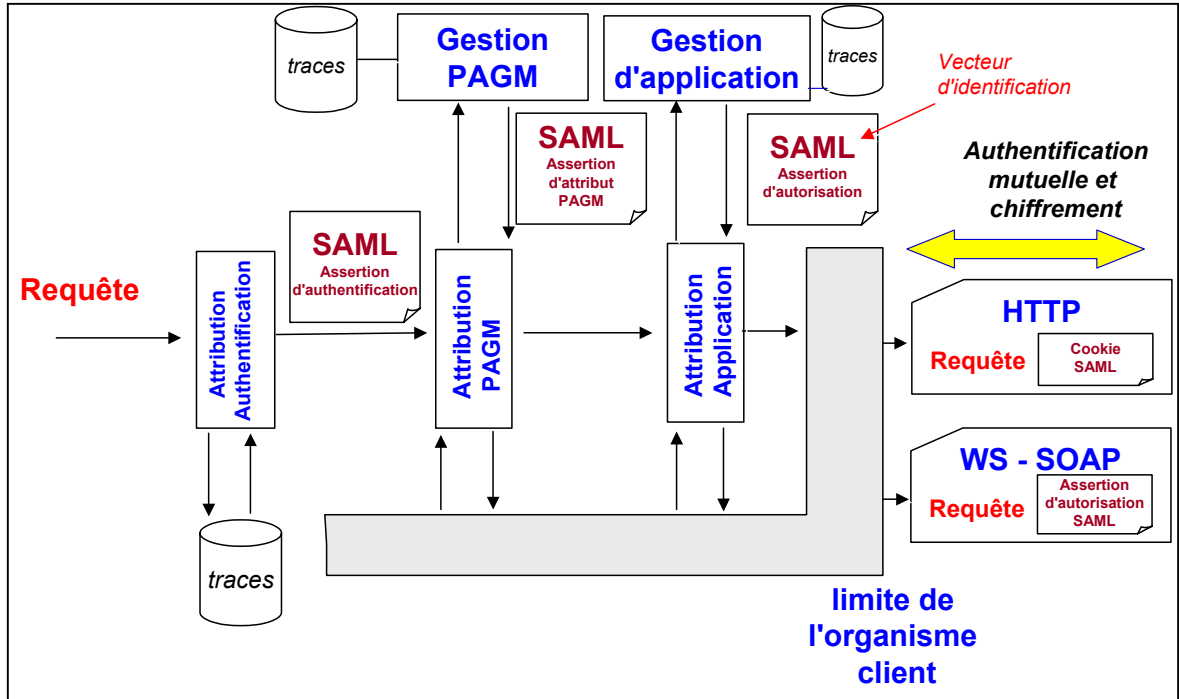
Terme	Définition
Personnalisable (diffusion)	L'utilisateur peut modeler (par l'intermédiaire du service de personnalisation) le contenu et sa présentation en choisissant explicitement parmi une sélection d'option ses services et ses préférences.
Profil	On ne retiendra pas cette notion qui : <ul style="list-style-type: none"> <input type="checkbox"/> Recopie le rôle ou l'ensemble (rôle + attributs) <input type="checkbox"/> Peut définir un profil applicatif <input type="checkbox"/> 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	<i>Acteur offrant des services de certification.</i>
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 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)	<i>Fonction associée à une entité. Une entité peut avoir plusieurs rôles métiers (exemples : directeur, maire professeur, parent, citoyen, etc.).</i>

Terme	Définition
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". [<i>Petit Robert</i>]
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	<p>Les services AAS (Authentification-Autorisation-SSO) assurent les fonctions suivantes :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Contrôle d'accès (identification, authentification, autorisation) <input type="checkbox"/> Gestion d'identité et des habilitations (gestion des rôles et des profils, gestion de la politique d'habilitation) <input type="checkbox"/> Propagation des identités et des droits à l'intérieur d'un espace de confiance et/ou entre plusieurs espaces.
Services applicatifs	<p>(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 :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Services pédagogiques (construction des ressources pédagogiques, cahier de texte) <input type="checkbox"/> Services de vie d'établissement (aide à la publication Web, publication de brèves, ...) <input type="checkbox"/> Services scolaires (gestion des absences, gestion des notes, emploi du temps, tableau d'affichage) <input type="checkbox"/> Services documentaires (ressources personnelles de l'élève ou de l'enseignant, ressources du CDI, ...) <input type="checkbox"/> Services de communication (services avancés de messagerie, chat, Forum de discussion, liste de distribution, ...) <input type="checkbox"/> Bureau numérique (carnet d'adresses, espace de stockage, outils bureautiques, ...) <p>Ces services font appel aux services socle.</p>
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 notamment).
Service applicatif intégré	Le service installé sur le portail lui-même ou sur une extension de celui-ci.
Services d'administration	<p>Les services d'administration représentent :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Outils d'exploitation <input type="checkbox"/> Gestion de la configuration <input type="checkbox"/> Gestion des alertes et des incidents <input type="checkbox"/> Outils de suivi et de pilotage <input type="checkbox"/> Statistiques de flux

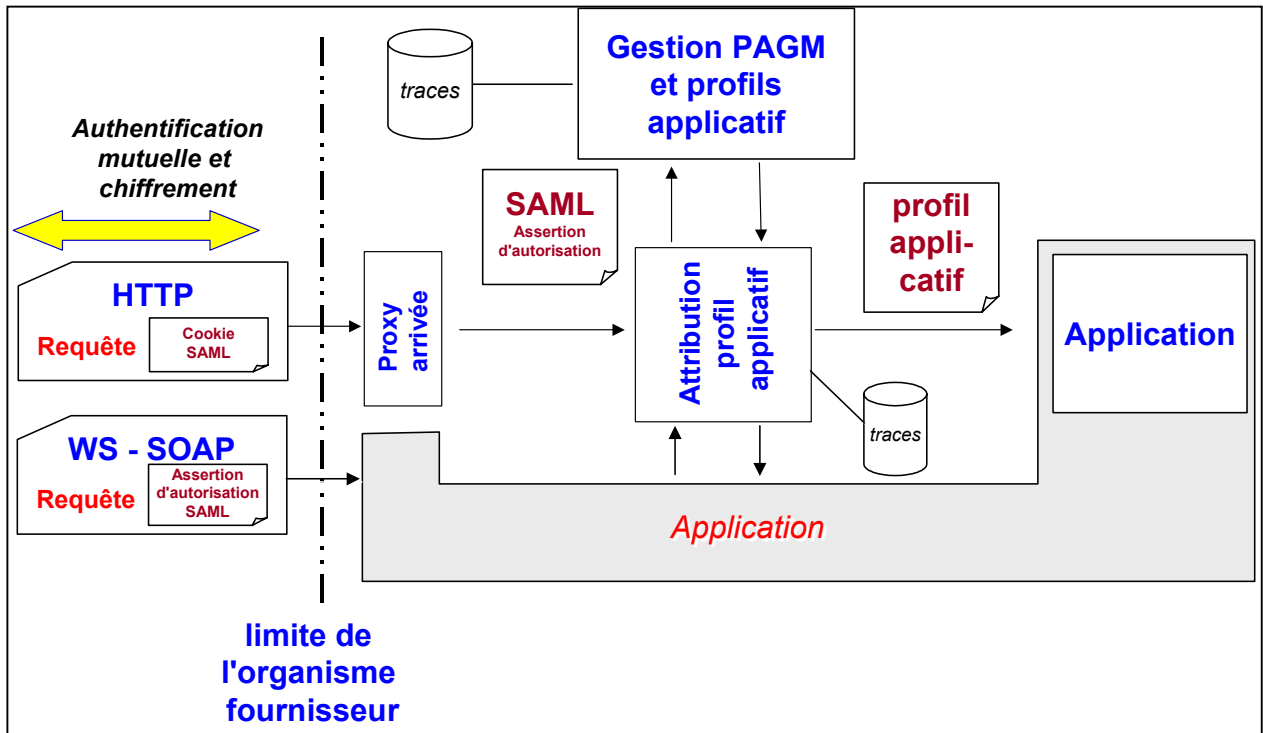
Terme	Définition
Services d'aide en ligne	<p>Les services d'aide en ligne pour les services socle, utilisables par les applications permettent d'assurer les fonctions suivantes :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Publication de guides de formation <input type="checkbox"/> Mise en place et maintien d'un FAQ <input type="checkbox"/> Forum de discussion <input type="checkbox"/> Help desk en ligne <input type="checkbox"/> Interface de communication entre les applications et l'aide en ligne
Services d'annuaire	<p>Les services d'annuaire assurent notamment les fonctions suivantes :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Alimentation de l'annuaire (ou Provisionning) <input type="checkbox"/> Synchronisation des données assurée par des connecteurs <input type="checkbox"/> Mise à jour des informations (réplication synchrone/asynchrone, partielle/complète)
Services d'échanges	<p>Les services d'échanges entre le socle et les services applicatifs désignent :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Interfaces applicatives (« web services ») <input type="checkbox"/> Fonctions d'interopérabilité (protocoles associés) <input type="checkbox"/> Annuaire d'objets techniques (UDDI) <p>Ces services sont placés dans le socle.</p>
Service de gestion des identités et des accès	<p>Les services de gestion des identités et des accès désignent :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Les services d'annuaire qui contiennent les informations des acteurs (identités et habilitations) <input type="checkbox"/> Les services AAS
Service de gestion des transactions	<p>Gère les échanges entre les services applicatifs et le client réseau.</p>
Service en ligne	<p>Service mis à disposition des usagers sous un format électronique et accessible depuis un client réseau.</p>
Service multi-canal	<p>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).</p>
Services réseaux	<p>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 :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Protocoles (HTTP, WAP, ...) <input type="checkbox"/> Supports de communication (Lignes spécialisées, RTC, ...) <p>Les services réseaux assurent également les premières fonctions de contrôle d'accès (pare-feu, proxy) et de contrôle de contenu (anti-spam, antivirus).</p>
Single Sign-On (ou authentification unique)	<p>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).</p>
Socle technique	<p>Terme utilisé pour définir les éléments techniques du socle de services minimum. Typiquement, les serveurs, les logiciels sont des éléments techniques.</p>

