Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2014/07

PASS v2.0 : solution d'authentification unique basée sur les composants Shibboleth Service Provider v2.5.1 et Identity Provider v2.3.6

Paris, le 22 décembre 2014

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2014/xx

Nom du produit

PASS v2.0 : solution d'authentification unique basée sur les composants Shibboleth Service Provider v2.5.1 et Identity Provider v2.3.6

Référence/version du produit

Shibboleth Service Provider : version 2.5.1
Shibboleth Identity Provider : version 2.3.6

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Développeur

Shibboleth Consortium / Thales Communications & Security

Commanditaire

Thales Communications & Security
4 Avenue des Louvresses
92622 Gennevilliers Cedex – France

Centre d'évaluation

OPPIDA
6 avenue du Vieil Etang
Bâtiment B
78180 Montigny-le-Bretonneux
France

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

PASS v2.0 est une solution d'authentification unique développée par THALES COMMUNICATIONS AND SECURITY et basée sur les composants *Shibboleth Service Provider (SP)* et *Shibboleth Identity Provider (IDP)*, lesquels sont déployés dans une infrastructure de type client/serveur où un utilisateur doit s'authentifier pour accéder à des services web. L'authentification n'est alors pas gérée directement par ceux-ci mais est déléguée aux modules *Shibboleth*, qui assurent ainsi une fonction d'authentification unique (SSO – *Single Sign On*) basée sur le standard SAML2.
Schématiquement le produit fonctionne comme suit :

- un utilisateur accède à un service protégé : le module *Shibboleth SP*, placé en amont du service, traite la requête afin de vérifier si l'utilisateur est déjà authentifié ; si c'est le cas, le SP transmet la requête ainsi que les *credentials* nécessaires au service ;
- si l'utilisateur n'est pas authentifié, il est redirigé vers l'IDP sur lequel il s'authentifie, soit à l'aide d'un login/mot de passe, soit à l'aide de la clé privée associée à son certificat X509 ; une fois les données d'authentification validées, l'IDP fournit au SP un jeton au format SAML2 permettant l'accès au service demandé ;
- le SP crée alors une session permettant à l'utilisateur de rester authentifié auprès du service désiré, auquel il peut alors accéder de façon transparente.

