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-2015/09 du profil de protection « Cryptographic Module for CSP key generation services - PP CMCKG »

ref 419221-3:2015, Version 0.20 et ref 419221-1:2015

Paris, le 17 septembre 2015

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-PP-2015/09

Nom du profil de protection

Cryptographic Module for CSP key generation services - PP CMCKG

Référence/version du profil de protection

ref 419221-3:2015, Version 0.20 et ref 419221-1:2015

Conformité à un profil de protection

Néant

PP-Base certifiée

Néant

PP-Modules associés aux PP-Configurations certifiées

Néant

Critères d'évaluation et version

Critères Communs version 3.1, révision 3

Niveau d'évaluation imposé par le PP

EAL 4 augmenté

AVA_VAN.5

Rédacteur

CEN/TC 224

Rue de Stassart 36
1050 Bruxelles - Belgique

Commanditaire

CEN

Rue de Stassart 36
1050 Bruxelles - Belgique

Centre d'évaluation

OPPIDA

6, avenue du Vieil Etang
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 : Cryptographic Module for CSP key generation services protection profile CMCKG-PP - Protection Profile CMCKG PP
Référence : 419221-3:2015 Version:0.20 et 419221-1:2015

Date : août 2015

1.2. Rédacteur

Ce profil de protection a été rédigé par le comité technique :

CEN/TC 224
Rue de Stassart 36
1050 Bruxelles
Belgique

1.3. Description du profil de protection

Le profil de protection [PP] a été rédigé par le groupe de travail 17 du comité technique européen CEN/TC 224. Ce groupe de travail a pour mission la définition de profils de protection relatifs aux dispositifs sécurisé de création de signatures électronique (*SSCD*)[1].

Le présent profil de protection [PP] définit les exigences fonctionnelles d'un module cryptographique *(Cryptographic Module*) utilisé par un prestataire de service de certification *(Cryptographic Service Provider)* comme un élément de son système de confiance pour fournir des services de génération de clés.

La cible d'évaluation est le module cryptographique, qui est utilisé pour la création des clés privés de l'abonné et leur chargement au sein du dispositif sécurisé de création de signature électronique (*SSCD*).

1.4. Exigences fonctionnelles

Le profil de protection reprend les exigences fonctionnelles de sécurité[2] suivantes définies dans la partie 2 des Critères Communs [CC] :

- Audit data generation (FAU_GEN.1) ;
- User identity association (FAU_GEN.2) ;
- Guarantees of audit data availability (FAU_STG.2) ;

[1] *Secure Signature Création Device.*
[2] Exigences fonctionnelles étendues non issues de la partie 2 des [CC].

- Cryptographic key generation (FCS_CKM.1) ;
- Cryptographic key destruction (FCS_CKM.4) ;
- Cryptographic operation (FCS_COP.1) ;
- Subset access control (FDP_ACC.1) ;
- Subset access control (FDP_ACF.1) ;
- Export of user data without security attributes (FDP_ETC.1) ;
- Subset residual information protection (FDP_RIP.1) ;
- Stored data integrity monitoring and action (FDP_SDI.2) ;
- Basic data exchange confidentiality (FDP UCT.1) ;
- Authentication failure handling (FIA_AFL.1) ;
- User attribute definition (FIA_ATD.1) ;
- Verification of secrets (FIA_SOS.1) ;
- Timing of authentication (FIA_UAU.1) ;
- Timing of identification (FIA_UID.1) ;
- User-subject binding (FIA_USB.1) ;
- Management of security functions behavior (FIA_MOF.1) ;
- Management of security attributes (FMT_MSA.1) ;
- Secure security attributes (FMT_MSA.2) ;
- Static attribute initialization (FMT_MSA.3) ;
- Management of TSF data (FMT_MTD.1) ;
- Specification of Management Functions (FMT_SMF.1) ;
- Security roles (FMT_SMR.1) ;
- Unobservability (FPR_UNO.1) ;
- Failure with preservation of secure state (FPT_FLS.1) ;
- Notification of physical attack (FPT_PHP.2) ;
- Resistance to physical attack (FPT_PHP.3) ;
- Manual recovery (FPT_RCV.1) ;
- Reliable time stamps (FPT_STM.1) ;
- TSF testing (FPT_TST.1) ;
- Inter TSF trusted channel (FTP_ITC.1) ;
- Trusted path (FTP_TRP.1).

1.5. Exigences d’assurance

Le niveau d’assurance exigé par le profil de protection est le niveau **EAL4 augmenté du composant d'assurance suivant AVA_VAN.5**.

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

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM]. Commanditaire

CEN
Rue de Stassart 36
1050 Bruxelles
Belgique

2.2. Centre d'évaluation

OPPIDA
6 avenue du vieil étang
78180 Montigny le Bretonneux
France

2.3. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 31 août 2015, 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** ».

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

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. 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. 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, Singapour, 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 of 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
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Sufficient 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_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
ASE Evaluation de la cible de sécurité	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_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
ATE Tests	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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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.
[PP]	“PP for TSP cryptographic modules – Part 1: Overview”, ref 419221-1, août 2015, “PP HSM CMCKG 14167-3”,version 0.20 ref 419221-34, août 2015.
[RTE]	PP_CMCKG_APE_v4.0, ref OPPIDA/CESTI/CMCKG/APE, version 4.0, 31 août 2015.