PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/34

BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302)

Paris, le 26 novembre 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

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.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Table des matières

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

[2] En novembre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et la Turquie.

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. Le produit évalué

1.1. Identification du produit

Le produit évalué est la **carte cryptographique BULL TrustWay PCI 2400 (PCA2) version 76675628-115A S302** développée par **BULL TrustWay**.
Le détail de la version évaluée est le suivant :

- référence de la carte : 76675628
- version hardware/firmware : 115A
- version software : S302
- version du profil : IOP_FULL_CRYPTO ; 400 signatures/seconde

1.2. Développeur

BULL TrustWay

Rue Jean Jaurès
BP 68
78340 Les Clayes sous Bois
France

1.3. Description du produit évalué

Les principales fonctions de sécurité offertes par le produit évalué sont les suivantes (la liste n'est pas exhaustive) :

- le chiffrement et la signature avec les algorithmes suivants :
  - DES et triple-DES
  - RC4 – 40 à 192 bits
  - RSA – 512 à 2048 bits
  - SHA-1 et HMAC SHA-1
  - MD5 et HMAC MD5
- une fonction de sauvegarde (sous forme chiffrée et signée) et de restauration des clés et de leurs attributs ;
- la mise à jour sécurisée des codes applicatifs, fournis chiffrés et signés par le développeur ;
- une installation sécurisée de la carte PCA2, puisque faisant intervenir un mécanisme de cartes à puce d'installation et d'administration, générées lors de l'installation, puis demandées pour toute demande de ré-installation et d'authentification de la carte PCA2 ;
- et des alarmes de sécurité, lors de l'arrachage de la carte, lors d'une utilisation en dehors des plages de température et de tension permises, ou lors des auto-tests que la carte PCA2 effectue à intervalles réguliers, vérifiant ainsi l'intégrité des codes et des données en mémoire et le fonctionnement correct des automates cryptographiques.

L'utilisation de la carte se fait par l'intermédiaire d'une interface PKCS#11, incluant entre autres la signature et la vérification de signature, le chiffrement et le déchiffrement, des fonctions de hachage, et de la gestion de clés.

1.3.1. Architecture

L'architecture technique du produit évalué est représentée sur la figure ci-dessous. Les sous-systèmes réalisant les tâches d'entrées/sorties sont indiqués en orange, tandis que ceux réalisant les fonctions de sécurité sont en gris. Ces deux systèmes sont logiquement et physiquement distincts.

