Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DU BUDGET
DES COMPTES PUBLICS
ET DE LA FONCTION PUBLIQUE

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

Spécifications détaillées du mode « portail à portail »

Standard d'interopérabilité entre organismes de la sphère sociale

Réf. : Standard Interops-P1.0_SpécificationsDétaillées
Version 1.0 du 07/10/2008

Référence : **Version :** **Date de dernière mise à jour :**	Standard Interops-P1.0_SpécificationsDétaillées 1.0 07/10/2008
Niveau de confidentialité :	PUBLIC

Table des mises à jour du document

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

SOMMAIRE

1. INTRODUCTION

1.1 Objet du document

Ce document présente les spécifications détaillées du Standard d'Interopérabilité des Organismes de la Sphère Sociale [R1] pour le mode « portail à portail ».

1.2 Relation avec d'autres documents

Ce document dérive et complète le Standard [R1]. Il est aussi prévu de le dériver en autant de documents que d'applications du standard.

1.3 Organisation et structure du document

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

- Le chapitre 2 « **Principes généraux** » présente macroscopiquement le mode portail à portail du Standard d'Interopérabilité des Organismes de la Sphère Sociale
- Le chapitre 3 « **Fonctionnement général** » définit le périmètre des spécifications et apporte des éclairages sur les contraintes d'implémentation du standard,
- Le chapitre 4 « **Lots à développer** » présente les blocs fonctionnels à développer
- Le chapitre 5 « **Lot 1 : Outils d'administration des accords** » décrit les spécifications détaillées du lot concernant les accords d'interopérabilité
- Le chapitre 6 « **Lot 2 : Vecteur et proxy organisme client** » décrit les spécifications détaillées du lot concernant la création du vecteur d'identification, sa propagation du côté de l'organisme client et la propagation des requêtes des utilisateurs finaux
- Le chapitre 7 « **Lot 3 : Vecteur et reverse-proxy organisme fournisseur** » présente les spécifications détaillées du lot concernant la réception, la manipulation du vecteur d'identification du côté de l'Organisme Fournisseur et traitement des requêtes provenant des organismes clients
- Le chapitre 8 « **Lot 4 : Traces** » représente les spécifications détaillées du lot concernant l'enregistrement et l'analyse des traces.
- Le chapitre 9 « **Annexes** » rassemble les annexes de ce document

1.4 Références

1.4.1 Documents internes

	Référence	Titre	Auteur	Ver.	Date
[R1]	Standard Interops1.0_SpecificationsFonctionnelles	Spécifications fonctionnelles	Groupe de travail Interops	1.0	07/10/2008
[R2]	Standard Interops1.0_SpecificationsVI	Spécifications du Vecteur d'Identification	Groupe de travail Interops	1.0	07/10/2008
[R3]	Standard Interops1.0_ConventionTechnique	Convention technique	Groupe de travail Interops	1.0	07/10/2008

1.4.2 Documents externes

	Titre	Auteur	Date
[SAMLCore2]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0	Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve, eds.	15/03/2005
[SAMLAuthnCxt]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0	J. Kemp et al.	15/03/2005
[SAMLProf]	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0	S. Cantor et al.	15/03/2005
[SAMLBind]	Bindings for the OASIS Security Assertion Markup Language	S. Cantor et al.	15/03/2005
[XMLDsig]	XML-Signature Syntax and Processing	Eastlake, Donald, Reagle, Joseph, Solo, David, eds.	12/02/2002
[TLS]	RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1	T. Dierks, E. Rescorla	Avril 2006
[HTTP1.0]	RFC 1945 - Hypertext Transfer Protocol -- HTTP/1.0	T. Berners-Lee, R. Fielding, H. Frystyk	Mai 1996
[HTTP1.1]	RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1	R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee	Juin 1999

1.5 Conventions

Sauf indication contraire, toutes les spécifications précisées par ce document sont OBLIGATOIRES (« MUST »).

2. PRINCIPES GENERAUX

Le standard d'interopérabilité entre les organismes pour le mode « portail à portail » repose sur deux principes :

- L'utilisation de SAML 2.0 [SAMLCore2] pour la transmission du vecteur d'identification
- La mise en coupure d'un proxy et d'un reverse-proxy pour la sécurisation des flux entre les deux organismes

Cette solution permet de répondre aux exigences émises par les OPS :

- 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 »

2.1 Cas d'usage de SAML 2.0

Le profil Web SSO sur POST de SAML 2.0 [SAMLProf] a été adopté par les différents OPS pour transmettre le vecteur d'identification dans le mode « portail à portail ». Les exigences et recommandations du standard SAML 2.0 sont à suivre sauf mention contraire dans ce document.

Le Web SSO sur plusieurs domaines est le cas d'usage le plus important et le plus courant de SAML 2.0 (cf. Figure 1). Il permet à un utilisateur final de s'authentifier sur son espace de confiance primaire, l'organisme client, et d'accéder à une ressource appartenant à un espace de confiance secondaire, l'organisme fournisseur, sans avoir à se réauthentifier. Un vecteur d'identification est utilisé pour transmettre à l'organisme fournisseur les informations relatives à l'utilisateur, comme son identité, ses PAGM, etc.

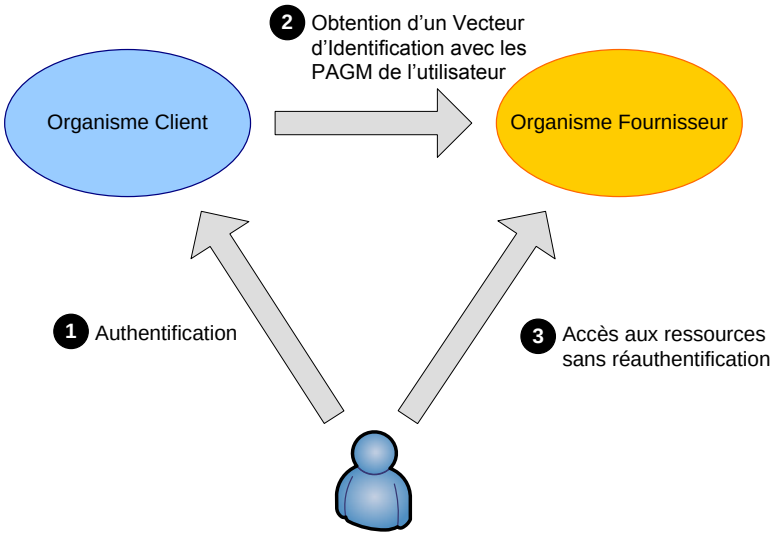


Figure 1 : Cas d'usage du Web SSO SAML 2.0

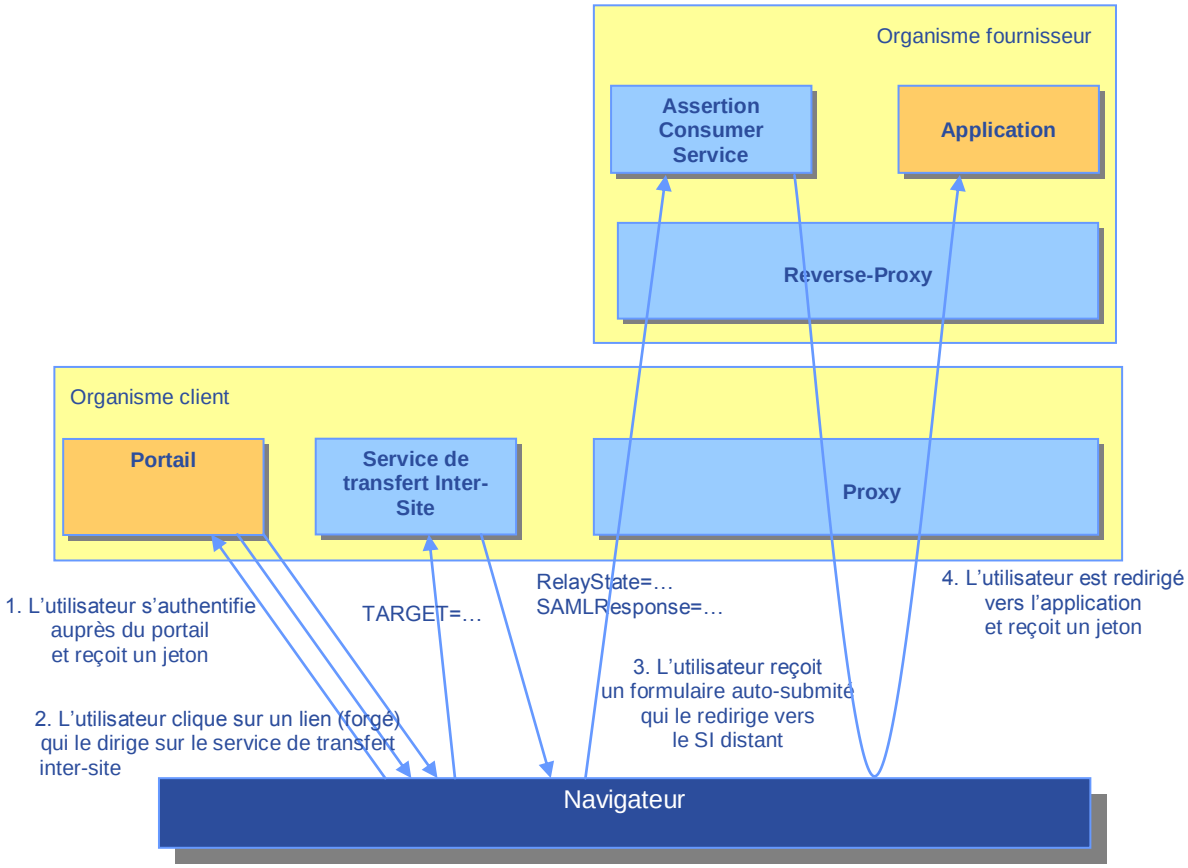
Les échanges SAML sont donc uniquement utilisés à la première connexion de l'utilisateur sur l'application. On distinguera alors les échanges lors de la première connexion de l'utilisateur des échanges lors des transactions effectuées dans la même session.

L'accord passé entre l'organisme client et l'organisme fournisseur vaut comme accord de fédération implicite. Dans le contexte de sécurité créé par le fournisseur, chaque utilisateur authentifié dans l'espace de confiance possédant un ou des PAGM pourra accéder à des applications de l'organisme fournisseur, conformément à l'accord passé avec l'organisme fournisseur, et aura les habilitations liées à son ou ses PAGM.

2.2 Modélisation des échanges

2.2.1 Echanges à la première connexion

Les échanges à la première connexion à l'application de l'utilisateur respectent le profil Web SSO/POST de SAML 2.0 et sont représentés sur la figure ci-dessous.

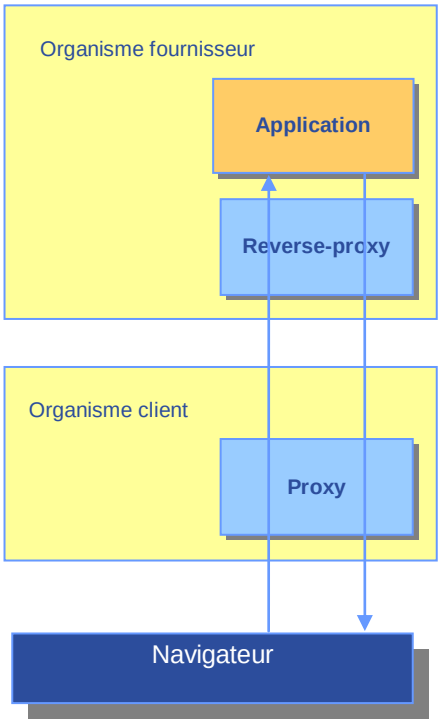


1. L'utilisateur s'authentifie sur un portail situé dans l'organisme client et obtient un jeton d'authentification afin de ne pas se réauthentifier à chaque échange avec le portail. Un lien vers l'application lui est présenté de façon à le rediriger vers le service de transfert inter-site.
2. L'utilisateur clique sur le lien et est dirigé vers le service de transfert inter-site avec en paramètre le service visé.
3. Le service de transfert inter-site intègre toute la logique SAML côté organisme client. Il retourne un formulaire web au navigateur, auto-soumis par JavaScript :
   - Le paramètre « action » du formulaire contient l'URL de l'Assertion Consumer Service de l'organisme fournisseur dans l'espace de nommage de l'organisme client
   - Le champ caché « SAMLResponse » contient une réponse SAML (qui joue le rôle de vecteur d'identification) encodée en base64 (cf. [R2])
   - Le champ caché « RelayState » contient l'URL du service visé

   La communication entre le navigateur de l'utilisateur final et l'Assertion Consumer Service traverse le proxy de l'organisme client et le reverse-proxy de l'organisme fournisseur, de manière transparente pour l'utilisateur.
4. L'Assertion Consumer Service intègre toute la logique SAML côté organisme fournisseur. Il vérifie les données contenues dans la réponse SAML et crée un contexte de sécurité pour l'utilisateur. Finalement, l'utilisateur est redirigé vers l'application et reçoit un jeton d'authentification propre à l'organisme fournisseur.