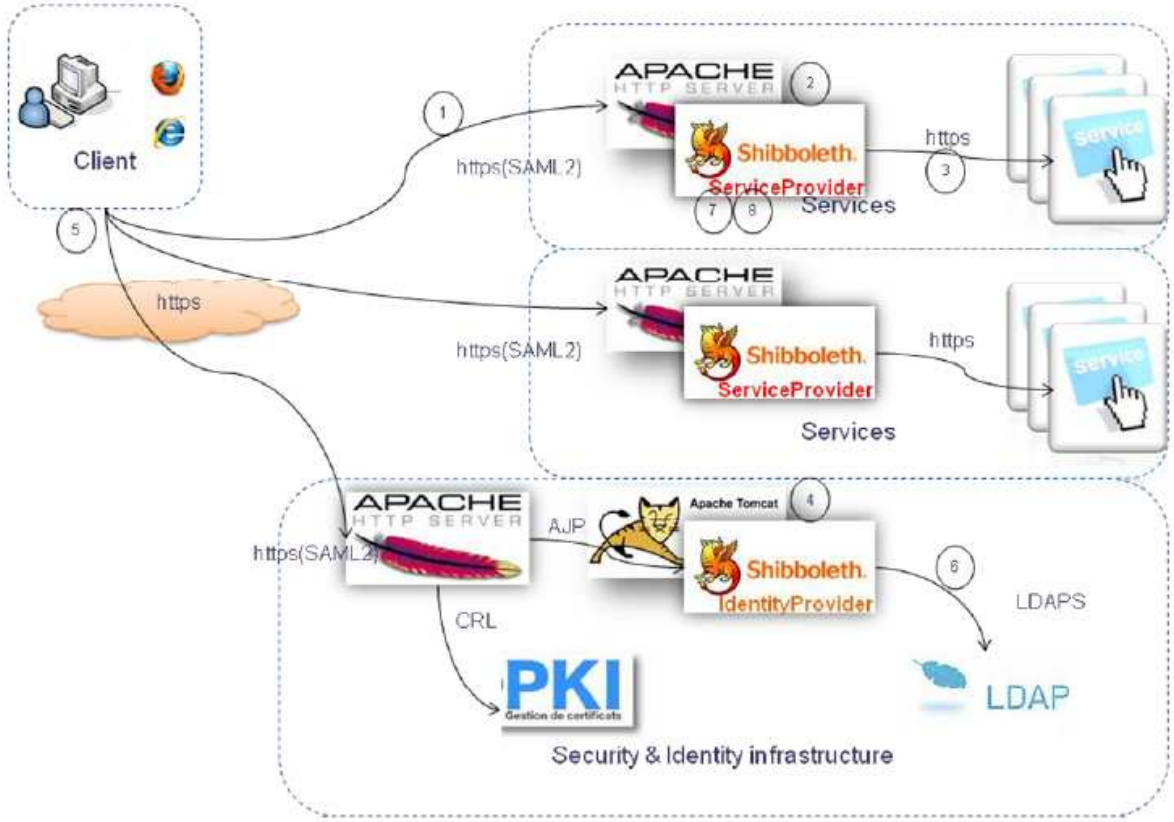

Figure 1 - schéma d'intégration du produit

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – pare-feu
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☒ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

Nom du produit	PASS
Numéro de version analysée	2.0

La version du produit n'est pas directement identifiable : il faut se référer aux versions des packages *Shibboleth* :

- version 2.5.1 pour le *Service Provider* ;
- version 2.3.6 pour l'*Identity Provider*.

1.2.3. Services de sécurité évalués

Les principaux services de sécurité fournis par le produit sont :

- l'authentification des utilisateurs par login/mot de passe ;
- l'authentification des utilisateurs par certificat X509 ;
- l'authentification unique *(Single Sign-On* - SSO) ;
- la protection des données utilisateur transmises au service métier ;
- la gestion des sessions utilisateurs ;
- la journalisation des authentifications ;
- l'administration sécurisée des serveurs SP et IDP.

1.2.4. Configuration évaluée

Pour l'évaluation, le produit a été configuré pour utiliser une authentification par mot de passe ou par certificats numériques avec identification du client à partir de son UID (identifiant) LDAP.
Les guides d'installation et de configuration fournis ont été suivis, aussi bien pour la TOE que pour le serveur LDAP.
Aucune option de configuration autre que celles définies dans les guides n'a été retenue.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN].

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 3 « argumentaire »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 5 « description des biens sensibles »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 6 « description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 7 « description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 4.3 « description des utilisateurs typiques »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Pour les besoins de l'évaluation, le CESTI a mis en place une architecture jugée représentative des plateformes web couramment déployées.

Les services *Identity Provider*, *Service Provider*, l'application métier et le serveur supportant les services d'infrastructure (PKI et annuaire) ont été installés sur des serveurs différents.

2.3.2.2. Particularités de paramétrage de l'environnement

Le *Service Provider* et l'*Identity Provider* sont installés sur des environnements d'exécution sécurisés conformément aux instructions du manuel d'installation.

Côté client, la seule exigence concerne l'utilisation d'un navigateur supportant notamment :
- les cookies,
- les certificats,
- JavaScript,
- TLS v1.0 ou au minimum les suites SSL AES256-SHA et AES128-SHA.

2.3.2.3. Options d'installation retenues pour le produit

Aucune option d'installation particulière n'a été utilisée.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

L'installation du produit n'est pas triviale, elle nécessite un temps conséquent et des connaissances sur le standard SAML, la gestion de PKI et LDAP.
Pour cette raison, le produit a été fourni prêt à fonctionner à l'évaluateur.

2.3.2.5. Durée de l'installation

L'installation, bien qu'elle n'ait pas été réalisée de façon complète par l'évaluateur, est estimée entre 2 et 3 jours selon le degré de maîtrise de l'administrateur.

2.3.2.6. Notes et remarques diverses

Néant.

2.3.3. Analyse de la documentation

Les guides fournis par le développeur sont complets et d'un bon niveau de détail. L'évaluateur a cependant noté deux écarts aux bonnes pratiques jugés non bloquants :
- le chiffrement des clés privées utilisées pour la génération des différents certificats n'est pas préconisé ;
- la définition des suites SSL pour la configuration du serveur LDAPS n'est pas précisée.

2.3.4. Fonctionnalités testées

Les fonctionnalités suivantes ont été soumises à des tests de conformité.

Fonctionnalité	Résultat
Authentification des utilisateurs par mots de passe	**CONFORME**
Authentification des utilisateurs par certificats X509	**CONFORME**
SSO (Single Sign-On ou authentification unique)	**CONFORME**
Protection des données utilisateurs transmises au service métier	**CONFORME**
Gestion des sessions utilisateurs	**CONFORME**
Journalisation des authentifications	**CONFORME**
Administration des serveurs Service Provider et Identity Provider	**CONFORME**

2.3.5. Fonctionnalités non testées

Néant.

