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-CC-PP-2016/03 du profil de protection « Protection Profile for Trusted Signature Creation Module in TW4S Holder-side authentication module base PP » (version 1.2)

Paris, le 11mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-PP-2016/03

Nom du profil de protection

Protection Profile for Trusted Signature Creation Module in TW4S

Référence/version du profil de protection

PP-RSCD-TSCM/TW4S 1.2

Conformité à un profil de protection

Néant

PP-Base certifiée

Holder-side authentication module base PP

PP-Modules associés aux PP-Configurations certifiées

PP-module Privacy module

PP-module External Key Storage module

Critères d'évaluation et version

Critères Communs version 3.1, révision 4

Niveau d'évaluation imposé par le PP

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Rédacteur

ANSSI

51 boulevard de La Tour-Maubourg 75700 Paris 07SP – France

Commanditaire

ANSSI

51 boulevard de La Tour-Maubourg 75700 Paris 07SP – France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B,

78180 Montigny le Bretonneux – France

Accords de reconnaissance applicables

CCRA

SOG-IS

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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Table des matières

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Protection Profile for Trusted Signature Creation Module in TW4S.
Référence, version : PP-RSCD-TSCM/TW4S, 1.2.
Date : 19 février 2016.

1.2. Rédacteur

Ce profil de protection a été rédigé par :

ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07SP - France

1.3. Description du profil de protection

Le profil de protection (PP) a été rédigé dans le cadre de la réglementation Européenne *electronic Identification and Signature* eIDAS [REGLE] sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

La TOE fait partie du système *Trustworthy Sytems Supporting Server Signing* (T4WS), décrit sur la figure 1.