2.2.2 Echanges de transaction

Les échanges de transaction effectués après la première connexion de l'utilisateur final à l'application sont représentés sur la figure ci-dessous :



L'utilisateur est déjà reconnu par l'application. Toutes les requêtes et les réponses de l'application transitent par le proxy de l'organisme client et le reverse-proxy de l'organisme fournisseur.

2.3 Vecteur d'identification

Les spécifications du vecteur d'identification pour le mode portail à portail sont décrites dans le document [R2].

3. FONCTIONNEMENT GENERAL

3.1 Architecture générale

Une architecture fonctionnelle qui respecte le standard d'interopérabilité comprend plusieurs composants qui sont largement indépendants. L'implémentation des composants doit prendre en compte les besoins et contraintes de l'environnement existant au sein des organismes.

3.1.1 Découpage fonctionnel modulaire

Une architecture fonctionnelle respectant le standard se décline autour des points suivants :

- L'administration des accords d'interopérabilité
- La manipulation des vecteurs d'identification côté organisme client
- La fonction de proxy côté organisme client
- La manipulation des vecteurs d'identification côté organisme fournisseur
- La fonction de reverse-proxy côté organisme fournisseur
- La gestion des traces

En termes de blocs fonctionnels en vue d'une implémentation du standard, ces éléments sont réorganisés en quatre lots dans les chapitres suivants.

3.1.2 Eléments génériques et spécifiques

Chaque lot à développer comprend une liste de modules fonctionnels. Ces modules sont de deux ordres du point de vue des développements :

- Les modules dits génériques dont les fonctions et implémentations sont potentiellement applicables par tous les organismes quelle que soit le domaine applicatif ou les services,
- Les modules dits spécifiques qui se reposent sur les éléments spécifiques des applications ou services en jeu (exemple environnement RNIAM ou environnement Retraite). Ces modules dépendent donc fortement de l'environnement SI de l'organisme fournisseur.

Dans la suite de ce document le code couleur suivant est utilisé pour les schémas :

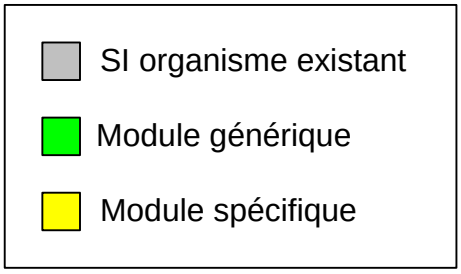


Figure 2 : Code couleur des schémas

Le gris correspond à des éléments existants des systèmes d'information ou à des éléments externes au sujet exposé dans le schéma.

Le vert clair correspond aux modules génériques.

Le jaune correspond aux modules spécifiques.

Le bleu clair correspond aux éléments hors standard mais à développer (par exemple les applications utilisant le standard).

3.1.3 Boîtes à outils

La mise en œuvre des blocs fonctionnels décrits dans les spécifications détaillées doit répondre à une logique de boîte à outils. En particulier, les implémentations proposées par les développeurs du standard devront permettre le plus possible le choix des organismes quant à l'utilisation ou non de ces blocs fonctionnels.

3.1.4 Schéma d'architecture

L'architecture d'un organisme client est représentée sur la Figure 3.

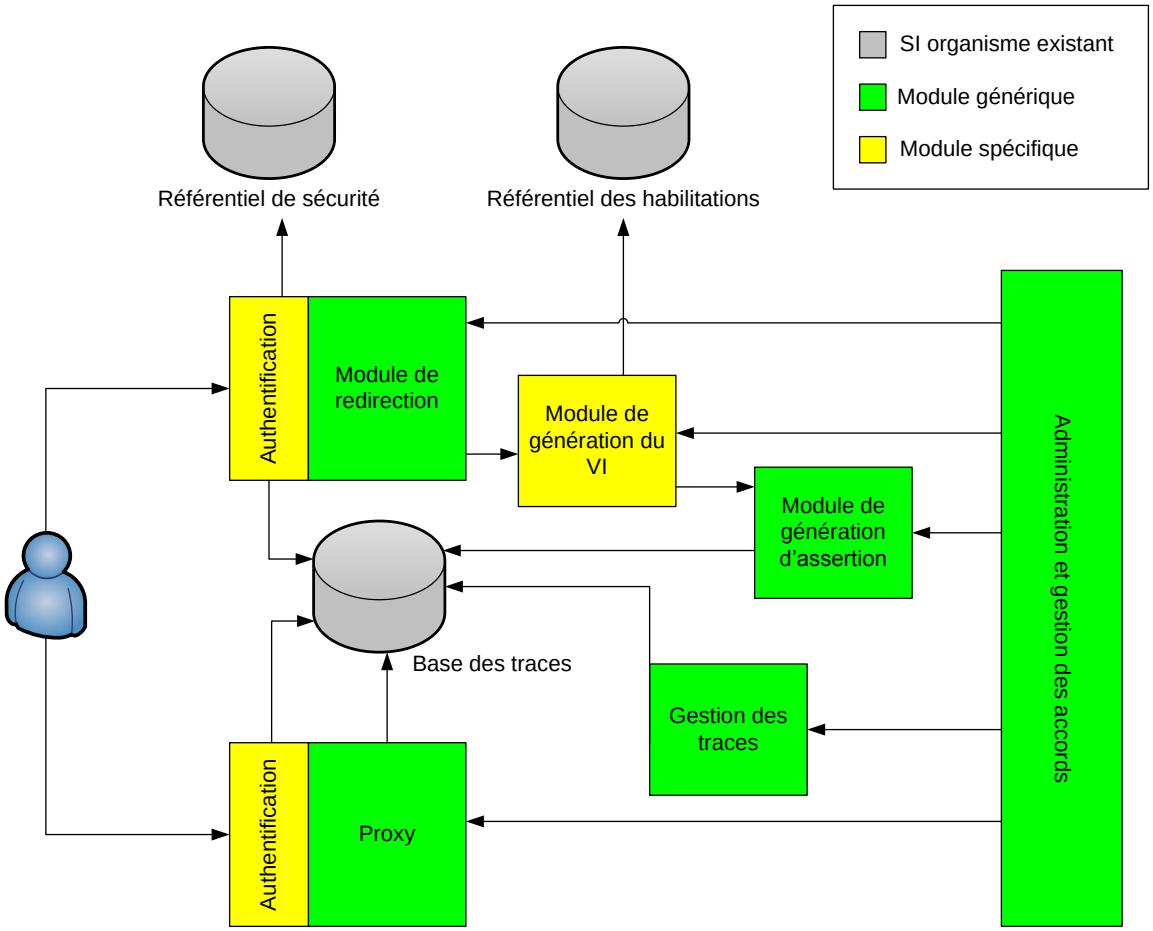


Figure 3 : Architecture générale d'un organisme client

L'architecture d'un organisme fournisseur est représentée sur la Figure 4.

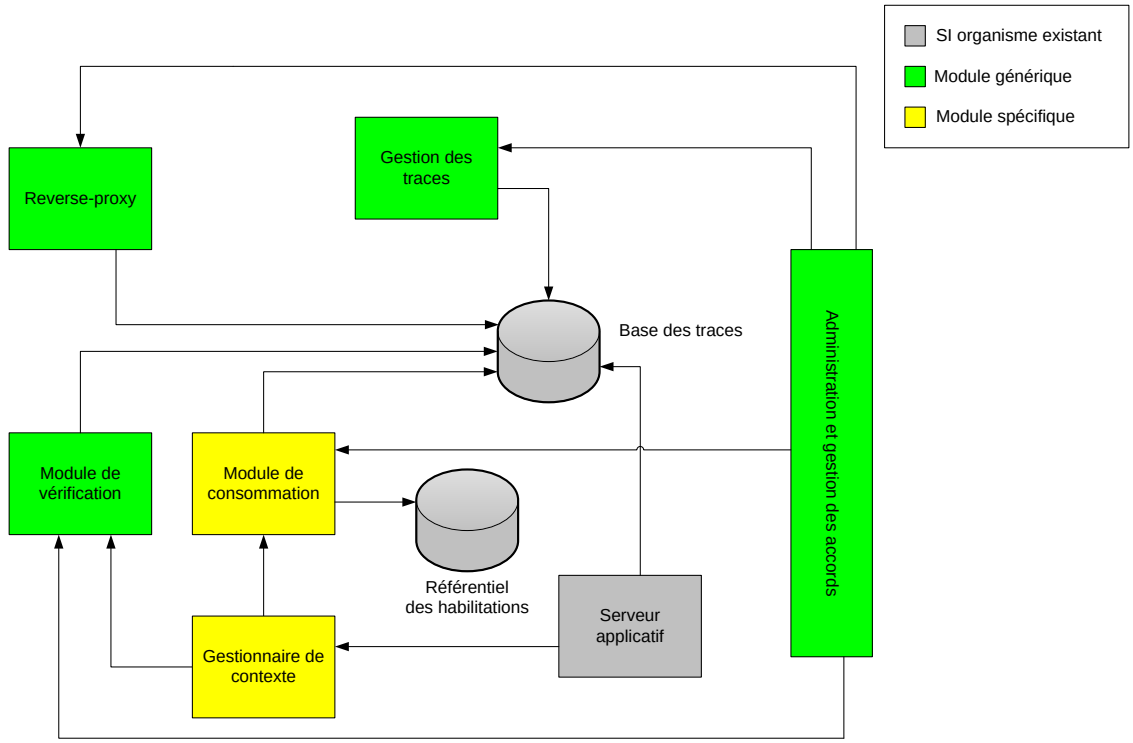


Figure 4 : Architecture générale d'un organisme fournisseur

Une description des éléments d'architecture est faite au paragraphe 3.1.5 p14.

3.1.5 Description des éléments d'architecture

3.1.5.1 Référentiel de sécurité

Le référentiel de sécurité contient les utilisateurs du système :

- Leurs authentifiants (login et mot de passe par exemple)
- Leurs informations relatives (nom, prénom, etc.)

Il est utilisé par le module d'authentification pour authentifier les utilisateurs.

3.1.5.2 Référentiel des habilitations

Le référentiel des habilitations contient les droits des utilisateurs sur des ressources.

Il est utilisé par le module de génération du vecteur d'identification pour calculer les droits d'accès d'un utilisateur final à une application distante, hébergée par un organisme fournisseur, et déterminer ses PAGM.

Il est utilisé par le module de consommation pour déterminer les droits d'accès d'un utilisateur final à une application locale à partir des PAGM présentés.

3.1.5.3 Module de redirection

Le module de redirection permet aux utilisateurs finaux de récupérer un vecteur d'identification et d'être redirigé vers l'organisme fournisseur pour atteindre l'application.

Toute communication avec le module de redirection doit être authentifiée par un module d'authentification.

Le module de redirection doit être capable à partir de l'identité de l'utilisateur et du service visé de fournir les informations nécessaires au module de génération du VI.

Il peut être intégré à un portail qui présenterait les services distants auxquels l'utilisateur a droit.

3.1.5.4 Module de génération du VI

Le module de génération du vecteur d'identification est appelé par le module de redirection.

A partir des informations passées par le module de redirection, il peut élaborer les éléments constituant le VI. Il est en autres responsable de la détermination des PAGM de l'utilisateur à partir du référentiel d'habilitation.

3.1.5.5 Module de génération d'assertion

Le module de génération d'assertion permet de construire l'assertion conforme aux spécifications du standard et à l'accord passé entre l'organisme client et l'organisme fournisseur.

Chaque génération d'assertion est tracée conformément aux accords inter-organismes.

3.1.5.6 Module d'authentification

Le module d'authentification s'appuie sur le référentiel de sécurité pour authentifier les utilisateurs. Il doit transmettre l'identité des utilisateurs aux modules qui en dépendent.

Il peut correspondre à une couche SSO existante chez l'organisme.

Dans tous les cas, il devra au minimum tracer les authentifications réussies et échouées et les éléments associés :

- Identifiant de l'utilisateur
- Date
- Méthode d'authentification

Un module d'authentification est intégré au module de redirection et au proxy

3.1.5.7 Proxy

Le proxy permet aux utilisateurs, après authentification, de communiquer avec l'application hébergée par l'organisme fournisseur. Il se place ainsi en coupure de la communication entre l'utilisateur et l'organisme fournisseur et peut tracer les URL d'accès de l'utilisateur.

Il réalise une authentification mutuelle avec le reverse-proxy de l'organisme fournisseur (cf.3.1.5.12) de manière à certifier l'origine du flux HTTP.

3.1.5.8 Administration et gestion des accords

L'administration doit permettre d'appliquer les accords passés entre les organismes :

- Configuration des certificats de signature
- Configuration des certificats d'authentification client et serveur
- Configuration du format du VI pour un service donné :
  - Configuration de la version de l'accord
  - Configuration des identifiants des organismes et de leurs formats
  - Configuration des PAGM possibles

- Configuration de la durée de validité des assertions
- Configuration des attributs supplémentaires nécessaires

- Déclaration des services visés
- Configuration de la politique de traces
- Etc.

Bien qu'ici toutes les fonctions soient regroupées, pour des raisons techniques, l'interface d'administration pourra être découpée par module à administrer (les traces, le proxy, etc.).

Ce module ne permet cependant pas d'attribuer les habilitations aux utilisateurs finaux.

3.1.5.9 Gestion des traces

Le module de gestion des traces permet d'administrer la politique de trace conformément aux accords inter-organismes et doit permettre de :

- Appliquer la politique de trace conformément aux accords inter-organismes.
- Consulter les traces / effectuer des recherches multicritères
- Archiver les traces
- Effacer les traces expirées (automatiquement ou manuellement)
- Consolider des traces suites à une demande
- Préparer une demande de rapprochement en fournissant une liste d'identifiants de PAGM
- Etc.

3.1.5.10 Module de vérification

Le module de vérification permet de vérifier la conformité d'une assertion SAML aux accords :

- Identifiants utilisés
- PAGM employés et autres attributs présents
- Version de l'accord
- Certificat de signature employé
- Validité de la signature
- Etc.

3.1.5.11 Module de consommation

Le module de consommation permet de traduire une assertion SAML transmise par un organisme client en un contexte de sécurité utilisable par l'application.

Par exemple, Il est chargé de

- Identifier l'utilisateur
- Traduire les PAGM contenus dans l'assertion en un profil applicatif avec les habilitations correspondantes.

Le module de consommation doit tracer la traduction des informations contenues dans une assertion SAML dans le contexte de sécurité afin de faire le lien entre l'assertion SAML et l'identité locale à l'organisme fournisseur.

3.1.5.12 Reverse-proxy

En plus d'une fonction de sécurité évidente de protection du SI, le reverse-proxy authentifie le flux entrant et vérifie les habilitations d'accès d'un organisme client.

Il se situe donc en coupure d'un utilisateur final et de l'application.

3.1.5.13 Base des traces

La base des traces contient les traces. Elle est alimentée par les différents composants intervenant dans les échanges inter-organismes :

- Proxy
- Reverse-proxy
- Module de génération d'assertion
- Module de vérification
- Module de consommation
- Serveur applicatif

Elle est accédée en lecture par le gestionnaire de trace.

3.1.5.14 Serveur applicatif et application

Le serveur applicatif contient l'application.

Il est capable en sus des traces d'audit de tracer l'activité d'un utilisateur authentifié, c'est-à-dire possédant un contexte de sécurité.

3.1.5.15 Gestionnaire de contexte

Le gestionnaire de contexte permet de :

- Vérifier les éléments du VI
- Créer un contexte de sécurité à partir des informations du VI
- Associer le contexte de sécurité à un utilisateur final pour le serveur applicatif

3.2 Sécurité des échanges

L'échange des transactions doit respecter plusieurs besoins de sécurité. Pour respecter certains besoins, des moyens cryptographiques sont utilisés :

- Le vecteur d'identification est signé numériquement. La signature numérique est basée sur la cryptographie asymétrique, utilisant les bi-clés numériques {clé publique, clé privée}
- Par ailleurs, les communications entre organismes sont chiffrées et authentifiées par la technique TLS

Les échanges doivent être sécurisés par des moyens classiques tels qu'un filtrage au niveau TCP/IP.

3.2.1 Filtrage TCP/IP

La vérification d'un certificat (cf. §3.2.2) est une opération qui peut être lourde en termes de calcul. Les infrastructures ne mettant en œuvre que cette protection pourraient donc être peu

résistantes à des attaques de type « déni de services » qui tenteraient des connexions avec des certificats clients invalides.

Toutes les communications entre l'organisme client et l'organisme fournisseur sortent de l'organisme client par son ou ses proxys et rentrent par le ou les reverse-proxys de l'organisme fournisseur.

La liste de ces composants avec leur adressage IP et la liste des ports mis en jeu doivent être définies afin d'établir des règles de filtrage. Ces règles pourront être appliquées sur les composants de sécurité périphériques des organismes clients et des organismes fournisseurs, tels que les firewalls.

3.2.2 Utilisation des bi-clés / certificats

Dans le standard, chaque organisme client devra posséder au moins un certificat d'authentification SSL client et un certificat de signature, et chaque organisme fournisseur un certificat d'authentification SSL serveur.

Les scénarios de gestion des certificats n'entrent pas dans les spécifications du standard.

Néanmoins, chaque organisme devra être à même de vérifier la validité du ou des certificats de son partenaire.

La vérification d'un certificat comprend la validation des points suivants :

- La date de validité du certificat est correcte
- Le certificat a été émis par une chaîne de certification de confiance
- Le certificat n'a pas été révoqué
- L'emploi du certificat correspond bien à l'usage qui en est prévu

> *Le choix du type de gestion de clés n'entre pas dans les spécifications du standard (il concerne l'organisation interne de chaque organisme vis à vis de la cryptographie). Néanmoins, l'application du standard implique pour les organismes de mettre en œuvre les clés pour la signature des vecteurs d'identification et le chiffrement des échanges, et par conséquent de protéger ces clés.*

3.2.3 Protection du vecteur d'identification

Le vecteur d'identification sera signé numériquement afin d'assurer :

- Un contrôle d'intégrité au moment de la transmission
- Une authentification de l'organisme client
- Une non-répudiation de l'organisme client
- Une valeur probante après archivage

Les organismes doivent donc disposer au moins d'un certificat numérique X.509 de signature à cette fin.

3.2.4 Authentification et confidentialité des échanges

L'authentification mutuelle et la confidentialité des échanges entre les organismes client et fournisseur s'appuient sur les éléments suivants :

- Le protocole TLS
- Le proxy de l'organisme client
- Le reverse-proxy de l'organisme fournisseur

Pour une authentification mutuelle de serveur et de client chaque partenaire doit disposer d'au moins un certificat numérique X509 d'authentification.

Pour garantir un niveau de sécurité suffisant, les implémentations doivent supporter au minimum (cf. [TLS]) :

- TLS 1.1
- AES 128 bits ou 256 bits
- SHA-1

Pour des clés RSA, ceci correspond aux « ciphersuites » suivants :

- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_256_CBC_SHA`

3.2.5 Protection contre le rejeu

Le standard Interops est soumis aux mêmes menaces de rejeu que le standard SAML 2.0.

Les risques associés au rejeu sont :

- Le déni de service
- La connexion frauduleuse

Il est à noter que seuls les agents ou les postes d'un organisme client sont susceptibles de se connecter à un organisme fournisseur ce qui limite les risques de déni de service.

De plus, une séparation stricte de l'Assertion Consumer Service et de l'application permet de limiter l'impact d'une attaque par déni de service

Les mêmes mécanismes mis en place actuellement contre les dénis de service pour protéger les applications peuvent être mis en œuvre pour protéger les éléments liés à Interops-P.

Concernant la connexion frauduleuse, en premier lieu, il est nécessaire d'empêcher le vol des assertions et des authentifiants. Dans le contexte d'Interops, les connexions entre l'organisme client et l'organisme fournisseur sont sécurisés par une authentification mutuelle sur TLS/SSL permettant une protection en confidentialité et en intégrité.

Pour empêcher le vol d'assertion ou d'authentifiants, en fonction des risques identifiés, les connexions internes de l'organisme client entre l'agent et le service de transfert inter-site ou le proxy doivent être sécurisées par TLS/SSL avec authentification afin d'assurer l'authentification des composants et la confidentialité des communications.

Côté organisme fournisseur, un certain nombre de contrôle doivent être mis en œuvre :

- L'organisme fournisseur doit vérifier qu'il est effectivement le destinataire de la réponse SAML en se basant sur l'attribut `Destination` de l'élément `Response`. Ceci empêche le rejeu de la réponse dans un autre domaine
- L'organisme fournisseur doit vérifier que le service visé est bien celui inclus dans le VI pour éviter de rejouer l'application sur une autre application du domaine.
- L'organisme fournisseur doit vérifier la validité temporelle (attributs `NotBefore`, `NotOnOrAfter`) des assertions. Cette validité doit être la plus courte possible pour minimiser la fenêtre de rejeu d'une assertion
- L'organisme fournisseur peut vérifier qu'un VI n'est pas retransmis en se basant sur son identifiant
- La signature du VI doit évidemment être vérifiée son intégrité et son authenticité. Ceci prévient de toute modification du VI et être rejoué.

3.3 Éléments techniques représentant les accords

La mise en place d'échanges de données entre deux organismes fait l'objet d'un accord (au travers de la convention telle que définie dans le standard). Cet accord inclut une partie descriptive dans laquelle sont indiqués les paramètres techniques précis de l'accord d'échanges de données.

Le standard défini par ailleurs un schéma XML pour l'échange des éléments techniques de l'accord.

La liste des paramètres techniques de l'accord et la description du schéma XML sont disponibles dans le document « Convention technique » ([R3]).

3.4 Administration

Ce document ne spécifie pas l'administration des éléments qui ne sont pas liés à l'accord d'interopérabilité tels que les serveurs applicatifs, les habilitations, etc.

L'outil d'administration des accords est décrit dans le chapitre 5 p32.

3.5 Interconnexion réseau, adressage et présentation de service

L'accès à un service de l'organisme fournisseur à travers un portail sortant de l'organisme client nécessite de distinguer proprement ces deux points d'accès. En outre, le portail sortant propose une fonctionnalité de présentation de service propre à chaque organisme client.

3.5.1 Interconnexion réseau

L'interconnexion des réseaux ne rentre pas dans le cadre du standard, en dehors d'une contrainte évidente : les services fournisseurs doivent être visibles par les portails/proxys des organismes clients. En d'autres termes, les proxys clients doivent disposer d'une adresse IP au moins visible par le système reverse-proxy du fournisseur et vice-versa.

> ✍ *Ceci ne signifie en aucune façon que les plans d'adressage plus large entre les organismes doivent être mis en commun.*

En prenant en compte le modèle proxy - reverse-proxy défini par le standard, l'adressage d'un service d'un organisme fournisseur par un client pourrait, par exemple, se faire en trois grandes zones :

- Adressage du service par le client selon le plan d'adressage interne à l'organisme client,
- Adressage du service, après translation d'adresse par l'organisme client, selon un plan d'adressage publié dans l'accord d'interopérabilité par l'organisme fournisseur,
- Adressage du service, après translation d'adresse par l'organisme fournisseur, selon le plan d'adressage interne à l'organisme fournisseur

La translation d'adresse se fait à l'intérieur des proxy et reverse-proxy au niveau applicatif.

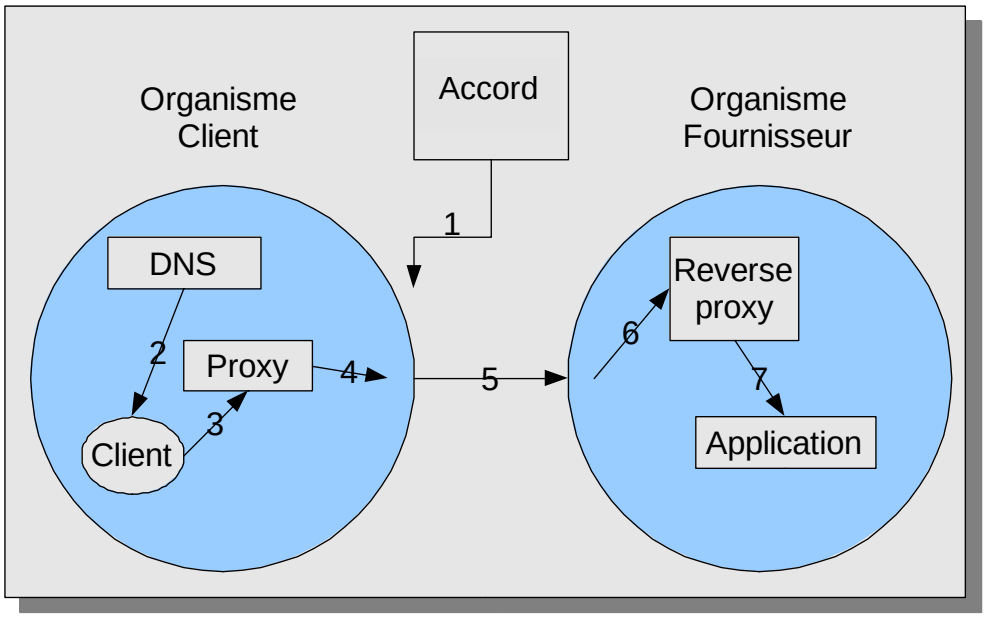


Figure 5 : Principe de communication entre services

Selon cette figure, l'adressage d'un service chez l'organisme fournisseur par un client suit ces étapes :

1. L'accord d'interopérabilité indique quelle est l'adresse affectée au service par l'organisme fournisseur,
2. A la demande du client, le DNS de l'organisme client fournit une adresse interne à l'organisme client,
3. Le client envoie une requête à cette adresse, qui est routée (selon le routage interne à l'organisme client) vers le Proxy, lequel ajoute les informations d'autorisation nécessaire et envoie vers la passerelle externe la requête,
4. La passerelle externe effectue une translation d'adresse entre l'adresse interne affectée au service et celle affectée (adresse publique) par le CPA,
5. Routage vers le point d'entrée de l'organisme fournisseur, une nouvelle translation d'adresse remplace l'adresse publique (adresse IP du reverse-proxy dans l'espace d'adressage de l'organisme client) par une adresse interne à l'organisme fournisseur,
6. Le routage interne de l'organisme fournisseur fait transiter la requête à travers le Reverse Proxy ou le frontal du service visé,
7. Le Reverse Proxy où le frontal du service visé effectue les vérifications nécessaires, transforment les vecteurs d'identification en fonction des besoins du service visé.

Bien que ce principe ne soit en rien imposé par le standard, il permet de montrer qu'une adresse unique est suffisante au client pour atteindre le service de l'organisme fournisseur.

3.5.2 Dénomination de service

Le standard ne spécifie pas de convention de dénomination (DNS) pour les services visés par les accords d'interopérabilité. De manière générale, comme indiqué au paragraphe précédent, l'adressage de service ne nécessite qu'une adresse IP. Toutefois, lors de la mise en place d'accords entre organismes, pour assurer la facilité l'installation et la maintenance des systèmes, il est demandé de suivre les règles suivantes :

- Un organisme fournisseur doit pouvoir gérer l'ensemble de ses services de manière indépendante du nom de ces services et en particulier la répartition sur des machines différentes d'une manière indépendante. Par exemple, le changement de la

répartition de services sur plusieurs serveurs de l'organisme fournisseur ne doit pas changer le nom du service. Cela implique donc un nom DNS par service (pas nécessairement plusieurs adresses),

- Un service visé est nommé par un nom DNS de la forme **service**.**nom-de-domaine-de-l-organisme**. Par exemple, dans le cas du RNIAM, le nom de service peut être de la forme **rniam.cnav.fr**,
- Dans un organisme client, un service est représenté par un portail sortant. Afin d'éviter une infrastructure complexe comme un DNS spécifique ou des plaques réseau avec adressage identique pour le portail, le portail sortant doit être capable au niveau applicatif de récrire des URL, donc les noms de services. Ainsi le portail peut être accédé par l'organisme client sous un autre nom géré par lui-même. Exemple : **portail-rniam.cnamts.fr**.

Le tableau suivant précise les éléments d'adressage, en particulier en ce qui concerne la notion de service :

Nom	Définition/Commentaires
Service	Groupe cohérent de fonctions mis à disposition de l'organisme client par l'organisme fournisseur dans le cadre de l'échange. Le service est nommé par un nom DNS, par exemple **rniam.cnav.fr**.
Service visé	Le service visé se réfère à la fois au service lui même ainsi qu'aux sous-groupes de fonctions de ce service proposé par l'organisme fournisseur dans les accords d'interopérabilité. Ainsi, le service visé est nommé par un nom DNS s'il s'agit du groupe complet (par exemple **rniam.cnav.fr**) ou par le même nom DNS suivi d'un préfixe de chemin s'il s'agit d'un sous-groupe du service (par exemple **rniam.cnav.fr/images** où **/images** est le préfixe de chemin). C'est cet élément que l'on retrouve dans le vecteur d'identification.
Adresse locale organisme client	Le service visé doit être connu par l'application cliente (le navigateur ou l'application web service) par un nom local, ce qui simplifie l'administration de DNS au sein de l'organisme client. Par exemple le service **rniam.cnav.fr** peut être visé par l'application cliente avec le nom **rniam-portail.cnamts.fr**, le portail de l'organisme client se chargera alors de transcrire l'adresse locale en adresse externe.
Adresse externe	Pour un service il s'agit du nom tel qu'il est publié dans les accords d'interopérabilité.
Service publié	Il s'agit du service tel qu'il est publié dans les accords ainsi que de l'ensemble des sous-groupes du service publiés de même dans les accords. Si un sous-groupe de services n'est pas publié, il ne peut pas être un service visé.
URL visée	L'URL complète représentant aussi bien une fonction ou une ressource particulière d'un service que le portail accueillant plusieurs services. Il est important de ne pas confondre service visé et URL visée.

Dans le reste du document il n'est fait référence qu'au service lui-même. Cela inclura autant le service en tant que tel que les sous-groupes du service.

> *La différence faite ici entre le service et ses sous-groupes est importante du point de vue nom-de-service : l'adressage du service ne devant pas imposer chez l'organisme fournisseur une implémentation (en particulier matérielle) de l'accès au service. Néanmoins, du point de vue du standard, cette différence n'a pas d'impact.*

En exemple de dénomination de service, un organisme fournisseur (nommé fournisseur) met à disposition un service (nommé service) composé de, au moins, une fonction (nommée fonction1). Il a alors le choix lors de la publication (la convention) de définir ce service comme :

- Un unique service (**service.fournisseur**) dont tous les PAGM associés doivent être transmis à toute requête dont le nom d'hôte de l'URL est **service.fournisseur**. Il n'y a alors qu'un seul service publié,
- Plusieurs services indépendants (**service.fournisseur** et **fonction1.fournisseur**) : du point de vue d'un organisme client le cas est identique au cas précédent à l'exception des fonctions qui sont ventilées sur deux services distincts. Il y a alors deux services publiés,
- Un unique service (**service.fournisseur**) et un sous groupe (**service.fournisseur/fonction1**). Dans ce cas les PAGM associés dans la convention à la fonction1 doivent être transmis à toute requête dont le nom d'hôte de l'URL est **service.fournisseur** et le préfixe de chemin est **/fonction1**. Toutes les autres requêtes dont le nom d'hôte de l'URL est **service.fournisseur** doivent être accompagnées des PAGM associés dans la convention au service lui même. Il y a alors aussi deux services publiés mais l'un (**fonction1**) sert d'exception en termes d'attribution de PAGM à l'autre service (**service**). Typiquement, un sous-groupe de service peut permettre d'accéder aux images du service en n'étant associé à aucun PAGM (« service gratuit »).

L'organisme fournisseur décide, par exemple, de publier selon le troisième cas (service.fournisseur et service.fournisseur/fonction1). Du point de vue du standard, l'organisme client peut donc *viser* les deux services qu'il trouve dans la convention : **service.fournisseur** et **service.fournisseur/fonction1**. Ce sont les noms que son proxy doit utiliser. Dans son organisation interne, l'organisme client utilise un nommage local pour accéder aux services, par exemple **service-fournisseur.client** et **service-fournisseur.client/fonction1**. Le proxy se charge alors de transcrire les noms locaux en noms externes.

3.5.3 Présentation de service

Le standard prévoit la possibilité de communiquer des éléments textuels pour la présentation dans des menus d'un portail au travers de la convention technique. L'implémentation d'un portail au sein d'un organisme client doit être capable de prendre en compte ces éléments.

La présentation de menus doit être personnalisée pour chaque utilisateur afin de ne présenter aux utilisateurs que les services accessibles selon leur profil et le ou les PAGM nécessaires.

3.6 Gestion des cookies en mode portail à portail

Les cookies sont couramment utilisés pour stocker des informations entre chaque requête du navigateur et ainsi donner un état au protocole de communication HTTP. Ils permettent également le plus souvent de stocker l'identifiant de session de l'utilisateur, même si l'identifiant de session peut également être passé par URL.

Pour des raisons de sécurité, un cookie ne peut pas être accédé ni en lecture ni en écriture à partir d'un autre domaine ou d'un autre « path » que celui pour lequel il a été émis. Le domaine d'un cookie ou son « path » sont deux paramètres de sécurité optionnels que peuvent mettre en place une application. Certains cookies ne possèdent pas de domaine et de « path ». Le navigateur se base sur le nom de la machine (FQDN) pour faire correspondre le cookie avec l'application.

Ainsi, un navigateur se connectant à une URL dans le domaine .cnav.fr pourra recevoir des cookies attachés au domaine .cnav.fr et enverra dans ses requêtes les cookies en sa possession attachés au domaine .cnav.fr. Par contre, le serveur ne pourra pas envoyer des cookies pour un autre domaine, .cnam.fr par exemple, ou lire les cookies du domaine .cnam.fr. Il en est de même pour le paramètre « path », mais en se basant sur la partie relative de l'URL.

Or, les noms de domaine de l'organisme client et de l'organisme fournisseur sont différents. Pour pouvoir placer le proxy de l'organisme client en coupure, le service offert par l'organisme fournisseur est appelé avec le nom de domaine de l'organisme client (cf. §3.5 p20). De plus, les mécanismes que peuvent mettre en place les organismes au niveau des proxys et des reverse-proxys peuvent modifier les URL d'accès, modifiant la partie relative des URL.

Le proxy de l'organisme client devra alors alternativement :

- Assurer optionnellement une traduction des domaines des cookies pour pouvoir être pris en compte par le navigateur de l'utilisateur final
- Assurer optionnellement une traduction des »path » des cookies pour pouvoir être pris en compte par le navigateur de l'utilisateur final

3.7 Gestion des sessions applicatives

Grâce au standard d'interopérabilité, un utilisateur pourra ouvrir une session sur une application externe à son organisme de départ sans avoir à se réauthentifier.

Les mécanismes de propagation de déconnexion d'un utilisateur (Single Logout) proposés par SAML 2.0 ne seront pas utilisés afin de ne pas complexifier les implémentations.

Ainsi, une déconnexion de l'utilisateur sur le portail de l'organisme client n'entrainera pas nécessairement une déconnexion sur les applications hébergées par les organismes fournisseurs auxquelles il aurait accédées.

Si l'utilisateur se déconnecte ou si la session est détruite sur le serveur, la session ne sera invalidée que pour la portée de la session, à savoir un espace de confiance ou un service proposé par un organisme fournisseur.

De même en cas d'expiration de la session, l'utilisateur devra réinitier une connexion à partir de son portail.

Les applications hébergées par l'organisme fournisseur devraient offrir la possibilité aux agents de l'organisme client de se déconnecter et ainsi invalider la session en cours. L'invalidation d'une session doit empêcher toute navigation ultérieure dans l'application à partir du navigateur de l'agent sans réauthentification.

3.8 Traces

Les traces peuvent être de deux types :

- Les traces d'audit, qui permettent d'archiver les actions des utilisateurs et de fournir une trace opposable en cas de litige ou contentieux
- Les traces techniques, relatives à chaque composant et permettant les événements techniques

Le standard impose les traces d'audit afin de pouvoir effectuer des contrôles *a posteriori*.

Par la suite, le terme « trace » se référera aux traces d'audit.

3.8.1 Traces d'audit

Etant donné la responsabilité partagée entre l'organisme client et fournisseur, l'accord impose aux deux parties la configuration associée aux traces :

- Les événements à tracer et les éléments constituant les traces propres au standard, et donc communs à tous les accords

- Les événements à tracer et les éléments constituant les traces propres à chaque accord, jugés nécessaires, par exemple en fonction de contraintes légales particulières, ainsi que le cadre d'utilisation de ces traces.
- La durée de conservation des traces

Les événements supplémentaires à tracer, propre à chaque accord peuvent provenir :

- Des modules génériques
- Des blocs techniques propres à chaque organisme

La fonction de traçage décrite dans ce document est, au sein d'un système d'information donné, un des éléments de l'ensemble des traces de ce système. Ainsi, si un vecteur d'identification est tracé, l'identifiant du demandeur, qui est une donnée relative (sur le long terme cet identifiant peut ne plus exister ou être modifié ou affecté à un autre demandeur), peut être rapproché d'autres traces d'audit du système d'information indiquant la signification de cet identifiant. De même un vecteur d'identification contient les habilitations sous forme de PAGM d'un demandeur à un instant donné. D'autres traces d'audit du système peuvent être rapprochées pour déterminer l'historique des habilitations d'un demandeur.

La durée de conservation étant conventionnelle, elle peut varier entre les accords. Les traces propres à chaque accord doivent être séparées ou marquées de manière à gérer des cycles de vie hétérogènes entre les différents accords.

Les présentes spécifications détaillées décrivent :

- La nature des traces de journalisation propres aux modules génériques et spécifiques objet des présentes spécifications détaillées
- Les processus de consolidation des traces
- Un outil de gestion des traces pour l'analyse des traces

> ✍ *Les traces d'audit propres aux blocs techniques hors spectre des présentes spécifications détaillées ne seront pas décrites. Elles devront être listées dans le cadre de la mise en place des accords d'interopérabilité entre organismes.*

3.8.2 Traces techniques

Les traces techniques (ou traces de fonctionnement à but de surveillance technique) concerne le fonctionnement interne des implémentations du standard. Bien que ces traces ne soient pas imposées par le standard lui-même, les besoins de surveillance des systèmes d'information existants nécessitent leur présence et leur compatibilité à leur contexte d'exploitation.

Les traces techniques devront notamment remonter les informations lorsqu'une anomalie survient. Par exemple, les traces techniques disponibles doivent être suffisantes pour déterminer :

- La nature et la gravité d'une anomalie
- Le composant qui a présenté l'anomalie
- Les impacts de l'anomalie (traitements en erreur, messages corrompus et / ou perdus, etc.)
- La date et l'heure de l'anomalie

Ces traces peuvent être utilisées dans des opérations de supervision, pour la création de statistiques ou pour l'analyse de dysfonctionnements, etc.

Les traces techniques ne seront pas décrites dans les présentes spécifications détaillées, parce que fournies par les briques techniques mises en places par le « constructeur » de la solution.

3.9 Gestion des erreurs

Le mode « portail à portail » s'appuie sur HTTP pour le transport des données et l'affichage d'information aux agents. HTTP 1.0 [HTTP1.0] ou 1.1 [HTTP1.1] fournissent un mécanisme permettant de remonter des erreurs. Dans la réponse faite au navigateur, un code de retour obligatoire inclus dans les entêtes HTTP indique l'état de la requête (200 si tout s'est correctement passé, 404 si le fichier n'a pas été trouvé, etc.) et du code HTML permettant d'afficher un texte explicatif.

Les erreurs éventuelles liées au standard s'appuieront sur ces mécanismes. Elles devront être présentées de façon claires afin d'en favoriser rapidement le diagnostique et d'informer l'agent du disfonctionnement du système.

En outre, on respectera les principes suivants :

- Utilisation des codes d'erreur HTTP
- Personnalisation des pages HTML

L'utilisation des codes d'erreur HTTP permet d'intercepter sur chacun des éléments le long de la chaîne du serveur applicatif jusqu'à l'agent l'origine de l'erreur, et éventuellement de la tracer à des fins de diagnostiques ou de statistiques.

La personnalisation des pages d'erreur permettra de faciliter le diagnostique en incluant :

- Une charte graphique propre à l'organisme client ou l'organisme fournisseur de manière à connaître l'organisme à l'origine du problème
- Un texte explicitant l'indisponibilité du système
- Des informations sur l'origine de l'erreur, à communiquer au support de l'agent
- Des informations sur la requête (identifiant du VI, identifiant de ticket ouvert automatique, etc.)

Ces pages d'erreur personnalisées ne peuvent être protégées par un mécanisme Interops ou tout autre mécanisme de contrôle d'accès et doivent se situer dans un espace non sécurisé.

Les éléments situés sur la chaîne et pouvant remonter des erreurs personnalisées liées aux communications avec les autres éléments sont :

- Le navigateur de l'agent (organisme client)
- Le module de redirection (organisme client)
- Le proxy (organisme client)
- Le reverse-proxy (organisme fournisseur)
- Le module de consommation (organisme fournisseur)
- Le serveur applicatif (organisme fournisseur)

Il est laissé par la suite la possibilité d'utiliser différents codes d'erreur, en fonction de la personnalisation possible des composants. En effet, pour certaines implémentations, une simple page HTML est renvoyée pour signaler une erreur avec un code 200 signifiant que tout s'est bien passé. Il est cependant recommandé d'utiliser d'autres codes de manière à détecter et tracer l'erreur sur l'ensemble de la chaîne.

Ces codes d'erreur HTTP sont des codes d'erreur standard. Aucune extension n'est apportée

Un label est utilisé pour apporter des informations supplémentaires quant à l'origine de l'erreur et ainsi différencier les différents types d'erreur. Ces labels sont obligatoires dans le cas où les implémentations ne renvoient que des codes 200.

Ces labels peuvent être transmis à l'utilisateur de manière à orienter son support.

Une description des différentes erreurs liées au standard pouvant être remontés par ces composants est faite ci-dessous. Toute autre erreur liée au service rendu lui-même est à spécifier dans la convention technique [R3].

Dans le cas où le système de trace est défaillant pour l'un des composants de son architecture (par exemple la brique de vérification du VI), le service ne peut être rendu. Une erreur « ServiceUnavailable » doit alors être transmise.

3.9.1 Le navigateur de l'agent

La personnalisation des erreurs au niveau des navigateurs des agents est difficile et ne rentre pas dans le cadre du standard.

Néanmoins, les erreurs pouvant survenir au niveau des navigateurs et pouvant être remontées à l'agent sont :

- Timeout de connexion au module de redirection
- Timeout de connexion au proxy

3.9.2 Le module de redirection

Le module de redirection peut remonter des erreurs dans les cas suivants :

Code HTTP	Label	Description
200 ou 403[1]	FailedAuthentication	Erreur d'authentification de l'utilisateur sur le module de redirection
200 ou 404	invalidService	Service visé inconnu
200 ou 403	AccessDenied	Utilisateur non autorisé ou n'ayant pas les PAGM nécessaires pour le service visé
200 ou 500	ServiceUnavailable	Indisponibilité du module de génération de VI
200 ou 403	ServiceUnavailable	Un des paramètres transmis au module de génération de VI est invalide
200 ou 500	ServiceUnavailable	Module de trace indisponible

Ces erreurs ne sont visibles que de l'intérieur de l'organisme client.

3.9.3 Le proxy

Le tableau suivant décrit les erreurs qui peuvent être remontées par le proxy :

Code HTTP	Label	Description
404	InvalidService	Service visé inconnu
500	InvalidTLSNegociation	Problème lors de l'établissement de la connexion TLS Ce problème peut survenir notamment quand l'un des certificats d'authentification client ou serveur est expirté
502	TimeOutConnexion	Problème de connexion
200 ou 500	ServiceUnavailable	Module de trace indisponible

3.9.4 Le reverse-proxy

Le tableau suivant décrit les erreurs qui peuvent être remontées par le reverse-proxy :

[1] Une authentification qui échoue résulte en un code 401 pour redemander à l'utilisateur de s'authentifier. C'est au bout de plusieurs tentatives (3 par défaut) que le code 403 est renvoyé

Code HTTP	Label	Description
404	InvalidService	Service visé inconnu
200 ou 403	AccessDenied	Utilisateur n'ayant pas les PAGM nécessaires pour le service visé
503	ServiceUnreachable	Le service applicatif est indisponible
500	ServiceUnavailable	Le module de consommation est indisponible

3.9.5 Le module de consommation

Le tableau suivant décrit les erreurs qui peuvent être remontées par le module de consommation :

Code HTTP	Label	Description
200 ou 403	UnsupportedSecurityToken	Le jeton n'est pas supporté
200 ou 403	UnsupportedAlgorithm	L'algorithme de signature ou de chiffrement utilisé n'est pas supporté
200 ou 403	InvalidPagm	Le ou les PAGM présents dans le VI sont invalides ou absents
200 ou 403	InvalidService	Le service visé par le VI n'existe pas ou est invalide
200 ou 403	InvalidIssuer	L'identifiant de l'organisme client présent dans le VI est invalide ou inconnu
200 ou 403	InvalidAuthLevel	Le niveau d'authentification initial n'est pas conforme à la convention
200 ou 403	SecurityTokenUnavailable	Le VI n'a pas été trouvé dans la requête
200 ou 403	InvalidVI	Le VI est invalide
200 ou 403	ExpiredVI	Le VI est expiré
200 ou 403	NotYetValidVI	Le VI n'est pas encore valide
200 ou 403	InvalidIdentifierFormat	Le format de l'identifiant est invalide
200 ou 403	MissingAttribute	Un attribut complémentaire obligatoire n'est pas présent dans le VI
200 ou 403	InvalidAttribute	Une des valeurs des attributs complémentaires est invalide
200 ou 403	FailedCheck	La signature ou le chiffrement n'est pas valide

3.9.6 Le serveur applicatif

Le tableau suivant décrit les erreurs qui peuvent être remontées par le serveur applicatif :

Code HTTP	Label	Description
200 ou 403	FailedAuthentification	Utilisateur non autorisé ou n'ayant pas les PAGM nécessaires pour le service visé
404	InvalidService	Service visé inconnu
200 ou 500	ServiceUnavailable	Composant interne indisponible, le service ne peut être rendu

3.10 Synchronisation temporelle

Pour faciliter le rapprochement des traces, les serveurs des organismes doivent se synchroniser sur un serveur NTP reconnu. Chacun communiquera alors le serveur NTP de

référence choisi. S'il s'agit d'un serveur NTP interne, l'organisme devra préciser quelle méthode est utilisée pour synchroniser ce serveur (GPS, DCF77, etc.).

Dans certains cas, un serveur NTP pourra être mis à disposition par l'un ou l'autre des deux organismes.

Si la synchronisation temporelle des serveurs est obligatoire, le choix du serveur de temps est conventionnel.

4. LOTS A DEVELOPPER

Les développements seront réalisés à travers quatre grands lots :

- Administration des accords, concernant organismes clients et organismes fournisseurs
- Vecteurs et proxy organismes clients, qui concerne la création et l'utilisation des vecteurs d'identification et le traitement des requêtes sortantes
- Vecteurs et reverse-proxy organismes fournisseurs, qui concerne la vérification et la consommation des vecteurs d'identification et le traitement des requêtes entrantes
- Traces, servant à tracer les opérations d'insertion et d'interception des vecteurs d'identification, concernant organismes clients et organismes fournisseurs

Ce découpage en lot respecte une logique fonctionnelle mais n'impose en rien le découpage et l'implémentation à définir par le constructeur / éditeur. Ainsi, un ou plusieurs modules fonctionnels de ces lots peuvent très bien être implémentés en un ou plusieurs modules logiciels indifféremment.

Le constructeur / éditeur s'attachera cependant à respecter le principe de « boîte à outils » exposé précédemment.

4.1 Lot 1 : Administration des accords

Les outils d'administration des accords ont pour objectif de fournir un moyen d'alimenter les autres modules en éléments de configuration (liste de PAGM, URL, certificats,…) de façon automatisée. Il s'agit des éléments fonctionnels suivants :

- Outil de création des accords, il permet de récapituler dans un format d'échange normalisé les besoins d'un organisme fournisseur et d'un organisme client afin de créer l'annexe technique d'une convention d'interopérabilité,
- Outil de mise en œuvre des accords, il utilise l'accord (l'annexe technique à la convention) pour paramétrer les systèmes des organismes client et organismes fournisseur.

4.2 Lot 2 : Vecteur et proxy organisme client

Le lot 2 décrit les scénarii associés à la création des vecteurs d'identification signés et la transmission des requêtes sortantes :

- Première connexion d'un utilisateur final
- Transactions entre l'utilisateur final et l'application

4.3 Lot 3 : Vecteur et reverse proxy organisme fournisseur

Le lot 3 décrit les scénarios associés à la vérification et la consommation des vecteurs d'identification, ainsi que le traitement des requêtes entrantes :

- Première connexion d'un utilisateur final
- Transactions entre l'utilisateur final et l'application

4.4 Lot 4 : Traces

Les traces renforcent la confiance en permettant le contrôle à posteriori. Pour remplir cette fonction, le lot Traces est composé de deux modules :

- Module d'enregistrement des traces : il permet d'insérer des traces dans une base
- Outil de gestion de traces : il permet l'analyse des traces et le contrôle à posteriori.

5. LOT 1 : OUTILS D'ADMINISTRATION DES ACCORDS

Ce lot regroupe les blocs fonctionnels (sous forme d'outils) servant à la mise en place des accords. En termes d'implémentation ils représentent essentiellement un format normalisé d'échange de données contenant les éléments de configuration des systèmes de chaque organisme. De ce point de vue, le format d'échange approprié est un format XML.

5.1 Outil de création des accords

5.1.1 Rôle de l'outil

Cet outil a pour objet de créer et modifier des conventions techniques d'interopérabilité entre les organismes client et fournisseur.

Il propose une interface permettant à chaque organisme de déclarer les éléments conventionnels le concernant.

Il produit un fichier au format XML contenant les éléments de paramétrage de l'interopérabilité souhaités par les organismes conforme au schéma défini dans [R4] Convention technique Interops.

Cet outil doit permettre de signer ce document.

Cet outil doit pouvoir valider le document XML, du point de vue de la syntaxe XML et de la conformité au schéma.

5.1.2 Cinématique générique

Pour créer une convention technique, la cinématique générique est la suivante :

- Création d'un nouveau projet dans l'outil
- Remplissage des champs des formulaires de l'outil par un premier organisme à partir des informations en sa possession
- Exportation depuis l'outil de la convention partiellement remplie au format XML spécifié par le standard Interops
- Envoi (mail, etc.) de ce fichier au second organisme
- Importation dans l'outil du fichier de convention XML Interops par le second organisme
- Remplissage des champs des formulaires de l'outil par le second organisme à partir des informations en sa possession
- Exportation depuis l'outil de la convention complétée au format XML Interops
- Exportation éventuelle de la convention dans d'autres formats (HTML, etc.)

5.1.3 Interface d'entrée

5.1.3.1 Éléments constituants une convention technique Interops

Cet outil prend en entrée les informations constituant une convention technique Interops (cf. [R4] Convention technique Interops).

Ces informations peuvent éventuellement être sous la forme de fichiers techniques (certificats).

Ils sont fournis à l'outil par le biais d'une IHM (Interface Homme Machine).

5.1.3.2 Convention technique XML

L'outil peut également prendre en entrée un fichier de convention technique Interops au format XML complet ou partiel.

5.1.4 Interface de sortie

5.1.4.1 Convention technique XML

L'outil permet d'exporter un fichier de convention technique Interops au format XML. Ce fichier a vocation à être échangé et complété par les deux organismes. Il respecte le schéma des conventions Interops sauf dans le cas où le document est incomplet (les éléments obligatoires peuvent ne pas être renseignés par exemple).

La convention au format XML est le fichier des éléments techniques des accords et, à ce titre, est annexée à la convention passée entre les deux organismes établissant les modalités d'interopérabilité.

Ce fichier peut être signé en utilisant le ou les bi-clés / certificats fournis du ou des auteurs. Les moyens utilisés pour générer les bi-clés ou distribuer les certificats de signature et de leurs chaînes de confiance sont hors-scope du standard.

5.1.4.2 Convention technique « lisible »

L'outil doit permettre de générer un fichier de convention technique Interops dans un format « lisible » par un utilisateur (HTML, PDF, etc.).

Cette version lisible des éléments techniques des accords peut également être annexée à la convention passée entre les deux organismes établissant les modalités d'interopérabilité.

5.2 Outil de mise en œuvre des accords

5.2.1 Rôle de l'outil

Cet outil a pour objet de générer les éléments de configuration des différentes briques techniques du système à partir du fichier XML de convention technique Interops.

Il peut également servir à déployer ces éléments dans chacun des deux systèmes d'information client et fournisseur.

5.2.2 Interface d'entrée

Cet outil prend en entrée un fichier de convention technique Interops au format d'échange XML.

Il s'agit ici d'un fichier « complet » conforme au schéma de donnée.

5.2.3 Interface de sortie

L'outil doit permettre de générer, à partir de la convention technique XML, les éléments de configuration des différents modules définis au paragraphe 3.1.5 « Description des éléments d'architecture » et en particulier :

- Module de génération du VI

- Module de génération d'assertion
- Module de vérification d'assertion
- Proxy
- Reverse-proxy
- Base des traces

> *Remarques de sécurité : la mise en place de ces accords ne peut pas être entièrement automatisée. Le traitement doit être coordonné et respecter les contraintes de sécurité de chaque organisme.*

6. LOT 2 : VECTEUR ET PROXY ORGANISME CLIENT

Le déploiement, côté organisme client, des éléments relatifs au vecteur d'identification est composé de trois modules :

- Module de redirection
- Module de génération du VI
- Module de génération d'assertion

Ils ne sont appelés qu'à la première connexion de l'utilisateur sur l'application.

Le module proxy authentifie l'utilisateur final et redirige toutes les requêtes, y compris la première connexion, vers l'organisme fournisseur approprié.

6.1 Première connexion

Le scénario de première connexion est utilisé par l'**utilisateur final** pour initier un contexte de sécurité chez un **organisme fournisseur**. Il est automatiquement déclenché lorsque l'utilisateur final décide d'accéder à une ressource externe à l'organisme client.

Dans ce chapitre, nous ne décrirons que les échanges **internes à l'organisme client**.

6.1.1 Description du scénario

L'utilisateur final, à l'aide d'un navigateur classique, se connecte sur son portail.

Il décide d'accéder à une ressource hébergée par un organisme fournisseur, avec lequel un accord a été préalablement établi.

Il doit pour ce faire se connecter au module de redirection. Cela peut être fait en générant dynamiquement un lien sur un portail contenant en paramètre le service visé (NB : le service visé peut être le portail de l'organisme fournisseur) sur lequel l'utilisateur aurait cliqué. Si l'utilisateur n'est pas déjà authentifié auprès du module de redirection, Il s'authentifie alors.

Il est ensuite redirigé vers l'organisme fournisseur grâce à un formulaire auto-soumis, qui contient le VI.

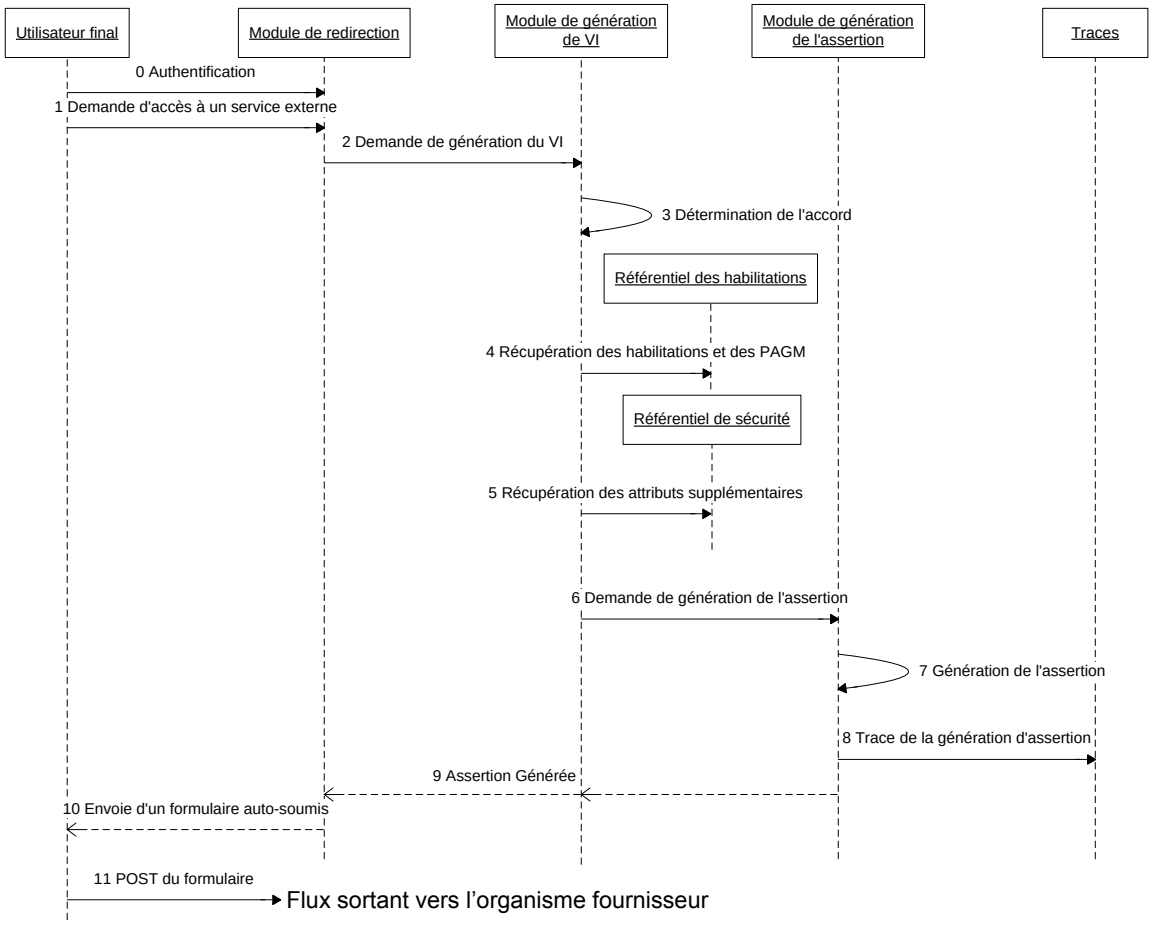
6.1.2 Composants utilisés

Les composants mis en œuvre dans ce scénario sont les suivants :

- Module d'authentification intégré au module de redirection
- Module de redirection
- Module de génération du VI
- Module de génération de l'assertion
- Bases des traces

6.1.3 Diagramme de séquence nominal

Le diagramme de séquence entre les objets identifiés précédemment est le suivant :



0. L'utilisateur final s'authentifie sur le module de redirection. Le module de redirection peut être intégré au portail, auquel cas, l'authentification a déjà été réalisée par le portail.
1. L'utilisateur fait la demande d'accès au service hébergé par un organisme fournisseur. Un identifiant du service visé est passé en paramètre de la demande d'accès. L'identifiant peut être sous forme d'URL, avec l'adresse locale de l'organisme client par exemple.
2. Le module de redirection fait alors la demande de génération du VI. Il passe en paramètre les informations utiles à la génération du VI :
   - L'identifiant local de l'utilisateur final
   - L'identifiant du service visé
   - La méthode d'authentification de l'utilisateur (login/mot de passe, certificat, etc.)
   - La date d'authentification
3. Le module de génération du VI détermine à partir du service visé l'accord et les informations techniques associées :
   - L'identifiant de l'accord et la version en cours
   - Le format de l'identifiant
   - Le niveau d'authentification acceptable
   - Les attributs supplémentaires nécessaires
   - L'identifiant de l'émetteur

4. Le module de génération du VI vérifie à partir du référentiel de sécurité les habilitations de l'utilisateur. Le ou les PAGM sont simplement récupérés ou déduits des habilitations de l'utilisateur.
5. Dans le cas où l'accord précise que des attributs supplémentaires doivent être contenus dans le VI, ils sont récupérés à partir du référentiel de sécurité.
6. Le module de génération du VI demande alors au module de génération d'assertion de générer une réponse SAML
7. Le module de génération d'assertion produit la réponse SAML à partir des éléments fournis par le module de génération du VI et en générant à la volée :
   - Identifiant unique du VI
   - Date d'émission du VI
   - Date de validité du VI
   - Signature
8. Le module de génération de l'assertion trace l'événement
9. Le VI ainsi généré est retourné au module de redirection.
10. Le module de redirection génère alors un formulaire auto-soumis par JavaScript :
    - Le paramètre « action » du formulaire contient l'URL de l'Assertion Consumer Service de l'organisme fournisseur
    - Le champ caché « SAMLResponse » contient une réponse SAML (qui joue le rôle de vecteur d'identification) encodée en base64 (cf. [R2])
    - Le champ caché « RelayState » contient l'URL du service visé
11. Le formulaire est transmis par le navigateur de l'utilisateur final vers l'organisme fournisseur afin de créer un contexte de sécurité associé à l'utilisateur

6.2 Transactions entre l'utilisateur final et l'application

Ce scénario est utilisé systématiquement par l'**utilisateur final** pour chaque échange avec l'organisme fournisseur, y compris le « POST » du formulaire généré à la première connexion.

Dans ce chapitre, nous ne décrirons que les échanges **internes à l'organisme client**.

6.2.1 Description du scénario

L'utilisateur final, à l'aide d'un navigateur classique, se connecte à une URL avec un adressage local.

Le Proxy authentifie l'utilisateur s'il n'est pas déjà authentifié. Pour éviter des authentifications multiples (sur le portail, le module de redirection et sur le proxy), un mécanisme de SSO client ou Web propre à l'organisme client est nécessaire.

L'authentification de l'utilisateur final est utile dans le cas où l'organisme client veut garder les traces des transactions.

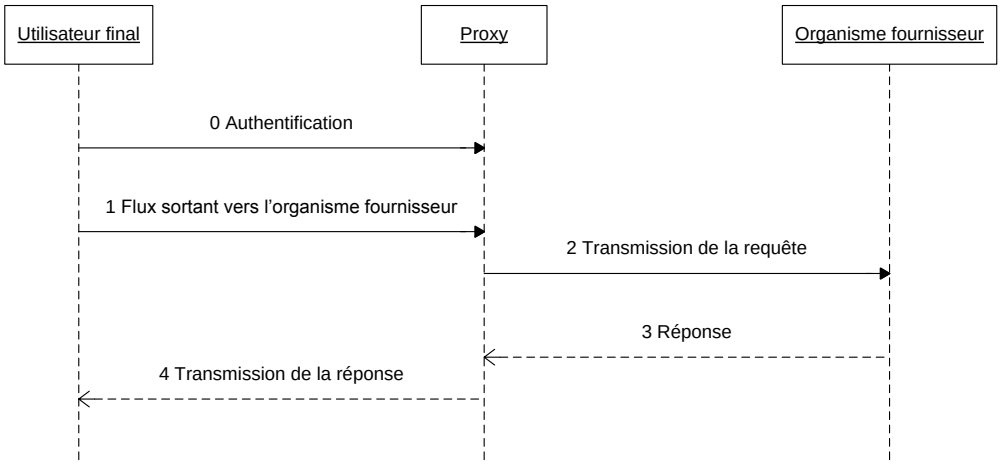
6.2.2 Composants utilisés

Les composants mis en œuvre dans ce scénario sont les suivants :

- Module d'authentification intégré au proxy
- Proxy
- Base des traces

6.2.3 Diagramme de séquence nominal

Le diagramme de séquence entre les objets identifiés précédemment est le suivant :



0. Si l'utilisateur final n'est pas déjà authentifié auprès du proxy, il s'authentifie.
1. L'utilisateur final par le biais de son navigateur transmet sa requête HTTP au Proxy.
2. Le proxy soumet la requête à l'organisme fournisseur après avoir réalisé une authentification mutuelle (TLS).

   Le proxy peut également tracer la requête de l'utilisateur final pour déterminer les accès aux externes.
3. La réponse est envoyée de l'organisme fournisseur au proxy dans le canal TLS sécurisé.
4. Le proxy transmet la réponse au navigateur de l'utilisateur final en effectuant des opérations suivantes :
   - Traduction des noms de machine de l'organisme fournisseur dans le nom local du service dans les entêtes HTTP de redirection (par exemple, `Location`)
   - Traduction du nom de domaine et des « path » des cookies de manière à être traités par le navigateur ou gestion complète des cookies (création, modification ou destruction)
   - Traduction des liens statiques dans les pages de portail (définies dans l'accord entre les deux organismes)

7. LOT 3 : VECTEUR ET REVERSE-PROXY ORGANISME FOURNISSEUR

Le déploiement, côté organisme fournisseur, des éléments relatifs au vecteur d'identification est composé de trois modules :

- Gestionnaire de contexte
- Module de vérification
- Module de consommation

Ils ne sont appelés qu'à la première connexion de l'utilisateur sur l'application.

Le module reverse-proxy authentifie le flux entrant et redirige toutes les requêtes, y compris à la première connexion, vers les composants appropriés.

7.1 Première connexion

Le scénario de première connexion est utilisé par l'**utilisateur final** pour initier un contexte de sécurité chez un **organisme fournisseur**. Il est automatiquement déclenché lorsque l'utilisateur final décide d'accéder à une ressource externe à l'organisme client.

Dans ce chapitre, nous ne décrirons que les échanges **internes à l'organisme fournisseur**.

7.1.1 Description du scénario

A la première connexion, l'utilisateur final est redirigé vers l'organisme fournisseur avec un VI (cf. §6.1 p35).

Le VI est alors vérifié et consommé de manière à créer un contexte de sécurité pour l'utilisateur final.

A la fin du scénario, l'utilisateur est en possession d'un jeton de sécurité et est redirigé vers l'application proprement dite.

Tous les flux entrant et sortant de ce scénario sont soumis aux mêmes règles que les flux de transaction (cf. 7.2 p41) et sont donc authentifiés et chiffrés entre les deux organismes.

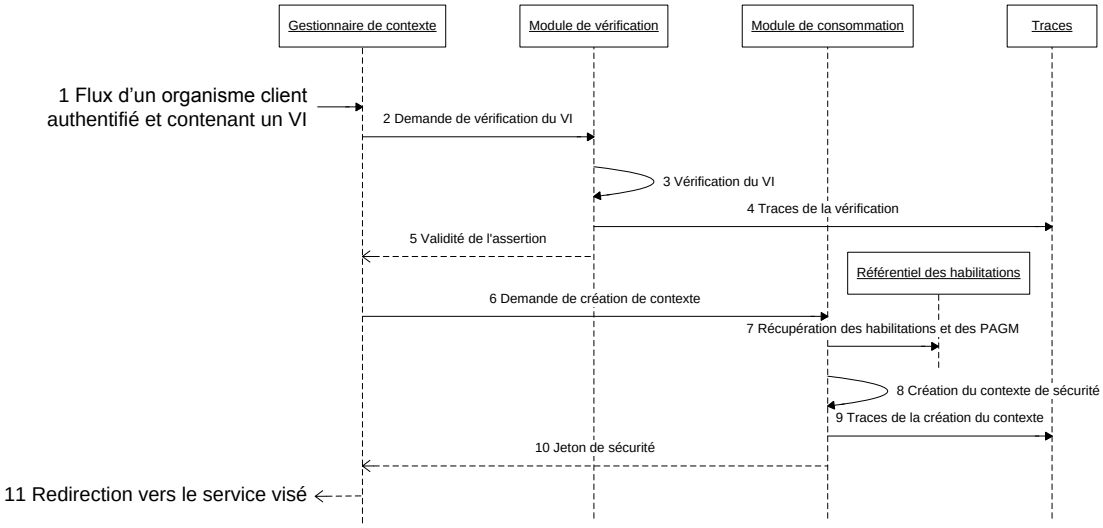
7.1.2 Composants utilisés

Les composants mis en œuvre dans ce scénario sont les suivants :

- Gestionnaire de contexte
- Module de vérification
- Module de consommation
- Bases des traces

7.1.3 Diagramme de séquence nominal

Le diagramme de séquence entre les objets identifiés précédemment est le suivant :



1. Le flux généré par l'organisme client est transmis à l'organisme fournisseur après authentification. Le gestionnaire de contexte récupère la requête POST contenant la réponse SAML.
2. Le gestionnaire de contexte vérifie le VI en transmettant au module de vérification :
   - La réponse SAML
   - Le service visé
   - L'identifiant de l'organisme client (déterminé à partir du certificat d'authentification)
3. Le module de vérification détermine l'accord correspondant à l'échange et vérifie la validité du VI, c'est-à-dire vérifie :
   - Le format de l'assertion (champs obligatoires et format des champs)
   - L'émetteur de la réponse et de l'assertion (par rapport à l'organisme client)
   - La durée de validité de l'assertion
   - Le service visé et les restrictions de l'assertion
   - Le niveau d'authentification
   - La signature de la réponse
   - Etc.
4. La réponse SAML et le résultat de la vérification sont tracés.
5. Le résultat de la vérification du VI est retourné au gestionnaire de contexte. Si la réponse SAML est valide, le traitement peut continuer.
6. Le gestionnaire de contexte demande la création d'un contexte de sécurité en transmettant au module de consommation :
   - La réponse SAML vérifiée
   - Le service visé
   - L'identifiant de l'organisme client
7. A partir des informations contenues dans le VI et notamment les PAGM, le module de consommation détermine le profil avec les habilitations associées
8. Le module de consommation génère un contexte de sécurité avec les informations d'identification de l'utilisateur final dans l'espace de confiance de l'organisme fournisseur
9. La création du contexte de sécurité est tracée.
10. Le module de consommation retourne un jeton de sécurité correspondant au contexte de sécurité

11. Le gestionnaire de contexte redirige l'utilisateur vers le service visé en retournant le jeton de sécurité

7.2 Transactions entre l'utilisateur final et l'application

Ce scénario est utilisé systématiquement par l'**utilisateur final** pour chaque échange avec l'organisme fournisseur, y compris le « POST » du formulaire généré à la première connexion.

Dans ce chapitre, nous ne décrirons que les échanges **internes à l'organisme fournisseur**.

7.2.1 Description du scénario

Toute requête entrante, provenant d'un organisme client avec lequel un accord a été passé, est authentifiée et déchiffrée par le reverse-proxy de l'organisme fournisseur.

Elle est ensuite transmise au serveur applicatif pour traitement. Sa réponse transite ensuite par le même canal sécurisé.

Le serveur applicatif réalise une trace des transactions effectuées sur l'application, avec une granularité conforme aux accords passés avec les organismes.

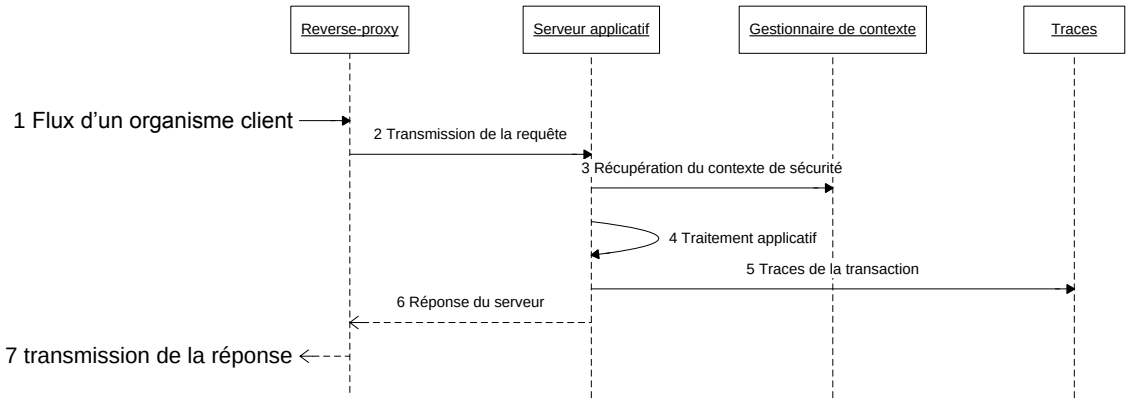
7.2.2 Composants utilisés

Les composants mis en œuvre dans ce scénario sont les suivants :

- Reverse-proxy
- Serveur applicatif
- Gestionnaire de contexte
- Base des traces

7.2.3 Diagramme de séquence nominal

Le diagramme de séquence entre les objets identifiés précédemment est le suivant :



1. Le reverse-proxy de l'organisme fournisseur réceptionne un flux provenant d'un organisme client protégée par TLS :
   - Une authentification mutuelle est réalisée
   - La communication est déchiffrée

   Le reverse-proxy vérifie que l'organisme client est habilité à accéder à l'application, conformément aux accords signés par les organismes.

2. La requête est transmise au serveur applicatif grâce à une traduction de la requête HTTP dans un adressage interne.
3. Le serveur applicatif récupère le contexte de sécurité associé à la requête, grâce au jeton de sécurité attaché. L'utilisateur final est alors identifié, ainsi que ses droits applicatifs.
4. L'application réalise le traitement relatif à la requête.
5. Des traces de la transaction sont conservées, conformément à l'accord passé avec l'organisme client.
6. La réponse du serveur est retournée au reverse-proxy.
7. La réponse est transmise à l'organisme client en utilisant le canal sécurisé, après traduction de l'adressage interne en un adressage public.

8. LOT 4 : TRACES

8.1 Présentation générale

Dans ce chapitre, ne sont présentés que les éléments des traces relatifs au standard.

Les paragraphes 8.1.1 et 8.1.2 présentent les événements et les éléments constituant les traces.

8.1.1 Eléments de traçage côté organisme client

L'organisme client doit tracer dans le cadre de la fourniture de la solution :

- L'authentification de l'utilisateur final
- La génération d'un VI pour l'utilisateur final

La trace d'une authentification de l'utilisateur final doit comporter les éléments suivants :

- Date de l'événement
- Identifiant local à l'organisme client de l'utilisateur final
- Méthode d'authentification
- Statut de l'authentification (échec ou réussite)

La trace de génération du VI doit comporter les éléments suivants :

- Date de l'événement
- Identifiant local à l'organisme client de l'utilisateur final
- Identifiant du service visé
- Identifiant « impersonnifié » de l'utilisateur final, contenu dans le sujet de l'assertion
- Identifiant du VI
- VI transmis, contenant la signature
- Statut de la génération (échec ou réussite)

Optionnellement, l'organisme pourra indiquer les conditions de génération du VI dans les traces : à partir de quel poste ou quel type de poste, de quelle entité de l'organisme, etc.

Les éléments à tracer par les organismes hors cadre de la fourniture de la solution sont ceux nécessaires à l'interprétation des éléments décrits ci-dessus. La liste ci-dessous donne l'ensemble des éléments possibles, à charge pour chaque organisme de définir ceux nécessaires à conserver pour l'interprétation :

- Les mises à jour des définitions de services selon l'accord d'interopérabilité (URI des services, listes de PAGM associés ainsi que niveaux d'authentification requis, dates d'application)
- Dans le cadre de l'administration du système d'habilitation : les attributions de PAGM (identifiant local, niveau d'authentification, identifiant vecteur d'identification, identifiant dépersonnalisé, liste de PAGM attribués, date d'attribution, commentaire)
- Dans le cadre opérationnel, lors de la création d'un vecteur d'identification : les attributions d'autorisations (identifiant local, niveau d'authentification, identifiant vecteur d'identification, identifiant dépersonnalisé, identifiant de l'organisme

fournisseur, URI du service visé, liste de PAGM proposés, liste de PAGM retenus, date d'attribution, commentaire)

- Eventuellement, le traçage du système local concernant l'administration des agents et applications (ajout, modification, suppression d'identifiants agent / application, de même que rôles, niveaux d'authentification et autres informations qui seront utilisés lors de l'attribution des PAGM et autorisations, dates d'application)

8.1.2 Eléments de traçage côté organisme fournisseur

L'organisme fournisseur doit tracer dans le cadre de la fourniture de la solution :

- La réception et la vérification du VI
- La transaction effectuée par un agent

La trace de réception et vérification du VI doit comporter les éléments suivants :

- Date de l'événement
- Identifiant « impersonnifié » de l'utilisateur final, contenu dans le sujet de l'assertion
- Identifiant du service visé
- Identifiant local à l'organisme fournisseur de l'utilisateur final
- Identifiant du VI
- VI reçu, contenant la signature
- Statut de la vérification (échec ou réussite)

La trace d'une transaction doit comporter les éléments suivants :

- Date de l'événement
- Identifiant local à l'organisme fournisseur de l'utilisateur final
- URL de la page
- Action réalisée
- Statut de la transaction (échec ou réussite)

L'Identifiant local à l'organisme fournisseur peut être la représentation de l'utilisateur final dans l'espace de confiance de l'organisme fournisseur. Préférentiellement, l'Identifiant local à l'organisme fournisseur sera égal à l'identifiant « impersonnifié » de l'utilisateur final.

Les éléments à tracer par les organismes hors cadre de la fourniture de la solution sont :

- les mises à jour des associations rôles applicatifs / PAGM (URI service, rôles applicatifs, PAGM, date d'application) –par organisme client (c'est à dire par accord d'interopérabilité),
- les requêtes d'accès (le vecteur d'identification, code résultat des vérifications, code résultat de la requête, date de la requête),
- association entre les PAGM des requêtes d'accès et des rôles applicatifs,
- éventuellement, le traçage du système local (ajout, modification, suppression d'identifiant application, rôles applicatifs / niveaux d'authentification requis, dates d'application).

8.1.3 Sécurisation des traces

Un mécanisme de sécurisation des traces doit être incorporé au module d'enregistrement des traces. Il prémunit contre les risques liés aux modifications à posteriori (quelles que soient les raisons des modifications).

Etant donné les impacts induits par une signature de chaque élément de trace (ex : l'accès à une URL), en fonction des exigences, une protection physique et logicielle d'accès aux traces peut être suffisante.

Dans tous les cas, l'accès aux traces, même en lecture, devra être conservé à des fins d'audit.

