THALES

# CIBLE DE SECURITE CSPN

# DU PRODUIT PASS

# (Product for Advanced SSO)

**Préparé pour** :
**ANSSI**

**Préparé par:**
**Thales Communications & Security S.A.**
**4 Avenue des Louvresses**
**92622 GENNEVILLIERS CEDEX – France**

# EVOLUTIONS

| | Date (JJ/MM/AA) | Ecrit par | Vérifié par | Approuvé par | Description |
|---|---|---|---|---|---|
| - | 28/09/2012 | Frederic Motte | Vladimir KSINANT | Jean-Francois WIOREK | Document initial |
| A | 14/05/2013 | Frederic Motte | Benoit Bruyère | | Révision de la cible d'évaluation suite à la réunion ANSSI du 14/05/2013 |
| B | 26/05/2013 | Frederic Motte | Cyril Dangerville | | Modification du document suite à la revue de l'ANSSI du 24/06/2013 |
| C | 16/06/2014 | Frederic Motte | Stéphane Solier<br>Cyril Dangerville | | Modification suite à l'évaluation CSPN |
| D | | | | | |
| E | | | | | |
| F | | | | | |

# TABLE DES MATIERES


1. GLOSSAIRE ..... 4

2. IDENTIFICATION ..... 5

2.1. IDENTIFICATION DU DOCUMENT ..... 5

2.2. IDENTIFICATION DU PRODUIT ..... 5

3. ARGUMENTAIRE DU PRODUIT ..... 6

3.1. DESCRIPTION GENERALE DU PRODUIT ..... 6

3.1.1. METHODE D'AUTHENTIFICATION ..... 8

3.1.2. RECHERCHE D'ATTRIBUTS UTILISATEUR ..... 8

3.2. DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT ..... 8

4. DESCRIPTION DE L'ENVIRONNEMENT DU PRODUIT ..... 9

4.1. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT ..... 9

4.2. DESCRIPTION DES DEPENDANCES ..... 9

4.3. DESCRIPTION DES UTILISATEURS TYPIQUES ..... 10

4.4. DEFINITION DU PERIMETRE DE L'EVALUATION ..... 10

4.5. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DANS LEQUEL LE PRODUIT DOIT FONCTIONNER ..... 11

5. DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER 13

6. DESCRIPTION DES MENACES ..... 14

6.1. ELEVATION DE PRIVILEGES ..... 14

6.2. CONTOURNEMENT DES FONCTIONS DE SECURITE ..... 14

6.3. VOL D'INFORMATION PERSONNELLE ..... 14

7. DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT ..... 15


# TABLE DES ILLUSTRATIONS


FIGURE 1 : WORKFLOW ..... 7

FIGURE 2 : CIBLE DE SÉCURITÉ ..... 11

FIGURE 3 : FLOT D'ADMINISTRATION ..... 16

# 1. GLOSSAIRE

| | |
|---|---|
| **CC** | Critères communs |
| **CSPN** | Certification de Sécurité de Premier Niveau |
| **IDP** | Identity Provider (fournisseur d'identité) |
| **SP** | Service Provider (fournisseur de service) |
| **SSO** | Single Sign On |
| **SAML** | Security Assertion Markup Language |
| **TOE** | Target Of Evaluation |
| | |

# 2. IDENTIFICATION

## 2.1. IDENTIFICATION DU DOCUMENT

Ce document décrit la cible de sécurité relative au produit PASS en vue de l'obtention d'une certification de sécurité de premier niveau des technologies de l'information (CSPN). Ce produit est constitué du logiciel Shibboleth adapté et déployé dans un environnement sécurisé.

## 2.2. IDENTIFICATION DU PRODUIT

| | |
|---|---|
| **Organisation éditrice** | **Thales** |
| **Lien vers l'organisation** | http://www.thalesgroup.com/ |
| **Nom commercial du produit** | PASS |
| **Numéro de version évaluée** | PASS V2.0 |
| **Catégorie de produit** | Dispositif d'authentification (SSO) |

# 3. ARGUMENTAIRE DU PRODUIT

## 3.1. DESCRIPTION GENERALE DU PRODUIT

Le système d'information d'une entreprise regroupe tout un ensemble de services souvent hétérogène dont chacun gère sa propre base utilisateurs et ses méthodes d'authentification.

Shibboleth, basé sur la spécification SAML2, apporte une souplesse ainsi qu'une homogénéité dans le moyen d'authentifier l'utilisateur et de propager l'identité de celui-ci jusqu'aux services. En effet, les services n'ont plus à se préoccuper de la gestion des utilisateurs et de leur authentification. Tout ceci est transféré au référentiel de l'entreprise (LDAP ou Active directory) pour la gestion des utilisateurs et à Shibboleth pour l'authentification.

Les avantages de l'externalisation de ces deux fonctions d'administration sont :

- L'utilisation d'un seul référentiel d'utilisateurs. Le maintien en cohérence de ce référentiel est facilité par le fait qu'il soit unique, la multiplication des référentiels entrainant inévitablement un problème de maintien en cohérence de l'ensemble.
- La délégation de l'authentification à un module conçu pour cette fonctionnalité. Le module d'authentification permet ainsi une meilleure cohérence dans les modes d'authentification ainsi qu'une plus grande souplesse d'utilisation pour l'utilisateur final. En effet, il n'est plus dans l'obligation de s'authentifier à chaque service accédé. Une authentification globale est ainsi assurée.
- Les services métiers sont ainsi allégés de ces fonctionnalités et peuvent ainsi se concentrer sur leurs fonctionnalités propres.

Shibboleth est le module d'authentification permettant de réaliser l'authentification des utilisateurs dans un contexte web. (La partie référentiel utilisateur ne fait pas partie de la solution proposée.)

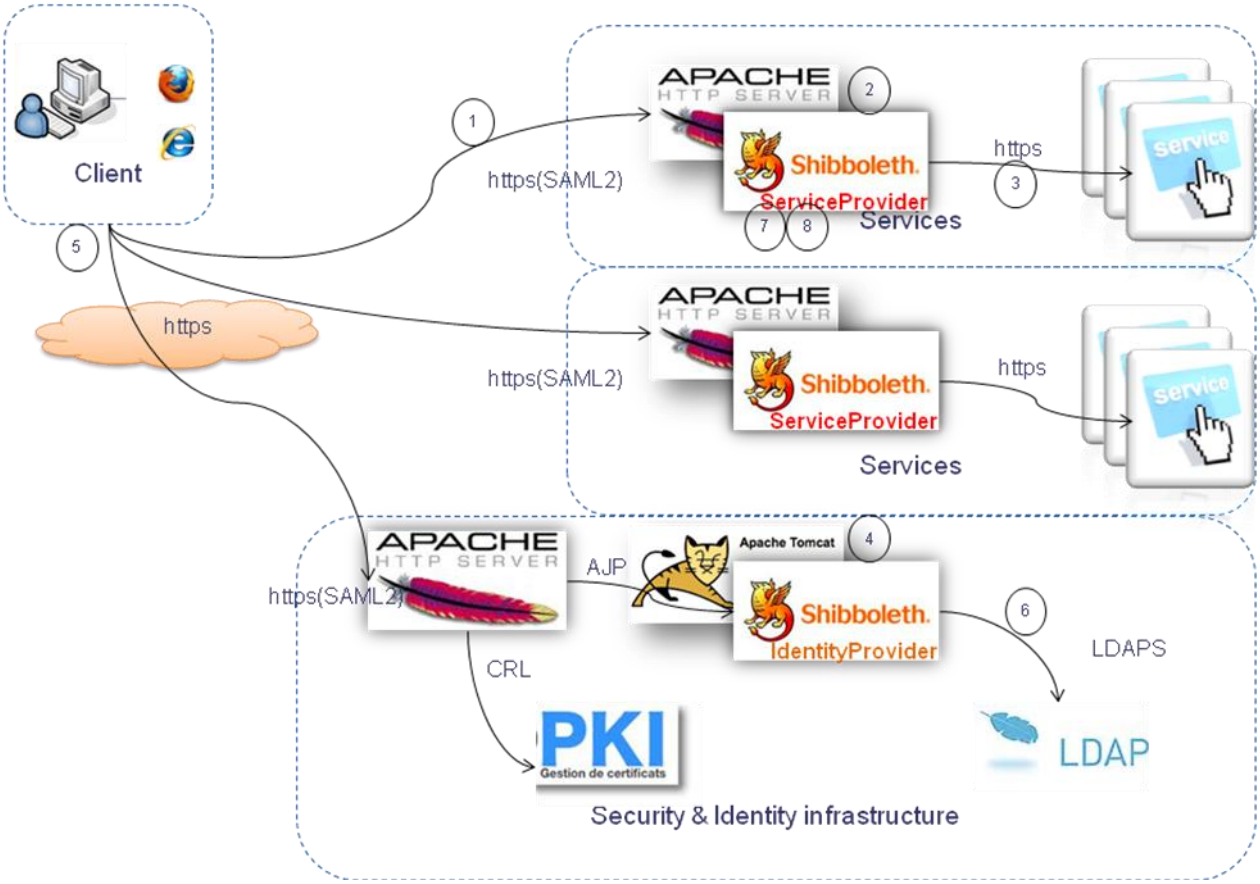
Le Produit Shibboleth se décompose en deux parties :

- Le Service Provider : Le fournisseur de service (SP) est un reverse proxy en frontal de toutes les applications web que l'on désire protéger. Lorsque l'utilisateur cherche à accéder à une ressource ou un service, le fournisseur de service traite la requête afin de s'assurer de l'identité de l'utilisateur. Dans le cas où l'utilisateur n'a pas déjà été authentifié, il délègue l'authentification à l'Identity Provider.

  En général, un Service Provider est en frontal à chaque service à protéger. Physiquement, il peut être sur la même machine ou sur une machine distante au service à protéger.

- L'Identity Provider : Le Fournisseur d'identité (IDP) est la brique logicielle chargée de réaliser l'authentification des utilisateurs pour le compte du service. Il est en charge de proposer à l'utilisateur de s'authentifier afin de valider son identité. Cette authentification peut se réaliser soit par login/mot de passe, soit par certificat X509. Dans un second temps, l'Identity Provider peut se connecter aux différents référentiels de données enregistrés afin de pouvoir récupérer les informations utilisateur nécessaires pour le service cible.

  L'identity Provider est installé physiquement sur une machine distincte aux différents Service Providers




-

**Figure 1 : workflow**

-

Le workflow d'authentification est le suivant :

1. L'utilisateur veut accéder à un service protégé
2. Le Service Provider traite la requête afin de valider si l'utilisateur a déjà été authentifié au préalable.
3. Si oui, le Service Provider transmet la requête au service en ajoutant les informations d'authentification propres à l'utilisateur ainsi que différentes informations sur l'utilisateur nécessaires au service cible. Ces informations peuvent être du type adresse, adresse mail, grade, localisation, etc…
4. Sinon, l'authentification est déléguée à l'Identity Provider qui est en charge de valider l'identité de l'utilisateur.
5. L'Identity Provider fournit à l'utilisateur le moyen de s'authentifier et valide ces informations.
6. Dans le cas où ces informations sont validées, l'Identity Provider cherche les informations requises sur l'utilisateur pour le service.
7. L'Identity Provider fournit ensuite toutes ces informations au Service Provider afin de lui indiquer que l'utilisateur est bien authentifié. Ces informations sont transportées sous la forme d'un jeton au format SAML2.
8. Le Service Provider crée une session permettant ainsi à l'utilisateur d'accéder au service de manière transparente.

Une fois l'authentification réalisée, elle peut être réutilisée pour un autre service auquel l'utilisateur veut accéder. Dans le cas où la session n'a pas expiré, la connexion au nouveau service est transparente.

### 3.1.1. METHODE D'AUTHENTIFICATION

L'utilisateur doit s'authentifier afin d'accéder aux services demandés. Suivant le service, la méthode d'authentification peut être différente, Shibboleth permet deux méthodes d'authentification:

- Par Login/mot de passe : Lorsque le service demande à ce que l'utilisateur soit authentifié, une page d'authentification est retournée à l'utilisateur lui permettant de rentrer ses informations de connexion. Grâce à ces informations de connexion et à l'utilisation du référentiel utilisateur, l'authentification de l'utilisateur peut être validée ou rejetée.
- Par certificat X509. L'utilisateur détient un certificat X509 qui lui a été attribué par une PKI externe à la TOE, et qui représente son identité dans le système d'information. Si le service demande à ce que les utilisateurs soient authentifiés grâce à leur certificat, une communication en SSL authentification mutuelle est etablie entre l'IdP et le navigateur Web. Dans ce dernier, une fenêtre spécifique du navigateur web demande à l'utilisateur de choisir le certificat à utiliser. Ce certificat est par la suite validé afin de s'assurer qu'il est conforme et toujours valide (CRL). Le certificat X509 n'est utilisé que pour l'authentification. Aucune fonctionnalité de chiffrement ou de signature n'est associée à ce certificat, une fois la session etablie.

### 3.1.2. RECHERCHE D'ATTRIBUTS UTILISATEUR

Shibboleth réalise l'authentification de l'utilisateur en se basant sur un référentiel commun à l'ensemble des services. Ce référentiel contenant également toutes les informations de l'utilisateur, Shibboleth est capable de récupérer des informations sur l'utilisateur nécessaires au service cible. (Les informations sur l'utilisateur que le service a besoin de connaitre sont indiquées par simple configuration.)

## 3.2. DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

Le produit Shibboleth une fois installé, configuré et mis en route dans son environnement, est utilisé par l'utilisateur final afin de s'authentifier auprès des services auxquels il veut accéder. Suivant le service désiré et la méthode d'authentification configurée, l'utilisateur entre son couple login/Password (page web) ou bien présente un certificat X509 (par l'intermédiaire de son navigateur Web).

Une fois cette authentification réalisée et validée par l'infrastructure, l'utilisateur peut accéder à tous les services que Shibboleth protège (pour une durée de session donnée et pour une méthode d'authentification donnée). Cela permet ainsi à l'utilisateur de n'avoir qu'une seule méthode d'authentification à connaitre pour pouvoir accéder à de nombreux services ainsi que de ne pas avoir à renseigner ses paramètres de connexion pour chaque service accédé.

# 4. DESCRIPTION DE L'ENVIRONNEMENT DU PRODUIT

## 4.1. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Le Service Provider et l'Identity Provider sont installés sur des environnements d'exécution sécurisés comme décrit dans le manuel d'installation. Ces machines sont physiquement sécurisées (dans un local sécurisé) à la manière des infrastructures physiques de l'entreprise (annuaire, PKI, etc…).

Du point de vue de l'utilisateur, aucune exigence particulière n'est demandée excepté l'utilisation de navigateurs supportant un minimum de fonctionnalités telles que les cookies, les certificats, le JavaScript et doit supporter des algorithmes de communication SSL (TLSv1.0) requis coté serveur, soit au moins un de la suite SSL suivante : AES256-SHA :AES128-SHA. Les dernières versions des implémentations des références telles qu'Internet Explorer, Firefox sont compatibles. La configuration physique et logicielle doit permettre l'utilisation de ces navigateurs sans restriction. Le poste client doit être administré selon la politique de sécurité de l'entreprise (du point de vue antivirus, mise à jour, patch de sécurité, etc.).

Les administrateurs sont considérés comme non hostiles, de confiance et formés à l'administration du produit..

Les Services périphériques (les services Web, l'annuaire LDAP et la PKI) doivent être correctement configurés et administrés et à jour des correctifs de sécurité Le Poste de l'utilisateur est un poste hébergeant un OS à jour des patchs de sécurité, correctement administré et équipé d'un anti-virus lui aussi à jour.

## 4.2. DESCRIPTION DES DEPENDANCES

Shibboleth nécessite d'être installé dans un environnement sécurisé composé par :

- Un OS sécurisé basé sur un Linux Debian squeeze configuré avec les règles décrites dans le document d'installation du produit PASS. (GR-Security, administration, contrôle d'accès, etc.…)
- De serveur Apache HTTP ainsi que de serveur d'application Tomcat. Les règles de sécurisation de ces serveurs sont également décrites dans le document d'installation du produit PASS. Chaque serveur Apache HTTP sera pourvu d'un module mod_security permettant une protection applicative contre des attaques de type XSS, infection SQL, etc.…De plus, chaque serveur Apache HTTP sera pourvu d'un module de communication SSL (mod_ssl) afin de sécuriser la communication entre le client, le service métier, le Service Provider et l'Identity Provider. Dans un contexte industriel, chaque serveur Apache devra utiliser un certificat pour la communication SSL provenant d'une autorité de certification. Les caractéristiques de ces certificats sont décrites dans le guide d'installation (Dans le cadre du CSPN, l'évaluation sera réalisée avec des certificats auto signés)Shibboleth utilise des certificats pour la signature et le chiffrement des requêtes et des assertions. Chaque partie (Service Provider et Identity Provider) sera pourvue de certificats différents :
    - Un certificat pour la signature (un coté Service Provider et un coté Identity Provider)
    - Un certificat pour le chiffrement (un coté Service Provider)

  Dans un contexte industriel, chaque certificat sera fourni par une autorité de certification. Les caractéristiques de ces certificats sont décrites dans le guide d'installation (Dans le cadre du CSPN, l'évaluation sera réalisée avec des certificats auto signés)

Shibboleth s'appuie sur des composants externes faisant partie d'une infrastructure standard dans une entreprise :

- Un annuaire (compatible LDAPS) contenant les informations sur les utilisateurs susceptibles d'accéder aux services exposés (ex : OpenLDAP). Suivant le schéma de l'annuaire et des informations contenues dans celui-ci, la configuration de l'Identity provider sera adaptée pour permettre la récupération des attributs utilisateur
- Une PKI permettant la création des certificats serveur (SP et IdP) et certificats X509 que l'utilisateur peut utiliser pour s'authentifier. (ex : EJBCA). Elle gérera également la mise à disposition d'une CRL. Cette CRL sera utilisée par l'IdP afin de vérifier la validité des certificats que l'utilisateur présentera pour son authentification. Cette CRL sera périodiquement mise à jour comme décrit dans la documentation d'installation.
- Des services de type WEB. Ce sont ces services que l'utilisateur doit pouvoir atteindre une fois l'authentification réalisée. Les exigences sur les services sont :
    - Ils doivent être du type web
    - Ils doivent pouvoir récupérer les informations utilisateurs dans les entêtes HTTP s'ils veulent les exploiter.
    - Ils ne doivent pas être accessible directement par l'utilisateur. Le passage par un Service Provider (qui réalise la fonction de proxy) est obligatoire.
    - La communication entre le Service Provider et le service métier doit être sécurisée (HTTPS avec authentification mutuelle et certificats dédiés), afin de garantir une confidentialité et l'intégrité des données échangées ainsi que la vérification de l'identité du SP par le service métier, et réciproquement. Un certificat dédié par partie sera utilisé pour la communication entre le Service provider et le service métier.
    - L'administrateur du service métier est considéré de confiance. L'environnement de déploiement du service métier sera considéré comme sûr.
- Les Browsers Web utilisés par les utilisateurs sur leur poste client. Ils seront installés avec leurs dernières mises à jour

## 4.3. DESCRIPTION DES UTILISATEURS TYPIQUES

Cette section présente les différents intervenants possibles

- Un ou plusieurs administrateurs dont le rôle est de procéder aux opérations d'installation, de configuration, et de maintenance. Ces administrateurs disposent de droits d'accès privilégiés au système d'exploitation : compte administrateur et accès par réseau à l'administration (SSH). Ces administrateurs sont de confiance.
- Des utilisateurs qui utilisent les capacités du système pour réaliser leur authentification. Le Login/mot de passe est personnel à chaque utilisateur, n'est connu que de lui seul et son certificat ainsi que la clé privée associée ne sont utilisés que par lui. Le certificat lui sera délivré par la PKI du système suivant les possibilités de la PKI et de l'infrastructure (Interface web, email, carte à puce, etc.).

## 4.4. DEFINITION DU PERIMETRE DE L'EVALUATION

La cible de l'évaluation est constituée des deux composants, Service Provider (Shibboleth SP v2.5.1) et Identity Provider (Shibboleth IdP v2.3.6) du logiciel Shibboleth.

Toutes les fonctionnalités d'authentification (Login/password et certificat X509) ainsi que la recherche d'attributs utilisateur font partie du périmètre d'évaluation.

Ces composants sont déployés et s'exécutent sur des serveurs web, Apache et Tomcat. Ces serveurs web sont sécurisés ainsi que le système d'exploitation les hébergeant mais ces éléments sont considérés comme faisant partie de l'environnement de la cible d'évaluation.
Les ressources externes comme la PKI (EJBCA), l'annuaire (OpenLDAP), les postes clients et les services périphériques sont exclus de la cible.

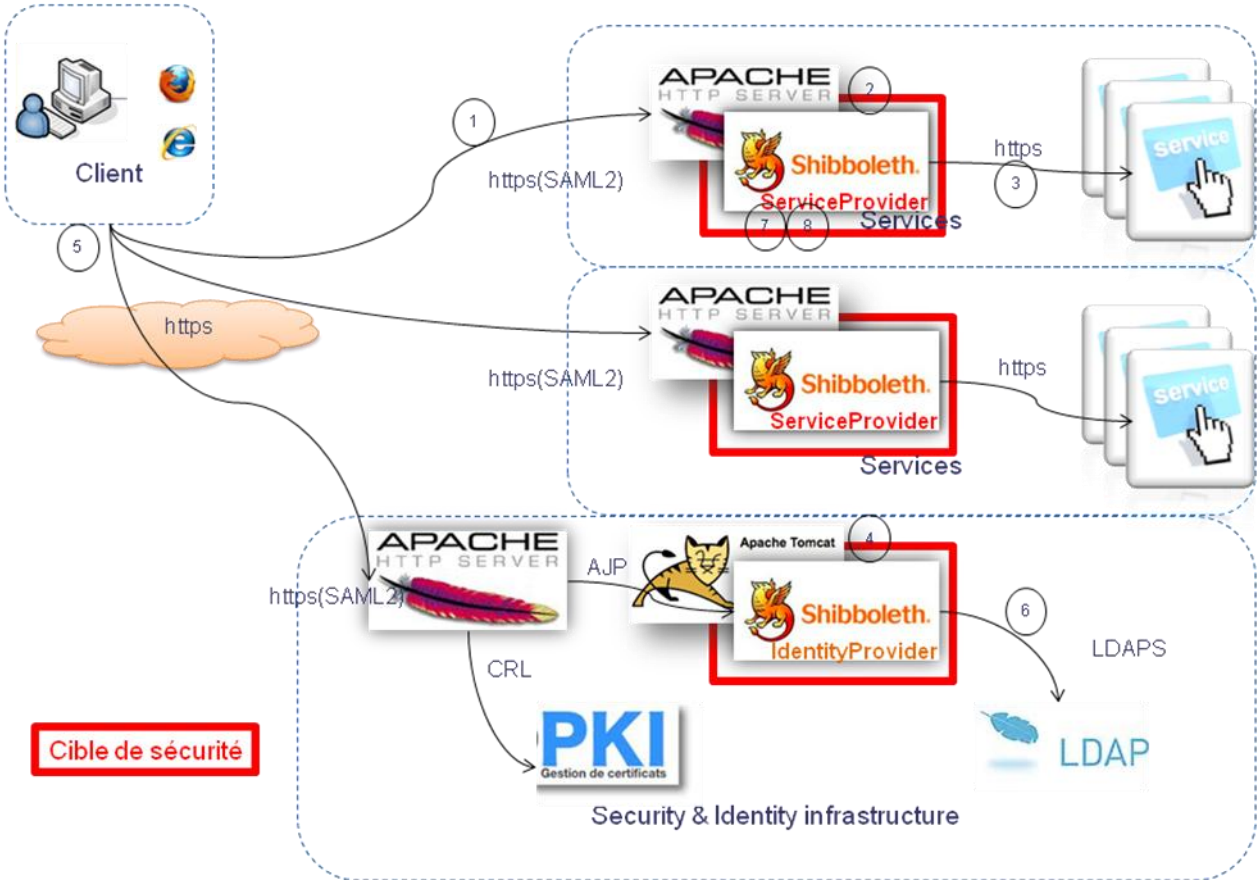



**Figure 2 : Cible de sécurité**

## 4.5. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DANS LEQUEL LE PRODUIT DOIT FONCTIONNER

Les exigences relatives aux moyens matériels au minimum sont :

- Processeur de type X86
- Mémoire de 2Go de RAM
- Espace disque de 4Go
- Interface réseau de type Ethernet

Les exigences relatives aux versions de l'OS et des logiciels utilisés sont (au minimum) :

- Un OS de type Linux Debian squeeze 6.0.5 basé sur un noyau 2.6.32.59-grsec
- Un serveur d'application Tomcat 6.0.35-1+squeeze2
- Un serveur web Apache2 2.2.16-6+squeeze7
- Un OpenSSL V0.9.8o-4squeeze12
- Un OpenSSH 6.6p1 (avec OpenSSL V1.0.1 embarqué)
- Un mod_security 2.5.12-1+squeeze1
- Un navigateur web Firefox 15 ou supérieur
- Un navigateur web Internet Explorer 8 ou supérieur
- Un annuaire OpenLdap (Externe à la cible)
- Une PKI EJBCA (Externe à la cible)

L’OS et les outils seront mis à jour par rapport aux derniers patchs de sécurité publiés pour leurs versions respectives. Ils seront également sécurisés conformément à l’état de l’art.

# 5. DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Les biens que doit pouvoir protéger Shibboleth sont de plusieurs types :

- Les données utilisateur : Les données personnelles (identité, mot de passe, attributs utilisateurs) transitant entre le navigateur client et la partie Service Provider d'une part et la partie Identity Provider d'autre part, ne doivent pas être transmises en clair. Ces informations personnelles échangées doivent rester confidentielles et intègres.
- Les informations de sessions : Les sessions ouvertes pour un utilisateur ne doivent en aucun cas être utilisées par une personne malveillante qui pourrait usurper l'identité de la personne. Les cookies servant de représentation de session ne doivent pas être volés et/ou réutilisés. Par conséquent, ils doivent rester confidentiels et intègres. De même pour les jetons SAML échangés entre l'Identity Provider et le Service Provider.
- Les données de configuration : les différents fichiers de configuration nécessaires à la plateforme (Shibboleth, Apache, Tomcat, SSH, NTP) sont sécurisés et accessible uniquement aux personnes autorisés. Ils doivent rester confidentiels et intègres.
- Les Secrets cryptographiques utilisés pour les communications et l'élaboration des jetons SAML sont protégés afin de conserver la confidentialité et l'intégrité.

# 6. DESCRIPTION DES MENACES

Les agents menaçants considérés sont des attaquants essayant d'utiliser des services illégitimement ou essayant de récupérer les informations des personnes utilisant ces services.

Les administrateurs et les services internes ne sont pas considérés comme des agents menaçants.

## 6.1. ELEVATION DE PRIVILEGES

Un utilisateur possédant des droits légitimes pour accéder aux services peut essayer de se faire passer pour quelqu'un d'autre ou essayer d'altérer les informations qui sont transmises sur lui au service métier afin d'augmenter ses privilèges au niveau du service métier. De même, le réseau d'administration pourrait être la cible privilégiée par l'attaquant, afin de court-circuiter les mécanismes de sécurités mis en place.

## 6.2. CONTOURNEMENT DES FONCTIONS DE SECURITE

Différents mécanismes de sécurités sont mis en place afin de garantir l'accès aux services et à la confidentialité des données personnelles. Un attaquant pourrait tenter de contourner les politiques de sécurité afin d'avoir accès au service sans être légitimement autorisé (utilisation de faux jeton, utilisation de faux certificat d'authentification, vol de session, modification des politiques de sécurité, etc.).

De même, le système est sécurisé afin de ne pas permettre à un attaquant de récupérer des informations de configuration et des clés pouvant lui servir à contrecarrer la politique de sécurité du système.

## 6.3. VOL D'INFORMATION PERSONNELLE

Les données personnelles que le système doit protéger sont

- les informations personnelles que le système manipule sur l'utilisateur et provenant du LDAP
- les informations personnelles des sessions utilisateur que le système produit. Ces informations personnelles doivent rester secrètes et ne doivent pas être divulguées à l'extérieur du système et/ou manipulées à des fins illégitimes.

Ces informations doivent restées confidentielles. Le système doit permettre la protection de ces informations afin qu'aucun attaquant ne puisse les récupérer et les utiliser à des fins malveillantes.

# 7. DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les principales fonctions de sécurité que le produit fournit sont :

- Authentification des utilisateurs par mots de passe

L'utilisateur désirant accéder aux services métiers protégés par le système doit s'authentifier auprès du système afin de pouvoir y accéder. L'utilisateur peut s'authentifier sur le système en fournissant ses identifiants login/mot de passe. Ce couple login/mot de passe permettra l'authentification de l'utilisateur permettant ainsi l'accès aux services.

- Authentification des utilisateurs par certificats X509

L'utilisateur désirant accéder aux services métiers protégés par le système doit s'authentifier auprès du système afin de pouvoir y accéder. L'utilisateur peut s'authentifier sur le système en fournissant son identifiant basé sur un certificat X509. Ce certificat doit être valide et doit provenir d'une autorité de certification connue par le système.

- SSO (Single Sign-On ou authentification unique)

L'utilisateur ne réalise qu'une seule authentification pour accéder aux différents services métiers protégés

- Protection des données utilisateurs transmises au service métier

Le service métier n'a plus besoin de se connecter au référentiel afin de récupérer les informations concernant l'utilisateur. Par simple configuration du Service Provider (Configuration des attributs utilisateur pour le service métier cible), le service cible recevra la totalité des informations qu'il a besoin de connaitre sur l'utilisateur en même temps que l'authentification de celui-ci. La recherche des attributs utilisateur est réalisée par l'Identity Provider. La configuration des attributs utilisateurs est réalisé au niveau des fichiers de configuration de l'Identity Provider (afin de limiter la fourniture d'information uniquement à un sous-ensemble des données utilisateur contenues dans le LDAP pour un Service Provider donné) et au niveau des fichiers de configuration du Service Provider (afin de fournir uniquement les données utiles pour le service métier protégé). Le transfert des informations utilisateur sera réalisé par insertion de celles-ci dans le jeton SAML (signé et chiffré) garantissant ainsi la confidentialité des informations entre la partie Identity Provider et Service Provider. Puis, ces informations sont ensuite transmises au service cible sous forme d'entête HTTP.

- Gestion des sessions utilisateurs

Le couple Identity Provider et Service Provider permet la gestion des sessions utilisateurs basée sur les jetons SAML et l'utilisation de cookies sécurisés. Ceci permettant la gestion fine des autorisations d'accès au service métier.

- La journalisation des authentifications

Les connexions et erreurs de connexions font l'objet d'une journalisation dans les fichiers de log de la partie Identity Provider afin de tracer les accès aux différents services protégés.

- Administration des serveurs Service Provider et Identity Provider

La configuration des Service Provider et Identity Provider est assurée par un lien SSH entre le poste de l'administrateur et les serveurs administrés. La communication SSH empruntera le même réseau que les

communications clientes. Toute l'administration est basée sur des fichiers de configuration aux formats texte et XML.

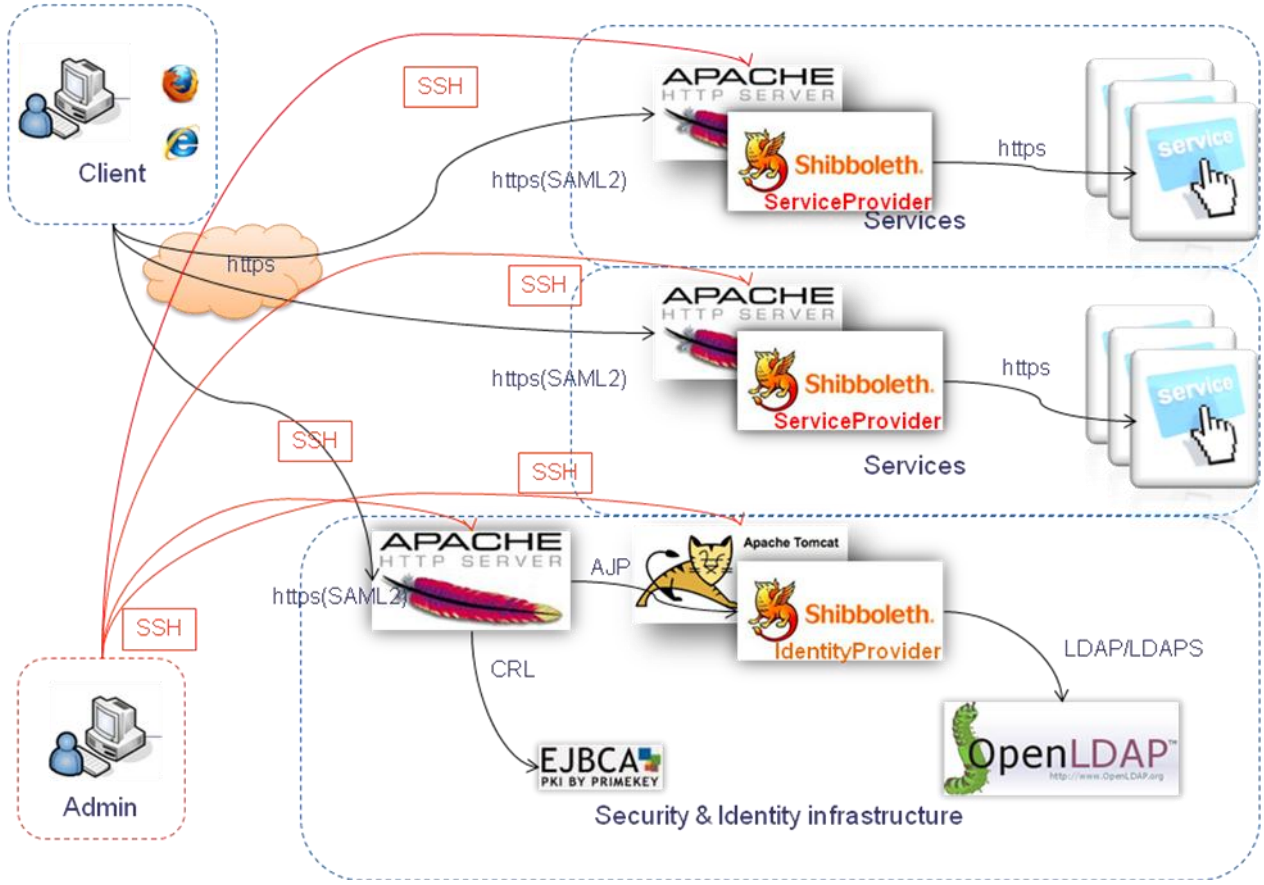



**Figure 3 : flot d'administration**