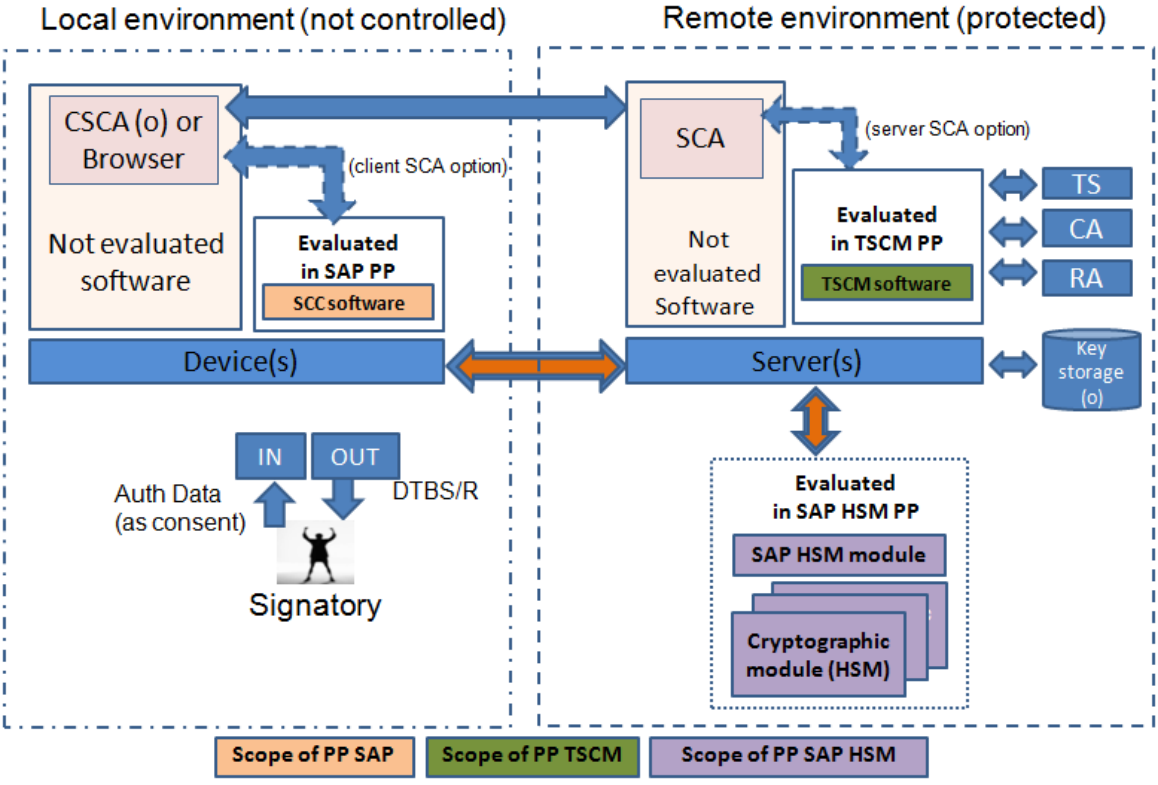

Figure 1 : Aperçu du système TW4S et périmètre du PP

Le système se décompose ainsi :

- un environnement distant (*Remote environment* sur la figure 1, également appelé *Server Side*) et qui dispose :

    - de l'application *Signature Creation Application* (SCA*)* : application de création de la signature comportant un composant serveur connecté à un composant client *Client SCA* (CSCA) qui initie la demande de signature ;
    - du module *Trustworthy Signature Creation Module* (TSCM): module de création de signature de confiance conforme au [PP TSCM] qui gère les demandes de signature. Ce composant doit être conforme au présent PP
    - du module SAP *Hardware Security Module* (HSM) : ce module doit être certifié selon le [PP SAP HSM], lui-même conforme au [PP CEN]. Ce module réalise le contrôle d'accès aux opérations de signature réalisées par le module cryptographique du HSM afin de réaliser les opérations de signature pour le signataire ;
    - d'autres modules sont présents: *Time Source* (TS), *Certification Authority* (CA), *Registration Authority* (RA);

- un environnement local (*Local environment* sur la figure 1 également appelé *Holder-Side environnement* dans le PP) ne faisant pas partie du périmètre de ce PP et qui dispose :

    - de l'application *Client Signature Creation Application* (CSCA), ainsi que d'autres composants en dehors du périmètre de ce PP ;
    - du composant *Sole Control Component* (SCC) qui exécute les différentes opérations de la signature et doit en garantir le contrôle exclusif par le signataire ;
    - des interfaces gérant l'échange des données en entrée du signataire (IN) et l'affichage (OUT).

  Dans ce contexte, la notion de serveur (*server*) signifie que les applications peuvent soit se trouver sur le même serveur, soit être reliées au serveur par un lien sécurisé logique ou physique. De façon similaire la notion de client (device) signifie que les applications peuvent soit se trouver sur le même environnement client, soit être reliées au client par un lien sécurisé logique ou physique.

  Les modules HSM et SAP font l'objet d'une description complète respectivement dans les cibles de sécurité conformes aux PP [PP SAP HSM] et [PP SAP].

Le système pris dans son ensemble doit :

- garantir que les données à signer *Data To Be Signed* (DTBS) en entrée du processus de signature ont effectivement été vues ou sélectionnées par le signataire ;
- garantir l'authentification du signataire sur le serveur en utilisant une vérification des données du signataire soit directement par le serveur, soit par le client SCC qui réalise lui-même une authentification avec le serveur (TSCM ou SAP HSM) au nom du signataire ;
- garantir que les données de création de signature *Signature Creation Data* (SCD) ont été activées uniquement après authentification du signataire ; et que le lien entre

l'authentification du signataire, les données SCD à utiliser et les données à signer DTBS a été validé.

Toutes ces étapes doivent garantir l'absence de rejeu de l'authentification sur le SCC, ainsi que l'intégrité et la confidentialité des données à signer et des résultats de la signature.

Ce PP définit les exigences de sécurité du composant logiciel (TSCM), garantissant que les échanges provenant directement du signataire ou les informations collectées du signataire par l'agent de personnalisation sont transmis sans compromettre leur intégrité et confidentialité

Le PP comprend deux profils de protection de base :

- *Holder-side authentication module :* lorsque l'authentification du signataire est effectuée par le *« Sole Control Component » ;*
- *Server-side authentication module :* lorsque l'authentification du signataire est effectuée par le serveur ;

et deux PP-modules optionnels :

- *Privacy module* : qui correspond aux principales fonctions de protection de la confidentialité des données du signataire *Data To Be Signed*, données à signer ;
- *External Key Storage module* : qui correspond aux fonctions requises lorsque les clés du signataire ne sont pas utilisées et qu'elles sont stockées en dehors du HSM.