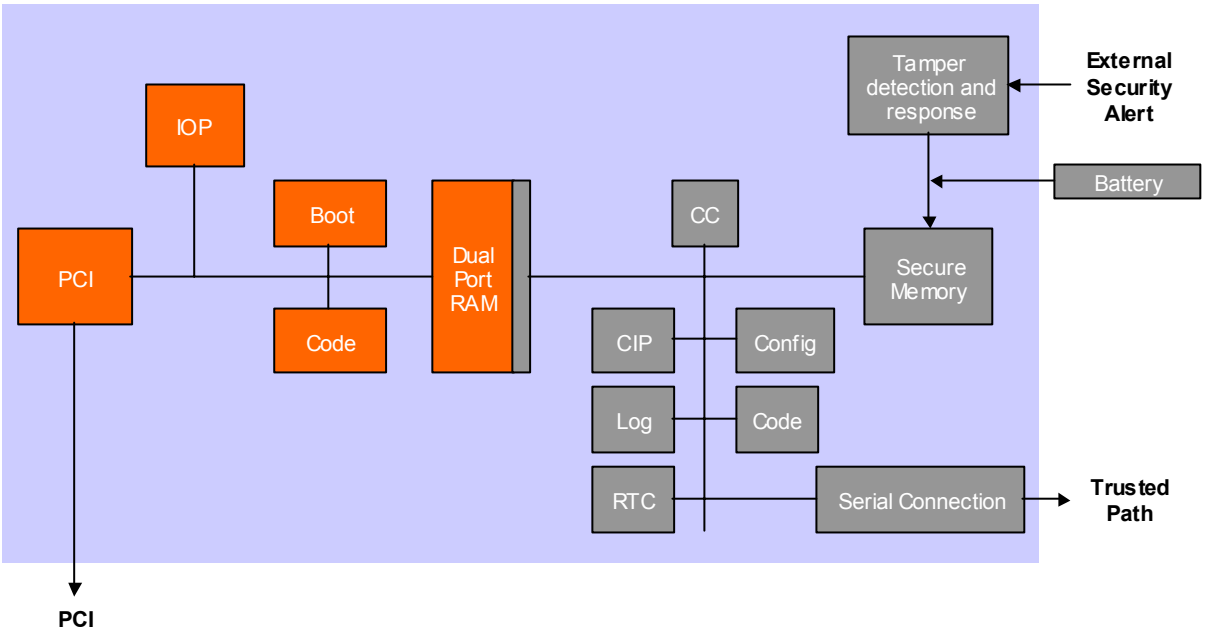

Figure 1 - Architecture générale de la carte cryptographique

- Interface PCI. (spécifications PCI 2.2) ;
- IOP (Input/Output Processor) : processeur de gestion des entrées / sorties,
- Code : Mémoire de programme pour l'IOP ;
- DPRAM : Dual Port Random Access Memory;
- CC (Cryptographic Component) : composant cryptographique effectuant les opérations cryptographiques ;
- CIP (Control and supervision processor) : processeur de contrôle et supervision gérant les opérations cryptographiques et effectuant les auto-tests périodiques ;
- Code : Mémoire de programme pour le CIP et le CC ;
- Secure Memory (alimentée par la batterie) : contient les données secrètes, dont les clés cryptographiques ;
- Serial Connection[1] : connecteur vers le SafePad pour l'installation et l'authentification des administrateurs ;

[1] Le Chemin de confiance (*Trusted Path*) est une liaison série entre la carte PCA2 et le SafePad. Cette liaison est réalisée en « local ». Elle ne peut être déportée.

- RTC (Real Time Clock) : signal d'horloge ;
- LOG : mémoire contenant les journaux d'audit de sécurité ;
- Config : mémoire non volatile contenant la configuration du produit évalué ;
- Tamper detection and response : logique de détection et de réponse après remontée d'une alarme.

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

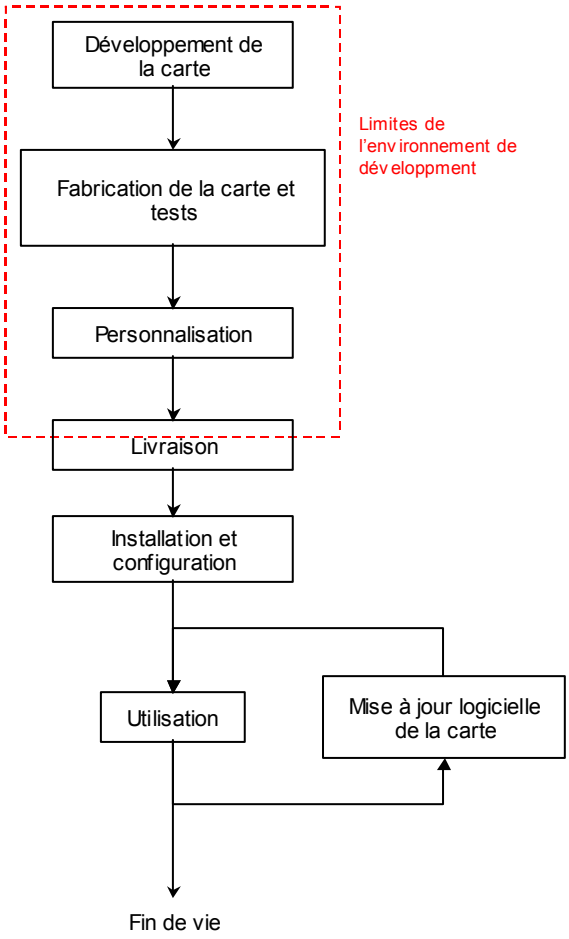

Figure 2 - Cycle de vie de la carte PCA2

1.3.3. Périmètre et limites du produit évalué

Le produit évalué est la carte cryptographique BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302) dans son ensemble. Cela correspond aux éléments matériels (PCB[1] et

[1] PCB : Printed Circuit Board (circuit imprimé).

composants électroniques, configuration du FCE[1]) et logiciels (codes firmware et software).

Pour les besoins de l'évaluation, le produit a été considéré comme étant utilisé en environnement physique protégé, lors de ses phases d'installation et d'exploitation.

Plusieurs profils d'utilisation de la carte PCA2 sont disponibles. Seul le profil nommé IOP_FULL_CRYPTO, paramétré pour 400 signatures/seconde a fait l'objet de l'évaluation. Ce profil implique en particulier que les commandes USER_CODE (chargement d'un code utilisateur) et CREATE_OBJECT (import de clés privées et de clés secrètes) ne soient pas disponibles.

Pour réaliser certaines exigences fonctionnelles de la carte PCA2, les recommandations sécuritaires du développeur identifient la mise sous contrôle d'authentification d'un certain nombre d'opérations.

Enfin, le lecteur de carte à puce SafePad et les cartes à puce[2] ne font pas partie du périmètre de l'évaluation, bien qu'ils aient été utilisés pour les tests de la carte PCA2. L'exigence fonctionnelle de sécurité Truted Path[3] (FPT_TRP.1) repose en majeure partie sur l'environnement d'exploitation du produit.

[1] FCE : FPGA Crypto Engine (composant cryptographique programmé dans un FPGA).
[2] Le lecteur et les cartes à puce sont livrés avec la carte PCA2 et utilisés lors de l'installation de la carte et des demandes d'authentification des administrateurs par la carte.
[3] chemin de confiance.

2. L'évaluation

2.1. Commanditaire

BULL TrustWay

Rue Jean Jaurès
BP 68
78340 Les Clayes sous Bois
France

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.3. Centre d'évaluation

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC], à l'exception des deux exigences fonctionnelles suivantes :

- FCS_RND.1 : Quality metrics for random numbers
- FDP_BKP.1 : Backup and Recovery

Ces exigences fonctionnelles étendues sont décrites au paragraphe 8.7 de la cible de sécurité [ST].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation satisfont aux exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].
L'évaluation s'est déroulée de novembre 2002 à octobre 2004.

2.5.1. L'environnement de développement

Le produit est développé sur les sites de :

BULL TrustWay

Rue Jean Jaurès
78340 Les Clayes sous Bois
France

BULL Angers

357 avenue Patton
BP 20845
49008 Angers
France

SELCO

Le Val d'Ombrée
49520 Combrée
France

Les mesures de sécurité permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.

Un système de gestion de configuration est utilisé conformément au plan de gestion de configuration défini par le développeur du produit. La liste de configuration [LGC] identifie les éléments gérés par ce système. Les procédures de génération permettent par ailleurs de s'assurer que les bons éléments de configuration sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures de développement et de gestion de configuration a été effectuée par une visite des trois sites ci-dessus (cf Annexe 1, Annexe 2 et Annexe 3).

Les procédures de correction d'anomalies décrivent la manière dont toute anomalie découverte sera suivie et corrigée, ainsi que la diffusion des informations et corrections relatives à ces anomalies, tant que le produit est maintenu par le développeur.

Ces procédures ont été évaluées, bien que le respect de ces procédures ne puisse pas être déterminé au moment de l'évaluation.

2.5.2. La conception du produit

La classe d'assurance ADV définit les exigences de raffinement des fonctions de sécurité du produit depuis les spécifications globales présentes dans la cible de sécurité [ST] jusqu'à l'implémentation de ces fonctions.

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit :

- spécifications fonctionnelles (FSP) ;
- conception de haut-niveau (HLD) ;
- conception de bas-niveau (LLD) ;
- implémentation des fonctions de sécurité (IMP).

2.5.3. La livraison et l'installation

La livraison est considérée après la fabrication du produit. Le produit évalué développé est livré à l'utilisateur final. La procédure de livraison utilisée [DEL] permet de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison.

L'installation du produit correspond à la phase « Installation et configuration » (Figure 2). Les procédures d'installation [IGS] permettent d'obtenir la configuration évaluée du produit. Lors de la phase des tests fonctionnels (cf §2.5.5), l'installation de la carte PCA2 a été testée en mode « saisie ».

2.5.4. La documentation d'exploitation

Du point de vue de l'évaluation, les administrateurs sont les *crypto-officers* et l'*auditor*. Les guides livrés à ces administrateurs [ADM] ont été fournis pour évaluation. Ces guides présentent la liste des fonctions C permettant d'administrer la carte, ainsi que les paramètres de configuration du produit définissant une configuration sûre.

Du point de vue de l'évaluation, les utilisateurs sont les *crypto-users*. La seule fonction de sécurité disponible aux utilisateurs concerne les opérations de cryptographie. Le référentiel PKCS#11 contient une description précise des fonctions à utiliser et des objets à manipuler pour mettre en œuvre cette fonction. Les guides livrés à ces utilisateurs [USR] ont été fournis pour évaluation.

