Etude comparative des solutions de sécurité Open Source existantes pour la mise en œuvre du standard

Version 1.0

ON-X S.A. *est une société du* ***Groupe ON-X***
15, quai Dion Bouton – 92816 PUTEAUX cedex. Tél : 01 40 99 14 14 – Fax : 01 40 99 99 58.
SA au capital de 3 752 000 Euros. RCS Nanterre B 391 176 971. Siret 00037. Code APE 721 Z.
www.on-x.com

Identification et historique

Identification client

Référence client	CCTP 0592110
Interlocuteur	Thierry LAHALLE – thierry.lahalle@sante.gouv.fr
Interlocuteur	Michel JANIN – michel.janin@cnav.fr

Identification ON-X

Référence ON-X	2005-1001-006
Version	1.0
Date	03/04/2006
Nombre de pages	34
Interlocuteur	Olivier Chapron – Directeur du projet – Consultant Manager 01 40 99 14 14 – olivier.chapron@edelweb.fr
Interlocuteur	Patrick Vigneras – Chef de projet 01 40 99 14 14 – pvigneras@on-x.com

Visa

Fonction	Nom
Rédaction	Patrick VIGNERAS
Vérification	Peter SYLVESTER
Approbation	Olivier CHAPRON

Historique

Date	Auteur	Version	Objet
10/01/06	PVS	0.1	Création du document, version préliminaire
13/02/06	PVS	0.8	Révision interne
21/02/06	OCN	0.9	Version pré-finale à diffuser
07/03/06	PVS	0.99	Révision finale
03/04/06	OCN+PSR +PVS	1.0	Version finale approuvée formellement

Références

Identifiant	Titre
R1	Standard d'interopérabilité inter-organismes – *Olivier CHAPRON, Peter SYLVESTER – version 1.0 (13 juillet 2005)*
R2	http://www.ssi.gouv.fr/fr/
R3	Spécifications détaillées et de mise en œuvre (Réf. 2005-1001-001) – *Patrick Vigneras*
R4	Application des Spécifications détaillées pour le RNIAM, architecture WebService (Réf. 2005-1001-003) – *Patrick Vigneras*
R5	Application des Spécifications détaillées pour le RNIAM, architecture Portail à Portail (Réf. 2005-1001-004) – *Patrick Vigneras*
R6	Application des Spécifications détaillées pour la Retraite, architecture Portail à Portail (Réf. 2005-1001-005) – *Patrick Vigneras*

TABLE DES MATIERES

1. Introduction

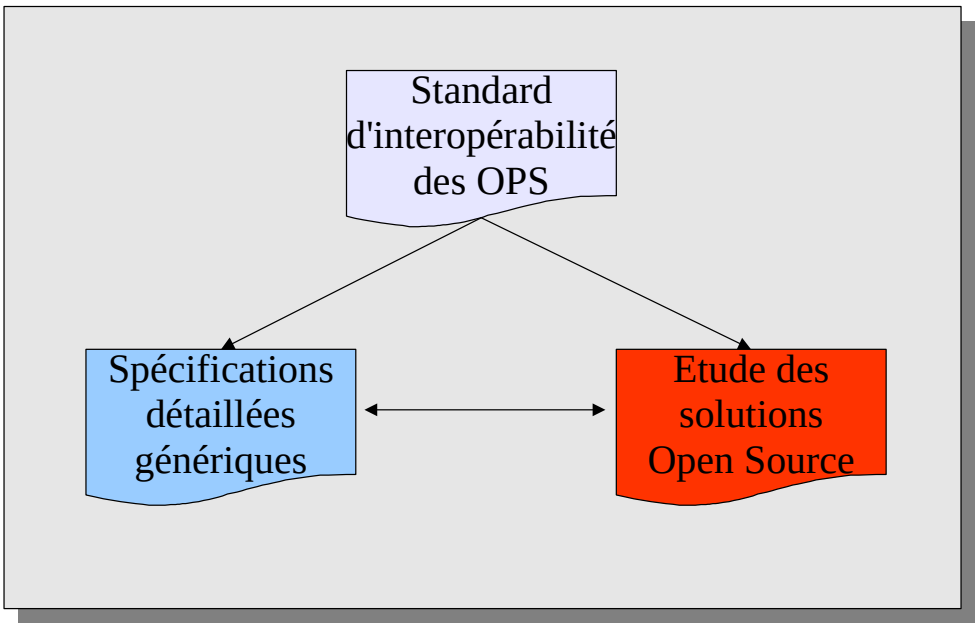
1.1. Objet du document

Ce document présente un ensemble de produits et solutions Open Source existants dont les caractéristiques recouvrent des fonctionnalités telles que décrites dans le document [R3] de spécifications détaillées du standard.

Il a pour but d'éclairer les acteurs de la sphère sociale sur les utilisations potentielles de ces composants en matière de conception et d'intégration de composants logiciels pour la mise en œuvre d'une solution remplissant les fonctionnalités du standard.

1.2. Relation avec d'autres documents

Ce document est en relation avec le Standard [R1] et le document de spécifications détaillées [R3].



Relation entre les documents

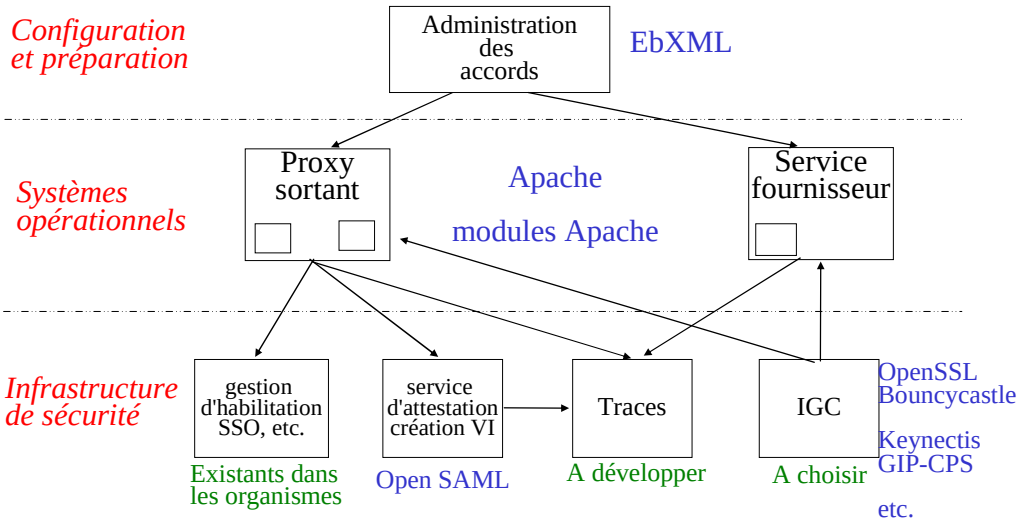
1.3. Organisation et structure du document

Outre le présent chapitre d'introduction, le document se décline selon les chapitres suivants :

- chapitre 2 : Synthèse des produits et solutions étudiés,
- chapitre 3 : Etude des produits et solutions.

2. Synthèse des produits et solutions étudiés

Ce chapitre offre une synthèse de la couverture fonctionnelle des produits et solutions Open Source étudiés au regard des fonctions décrites dans le document de spécifications détaillées.



Rappel de la structuration des composants

La présentation des produits est découpée en deux parties :

- La synthèse des produits couvrant les fonctions intrinsèques du standard,
- La synthèse des produits couvrant les fonctions générales du standard (administration des accords, gestion des traces, IGC).

1.4. Solutions Open-Source couvrant les fonctions intrinsèques du standard

1.4.1. Produits « étendus »

Les fonctions intrinsèques comprennent les éléments du système opérationnel et les éléments de l'infrastructure de sécurité hors Traces et IGC. Elles sont :

- Le support de proxy / reverse-proxy HTTP et Web Service,
- Le support de SAML, LDAP, SSL,
- L'interface avec la gestion des identifications et habilitations.

Le tableau ci-dessous résume par produit le support de fonctions ou caractéristiques nécessaires pour l'implémentation du standard. Il ne s'agit pas de faire une comparaison stricte des produits, chacun couvrant des domaines particuliers, mais plutôt de mettre en avant les possibilités de combinaisons de

35 tous. En outre, toutes les possibilités offertes par les produits ne sont pas exhaustivement reportées (à
36 l'instar d'Apache) ; seuls les éléments « caractéristiques forts » sont exprimés.

Produit Fonctions	Shibboleth	Apache	PERMIS	LemonLDAP
(Reverse)Proxy	à travers Apache, voir mod_shib	Les modules mod_proxy, mod_jk2	à travers Apache	Reverse-proxy s'intégrant à Apache
Web Service	-	Module à développer avec Extensions SOAP (SOAP v1.1)	-	-
SAML	Supporté	-	Supporté à l'aide d'OpenSAML	Non supporté en natif
LDAP	Supporté	Mod_auth_ldap	Supporté	Supporté
SSL	Supporté	mod_ssl, mod_gnutls, mod_ssl_error	-	Supporté
SSO	Supporté	Nombreux modules de SSO, dont mod_shib, AARAS, mod_auth_remote	Supporté	Avec Apache::Session::MySQL et Apache::Session::Memorycached
Equivalent PAGM	Attribut de rôle	-	Attribut de rôle	Attribut de rôle
Utilisation d'une IGC/PKI	-	Utilise une IGC à travers OpenSSL si elle est désignée	Utilise une IGC si elle est désignée	-
Caractéristiques techniques				
Java	API Java du Module Identification/autorisation	Accepte du code Java (à travers mod_jserv)	PERMIS est écrit en Java	-
Systèmes D'exploitation	Solaris, Linux et Windows 2000/XP	Toutes les principales plateformes	Toutes les principales plateformes (écrit en Java)	Linux. Module webmin disponible. Supporte authentification domaine Windows

La quasi-totalité des serveurs Web utilisent des souches du serveur HTTPD Apache. Les produits couvrant les fonctions spécifiques du standard permettent donc d'utiliser les moyens d'extension par module Apache pour implémenter une solution complète.

Chaque produit est plutôt à considérer comme une source d'inspiration pour le développement et une source de code à recombiner et réutiliser, selon les conditions des licences de chaque produit.

1.4.2. Produits « toolkits

L'autre groupe de logiciels (type middleware) est constitué d'outils remplissant une fonction précise : il ne s'agit pas de produits complets comme peut l'être Shibboleth. Il s'agit d'OpenSSL, BouncyCastle, OpenSAML et OpenLDAP.

Un dernier point à noter : suite à des problèmes légaux concernant le support cryptographique dans le contexte Java, les solutions SSL ne sont pas considérées très stables et performantes en comparaison avec Apache.

1.5. Solutions couvrant des fonctions générales

Les fonctions générales comprennent les éléments Traces et IGC de l'Infrastructure de sécurité ainsi que les éléments de Configuration et préparation. Elles sont :

- Les outils d'administration des accords d'interopérabilité,
- Les outils de gestion de traces,
- Les outils IGC (Infrastructure de Gestion de Clés),
- Les outils de gestion des identifications et habilitations existants seront aussi rapidement évoqués en ce qui concerne les interfaces avec le Système opérationnel.

1.5.1. Accords d'interopérabilité

Il existe de nombreux formats d'échange (tels ebXML, BPEL, WSFL, BPNM, XLang,…).

L'approche la plus adaptée pour la création des fichiers de configuration des accords d'interopérabilité est ebXML (electronic business eXtensible Markup Language). Il s'agit du standard (ISO 15000) défini par l'OASIS et l'UN/CEFACT.

Dans ce cadre, les accords techniques sont représentés par des fichiers CPP (Collaboration Protocol Profile) et CPA (Collaboration Protocol Agreement).

OASIS reconnaît un nombre d'outils propriétaires comme implémentant ebXML. La dernière liste en date est : Cleo Communications VersaLex™ 2.3 tested in LexiCom™ v2.3 Cyclone Commerce Cyclone Interchange/Activator v5.3 Inovis BizManager v3.0 Oxlo Systems, Inc. AutoTPX ebMS MSH, v1.3 Sterling Commerce Gentran Integration Suite / Sterling Integrator v4 webMethods, Inc. webMethods ebXML Module v6.0.1.

Une initiative Open Source (FreebXML) propose FreebXMLBP contenant les outils nécessaires à la création des CPP et CPA.

1.5.2. Traces

Les outils concernant les traces sont en limite du standard : en effet, il n'y a pas d'outil couvrant l'ensemble des besoins (enregistrement des traces, sécurisation de la notarisation et analyse des traces). Si l'enregistrement en tant que tel peut être satisfait par une base de données interfacée par ODBC, telle que MS SQL, Oracle, PostGreSQL ou encore MySQL, il est aisé de trouver des outils de rapport se connectant à cette base : par exemple les outils rapports MS Access, OpenOffice Base, Business Object.

De manière générale les bases de données (en particulier celles indiquées ci-dessus) ont depuis longtemps fait leurs preuves en termes de fonctionnalité et de maturité. De même, les outils de rapport usuels tels MS Access ou Business Object mais aussi plus récents tel OpenOffice Base permettent de créer, éditer et publier des rapports tant en local qu'à travers un serveur web.

En ce qui concerne la sécurisation des traces pour répondre au besoin de non-répudiation, le constat est le suivant :

- Très souvent, les traces ou le journal sont simplement stockés dans un système de base de données sans soucis d'authenticité,
- Quant aux fournisseurs de services d'archivage, ils n'utilisent que des protocoles et interfaces propriétaires.

Un produit récent de la société LexBox couvre le besoin de stockage non falsifiable et d'authenticité vérifiable des données stockées.

Pour le protocole d'interface entre une application et un service d'archivage : il existe DVCS (Data Validation and Certification Service de l'IETF), précurseur des travaux actuellement menés par le groupe LTANS de l'IETF (Long Term Archiving and Notary Services).

Le projet OpenEvidence (qui répond à la ligne d'action IV 3.3 du 7th appel IST du 6ème PCRD (Programme Cadre Recherche et Développement) de l'Union Européenne) regroupe des implémentations Open Source de démonstration du protocole DVCS et d'autres techniques d'horodatage et dont les composants sont intégrables pour des solutions en production.

1.5.3. Infrastructure de Gestion de Clés

Les outils et solutions ci-dessous couvrent chacun les fonctionnalités des Infrastructures de Gestion de Clés :

- Utilisation de logiciels de base comme OpenSSL et BouncyCastle pour la génération des certificats. Ces outils fournissent toutes les fonctions de base nécessaires à la génération de clés et de certificats,
- Utilisation d'outils IGC intermédiaires tels que roCA tant pour la génération et le déploiement des certificats. Ces logiciels utilisent les outils de base. Ils sont adaptés aux contextes requérant un petit nombre de certificats. Ainsi, roCA ne nécessite qu'une machine « vide », la solution elle-même apportant le système d'exploitation bootable sur CD-ROM –ce qui n'est pas le cas pour la plupart des solutions,

- Utilisation d'outils IGC lourds, dimensionnés pour la génération et le déploiement de grands nombres de certificats (tels que RSA, Entrust Technologies-Entrust, Utimaco, IdealX-OpenTrust, Sagem-Confidence, Baltimore Technologies-Unicert),

- Utilisation d'un opérateur de certification existant (tel que Keynectis) : les certificats sont émis par l'opérateur au nom du client. Nous notons que, pour un opérateur comme Keynectis, les certificats d'autorités sont affectés par client et gérés au niveau de l'opérateur,

- Utilisation des certificats émis par un opérateur de certification (exemple de Certinomis ou Verisign) ou d'une autorité externe (exemple du GIP-CPS ou de la DGME).

Même si chaque solution est utilisable en production, une première implémentation du standard peut donc avantageusement s'appuyer sur les outils IGC intermédiaires de part leur facilité de mise en œuvre.

Il est important de rappeler que la sécurité concernant la protection des serveurs est un des éléments fondamentaux sur lesquels repose le standard.

1.5.4. Gestion des identifications et habilitations

Ces outils en général non Open-Source, du type AccessMaster, SiteMinder, SelectAccess ou Oracle SSO sont en limite externe du standard (ils s'interfacent avec les outils du standard). Toutefois, à l'interface avec le standard, ils proposent des API de type LDAP ainsi que des messages formatés SAML.

