



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-2018/02
du profil de protection
« Trustworthy Systems Supporting Server
Signing Part 2 : Protection Profiles for QSCD
for Server Signing »
(prEN 419 241-2, version 0.16)**

Paris, le 19 juin 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]





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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CC-PP-2018/02
Nom du profil de protection	Trustworthy Systems Supporting Server Signing Part 2 : Protection Profiles for QSCD for Server Signing
Référence/version du profil de protection	prEN 419 241-2, version 0.16
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 4
Niveau d'évaluation imposé par le PP	EAL 4 augmenté AVA_VAN.5
Rédacteur(s)	CEN/TC 224/WG17 CEN/ISSS Secretariat 17 avenue Marnix, 1000 Bruxelles, Belgique
Commanditaire	ANSSI 51 boulevard de la Tour Maubourg, 75700 Paris cedex 07 SP, France
Centre d'évaluation	Oppida 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables	 

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. PRESENTATION DU PROFIL DE PROTECTION.....	6
1.1. IDENTIFICATION DU PROFIL DE PROTECTION.....	6
1.2. REDACTEUR.....	6
1.3. DESCRIPTION DU PROFIL DE PROTECTION	6
1.4. EXIGENCES FONCTIONNELLES.....	6
1.5. EXIGENCES D'ASSURANCE	7
2. L'EVALUATION	8
2.1. REFERENTIELS D'EVALUATION	8
2.2. COMMANDITAIRE	8
2.3. CENTRE D'EVALUATION.....	8
2.4. TRAVAUX D'EVALUATION.....	8
3. LA CERTIFICATION.....	9
3.1. CONCLUSION	9
3.2. RECONNAISSANCE EUROPEENNE (SOG-IS)	9
3.3. RECONNAISSANCE INTERNATIONALE (CC RA).....	9
ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT.....	10
ANNEXE 2. REFERENCES.....	11

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : « *Trustworthy Systems Supporting Server Signing Part 2 : Protection Profiles for QSCD for Server Signing* »

Référence, version : prEN 419 241-2, 0.16

Date : 11 mai 2018

1.2. Rédacteur

Ce profil de protection a été rédigé par :

CEN/TC 224/WG17

CEN/ISSS Secretariat

17 avenue Marnix

1000 Bruxelles

Belgique

1.3. Description du profil de protection

Le profil de protection [PP] a été rédigé par le Comité européen de normalisation (CEN) dans le cadre de travaux liés à la réglementation européenne « *electronic Identification and Signature* » [eIDAS].

Le profil de protection [PP] définit les exigences de sécurité d'un module d'activation de signature (*Signature Activation Module* – SAM) faisant partie d'un dispositif de création de signature qualifiée (*Qualified electronic Signature Creation Device* – QSCD).

Le module d'activation de signature est un composant logiciel qui implémente le protocole d'activation de signature (*Signature Activation Protocol* – SAP). Il est soit déployé dans la partie protégée d'un module cryptographique (*Cryptographic Module*) soit dans un environnement protégé et connecté au module cryptographique via un canal de confiance. Il utilise les données d'activation de signature (*Signature Activation Data* – SAD) du signataire pour activer les clés de signature utilisées dans un module cryptographique.

La TOE et le module cryptographique définissent le dispositif de création de signature qualifiée.

1.4. Exigences fonctionnelles

L'exigence fonctionnelle de sécurité définie par le profil de protection¹ est la suivante :

- FCS_RNG.1 Random numbers generation.

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

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

- Audit data generation (FAU_GEN.1) ;
- User identity association (FAU_GEN.2) ;
- Cryptographic key generation (FCS_CKM.1) ;
- Cryptographic key destruction (FCS_CKM.4) ;
- Cryptographic operation (FCS_COP.1) ;
- Subset access control (FDP_ACC.1) ;
- Security attribute based access control (FDP_ACF.1) ;
- Export of user data with security attributes (FDP_ETC.2) ;
- Subset information flow control (FDP_IFC.1) ;
- Simple security attributes (FDP_IFF.1) ;
- Import of user data with security attributes (FDP_ITC.2) ;
- Basic data exchange confidentiality (FDP_UCT.1) ;
- Data exchange integrity (FDP_UIT.1) ;
- Authentication failure handling (FIA_AFL.1) ;
- User attribute definition (FIA_ATD.1) ;
- Timing of authentication (FIA_UAU.1) ;
- Multiple authentication mechanisms (FIA_UAU.5) ;
- User identification before any action (FIA_UID.2) ;
- User-subject binding (FIA_USB.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) ;
- Restrictions on security roles (FMT_SMR.2) ;
- Passive detection of physical attack (FPT_PHP.1) ;
- Resistance to physical attack (FPT_PHP.3) ;
- Replay detection (FPT_RPL.1) ;
- Reliable time stamps (FPT_STM.1) ;
- Inter-TSF basic TSF data consistency (FPT_TDC.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 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 4** [CC], à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2. Commanditaire

ANSSI

51 boulevard de la Tour-Maubourg
75700 Paris cedex 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 13 juin 2018, 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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique à la classe d'assurance APE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



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 signataires², des certificats Critères Communs. La reconnaissance s'applique à la classe d'assurance APE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Product support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ADO_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	1	Identification of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	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, revision 4, ref CCMB-2012-09-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[eIDAS]	Règlement (UE) n°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 direction 1999/93/CE.
[PP]	Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, référence prEN 419 241-2, version 0.16, 11 mai 2018.
[RTE]	Evaluation Technical Report – PP_QSCD, référence : OPPIDA/CESTI/PP_QSCD/APE/3.0, 13 juin 2018.