Le PP faisant l'objet de ce certificat correspond au *Holder-side authentication module.*

Ce profil de protection autorise ainsi plusieurs configurations. Les configurations évaluées sont définies dans le chapitre 1.6.

1.4. Exigences fonctionnelles

Le profil de protection définies une **exigence fonctionnelle de sécurité**[1] :

- FIA_API.1 Authentication Proof of Identity.

De plus, le profil de protection reprend des exigences fonctionnelles de sécurité définies dans la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4 augmenté des composants d'assurance suivants : AVA_VAN.5, ALC_DVS.2**.

Toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

[1] Exigences fonctionnelles étendues non issues de la partie 2 des [CC].

1.6. Configurations évaluées

Quatre PP-configurations ont été évaluées et sont certifiées :

1. Profil de protection de base « *Holder-side authentication module* » ;
2. Profil de protection de base « *Holder-side authentication module* » et PP-module « *Privacy module* » ;
3. Profil de protection de base « *Holder-side authentication module* » et PP-module « *External Key Storage module* » ;
4. Profil de protection de base « *Holder-side authentication module* » et PP-modules « *External Key Storage module* » et « *Privacy module* ».

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'addendum à ces deux méthodologies [Modular-PP].

2.2. Commanditaire

ANSSI
51 boulevard de la Tour-Maubourg,
75700 Paris 07 SP,
France

2.3. Centre d'évaluation

OPPIDA
4-6 avenue du vieil étang
Bâtiment B
78180 Montigny le Bretonneux,
France

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 février 2016, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives aux composants d'assurance ci-dessous sont à « **réussite** ».

Pour la configuration 1 (Profil de protection de base, voir le chapitre 1.6), les composants évalués (définis dans [CC]) sont les suivants :

Composants	Descriptions
APE_CCL.1	Conformance claims
APE_ECD.1	Extended components definition
APE_INT.1	Protection profile introduction
APE_OBJ.2	Security objectives
APE_REQ.2	Derived security requirements
APE_SPD.1	Security problem definition

Tableau 1 - Evaluation du PP pour la configuration 1

Pour les configurations 1,2,3, 4 (Profil de protection de base et les différents PP-modules) les composants évalués (définis dans [Modular-PP]) sont les suivants :

Composants	Descriptions
ACE_CCL.1	PP-module conformance claims
ACE_ECD.1	PP-module Extended components definition
ACE_INT.1	PP-module introduction
ACE_OBJ.1	PP-module objectives
ACE_REQ.1	PP-module security functional requirements
ACE_SPD.1	PP-module Security problem definition
ACE_MCO.1	PP-module consistency
ACE_CCO.1	PP-module configuration consistency

Tableau 2 - Evaluation du PP pour les configurations 1, 2, 3 et 4

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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

3.2. Reconnaissance européenne (SOG-IS)

Ce rapport de certification est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour classes d'assurance APE et ACE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

3.3. Reconnaissance internationale (CC RA)

Ce rapport de certification est émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs. La reconnaissance s'applique pour les classes d'assurance APE et ACE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	**2**	**1**	Implementation representation ofthe TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ADO_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Identification of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références

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.	
[CPP-P-01]	Procédure ANSSI-CC-CPP-P-01 Certification de profils de protection, version 2 du 30 mai 2011. ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[Modular-PP]	CC and CEM addenda - Modular PP, March 2014, version 1.0, ref CCDB-2014-03-001.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[RTE]	Evaluation Technical Report PP TSCM, 26 février 2016, version 2.0, Oppida.
[REGLE]	Règlement (UE) No 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.
[PP SAP HSM]	en cours de rédaction.
[PP CEN]	Protection Profile for TSP Cryptographic modules – part 5 Cryptographic module for Trust Services, référence 419 221-5 en cours d'évaluation.
[PP SAP]	Protection profile for Signature Activation Protocol, version 1.4, 15 janvier 2016.