2.3.6. Synthèse des fonctionnalités testées / non testées et des non-conformités

Les fonctionnalités testées sont conformes à ce qui est décrit dans la cible de sécurité [CDS].

2.3.7. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à sa cible de sécurité.

2.3.8. Analyse de la résistance des mécanismes et des fonctions

2.3.8.1. Liste des fonctions et des mécanismes testés

Les fonctionnalités suivantes ont été soumises à des tests de pénétration :

Fonctionnalité	Résultat
Authentification des utilisateurs par mots de passe	**Réussite**
Authentification des utilisateurs par certificats X509	**Réussite**
SSO (Single Sign-On ou authentification unique)	**Réussite**
Protection des données utilisateurs transmises au service métier	**Réussite**
Gestion des sessions utilisateurs	**Réussite**
Journalisation des authentifications	**Réussite**
Administration des serveurs Service Provider et Identity Provider	**Réussite**

2.3.8.2. Avis d'expert sur la résistance des mécanismes

L'évaluateur n'a pas pu mettre en évidence de faiblesse dans l'implémentation des mécanismes selon les conditions définies dans la cible de sécurité.

2.3.9. Analyse des vulnérabilités (conception, construction…)

2.3.9.1. Liste des vulnérabilités connues

Des vulnérabilités publiques connues au moment de l'évaluation ont été analysées ; elles ont été jugées non applicables au produit par l'évaluateur dans le contexte d'emploi et la configuration retenus, sauf une permettant de réaliser un déni de service sur le parseur XML.

2.3.9.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été identifié de vulnérabilité exploitable dans le périmètre d'évaluation et pour le cas d'usage considéré.

2.3.10. Accès aux développeurs

Aucun support du développeur n'a été requis au cours de l'évaluation.

2.3.11. Analyse de la facilité d'emploi et préconisations

2.3.11.1. Cas où la sécurité est remise en cause

Néant.

2.3.11.2. Recommandations pour une utilisation sûre du produit

L'évaluateur recommande que les serveurs composant la solution PASS soient isolés des utilisateurs via un équipement filtrant de type pare-feu.

2.3.11.3. Avis d'expert sur la facilité d'emploi

L'utilisation du produit est transparente pour l'utilisateur et de ce fait accessible à un public sans connaissances spécifiques.

2.3.11.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

L'évaluateur a procédé à une analyse des mécanismes cryptographiques offerts par le produit. Celle-ci n'a pas relevé de manquements jugés bloquants, néanmoins l'évaluateur a mis en évidence les non-conformités suivantes :

- l'algorithme de signature utilisé pour signer les requêtes et les réponses est RSASSA-PKCS1v1_5 qui n'est pas conforme aux recommandations du [RGS] car ne disposant pas de preuve de sécurité ;
- le guide d'installation valide l'emploi de clés RSA de 2048 bits pour une utilisation allant jusqu'en 2030 ; le [RGS] prévoit que cette longueur de clé ne doit pas être employée au-delà de 2020.

2.5. Analyse du générateur d'aléas

Le produit fait appel au générateur d'*OpenSSL* pour la génération de nombres pseudo-aléatoires.
L'évaluation n'a pas mis en évidence de vulnérabilités dans le produit liées à l'utilisation de ce générateur.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « PASS v2.0 : solution d'authentification unique basée sur les composants Shibboleth Service Provider v2.5.1 et Identity Provider v2.3.6 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport, notamment assurer la protection physique du produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	*CIBLE DE SECURITE CSPN* *DU PRODUIT PASS (Product for Advanced SSO)* Référence : TH/DSC/R&T/CEA/SC2/ar,12/0008/TECH ; Version : C ; Date : 16/06/2014.
[RTE]	*Rapport Technique d'Évaluation (RTE) CSPN PASS ;* Référence : OPPIDA/CESTI/PASS2/RTE/1.0 ; Version : 1.0 ; Date : 31/07/2014.
[GUIDE]	*Guide d'administration ;* Référence : Guide d'administration-v29-20140423_1120 ; Version du 23 avril 2014. *PLAN D'INSTALLATION DU PRODUIT PASS (Product for Advanced SSO) ;* Référence : Installation PASS V20.pdf ; Version 2 ; Date : 28/06/2013.
[CRY]	*DOCUMENT CRYPTOGRAPHIQUE CSPN* *DU PRODUIT PASS (Product for Advanced SSO) ;* Référence : Document cryptographique CSPN V3.pdf ; Version : 2 ; Date : 30/06/2014.

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr.