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-2016/07

HSM TrustWay Proteccio
Version V128/X130

Paris, le 17 février 2016

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

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

Référence du rapport de certification

ANSSI-CC-2016/07

Nom du produit

HSM TrustWay Proteccio

Référence/version du produit

TrustWay Proteccio EL : 1.05.03 - 76681604-004D/76681604-005 (hardware), V128 (module de sécurité), X130 (système)

TrustWay Proteccio HR : 1.05.03 - 76681610-004D/76681610-005 (hardware), V128 (module de sécurité), X130 (système)

Conformité à un profil de protection

Aucun

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5

Développeur

BULL SAS

Avenue Jean Jaurès, BP 68, 78340 Les Clayes-sous-Bois, France

Commanditaire

BULL SAS

Avenue Jean Jaurès, BP 68, 78340 Les Clayes-sous-Bois, France

Centres d'évaluation

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Amossys

4 bis allée du bâtiment, 35000 Rennes, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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

Le produit évalué est le « HSM TrustWay Proteccio, version V128/X130 » développé par *BULL*. Il se présente sous la forme d'une *appliance*, composée d'une carte électronique principale, intégrée dans un boitier 19 pouces 2U avec une interface Ethernet Gigabit, et qui offre une protection physique contre les tentatives d'altérations physiques.

La plate-forme TrustWay Proteccio existe sous deux formes :

- une forme dite d'entrée de gamme (EL – *Entry Level*) avec un module Com Express au format micro et basée sur un processeur *ATOM* et un FPGA[1] *ARRIA2GX125* ;
- une forme dite à haute performance (HR – *High Range*) avec un module Com Express au format basique embarquant un processeur *Core 2 Duo* ou *Core I5* et un FPGA *ARRIA2GX260*.

Le HSM fournit des fonctions cryptographiques de type :

- chiffrement ;
- signature numérique ;
- gestion de clés (y compris la génération et le stockage sécurisé).

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité se base sur le profil de protection [PP-CM-SOB], *Cryptographic Module for CSP Signing Operations with Backup – Protection Profile* - prEN 14167-2:2012.

[1] *Field-Programmable Gate Array* ou circuit logique programmable.

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

Nom	TrustWay Proteccio EL	TrustWay Proteccio HR
Cible d'évaluation		
Version matérielle	**76681604-004D** **76681604-005**	**76681610-004D** **76681610-005**
Version logicielle « module de sécurité »	**V128**	**V128**
Version logicielle « système »	**X130**	**X130**
Environnement IT		
Version logicielle	**1.05.03**	**1.05.03**

Tableau 1 - identification des versions de la TOE

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la signature et la vérification de signature ;
- le chiffrement et le déchiffrement ;
- le calcul de condensats (*hash*) ;
- *le wrapping* et l'*unwrapping* de clefs ;
- la gestion sécurisée de clés : génération, stockage, sauvegarde, restauration, destruction ;
- la protection en intégrité et en confidentialité du code du FPGA : vérification de la signature lors du démarrage et de la mise à jour, déchiffrement à la volée lors de l'exécution ;
- l'installation sécurisée via notamment la génération de cartes à puces d'installation et d'administration ;
- la gestion des évènements de sécurité (journalisation et protection en intégrité) et la génération d'alarmes ;
- la protection des services de la TOE, qui s'appuie sur un mécanisme d'authentification et un contrôle d'accès basé sur les rôles des utilisateurs (RBAC, *Role-Based Access Control*).

1.2.4. Architecture

Le produit se présente sous la forme d'un boîtier au format 19 pouces 2U rackable avec alimentation intégrée et interfaces en face avant. La plate-forme est reliée au système hôte par le biais d'une interface Ethernet Gigabit. Elle comprend un processeur réseau (ComExpress) et un processeur cryptographique (FPGA).

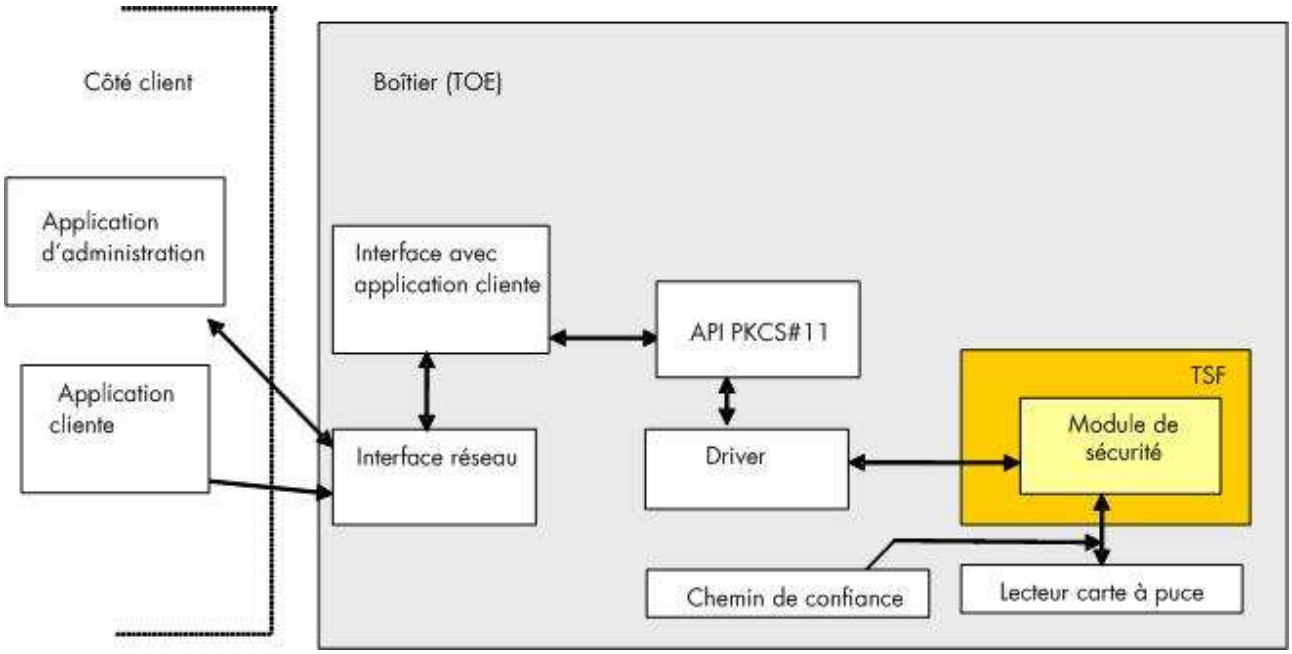

Figure 1 - Description de la TOE dans son environnement

Le produit est constitué :

- d'une carte électronique principale (appelée carte mère) sur laquelle sont montés les éléments suivants :
  - un processeur réseau implémenté sous la forme d'un module ComExpress comprenant un processeur *INTEL* sur lequel tourne *LINUX* et le logiciel applicatif ;
  - un composant Ethernet 10/100/1000 à interface PCI Express ;
  - un composant chiffre FPGA *ALTERA*, appelé CC, embarquant trois processeurs NIOS2 et toutes les interfaces de programmation de chiffrement symétriques et asymétriques requises ;
  - un microcontrôleur *ATMEL* appelé MCS pour le chargement sécurisé du *bitstream*[1] du FPGA, la gestion des alarmes anti-intrusion et la sauvegarde d'une clé rouge *BULL* et/ou des CIK (*Crypto Ignition Key*) ;
  - 512 Mo de RAM DDR2 protégée par ECC (*Error Correction Code*) pour le code, les données et clés du composant CC ;
  - 128 Mo de FLASH NOR incluant le *bitstream* du FPGA et le code du processeur cryptographique ;
  - 2 GB de FLASH NAND pour le stockage de clés noires ;
  - un CPLD (*Complex Programmable Logic Device*) pour le partage de la FLASH et de l'afficheur entre le CC et le MCS ;
- d'un disque dur 2,5 pouces relié en SATA au module ComExpress ;
- d'une pile lithium 3.6V pour le maintien de la clé rouge dans le MCS et l'alimentation des alarmes actives hors Tension ;
- d'une alimentation ATX AC/DC d'au moins 100 W ;
- de deux ou trois ventilateurs en fonction du modèle.