Dans ce cadre il existe aussi des implémentations Open Source comme Shibboleth et PERMIS qui peuvent être considérés comme des implémentations de référence et de validation de concepts et de protocoles. Il existe aussi des implémentations du protocole LDAP comme OpenLDAP ou LemonLDAP. De manière générale, pratiquement tous les systèmes de gestion d'habilitation permettent d'exporter les informations à travers un annuaire LDAP. Ceci permet de disposer d'une interface normalisée.

3. Etude des produits et solutions

Ce chapitre constitue l'étude de produits et solutions. Les aspects de chaque produit sont mis en avant vis-à-vis des fonctions à développer pour chacun des lots définis dans les spécifications détaillées du standard d'interopérabilité. Ceci concerne autant aussi bien les caractéristiques techniques des produits que les types de licence utilisés ou encore leur maturité.

L'ensemble des versions indiquées dans ce chapitre correspond aux existants de février 2006.

1.6. Shibboleth

Shibboleth est un projet Internet2/MACE. Internet2 est un regroupement de plus de 200 universités américaines en partenariat avec leur gouvernement et des industriels pour le déploiement d'applications et technologies réseaux. MACE est la branche concernant les architectures middleware pour l'éducation.

Shibboleth est intégré au NMI (National Science Foundation Middleware Initiative).

1.6.1. Synthèse du produit/solution

Shibboleth est un ensemble de composants middleware fournissant une infrastructure cohérente sécurisée d'accès à des données protégées : identification, authentification, autorisation et répertoire d'attributs. La version courante est 1.3.

Shibboleth est sous licence Apache 2.0, disponible sur Solaris, Linux et Windows 2000/XP.

Shibboleth :

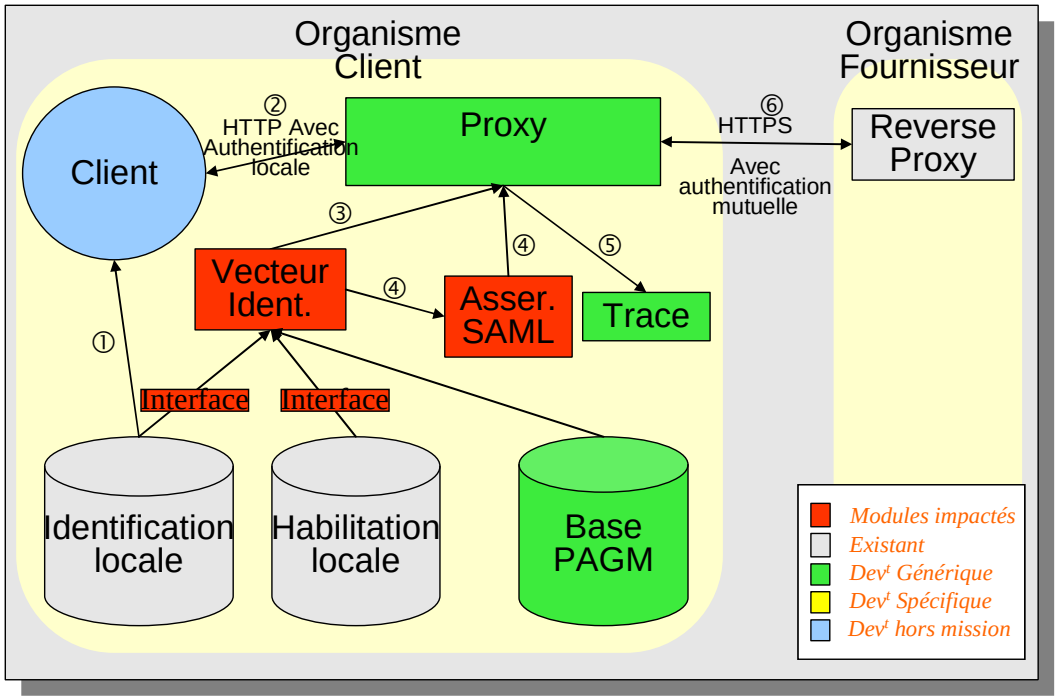
- Implémente une plateforme SSO cross-domain web basée sur SAML 1.1,
- Fournit une API Java ainsi qu'un module Apache (mod_shib) pour le composant générant les assertions d'identification, d'authentification et d'autorisation

1.6.2. Positionnement du produit au regard des fonctionnalités

Shibboleth peut être vu comme un ensemble complet à mettre en œuvre ou comme une source de composants, éventuellement à adapter, pour s'intégrer dans un environnement existant.

Shibboleth peut être utilisé pour la gestion des autorisations et attributs supplémentaires en fonction des identifications et authentifications. Incorporé dans le code du module Vecteur d'Identification, Shibboleth est capable de fournir la liste des PAGM et attributs supplémentaires pour une identification donnée.

Nous constatons que les organismes disposent de systèmes d'habilitation du marché. Shibboleth peut aussi être utilisé comme implémentation de référence pour des tests et qualifications lors de l'expérimentation (ce qui s'applique principalement aux Organismes Fournisseurs).



157 **Utilisation de Shibboleth côté Organisme Client**

158 1.6.3. Diffusion actuelle et maturité du produit

159 Shibboleth bénéficie, depuis plusieurs années, de retour d'expérience en production tant sur des
160 applications universitaires que commerciales. La version courante est v1.3, elle date d'août 2005. Elle est
161 intégrée au paquetage NMI-R8. Voir la liste des références ci-dessous.

162 La diffusion de Shibboleth concerne en grande partie les systèmes universitaires, les sociétés
163 d'apprentissage à distance (eLearning) ou encore les robots logiciels sur serveurs.

164 Une liste de références annoncée par Internet2 est disponible à l'adresse :

http://shibboleth.internet2.edu/seas.html

165 1.6.4. Complexité de la mise en œuvre dans le cadre du standard

166 La complexité de l'utilisation de Shibboleth dépend de l'utilisation :

167 ❑ En tant que module Apache (mod_shib) pour l'utilisation de l'API gérant SAML, auquel cas
168 l'apport fonctionnel est léger mais l'intégration est rapide,

169 ❑ En tant que source de composants fonctionnels, à adapter à chaque système, auquel cas l'apport
170 fonctionnel est large mais requiert une bonne connaissance du fonctionnement interne de
171 Shibboleth.

172 ### 1.6.5. Eléments complémentaires

http://shibboleth.internet2.edu/

http://www.nmi-edit.org/releases/index.cfm#software

1.7. PERMIS

PERMIS est l'acronyme de PrivilEge and Role Management Infrastructure Standard. Il s'agit d'un projet financé à l'origine par l'ISIS (Information Society Initiative in Standardization) une initiative de la Commission Européenne. Le projet est désormais intégré au NMI (National Science Foundation Middleware Initiative) des Etats-Unis.

1.7.1. Synthèse du produit/solution

PERMIS fournit une PMI (Privilege Management Infrastructure) basée sur des rôles de type X509.

L'architecture PERMIS PMI comprend un système d'allocation de privilèges et un système de vérification de privilèges. L'allocation délivre des certificats X509 d'attribut d'assignation de rôle aux utilisateurs et les enregistre dans un répertoire LDAP. La vérification utilise ce répertoire LDAP. En outre, à chaque utilisateur est attribué un objet d'authentification : si une IGC est désignée il s'agit d'un certificat numérique, autrement il s'agit d'une paire *nom utilisateur/mot de passe*.

La version courante de PERMIS est 1.9.

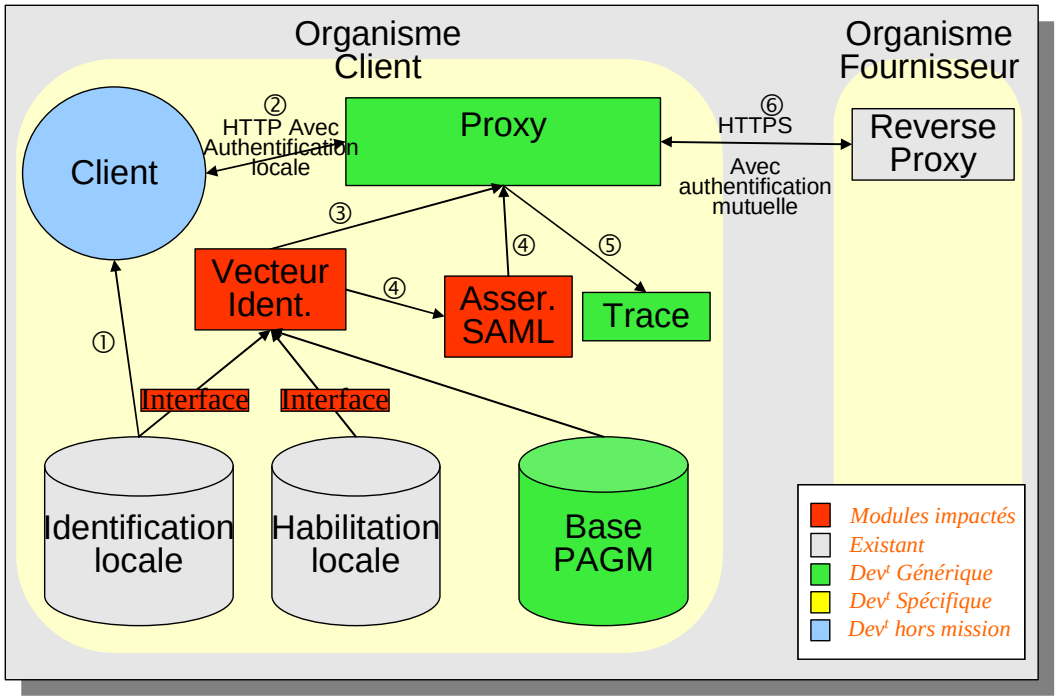
PERMIS :

- Offre une API Java simple,
- Est utilisable avec OpenSAML où PERMIS est un serveur d'autorisation stand-alone,
- Est utilisable à travers Apache où PERMIS est un serveur d'autorisation sous forme de module,
- Est utilisable à travers Apache et Shibboleth où PERMIS est un serveur d'autorisation sous forme de module.

1.7.2. Positionnement du produit au regard des fonctionnalités

De même que Shibboleth, PERMIS peut être utilisé pour la gestion des autorisations ainsi que des attributs supplémentaires en fonction des identifications et authentifications. Incorporé dans le code du module Vecteur d'Identification, PERMIS est capable de fournir la liste des PAGM et attributs supplémentaires pour une identification donnée. PERMIS gère en outre les accès à une Infrastructure de Gestion de Clés si celle-ci est fournie.

A l'instar de Shibboleth, PERMIS est aussi utilisable comme implémentation de référence pour tests et qualifications, en particulier pour les Organismes Fournisseurs.



Utilisation de PERMIS côté Organisme Client

1.7.3. Diffusion actuelle et maturité du produit

PERMIS est éprouvé dans trois cas de déploiements sous l'égide de l'INIS. Après son intégration au NMI, PERMIS est resté sous le contrôle de ses développeurs originaux (l'Université du Kent, Royaume Uni).

La version courante de PERMIS est v1.9 est fait partie du paquetage NMI-R8. Elle date du 16 octobre 2005.

Les déploiements sont :

- Bologne, Italie : système de mise à disposition de cartes numériques pour des ingénieurs et architectes par la municipalité de Bologne,
- Salford, Royaume Uni : système électronique d'appels d'offre et de réponses à appels d'offre pour la municipalité de Salford et ses fournisseurs,
- Barcelone, Espagne : système de notification de contraventions entre la municipalité de Barcelone et les sociétés de location de véhicules.

1.7.4. Complexité de la mise en œuvre dans le cadre du standard

De manière similaire à Shibboleth la complexité de mise en œuvre de PERMIS repose sur les deux scénarii :

- Utilisation du module gérant SAML, éventuellement avec mod_shib (le module Apache de Shibboleth), auquel cas l'intégration est rapide mais la couverture fonctionnelle est réduite,

- Utilisation de PERMIS en tant que tel ou prise en compte et adaptation au système local de composants de PERMIS, auquel cas il est nécessaire de bien connaître le fonctionnement interne de PERMIS.

1.7.5. Eléments complémentaires

http://www.permis.org

http://www.nmi-edit.org/releases/index.cfm#software

http://www.openpermis.org/

http://sec.cs.kent.ac.uk/

1.8. LemonLDAP

LemonLDAP est un système SSO fonctionnant en tant que reverse-proxy d'authentification s'appuyant sur les informations d'un annuaire LDAP. Il a été développé et mis à disposition en Open Source par la Direction Générale de la Comptabilité Publique dans le cadre sur de travaux concernant l'adaptation d'Apache en reverse-proxy. Ces travaux ont permis de réaliser un système SSO pour des applications métier du Trésor Public.

1.8.1. Synthèse du produit/solution

LemonLDAP est, à la base, composé des éléments suivants : le serveur web Apache avec les modules mod_perl et mod_ssl, de MySQL, d'un module webmin et les Net:LDAP. Il s'agit d'un environnement exclusivement composé de logiciels libres.

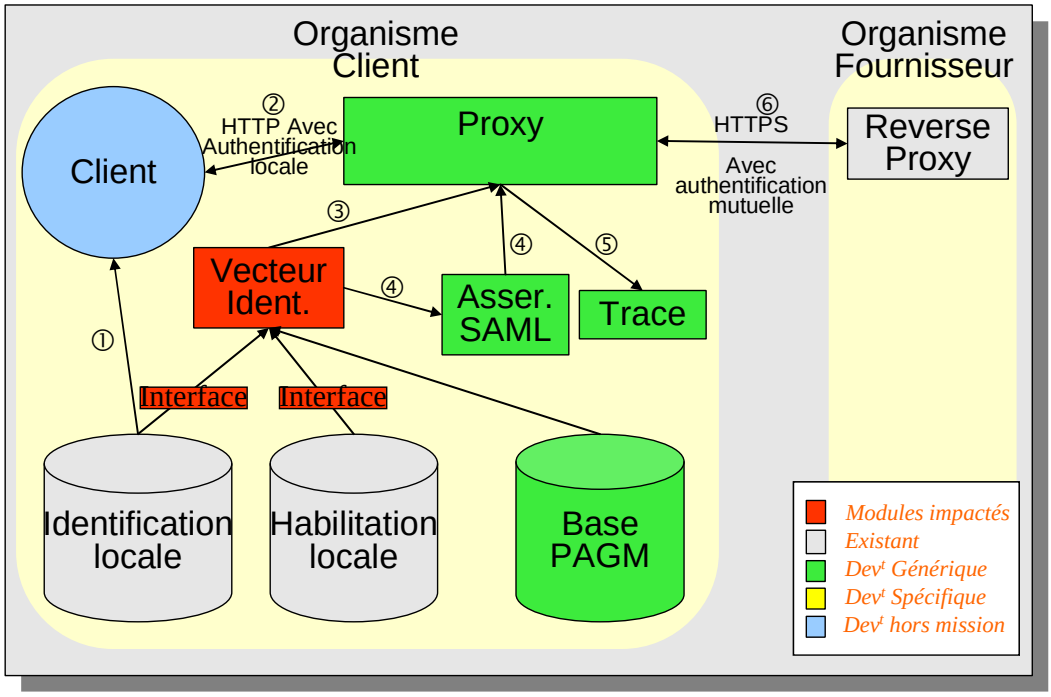
LemonLDAP supporte les authentifications domaine de Windows NT/2000 mais il n'est disponible que sur Linux. La version courante de LemonLDAP est 1.0, elle date de février 2005.

LemonLDAP :

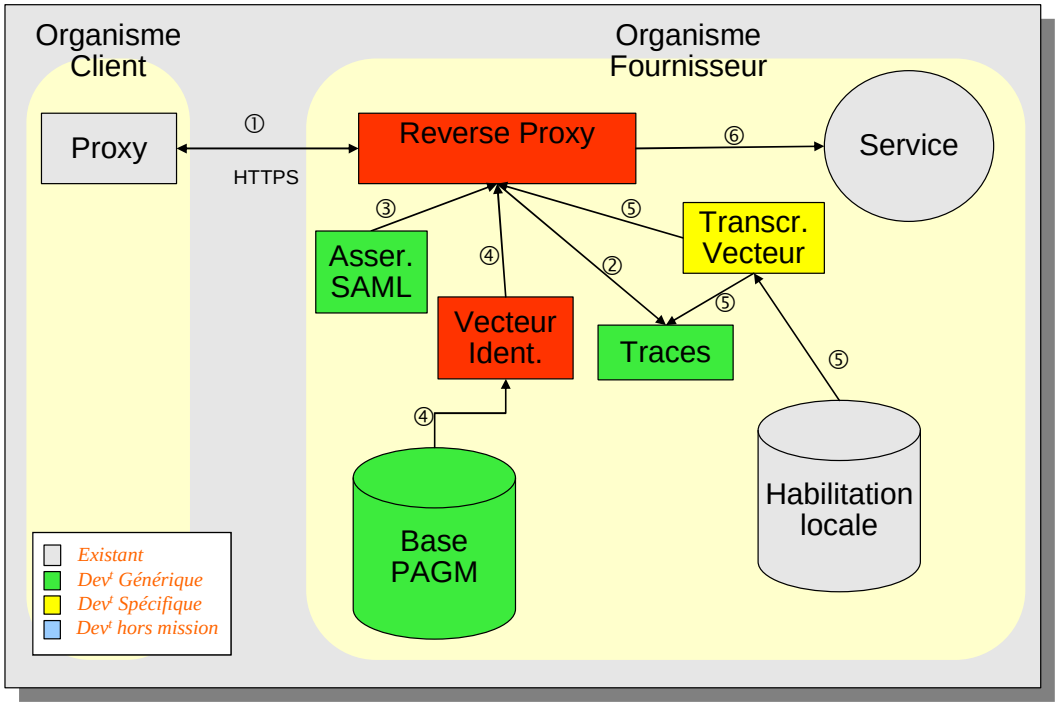
- Est un système reverse-proxy SSO,
- Gère des profils applicatifs (avec LemonLDAP::NG),
- Assigne des attributs LDAP à des utilisateurs pour le contrôle d'accès,
- Est un handler Apache.

1.8.2. Positionnement du produit au regard des fonctionnalités

LemonLDAP est partiellement adaptable tant du côté Organisme Fournisseur que du côté Organisme Client. De manière générale il peut servir de démonstrateur ou d'exemple d'intégration de modules Apache pour simplifier l'implémentation d'une solution.



243 **Utilisation de LemonLDAP côté Organisme Client**



244 **Utilisation de LemonLDAP côté Organisme Fournisseur**

1.8.3. Diffusion actuelle et maturité du produit

LemonLDAP a été mis en place dans certaines administrations françaises (en premier lieu le Ministère des Finances) en 2003. Il bénéficie du retour d'expérience de ces administrations.

Il est actuellement en version 1.0 (février 2005) et le module pour webmin est en version 2.1 (aout 2005).

Un premier déploiement concerne la Direction Générale de la Comptabilité Publique (Ministère des Finances) en production (environ 60000 utilisateurs et 20 applications protégées). Deux déploiements suivants concernent le Ministère de la Défense (la Gendarmerie Nationale) et le Ministère de la Justice. LemonLDAP est aussi déployé au sein de la RATP.

1.8.4. Complexité de la mise en œuvre dans le cadre du standard

LemonLDAP apporte un exemple d'intégration. Il est en soit un moyen de simplifier le développement d'une solution.

1.8.5. Eléments complémentaires

http://sourceforge.net/projects/lemonldap/

1.9. Serveur HTTPD du projet Apache avec les modules AAA

Le serveur HTTPD Apache, de la fondation Apache (Apache Software Foundation), est le serveur HTTP le plus répandu. Développé à l'origine à partir de 1995 comme une collection de correctifs pour le serveur NCSA HTTPD pour les systèmes Unix, il est disponible sur toutes les plateformes principales. Le serveur HTTPD Apache est un projet parmi de nombreux autres projets de la fondation Apache.

Apache incorpore une grande liste de modules permettant d'étendre ses fonctionnalités, par exemple l'interprétation de langages de scripts (ainsi Perl, PHP, Python), la sécurisation (SSL), les fonctions proxy, le support de LDAP, etc.

Apache sert de base à de nombreux produits, tels que Websphere d'IBM ou Oracle WebServer.

1.9.1. Synthèse du produit/solution

Apache est diffusé sous la Licence Apache 2.0.

Pour les fonctions s'appliquant à l'IOPS il s'agit de la combinaison d'Apache et des modules AAA (Authentication, Authorization, Accounting – Authentification, Autorisation, Traçabilité).

Il est ainsi possible d'énumérer les fonctions suivantes (bien qu'Apache ne soit pas limité à celles-ci) :

- Quantité de types d'authentifications (NT Domain, NDS, MySQL/http, Lotus, Oracle 7/8/8i/9, NIS, SMB, LDAP…) par exemple :
- Authentification pour tout type de backend (mod_auth_any),
- Authentification (X509) et autorisation (LDAP) (modXLdapAuth),
- Autorisation LDAP et vérification de certificats (mod_authz_ldap),
- Fonctions de proxy et reverse-proxy/mirroir (mod_but, mod_proxy, mod_tproxt, mod_rewrite, mod_replace, mod_security, mod_headers, mod_rpaf),
- Fonctions de sécurisation (mod_ssl, mod_ssl_error basés sur OpenSSL).

La version courante d'Apache est 2.2.0.

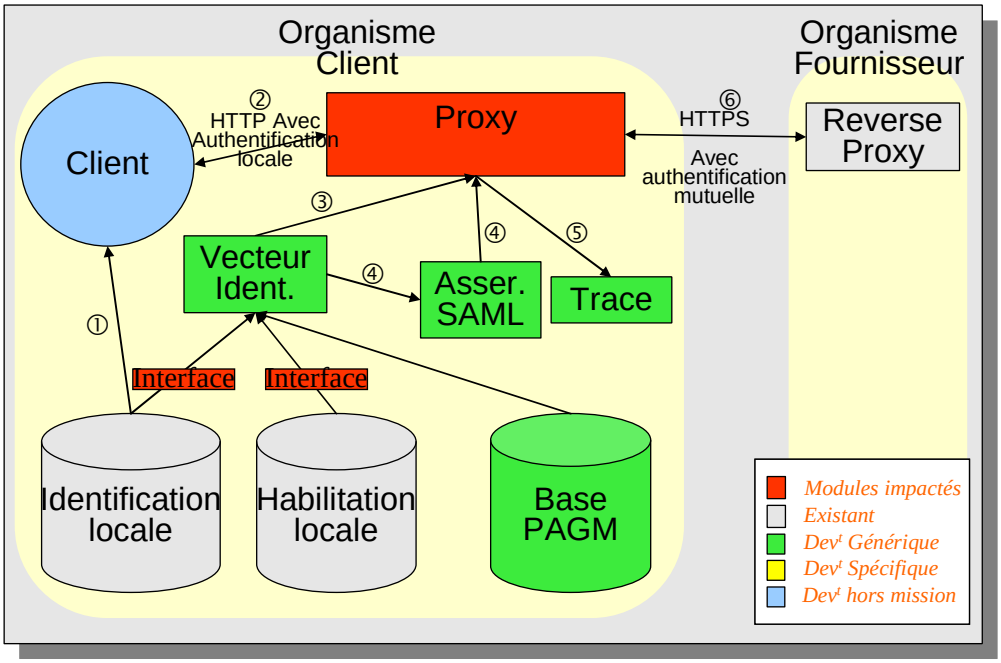
A noter que d'autres projets de la fondation Apache ou communautés affiliées s'intègrent dans la solution Apache pour l'IOPS :

- WebService SOAP : Soap v1.1 (version stable Apache SOAP 2.3.1 du 10 juin 2002) comprenant le patch du paquetage MS SOAP,
- Apache-SSL (Apache + mod_ssl + OpenSSL). A noter que, depuis la version 2.1 d'Apache le module mod_ssl est partie intégrante du serveur.

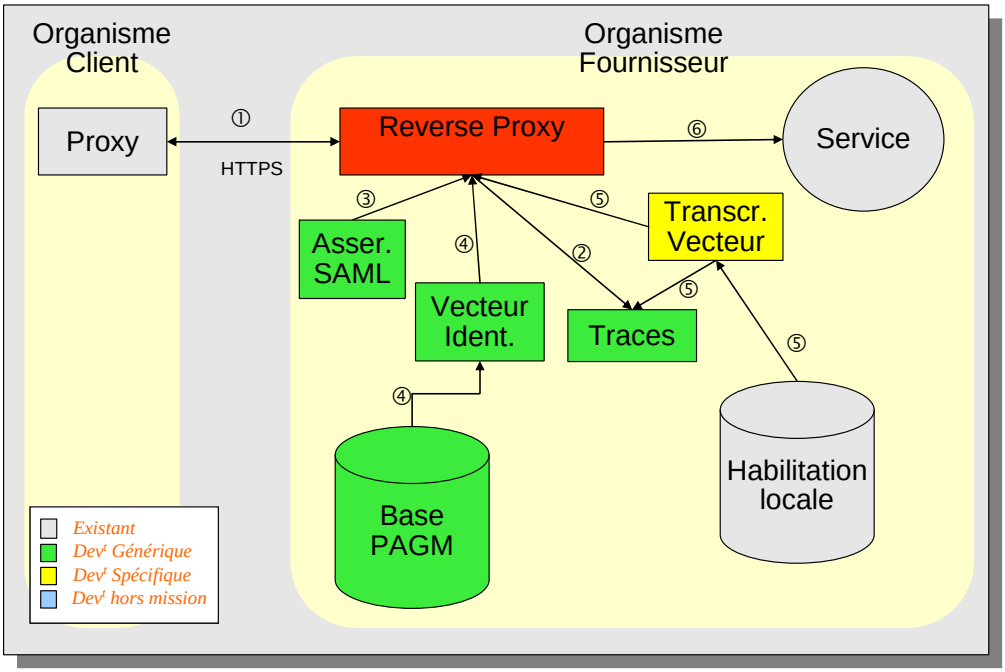
1.9.2. Positionnement du produit au regard des fonctionnalités

Apache est une piste privilégiée tant en termes de performance que de fonctionnalités.

Apache est, bien entendu, utilisable autant côté Organisme Client en tant que serveur proxy et interface aux systèmes locaux d'identification et authentification (en particulier grâce aux nombreux modules fournit, notamment, par les constructeurs) que côté Organisme Fournisseur en tant que reverse-proxy. En outre, l'intégration des fonctions restantes peuvent s'effectuer dans le cadre de modules supplémentaires développés pour l'occasion.



Utilisation d'Apache côté Organisme Client



294 **Utilisation d'Apache côté Organisme Fournisseur**

295 1.9.3. Diffusion actuelle et maturité du produit

296 Ainsi qu'indiqué précédemment Apache est le serveur HTTPD le plus répandu : les estimations actuelles
297 indiquent qu'il équipe les deux-tiers des serveurs à travers le réseau Internet.

298 La version 2.2.0 d'Apache est en phase de développement. Bien que cela soit limité, il est possible de
299 rencontrer des incompatibilités internes, en particulier du point de vue des modules implémentés pour les
300 versions précédentes d'Apache.

301 1.9.4. Complexité de la mise en œuvre dans le cadre du standard

302 Apache s'intègre rapidement dans la plupart des systèmes et avec des interfaces de sécurité externes, en
303 particulier grâce aux modules fournis par les constructeurs. Il a en outre l'avantage d'être très répandu et
304 donc bien connu techniquement.

305 Néanmoins le développement d'un module n'est pas trivial, il nécessite des compétences et de la
306 disponibilité pour en assurer la maintenance.

307 1.9.5. Eléments complémentaires

http://www.apache.org

http://news.netcraft.com/archives/web_server_survey.html

http://modules.apache.org

1.10. Liberty Alliance et Lasso

Le projet Liberty Alliance est un consortium de plus de 150 entreprises et organisations gouvernementales et non-gouvernementales, formé en 2001 pour servir d'organisation de standardisation pour les identités fédérées ainsi que les services à base d'identité. La DGME est un des membres sponsors de Liberty Alliance.

1.10.1. Synthèse du produit/solution

Liberty Alliance est un système de fédération d'identités. Les spécifications de Liberty Alliance distinguent cinq grands rôles :

- Le Principal (l'utilisateur) dont l'identité doit être authentifiée puis fédérée,
- Le Fournisseur d'identités auprès duquel le Principal s'identifie. Le Fournisseur d'identités authentifie l'identité du Principal,
- Le Fournisseur de services auprès duquel le Principal se connecte pour bénéficier des services ; le Fournisseur de services authentifie l'identité du Principal auprès du Fournisseur de d'identités,
- Le Fournisseur d'attributs qui divulgue (selon des règles précises) au Fournisseur de services les attributs du Principal identifié et authentifié,
- Le Service de découverte qui aiguille les demandeurs d'attributs vers le Fournisseur d'attributs approprié.

Liberty Alliance repose sur le principe d'une identification spécifique de l'utilisateur, même dans le cadre de protocoles avec identités dépersonnalisées (non divulgation de l'identité réelle de l'utilisateur). Liberty Alliance est donc adapté aux systèmes dont l'objectif est d'accéder à des données ou de réaliser des actions spécifiques à un utilisateur. Ainsi se créent des cercles de confiance entre des fournisseurs de services et d'identités pour mettre en commun l'identité de l'utilisateur.

Lasso est une implémentation des spécifications de Liberty Alliance en C fonctionnant sur les UNIX dont GNU/Linux (en particulier Lasso fait partie de la distribution Debian), Windows et Mac OS X.

Lasso est livré sous licence GPL, à l'exception de l'un de ses composants : OpenSSL, livré sous une licence de type Apache. Lasso a été certifié par le consortium Liberty Alliance en mai 2005.

1.10.2. Positionnement du produit au regard des fonctionnalités

Le positionnement de Liberty Alliance dans le cadre du standard est délicat : le standard concerne la délégation d'authentification et d'habilitation et non pas la fédération d'identité ou de profils.

L'utilisation de Liberty Alliance n'est donc pas directement applicable dans le cadre du standard d'interopérabilité. L'utilisation des composants de sécurité qui est faite par Lasso peut toutefois servir de source d'inspiration lors des phases de développement pour l'expérimentation.

1.10.3. Eléments complémentaires

http://www.projectliberty.org

http://lasso.entrouvert.org

1.11. ebXML et FreebXMLBP

ebXML (Electronic Business using eXtensible Markup Language) est une suite de spécifications de l'OASIS. ebXML a débuté en 1999 comme une initiative conjointe entre l'OASIS et le CEFACT (Centre for Facilitation or Pratices and Procedures for Administration, Commerce and Transport) de l'agence ECE (Economic Commission for Europe) des Nations Unis.

FreebXML est une initiative du CECID (Center for e-Commerce Infrastructure Development) de l'Université de Hong Kong visant à accueillir et aider le développement de technologies et le partage d'expérience autour d'ebXML. Le CECID est un membre d'OASIS participant entre autres à la standardisation ebXML. FreebXMLBP, développé à l'Université Technique du Moyen Orient à Ankara dans le cadre de l'initiative FreebXML, est une partie du projet Artemis IST 2103 parrainé par la DG Société de l'Information de la Commission Européenne.

1.11.1. Synthèse du produit/solution

Dans le cadre du standard les éléments d'intérêt d'ebXML et de FreebXMLBP concernent le protocole de collaboration (le standard ISO 15000-1 : ebXML CPPA Collaborative Partner Profile Agreement version 2). Ce protocole est basé sur un échange d'information pré-formatée en XML entre deux entités. Chaque entité délivre un CPP (Collaboration Protocol Profile), les deux CPP sont alors combinés en un accord d'échange : le CPA (Collaboration Protocol Agreement).

FreebXMLBP fournit les éditeurs ebBP et ebCPP en Java. ebCPP permet la création et la manipulation de documents CPPA.

FreebXMLBP est livré sous une licence libre spécifique à l'Université Technique du Moyen Orient à Ankara. FreebXMLBP est en version 1.0.

1.11.2. Positionnement du produit au regard des fonctionnalités

Les solutions ebXML/FreebXML entrent dans le cadre du développement du lot 1 concernant l'administration des accords.

1.11.3. Diffusion actuelle et maturité du produit

Le standard ebXML est devenu un standard ISO en 2004 et a connu nombre de mises en production.

FreebXML, initiative créée en 2002, bénéficie du support du CECID, organisation membre d'OASIS pour la standardisation ebXML. FreebXMLBP est, au contraire, un produit récent. Il a été publié en fin d'année 2005 en version 1.0.

Le standard ebXML connaît plusieurs grands déploiements tels que les universités de Hong Kong et d'Ankara, ainsi que le National Health Service du Royaume Uni ou bien encore les Centers for Desease Control and Prevention des Etats-Unis (le projet PHINMS).

En ce qui concerne FreebXMLBP, il s'agit d'un produit récent dont nous ne connaissons pas d'exemple d'utilisation. Sa nature Open Source en fait toutefois un bon point de départ pour une expérimentation d'un outil d'administration des CPP/CPA.

1.11.4. Complexité de la mise en œuvre dans le cadre du standard

La mise en œuvre de la solution concerne l'utilisation de l'éditeur ebCPP de FreebXMLBP dans le cadre d'un développement d'outils d'administration des accords. Cet éditeur ne couvre qu'une partie des fonctionnalités : la création et la manipulation des CPP/CPA (les publications des organismes). La mise en place de l'accord au niveau de chaque organisme n'est donc pas couverte par cet outil.

Dans le cadre de l'expérimentation il sera aussi nécessaire de vérifier l'extensibilité du produit concernant la gestion des PAGM, par exemple, et la génération de fichiers de configuration des systèmes.

De manière générale FreebXMLBP peut être considéré comme une base pour développer l'outil d'administration des accords.

1.11.5. Eléments complémentaires

http://www.ebxml.org

http://www.oasis-open.org/committees/ebxml-cppa/faq.php

http://www.oasis-open.org

http://www.freebxml.org

http://www.freebxml.org/freebXMLbp.htm

http://sourceforge.net/projects/freebxmlbp

1.12. OpenSSL

OpenSSL est basé sur SSLeay d'Eric A. Young et Tim J. Hudson. OpenSSL a démarré ses développements à partir de SSLeay en 1998 par un petit groupe de développeurs qui a utilisé le logiciel dans le contexte Apache. OpenSSL s'est largement développé depuis cette date.

1.12.1. Synthèse du produit/solution

OpenSSL est une boîte à outils qui implémente les protocoles SSLv2/v3 et TLS v1 et propose une bibliothèque généraliste de cryptographie qui comprend la quasi-totalité des algorithmes de cryptographie de base, de chiffrement symétrique et asymétrique ou de hachage (tels que AES, DES, Triple DES, RC4, RC5, blowfish, RSA, DSA, EC, SHA1, MD5) d'outils de codage comme ASN1-DER ou base64 et des algorithmes applicatifs de plus haut niveau comme PKCS7, SMIME, OCSP, X509. En outre, OpenSSL met à disposition un ensemble d'outils sous forme de commandes permettant une interface simple à toutes les fonctions ainsi que des outils de tests pour des connexions SSL.

OpenSSL supporte les cartes d'accélération à travers une API (engine).

OpenSSL est sous une licence de type Apache. Il est disponible pour la plupart des Unix dont Linux ainsi que Mac OS X et Windows. Les versions courantes d'OpenSSL sont 0.9.8a et 0.9.7i. La version 0.9.7i est maintenue pour des raisons de compatibilité.

OpenSSL est utilisé en particulier par Apache à travers le module mod_ssl pour les connexions HTTPS.

1.12.2. Positionnement du produit au regard des fonctionnalités

OpenSSL est utilisable avec mod_ssl comme extension à Apache (voir le paragraphe *1.9* Serveur HTTPD du projet Apache), pour les communications intra et inter-organismes tant pour les phases d'authentification que pour la confidentialité, et peut servir pour des fonctions de signatures de documents et des assertions SAML ainsi que comme outil simple d'IGC.

OpenSSL est utilisé dans de nombreux projets d'IGC, comme newPKI, Idealx, roCA, openCA. Ces outils IGC sont à regarder avec prudence pour ce qui concerne leur utilisation dans un contexte étendu.

1.12.3. Diffusion actuelle et maturité du produit

OpenSSL est utilisé dans de nombreux produits Open Source et commerciaux.

OpenSSL bénéficie bien entendu de la diffusion d'Apache. Au delà de la sécurisation des échanges avec Apache, ainsi que précisé ci dessus, il est utilisé dans d'autres contextes. Des exemples d'autres produits à grande diffusion utilisant OpenSSL sont : Samba, Sendmail, curl, SSH, BIND.

Bien que la version courante d'OpenSSL soit 0.9.8a, à comparer avec la version 0.9 remontant en 1998, le développement est très actif. Les contraintes de compatibilité binaire sont suffisamment bien maîtrisées par l'équipe de développement. En dehors du core-team, de nombreuses personnes contribuent au produit, mais l'intégration de code addition dans les sources principales nécessite souvent un long délai (plus d'un an).

La documentation est encore faible, mais il existe néanmoins de la documentation pour débutants.

La grande complexité du produit a motivé le développement de GnuTLS pour des nouveaux environnements TLS sans contrainte de compatibilité.

1.12.4. Complexité de la mise en œuvre dans le cadre du standard

Dans le cadre du standard la mise en œuvre est simple du fait de son intégration dans les outils existants, en particulier Apache. L'utilisation des fonctions de signature n'est pas très difficile.

1.12.5. Eléments complémentaires

http://www.openssl.org

1.13. BouncyCastle

On peut simplement décrire BouncyCastle comme l'équivalent d'OpenSSL pour le monde JAVA. Son existence est très liée à l'architecture des interfaces cryptographiques dans le contexte JAVA suite à des restrictions légales de fourniture par les Etats-Unis d'Amérique.

BouncyCastle est développé par l'organisation à but non lucratif The Legion of the BouncyCastle, depuis l'an 2000.

1.13.1. Synthèse du produit/solution

BouncyCastle fournit un ensemble d'API cryptographiques, en particulier un fournisseur (provider) de JCE et JCA, une version signée utilisable par le JDK 1.4/1.5 de Sun. En outre, des APIs pour des applications tels que X509, S/MIME, OCSP, TSP,OpenPGP sont fournies.

BouncyCastle est livré sous une licence basée sur la licence MIT X Consortium. La version courante de BouncyCastle est 1.31, elle date de décembre 2005.

1.13.2. Positionnement du produit au regard des fonctionnalités

Pour un contexte JAVA, la bibliothèque peut être utilisée pour les fonctions cryptographiques.

1.13.3. Diffusion actuelle et maturité du produit

Le produit existe depuis plusieurs années. Le développement est actif, il y a une centaine de contributeurs externes. La réactivité du développeur principal est agréable. Le produit à été utilisé pour le développement du logiciel EuropePKI du projet EU-IST EU-PKI sans grande difficulté.

Le produit est utilisé et dans les solutions Open Source et pour des services d'opérateurs de certification. La société Sun Microsystems, Inc. indique Bouncycastle comme l'un des CSP (Fournisseurs de Services Cryptographiques) pour l'extension de cryptographie de Java.

1.13.4. Complexité de la mise en œuvre dans le cadre du standard

BouncyCastle peut être utilisé comme remplacement d'un fournisseur cryptographique. Dans ce cas, il s'agit d'une configuration de machine virtuelle JAVA. L'autre utilisation concerne des fonctions de signature dans des proxys (en cas d'implémentation JAVA) ainsi que pour les outils ebXML.

1.13.5. Eléments complémentaires

http://www.bouncycastle.org

http://www.bouncycastle.org/licence.html

http://java.sun.com/products/jce/javase_providers.html

1.14. OpenSAML

OpenSAML a été produit par Internet2 dans le cadre du projet Shibboleth (voir le paragraphe *1.6* Shibboleth)

1.14.1. Synthèse du produit/solution

OpenSAML est un ensemble de bibliothèques servant à la construction, au transport et à l'analyse de messages SAML. Il implémente partiellement les spécifications SAML 1.0 et 1.1 (selon les spécifications émises par l'OASIS).

La version courante d'OpenSAML est 1.1.

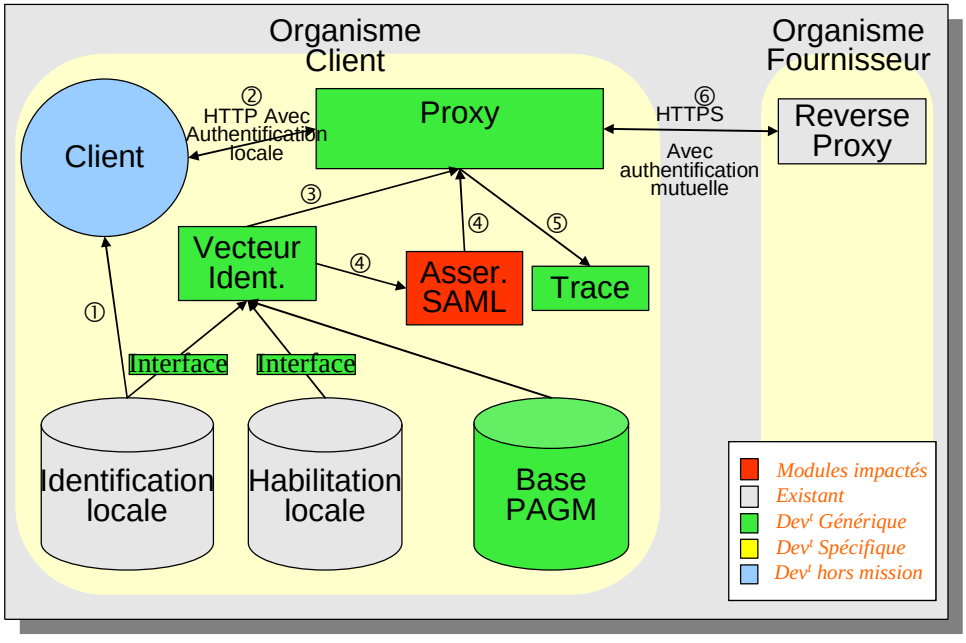
OpenSAML est livré sous les termes de la Licence Apache 2.0. Il existe en deux distributions :

- OpenSAML Java v1.1b
- OpenSAML C++ v1.1a

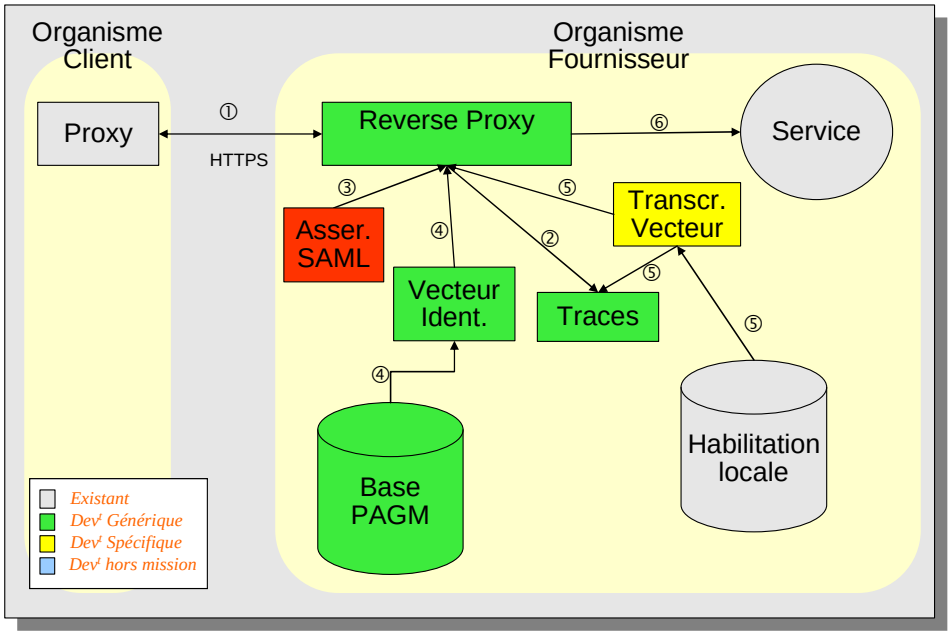
Il est disponible pour Windows XP/2000, Linux (pour Red Hat en termes de RPM) et Solaris 2.

1.14.2. Positionnement du produit au regard des fonctionnalités

OpenSAML est utilisable soit en tant que tel au niveau des Organismes Client et Fournisseur pour gérer la création et la vérification des assertions SAML –voir les schémas ci-dessous– soit à travers des outils complets, tels que Shibboleth.



Utilisation d'OpenSAML côté Organisme Client



470 **Utilisation d'OpenSAML côté Organisme Fournisseur**

471 1.14.3. Diffusion actuelle et maturité du produit

472 La diffusion d'OpenSAML recouvre naturellement celle de Shibboleth. OpenSAML est aussi intégré à
473 l'outil Globus Toolkit dans le cadre de constructions de grilles informatiques (computer grids). La version
474 courante date d'août 2005 pour l'implémentation C++ et d'octobre 2005 pour l'implémentation Java. La
475 version précédente, la 1.0, date d'août 2004.

476 OpenSAML ne supporte pas encore les spécifications SAML 2.0. A noter qu'une version 2 d'OpenSAML
477 est en cours de développement, elle implémente les spécifications SAML 1.x et SAML 2. La version Java
478 finalisée (après Beta test) est prévue en mars 2006, la version C++ en juillet 2006.

479 1.14.4. Complexité de la mise en œuvre dans le cadre du standard

480 Dans le cadre de Shibboleth la mise en œuvre est immédiate. Dans un cadre d'utilisation autonome,
481 OpenSAML a l'avantage de proposer les API Java et C++.

482 1.14.5. Eléments complémentaires

http://www.opensaml.org

http://shibboleth.internet2.edu

http://www.oasis-open.org/committees/security

1.15. OpenLDAP

OpenLDAP est un projet fondé par la société Net Boolean, Inc. en 1998. Il est désormais développé par l'OpenLDAP Foundation, toujours parrainée par Net Boolean ainsi que par l'ISC (Internet Systems Consortium, ex Internet Software Consortium) lequel gère des projets tels que BIND, DHCP, Lynx, INN.

1.15.1. Synthèse du produit/solution

OpenLDAP est une implémentation Open Source de LDAP (Lightweight Directory Access Protocol) version 3 (RFC 3377). Il s'agit d'une suite de logiciels incluant :

- Un serveur autonome LDAP,
- Un service de réplication LDAP,
- Les bibliothèques implémentant le protocole LDAP,
- Des outils, utilitaires et des exemples de code.

Le projet OpenLDAP fournit en outre une bibliothèque de classes Java LDAP ainsi qu'un pilote JDBC – LDAP.

OpenLDAP est livré sous l'OpenLDAP Public License. La licence publique OpenLDAP est consultable à l'adresse http://www.openldap.org/software/release/license.html.

OpenLDAP est disponible pour la plupart des Unix dont Linux ainsi que Windows 2000/XP. La version courante d'OpenLDAP est 2.3.19.

1.15.2. Positionnement du produit au regard des fonctionnalités

OpenLDAP, dans le cadre du projet et à travers ses bibliothèques implémentant LDAP, est utilisable en tant que moyen d'interfacer les systèmes d'identification et d'habilitation locaux.

1.15.3. Maturité du produit

OpenLDAP supporte un grand nombre d'extensions, en outre des fonctionnalités de base de LDAP v3. En ce qui concerne la partie bibliothèque, certaines variantes de LDAP v2 (telles que définies par U-Mich LDAP et, dans une certaine mesure, par la RFC 1777) sont aussi supportées bien que toutes les variantes de LDAP v2 devraient être considérées comme obsolètes.

1.15.4. Diffusion actuelle du produit

En termes de distribution, la fondation OpenLDAP recense 18 sociétés à travers le monde offrant un support OpenLDAP. Dans l'administration publique OpenLDAP est utilisé au sein du Ministère de l'Intérieur (annuaire de messagerie), à la Direction Générale de la Comptabilité Publique (annuaire des personnels), à la Direction Générale de la Consommation, de la Concurrence et de la Répression des Fraudes (annuaire des personnels) ainsi qu'au Ministère de la Culture (Portail MCC).

Un certain nombre de modules Apache utilisent OpenLDAP pour réaliser l'authentification LDAP (ainsi mod_ldap).

1.15.5. Complexité de la mise en œuvre dans le cadre du standard

La mise en œuvre d'OpenLDAP dans le cadre du standard concerne l'interfaçage des systèmes d'identification et d'habilitation locaux. Il ne s'agirait donc que de l'utilisation des bibliothèques clientes dans le cadre d'un développement particulier, que ce soit dans un développement C/C++ ou dans un développement Java.

1.15.6. Eléments complémentaires

http://www.openldap.org

http://www.openldap.org/faq

http://www.isc.org

FIN DU DOCUMENT