La sécurité des traces sera conventionnelle et devra prendre en compte les contraintes opérationnelles de la chaîne complète :

- Gestion des traces sur les différents composants
- Performance des composants
- Etc.

8.1.4 Processus de consolidation

L'intégralité des traces concernant un service ne peut être obtenue que par la consolidation des traces des organismes client et fournisseur. En effet, l'authentification de l'utilisateur final est réalisée par l'organisme client, alors que la transaction est effectuée chez l'organisme fournisseur.

Sans consolidation, chacun des organismes a donc une vue partielle des opérations :

- Un organisme client peut déterminer à quel service accède un utilisateur final sans savoir l'usage qui a été fait du service, ni la durée d'utilisation du contexte sécurisée
- Un organisme fournisseur peut déterminer quels organismes clients accèdent à ses applications sans connaître le nom de l'utilisateur final

La consolidation des traces d'un organisme client et d'un organisme fournisseur peut être à l'initiative d'un organisme client ou fournisseur et reste un événement exceptionnel.

Dans le respect de l'accord, la consolidation consiste en l'échange des traces d'un organisme liées à une assertion.

Concrètement, si un organisme client désire connaître l'activité précise d'un ou des utilisateurs finaux, il fournit à l'organisme fournisseur une liste d'identifiants d'assertion ayant été envoyée à l'organisme fournisseur. L'organisme fournisseur peut en déduire le ou les identifiants locaux et transmettre à l'organisme client les traces de vérification et les traces de transaction.

L'échange d'une assertion permet à l'organisme fournisseur de déterminer l'identifiant local de l'utilisateur (sans connaître sa réelle identité). Il n'est cependant pas possible de discerner les différentes sessions ouvertes. Pour restreindre le résultat de la recherche de transactions effectuées par l'utilisateur, en même temps que la liste d'identifiants d'assertion, l'organisme devra communiquer un intervalle de temps sur lequel sera restreinte la recherche des transactions.

De même, si un organisme fournisseur désire déclarer un comportement suspicieux, il fournit à l'organisme client une liste d'identifiants d'assertion à l'origine du comportement. L'organisme client peut alors déterminer le ou les identifiants des utilisateurs locaux ainsi que les conditions d'authentification.

Le processus de consolidation doit être facilité par l'outil de gestion des traces (cf. §8.3 p46), pour générer les demandes de consolidation ou y répondre.

8.2 Le module d'enregistrement des traces

Le module d'enregistrement des traces doit permettre aux différents modules de réaliser des traces d'audit. Chaque module doit cependant archiver différents événements avec un format également différent, rendant difficile la mutualisation de ce module au niveau des autres composants.

Les traces peuvent cependant être centralisées pour conservation et consultation ultérieure. Ce processus périodique peut alors collecter les différentes traces et les formater pour une exploitation postérieure. Sans contrainte de performance particulière, le module peut :

- Protéger l'intégrité et la cohérence des traces (par une signature)
- Formater les traces et les stocker dans une base commune
- Indexer les traces suivant les différents critères de recherche

8.3 L'outil de gestion des traces

L'outil d'analyse de traces doit être développé pour permettre l'exploitation des traces notamment lors d'un audit approfondi.

Il permet de valider la cohérence interne des traces et permet aussi d'extraire un historique des actions de sécurisation des échanges entre organismes.

Il a les fonctions suivantes :

- Consulter les traces
- Rechercher dans les traces en fonction de critères temporels et / ou de critères basés sur les éléments du vecteur d'identification tels que le service visé, l'identifiant de requérant (utilisateur ou application), de PAGM, etc.
- Vérifier l'intégrité de tout ou partie des traces
- Initier une demande de consolidation de traces en générant une liste d'identifiants d'assertion à partir de certains critères
- Réaliser la consolidation des traces à partir de la liste d'identifiants d'assertion

Les résultats des différentes opérations pourront être rendus selon différents modes de sortie (texte, HTML, PDF) et selon différents médiums de sortie (serveur HTTP, fenêtre graphique, console, fichier, imprimante).

9. ANNEXES

9.1 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
CPA	Collaboration Protocol Agrement
CPP	Collaboration Protocol Profile
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
VI	Vecteur d'Identification
WAP	Wireless Application Protocol
X.509	Norme relative aux certificats à clé publique
XML	eXtented Markup Language

9.2 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	
AES	Advanced Encryption Standard (aussi nommé Rijndael) est un algorithme de chiffrement symétrique.
Agent	Personne physique agissant au sein de la sphère publique de façon permanente ou temporaire et ayant l'un des statuts suivants : fonctionnaire, contractuel, partenaire institutionnel, prestataire, intérimaire ou stagiaire.
Annuaire	Service distribué permettant de localiser les ressources d'un système d'information/une personne et de leur affecter des propriétés/des droits (CTA). Interface donnant accès à des données de références. Ces données représentent des informations techniques ou structurelles auxquelles on accède plus fréquemment en lecture qu'en écriture (PYC).

Terme	Définition
Annuaire de sécurité ou annuaire d'identité	Annuaire du SI dédié au stockage des paramètres de sécurité des différents utilisateurs. Ces paramètres représentent pour ces derniers leurs éléments d'identification, d'authentification et de gestion de droits.
Approche métier	La gestion des habilitations peut s'appuyer sur un modèle dit « d'approche métiers » qui consiste en une approche collective issue de l'analyse des métiers exercés. Les droits d'une personne sont ceux du métier qu'elle exerce et sont identiques à ceux des personnes ayant le même métier.
Architecture logique	Description du système sous forme : ❑ d'une organisation structurée et hiérarchique des fonctions internes du système (fonctions, sous fonctions, composants logiques) et du couplage entre ces fonctions et l'environnement (vue statique) ❑ des flux de données et de contrôle entre ces entités logiques définissant le séquencement de leur exécution (vue dynamique). Cette description réalise les exigences fonctionnelles et les exigences de performances.
Architecture physique	Description d'un système, sous forme d'un ensemble d'organes matériels et de leurs interactions, constituant la solution traduisant l'architecture fonctionnelle et satisfaisant les exigences [IEEE1220]
Attribut	Qualificateur d'un individu, d'un rôle ou d'un objet (par exemple : adresse, âge, profession, fonction d'une organisation, etc.).
Autorisation	Mécanisme qui, à partir du vecteur d'autorisation, accorde ou non, à un utilisateur, l'accès à des applications, fonctions ou données spécifiques, en s'intéressant à des couples « objet, actions, conditions »
Authentification	Terme informatique pour l'opération d'identification réalisée par un processus informatique. Les principaux moyens d'authentification sont : ❑ mot de passe ❑ clé symétrique ❑ certificat ❑ biométrie
Base 64	Système d'encodage en caractère imprimable ASCII (26 lettres minuscules + 26 lettres majuscules + 10 numériques + 2 caractères variables) de toute donnée numérique. Les deux caractères variables varient en fonction des systèmes. Ainsi pour le format MIME il s'agit de « + » et « / », pour les paramètres URL il s'agit de « * » et « - »,…
C-D	
Certificat	Fonctionnellement, un certificat se définit comsme un objet informatique logique lié à une entité. Fonctionnellement, il s'agit d'une clé publique signée par une Autorité de Certification. L'ensemble bi-clé/certificat permet d'utiliser des fonctions cryptographique (cryptographie assymétique) permettant

Terme	Définition
	des opérations d'authentification et de signature numérique. ,
client réseau banalisé	Application logicielle de consultation et de traitement du contenu des pages Web accessibles à l'utilisateur. Par exemple : un navigateur Web tel que Netscape ou Internet Explorer ou une interface WAP.
Composant	Module logiciel ou matériel participant à la cohérence d'un dispositif plus vaste (services socle, services applicatifs, services réseaux, par exemple) Par exemple : ❑ un serveur web, un serveur d'application, un annuaire LDAP, une base de données sont des composants techniques logiciels ❑ un poste de travail, une machine serveur, un PC sont des composants techniques matériels certains composants tels qu'un pare-feu, un routeur, un Proxy, un antivirus ou un antispam peuvent être des composants logiciels ou matériels.
Contrôle d'accès	Principe ou dispositif de sécurité vérifiant l'identité et les droits associés à une entité en termes d'usage des services du système d'information.
Cookie	Petit fichier implanté sur le poste client et utilisé comme marqueur pour suivre le cheminement d'un utilisateur sur un site Web. Lorsque l'internaute retournera visiter ce même site, le serveur pourra alors récupérer les informations contenues dans ce fichier. Les cookies sont surtout utilisés à des fins statistiques et pour conserver le profil d'un internaute.
Cookie de session	Contrairement au cookie, pour des raisons de sécurité, un cookie de session est gardé dans la mémoire du navigateur. Ainsi, dès que le navigateur est fermé, le cookie de session est détruit. Il permet donc de stocker des informations temporaires, le plus souvent relative à une session ouverte sur une application, c'est-à-dire relative au processus en cours ou à l'authentification de l'utilisateur
Droit	Un droit correspond à l'habilitation d'un métier dans une application et se compose d'un ou plusieurs groupes d'actions unitaires.
E – F	
Entité	Elément accédant aux ressources d'une application : exemple : personne ou application
Espace de confiance	Ensemble de composants fonctionnels et techniques permettant de fournir à une personne les outils et les ressources nécessaires pour effectuer des opérations et des transactions électroniques. Un espace est dit de confiance quand il répond à des critères de sécurité considérés comme suffisants par la Maîtrise d'Ouvrage concernée.
Espace de travail	Ensemble d'interfaces, d'outils et de données permettant à l'utilisateur de réaliser des opérations et des transactions sur des

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

Terme	Définition
	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.
Jeton d'authentification	Un jeton d'authentification est délivré à un utilisateur après qu'il se soit authentifié. Il peut être valable pour un serveur uniquement ou un espace de confiance entier (par l'utilisation d'une solution de SSO). Il doit être gardé strictement par l'utilisateur car il matérialise le contexte de sécurité créé au niveau du serveur ou de l'espace de confiance. Un jeton d'authentification peut être un cookie de session contenant un identifiant de session sur un serveur.
Load balancing (répartition de charge)	Technique consistant à distribuer le travail à effectuer sur plusieurs machines, en particulier sur plusieurs serveurs. Cela permet de faire face plus efficacement aux grosses variations d'activité.
Métier	Ensemble d'opérations à réaliser répondant à un noyau commun pour une activité donnée au sein de l'organisme. Le métier se situe à un niveau plus élevé que les droits au sein des applications informatiques. Il couvre l'ensemble des droits accès de toutes les applications.
Objet métier	Unité structurée et limitée conçue pour représenter les processus et les connaissances d'un métier en particulier (souvent dans une application).
Organisme	Entité organisationnelle pouvant correspondre à une mairie, une entreprise, un ministère, etc.
P – R	
Personnalisée (diffusion)	Les éléments de personnalisation tels que l'accès aux services et la présentation de l'espace de travail sont définis par des règles s'appuyant sur les informations des utilisateurs (son profil notamment). Ces éléments ne sont pas modifiables par l'utilisateur.
Personnalisable (diffusion)	L'utilisateur peut modeler (par l'intermédiaire du service de personnalisation) le contenu et sa présentation en choisissant explicitement parmi une sélection d'option ses services et ses préférences.
Profil	On ne retiendra pas cette notion qui : ❑ Recopie le rôle ou l'ensemble (rôle + attributs) ❑ Peut définir un profil applicatif ❑ Pourrait correspondre au terme anglais « role »
Profil applicatif (PA)	Identifiant permettant d'attribuer des droits dans le cadre de l'accès aux ressources d'une application
PAGM Profil Applicatif générique métier	Profil défini en commun par les fournisseurs d'applications qui caractérise de manière générique un groupe de permissions représentant des actions sur une ressource applicative.Un PAGP pourra être mis en relation d'un ou plusieurs profils applicatifs d'une application.
Prestataire de service de certification	*Acteur offrant des services de certification.*
Propagation des identités et des droits	Transfert, échange des informations relatives au profil entre applications, services et autres entités (utilisation de carte de vie quotidienne, inter-administration, identités accord-Education, liaison sco-sup ...).

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

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

Terme	Définition
	spam, antivirus).
Single Sign-On (ou authentification unique)	Concept consistant à permettre à un utilisateur d'accéder à des services numériques différents en ne devant s'authentifier qu'une seule et unique fois. On parle par exemple de propagation de l'identité entre le portail et une application qui permet de ne pas redemander l'identifiant et le mot de passe. (cf. propagation des identités et des droits).
Socle technique	Terme utilisé pour définir les éléments techniques du socle de services minimum. Typiquement, les serveurs, les logiciels sont des éléments techniques.
SSO client	Outil placé sur le poste permettant de reconnaître les fenêtres d'authentification et de les renseigner automatiquement. Le magasin contenant les authentifiants est le plus souvent lui-même protégé par une passphrase. Une fois le magasin ouvert, les authentifiants pour les services visés ne sont plus demandés
SSO Web	Composant situé sur les serveurs Web communs à un espace de confiance de manière à ne s'authentifier qu'une seule fois sur l'un des serveurs de l'espace
Stockage	Action d'enregistrer sur un support numérique en vue d'une utilisation ultérieure. [*Petit Robert*]
Système d'information	Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.
U – W	
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
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).

1278
1279