[1] Données de configuration du FPGA.

Les interfaces externes de l'équipement sont les suivantes :

- en face avant :
  - deux interfaces Ethernet RJ45 (reliées au module ComExpress et au composant Ethernet de la carte mère), dont une seulement est active (eth0) ;
  - une interface VGA en face avant reliée au module ComExpress ;
  - quatre interfaces USB 2.0 (clavier, souris, disque externe, etc.) ;
  - un connecteur carte à puce relié au FPGA ;
  - un écran LCD relié au CPLD ;
  - un clavier 16 touches relié au FPGA ;
  - un bouton d'arrêt d'urgence relié au FPGA ;
  - une LED de statut bicolore (*Ready*, *Error*/*Alarm*) reliée au FPGA ;
  - une LED de statut pile faible reliée au FPGA ;
- en face arrière :
  - le connecteur d'alimentation 220 V ;
  - un interrupteur pour l'alimentation 220V ;
  - un connecteur liaison série DB9.

Le produit est en outre livré avec un jeu de cartes à puce vierges, décrites au 1.2.6 et destinées à l'installation et à l'administration de la TOE.

1.2.5. Cycle de vie

Le produit est développé sur les sites suivants :

***BULL* Les Clayes-sous-Bois**	***BULL* Angers**
Avenue Jean Jaurès, BP 68, 78340 Les Clayes-sous-Bois, France	357 avenue Patton, BP 20845, 49008 Angers France

Enfin, une partie de la conception du produit est sous-traitée à la société *ASTEELFLASH*. Le site suivant intervenant dans le cycle de vie du produit a été audité dans le cadre de la présente évaluation :

ASTELFLASH Atlantique

Le Clos de la Grée,
35660 Langon,
France

Le cycle de vie du produit est le suivant :

Phase		Responsabilité	Environnement
1	Développement	L'équipe de développement se charge de la conception matérielle et du développement du logiciel implémentant les services de la TOE. (responsabilité du développeur)	Cette phase est réalisée dans les locaux de *BULL* Les Clayes-sous-Bois
2	Signature des logiciels	Toutes les signatures utilisent des courbes elliptiques de 256 bits selon le mécanisme asymétrique EC-KCDSA. (responsabilité de l'intégrateur)	Cette phase est réalisée dans les locaux de *BULL* Les Clayes-sous-Bois
3	Fabrication	Cette phase comprend les étapes suivantes de la fabrication du HSM : - fabrication du circuit imprimé de la carte mère ; - fabrication du boîtier; - assemblage, programmation et test des composants ; - intégration dans le boîtier ; - tests du boitier.	Réalisées dans les locaux de : SOMACIS[1] ATOS ASTEEL
4	Tests et préparation par Bull	BULL Angers réalise des tests de robustesse complémentaires et prépare le HSM pour la phase suivante, réalisée sur réception d'une commande.	Ces phases sont réalisées dans les locaux de *BULL* Angers
5	Pré-personnalisation	Cette phase comprend la mise à jour du logiciel du composant cryptographique (FPGA) et du logiciel du module ComExpress, ainsi que l'injection des éléments de pré-personnalisation. A la fin de cette phase, le TrustWay Proteccio est prêt à être envoyé au client pour personnalisation.	
6	Livraison au client	Le TrustWay Proteccio est envoyé au client.	
7	Personnalisation	Personnalisation par le client.	Ces phases sont réalisées dans l'environnement du client
8	Mise à jour du logiciel implémentant les services de la TOE	Si nécessaire, l'Officier de sécurité maître du client peut effectuer la mise à jour du logiciel du HSM. (responsabilité du client)	
9	Utilisation de la TOE	Cette dernière phase est réalisée par le client.	

L'évaluation couvre les phases 1 à 6. Sont notamment exclues les processus de personnalisation, configuration et mise à jour du logiciel implémentant les services de la TOE dans l'environnement du client.

[1] Le site de SOMACIS n'a pas été audité, aucune menace n'ayant été reliée à cette étape de la conception du produit.

1.2.6. Configuration évaluée

L'évaluation a porté sur les versions de la TOE identifiées au chapitre 1.2.2.
La TOE existe en deux déclinaisons, EL et HR ; les deux modèles ont été mis à disposition du CESTI pour les besoins de l'évaluation. Si les tests chez le CESTI ont principalement été joués sur le modèle HR, celui-ci s'est assuré, notamment en rejouant une partie des tests fonctionnels dans les locaux du développeur, que les résultats observés étaient applicables aux deux versions du produit.

Le produit est livré dans un état dit « Prêt à être personnalisé par le client », avec un jeu de cartes à puce vierges (carte *Ideal Citiz* développée par *MORPHO*, certifiée au niveau EAL5+ sous la référence [ANSSI-CC-2010-56] et maintenue sous la référence [ANSSI-CC-2011/63-M01].

La personnalisation de la TOE et son administration ont été effectuées par l'évaluateur avec l'application d'administration fournie par le développeur telle que décrite dans [GUIDES].

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] et, lorsqu'applicable, au document [JIL-AP-HDSB].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 décembre 2015, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **Succès** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations contenues dans [MAN-D] doivent être suivies.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI (annexe G de [RTE]). Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le mécanisme de génération d'aléas a été analysé et est jugé conforme au référentiel [REF].

En particulier, l'analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties du générateur physique. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. En outre, le produit met en œuvre un retraitement algorithmique de nature cryptographique conforme aux exigences énoncées dans [REF].

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.

Ce certificat atteste que le produit « HSM TrustWay Proteccio, Version V128/X130 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3 et AVA_VAN.5.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], en particulier :

- les administrateurs autorisés ne sont pas hostiles, sont correctement formés et s'authentifient auprès de la TOE avant d'effectuer toute action (O.ENV_ADMIN) ;
- le système d'exploitation *LINUX* durci doit assurer l'intégrité de ses fichiers sensibles, et ne doit permettre l'accès qu'aux seules applications distantes autorisées (O.ENV_PROTECTION_HOST) ;
- les applications (cliente et administration) doivent effectuer les contrôles de sécurité nécessaires sur les données échangées avec la TOE afin de détecter toute manipulation non autorisée ;
- les applications (cliente et administration) doivent identifier et authentifier localement les utilisateurs et assurer un contrôle d'accès local (O.ENV_APPLICATION) ;
- l'environnement de la TOE doit assurer la disponibilité des fichiers d'audit générés et exportés par la TOE et prévoir l'examen des fichiers d'audit enregistrés par la TOE (O.ENV_SECURE_CHANNEL) ;
- le personnel utilisant les services de la TOE doit être conscient des responsabilités civiles, financières et juridiques, ainsi que des obligations auxquelles il doit faire face, en fonction de son rôle. Le personnel doit être formé sur l'utilisation correcte de la TOE (O.ENV_PERSONNEL) ;
- la TOE doit être protégée par des mesures de protection physiques, logiques et organisationnelles, afin d'empêcher toute modification de la TOE, ainsi que la divulgation des biens protégés de la TOE. Ces mesures doivent limiter l'utilisation de la TOE aux seules personnes autorisées (O.ENV_PROTECT_ACCESS) ;

- des procédures permettant une récupération sûre et rapide en cas de problème majeur avec la TOE (par exemple, si la TOE est bloquée suite à une défaillance, une interruption de service ou la détection d'une tentative d'attaque physique) doivent être mises en place. Elles doivent en particulier assurer :
    - que la confidentialité et l'intégrité des biens de la TOE et des clés de sauvegarde associées sont maintenues durant le processus de récupération ;
    - que cette récupération ne conduit pas à une situation où des personnels pourraient accéder à des services de la TOE auxquels ils n'ont légitimement pas accès (O.ENV_RECOVERY) ;
- des procédures et des contrôles doivent être définis et appliqués dans l'environnement de la TOE pour permettre de configurer et d'initialiser la TOE de manière sûre pour toutes les opérations cryptographiques, y compris la génération de signatures pour les certificats qualifiés. Cela inclut la génération et l'importation sécurisée des clés, ainsi que la configuration initiale d'autres données de la TSF, comme les rôles, utilisateurs et les informations d'authentification des utilisateurs ;
- la TOE doit être installée (initialisée) avec une procédure d'installation sûre, en utilisant des données secrètes fournies par un ou plusieurs administrateurs, lesquelles sont entrées par le chemin de confiance en utilisant des mécanismes de partage de connaissances (O.ENV_SECURE_INIT) ;
- pour permettre l'exploitation de la TOE dans un système de CA[1] conforme aux exigences de la directive de l'UE et à la politique concernant les autorités de certification délivrant des certificats qualifiés, des procédures et des contrôles adéquats doivent être définis dans l'environnement de la TOE (O.ENV_SECURE_OPER).

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat 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[2], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les équipements matériels avec boîtiers sécurisés, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] *Certification Authority* ou Autorité de Certification.
[2] 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.

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.
Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR.
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	**2**	Complete mapping of the implementation representation of the 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	**5**	Advanced support
	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	**2**	Sufficiency of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	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 documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - BULL TrustWay HSM - Cible de Sécurité, référence : PCA4_0003_CIB_Cible de sécurité_FR, version 2.14, Bull TrustWay. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *TrustWay PROTECCIO Security Target*, référence : PCA4_0003_CIB_Security Target_EN, version 1.5, Bull TrustWay.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation du projet PCA4-2, référence : PCA4-2_RTE_v1.1, version 1.1, 21 décembre 2015, Serma Technologies. - Addendum au Rapport Technique d'Évaluation du projet PCA4-2, référence : PCA4-2_RTE_Add_v1.2, version 1.2, 21 décembre 2015, Serma Technologies.
[CONF]	Liste de configuration du produit : - PCA4 – Document de synthèse pour évaluation CC, référence : PCA4_0012_CD_Document de synthèse pour évaluation, version 1.12, Bull TrustWay.
[GUIDES] [MAN-D]	Guide d'installation et d'administration du produit : - Proteccio: manuel d'installation et d'utilisation, référence : 86 F2 76 FH 09, février 2015, Bull TrustWay. Guide d'utilisation du produit : - Proteccio: manuel développeur, référence : 86 F2 75 FH 14, septembre 2015, Bull TrustWay.
[PP-CM-SOB]	Cryptographic Module for CSP Signing Operations with Backup – Protection Profile, référence : prEN 14167-2:2012.
[PP-CM-KG]	Cryptographic Module for CSP key generation services, référence: prTS 14167-3:2011.

Annexe 3. 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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-001; Part 2: Security functional components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-002; Part 3: Security assurance components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-004.
[JIL-AP-HDSB]	Application of Attack Potential to Hardware Devices with Security Boxes, version 1.0, Mai 2012.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31, version 1, 25 septembre 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).
[FIPS 140]	Security Requirements for Cryptographic Modules, référence : FIPS PUB 140-2, 25 mai 2001,NIST.