Terme	Définition
Stockage	Action d'enregistrer sur un support numérique en vue d'une utilisation ultérieure. [<i>Petit Robert</i>]
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

9.4 Exemple OASIS-ebXML/CPA pour WSDI

Dans cet exemple nous montrons comment augmenter une définition CPP/CPA pour un web service avec les extensions de ce standard. Nous avons repris un des exemples fournis par le standard OASIS-ebXML/CPA.

1. CPP d'émetteur

```
<?xml version="1.0"?>
<tp:CollaborationProtocolProfile xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2 x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-
cpa-2 x.xsd /Schemas/cpp-cpa-2 x.xsd " cppid="uri:companyA-cpp" version="2 x">
  <!-- Party info for CompanyA (one way) wsdl -->
  <tp:PartyInfo partyName="CompanyA" defaultMshChannelId="ChannelB1"
defaultMshPackageId="PlainSOAP">
    <tp:PartyId type="urn:oasis:names:tc:ebxml-cppa:partyid-
type:duns">123456789</tp:PartyId>
    <tp:PartyRef xlink:href="http://CompanyA.com/about.html"/>
    <tp:CollaborationRole>
      <tp:ProcessSpecification version="1.0" name="WebService"
xlink:type="simple" xlink:href="WSDLBPSS.xml" uuid="urn:webservice"/>
      <tp:Role name="WebClient" xlink:type="simple"
xlink:href=""/>
      <tp:ServiceBinding>
        <tp:Service>urn:webservice</tp:Service>
        <tp:CanSend>
          <tp:ThisPartyActionBinding
id="companyB TPAB3" action="OneWay" packageId="PlainSOAP">
            <tp:BusinessTransactionCharacteristics
              isNonRepudiationRequired="false"
              isNonRepudiationReceiptRequired="false"
              isConfidential="none"
              isAuthenticated="none"
              isTamperProof="none"
              isAuthorizationRequired="false"/>
            <tp:ChannelId>ChannelB1</tp:ChannelId>
            </tp:ThisPartyActionBinding>
            <frdss:Attribute name="ZoneFR"
              schemaLocation="http://www.frdss.org/schemasdss#zonefr" />
            <frdss:AuthnClass urn:oasis:names:tc:SAML:2.0:ac:classes:Password
              </frdss:AuthnClass>
          </tp:CanSend>
        </tp:ServiceBinding>
      </tp:CollaborationRole>
    <!-- Delivery channel -->
    <tp:DeliveryChannel channelId="ChannelB1"
transportId="transportB2" docExchangeId="docExchangeB1">
      <tp:MessagingCharacteristics syncReplyMode="none"
ackRequested="never" ackSignatureRequested="never"
duplicateElimination="never"/>
    </tp:DeliveryChannel>
    <tp:Transport transportId="transportB2">
      <tp:TransportSender>
        <tp:TransportProtocol
version="1.1">HTTP</tp:TransportProtocol>
      </tp:TransportSender>
    </tp:Transport>
    <tp:DocExchange docExchangeId="docExchangeB1">
      <tp:WSReceiverBinding version="2.1">
        <tp:WSDLOperation version="1.1"/>
      </tp:WSReceiverBinding>
    </tp:DocExchange>
  </tp:PartyInfo>

```

```

        </tp:DocExchange>
    </tp:PartyInfo>
    <!-- SimplePart corresponding to the SOAP Envelope -->
    <tp:SimplePart id="SOAPEnvelope" mimeType="text/xml"/>
    <!-- Convert this to new2.x and 3.x syntax -->
<tp:Packaging id="PlainSOAP">
    <tp:ProcessingCapabilities generate="true" parse="true"/>
    <tp:Constituent excludedFromSignature="false"
idref="SOAPEnvelope" maxOccurs="1" minOccurs="1"/>
</tp:Packaging>
    <tp:Comment xml:lang="en-US">Client WS Collaboration Protocol
Profile</tp:Comment>
</tp:CollaborationProtocolProfile>

```

CPP fournisseur

```

<?xml version="1.0"?>
<tp:CollaborationProtocolProfile xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2_x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-
cpa-2_x.xsd /Schemas/cpp-cpa-2_x.xsd" cppid="uri:companyA-cpp" version="2_x">
    <!-- Party info for CompanyA (one way) WSDL -->
    <tp:PartyInfo partyName="CompanyA" defaultMshChannelId="ChannelA1"
defaultMshPackageId="PlainSOAP">
        <tp:PartyId type="urn:oasis:names:tc:ebxml-cppa:partyid-
type:duns">123456789</tp:PartyId>
        <tp:PartyRef xlink:href="http://CompanyA.com/about.html"/>
        <tp:CollaborationRole>
            <!-- Process specification needed when not using choreography?
-->
            <tp:ProcessSpecification version="1.0" name="WebService"
xlink:type="simple" xlink:href="WSDLBPSS.xml" uuid="urn:webservice"/>
            <tp:Role name="WebService" xlink:type="simple"
xlink:href=""/>
            <tp:ServiceBinding>
                <tp:Service>urn:w3c:wsd:hello</tp:Service>
                <tp:CanReceive>
                    <tp:ThisPartyActionBinding
id="companyA TPAB2" action="OneWay" packageId="PlainSOAP">
                        <tp:BusinessTransactionCharacteristics isNonRepudiationRequired="false"
isNonRepudiationReceiptRequired="false"
isAuthenticated="none" isConfidential="none"
isAuthorizationRequired="false" isTamperProof="none"/>
                    </tp:ThisPartyActionBinding>
                </tp:ServiceBinding>
                <frdss:PAGM name="PAGM1">
                    <frdss:Attribute name="ZoneFR"
schemaLocation="http://www.frdss.org/schemasdss#zonefr" />
                    <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
                    </frdss:AuthnClass>
                </tp:CanReceive>
            </tp:ServiceBinding>
        </tp:CollaborationRole>
        <!-- Basdelivery channel -->
        <tp:DeliveryChannel channelId="ChannelA1"
transportId="transportA1" docExchangeId="docExchangeA1">
            <tp:MessagingCharacteristics syncReplyMode="none"
ackRequested="nev" ackSignatureRequested="never" duplicateElimination="never"/>
        </tp:DeliveryChannel>
        <tp:Transport transportId="transportA1">
            <tp:TransportReceiver>
                <tp:TransportProtocol
version="1.1">HTTP</tp:TransportProtocol>
            </tp:TransportReceiver>
        </tp:Transport>
    </tp:PartyInfo>
    <tp:AccessAuthentication>basic</tp:AccessAuthentication>

```

```

                <tp:Endpoint
uri="http://www.CompanyA.com/soap/hello" type="allPurpose"/>
                </tp:TransportReceiver>
            </tp:Transport>
            <tp:DocExchange docExchangeId="docExch
                <tp:WSReceiverB 2.1">
                    ion version="1.1">
                <wsdl:definitions
xmlns:tns="http://hello.org/hello1"
                xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                targetNamespace="http://hello.com/hello1"
name="HelloWorld">
                    <types/>
                    <message name="Hello">
                        <part name="String_1" type="xsd:string"/>
                    </message>
                    <wsdl:portType name="Hello">
                        <operati
parameterOrder="String 1">
                            <input message="tns:Hello"/>
                        </operation>
                    </wsdl:portType>
                </wsdl:definitions>
            </tp:WSDLOperation>
            </tp:WSReceiverBinding>
        </tp:DocExchange>
    </tp:PartyInfo>

    <!-- SimplePart correspond SOAP Envelope -->
    <tp:SimplePar elope" mimetype="text/xml"/>

    <tp:Packaging id="PlainSOAP">
        <tp:Proc >
            <tp:Constituent excludedFromSignature="false"
idref="SOAPEnvelope" maxOccurs="1" minOccurs="1"/>
        </tp:Packaging>
        <tp:Comment xml:lang="en-US">sayHello server (one way) Collaboration
Protocol Profile</tp:Comment>
    </tp:CollaborationProtocolProfile>

```

CPA pour one way WSDL-defined service.

```

<?xml version="1.0"?>
<tp:CollaborationProtocolAgreement xmlns:tp="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2_x.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-
cpa-2_x.xsd /Schemas/cpp-cpa-2_x-sep23.xsd " cpaId="urn:companyA-CompanyB-
cpa:wsdl:sayHello" version="2_x">
    <tp:Status value="proposed"/>
    <tp:Start>2005-05-20T07:21:00Z</tp:Start>
    <tp:End>2010-05-20T07:21:00Z</tp:End>
    <tp:ConversationConstraints invocationLimit="100"
concurrentConversations="10"/>
    <!-- Party info for CompanyA (one way) WSD -->

    <tp:PartyInfo partyName="CompanyA" defaultMshChannelId="ChannelA1"
defaultMshPackageId="PlainSOAP">
        <tp:PartyId type="urn:oasis:names:tc:ebxml-cppa:partyid-
type:duns">123456789</tp:PartyId>
        <tp:PartyRef xlink:href="http://CompanyA.com/about.html"/>
        <tp:CollaborationRole>
            <tp:ProcessSpecification version="1.0" name="WebService"
xlink:type="simple" xlink:href="WSDLBPSS.xml
            <tp:Role name="WebService" xlink:type="simple"
xlink:href=""/>

            <tp:ServiceBinding>
                <tp:Service>urn:w3c:wsd:hello</tp:Service>
                <tp:CanReceive>

```

```

        <tp:ThisPartyActionBinding

        <tp:BusinessTransactionCharacteristics isNonRepudiationRequired="false"

                                                isConfidential="none"
isAuthenticated="none"
                                                isTamperProof="none"
isAuthorizationRequired="false"/>

        <tp:ChannelId>ChannelA1</tp:ChannelId>
        <frdss:PAGM name="PAGM1">
        <frdss:Attribute name="ZoneFR"
            schemaLocation="
                .org/schemasdss#zonefr" />
        <frdss:AuthnClass> urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        </frdss:AuthnClass>

        <tp:OtherPartyActionBinding
>companyB TPAB3</tp:OtherPartyActionBinding>
        </tp:CanReceive>
        </tp:ServiceBinding>
        </tp:CollaborationRole>
        <!-- Basdelivery channel -->
        <tp:DeliveryChannel channelId="ChannelA1"
t      rt      ansportA1" docExchangeId="doc changeA1">
            <tp:MessagingCharacteristics syncReplyMode="none"
ackRequested="nev" ackSignatureRequested="never" duplicateElimination="never"/>
        </tp:DeliveryChannel>
        <tp:Transport transportId="transportA1">
            <tp:TransportReceiver
                <tp:TransportProtocol
version="1.1">HTTP</tp:TransportProtocol>

            <tp:AccessAuthentication>basic</tp:AccessAuthentication>

        </tp:TransportReceiver>
        </tp:Transport>
        <tp:DocExchange docExchangeId="docExchangeA1">
            <tp:WSReceiverBinding version="2.1">
                <tp:WSDLOperation version="1.1"
operationRef="http://hello.org/hello1#operation(Hello/sayHello)" >
                    <wsdl:definitions
xmlns:tns="http://hello.org/hello1"
                        xmlns:wSDL="http:
                            wsdl/"
                            www.w3.org/2001/XMLSchema"
                        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                        targetNamespace="http://hello.org/hello1"
name="HelloWorld">
                            <types/>
                            <message name="Hello">
                                <part name="String 1" type="xsd:string"/>
                            </message>
                            <wsdl:portType name="Hello">
                                <operation name="sayHello"
parameterOrder="String_1">
                                    <input message="tns:Hello"/>
                                </operation>
                            </wsdl:portType>
                            </wsdl:definitions>
                        </tp:WSDLOperation
                    </tp:WSReceiverBinding>
                </tp:DocExchange>
            </tp:PartyInfo>
            <tp:PartyInfo partyName="Company
                hannelId="ChannelB1"
defaultMshPackageId="PlainSOAP
            <tp:PartyId type="urn:oasis:names:tc:ebxml-cppa:partyid-
type:duns">123456789</tp:PartyId>
            <tp:PartyRef xlink:href="http://CompanyA.com/about.html"/>
            <tp:CollaborationRole>
                <tp:ProcessSpecification version="1.0" name="WebService"
xlink:type="simple" xlink:href="WSDLBPSS.xml" uuid="urn:webservice"/>
                <tp:Role name="WebClient" xlink:type="simple"
xlink:href=""/>
            <tp:ServiceBinding>

```

```

        <tp:Service>urn:webservice</tp:Service>
        <tp:CanSend>
        <tp:ThisPartyActionBinding
id="companyB TPAB3" action="OneWay" packageId="PlainSOAP">
            <tp:BusinessTransactionCharacteristics
                isNonRepudiationRequired="false"
isNonRepudiationReceiptRequired="false"
                isConfidential="none"
                isAuthenticated="none"
                perProof="none"
isAuthorizationRequired="false"/>
            <tp:ChannelId>ChannelB1</tp:ChannelId>
            </tp:ThisPartyActionBinding>
            <tp:OtherPartyActionBinding
>companyA TPAB2</tp:OtherPartyActionBinding>
            </tp:CanSend>
            </tp:ServiceBinding>
            </tp:CollaborationRole>
            <!-- Delivery channel -->
            <tp:DeliveryChannel channelId="ChannelB1"
transportId="transportB2" docExchangeId="docExchangeB1">
                <tp:MessagingCharacteristics syncReplyMode="none"
ackRequested="never" ackSignatureRequested="never"
duplicateElimination="never"/>
            </tp:DeliveryChannel>
            <tp:Transport transportId="transportB2">
                <tp:TransportSender>
                    <tp:TransportProtocol
version="1.1">HTTP</tp:TransportProtocol>
                </tp:TransportSender>
            </tp:Transport>
            <tp:DocExchange docExchangeId="docExchangeB1">
                <tp:WSReceiverBinding version="2.1">
                    <tp:WSDLOperation version="1.1"/>
                </tp:WSReceiverBinding>
            </tp:DocExchange>
        </tp:PartyInfo>
        <!-- SimplePart corresponding to the envelope -->
        <tp:SimplePart id="SOAPEnv" mimeType="text/xml"/>
        <
            <tp:ProcessingCapabilities generate="true" parse="true"/>
            <tp:Constituent
idref="SOAPEnvelope" maxOccurs="1" minOccurs="1"/>
        </tp:Packaging>
        <tp:Comment xml:lang="en-US">Buyer's Collaboration Protocol
Profile</tp:CollaborationProtocolAgreement>

```