2.5.5. Les tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test. Il a vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telles qu'elles sont décrites dans la conception de haut niveau [HLD], sont couvertes par les tests du développeur.

Les tests ont été réalisés sur les versions 76675628 – 112 et 76675628 – 107 sur lesquelles la version S302 du software était chargée. Ces deux cartes sont représentatives du point de vue matériel de la version identifiée au paragraphe 1.1.

2.5.6. L'analyse de vulnérabilité

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.

L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.

Les canaux « cachés » ont été interprétés dans le profil de protection [PP/0308] comme les canaux « auxiliaires ». C'est pourquoi, durant l'évaluation, aucun code caché n'a été cherché dans le code source du produit, alors que les attaques en SPA et DPA ont étudiées sur le produit.

Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du produit BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302).

3.2. Niveau d'évaluation

Le produit BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302) a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4[1] augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_FLR.3	Systematic flaw remediation
AVA_CCA.1[2]	Covert channel analysis
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite

[1] Annexe 5 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

[2] Les canaux « cachés » ont été interprétés dans le profil de protection [PP/0308] comme les canaux « auxiliaires ». C'est pourquoi, durant l'évaluation, aucun code caché n'a été cherché dans le code source du produit, alors que les attaques en SPA et DPA ont étudiées sur le produit.

Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite
Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic flaw remediation	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_CCA.1	Covert channel analysis	Réussite
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Guarantees of audit data availability (FAU_STG.2)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key distribution (FCS_CKM.2)

[1] Annexe 2 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Quality metrics for random numbers (FCS_RND.1)
- Subset access control (FDP_ACC.1)
- Security attribute based access control (FDP_ACF.1)
- Backup and recovery (FDP_BKP.1)
- Export of user data without security attributes (FDP_ETC.1)
- Subset information flow control (FDP_IFC.1)
- Partial elimination of illicit information flows (FDP_IFF.4)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- 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)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TSF data (FMT_MTD.1)
- Specification of Management Functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Abstract machine testing (FPT_AMT.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Inter-TSF confidentiality during transmission (FPT_ITC.1)
- Inter-TSF detection of modification (FPT_ITI.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- Manual recovery (FPT_RCV.1)
- Time stamps (FPT_STM.1)
- TSF testing (FPT_TST.1)
- Trusted path (FTP_TRP.1) [1]

[1] Le composant Trusted Path FTP_TRP.1 est une exigence pour l'environnement TI dans le profil de protection [PP/0308]. Cette exigence a été reprise dans la cible de sécurité [ST] afin de montrer qu'elle est réalisée en partie par le produit évalué. Toutefois, comme indiqué dans [ST] §5.1.7.1, c'est l'utilisation du produit évalué dans un environnement d'exploitation sécurisé qui permet d'assurer la confidentialité et l'intégrité des données sur cette liaison.

3.4. Résistance des fonctions

Seules les fonctions d'authentification ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI suivant la procédure [CRY/I/01].

3.6. Conformité à un profil de protection

Le produit répond aux exigences de sécurité du profil de protection CWA 14167-2 version 0.28 du 27 octobre 2003, certifié par la DCSSI sous la référence [PP/0308].

3.7. Reconnaissance européenne (SOG-IS)

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

3.8. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, AVA_CCA.1 et AVA_VLA.4 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur [USR] et administrateur [ADM et IGS].

Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.10. Objectifs de sécurité sur l'environnement

Tous les objectifs de sécurité sur l'environnement sont repris à partir du profil de protection [PP/0308], à l'exception de O.ENV_Human Interface, qui est couvert par le produit évalué, et O.ENV_Secure_Init pour lequel quelques précisions ont été apportées. Voici un extrait de ces objectifs de sécurité sur l'environnement :

- les applications utilisant le produit évalué doivent vérifier les données avant transmission et effectuer les contrôles d'accès et les authentifications d'utilisateur que le produit évalué ne peut effectuer. De plus, l'environnement du produit évalué doit aussi prévenir toute manipulation des données transmises au produit (O.ENV_Application) ;
- les journaux d'audit stockés en dehors du produit évalué doivent être accessibles et disponibles (O.ENV_Audit) ;

- les personnes utilisant le produit évalué doivent être informées de leurs responsabilités et obligations en fonction de leur « rôle ». Elles doivent aussi être formées à l'utilisation du produit évalué (O.ENV_Personnel) ;
- le produit évalué doit être protégé par des mesures physiques et organisationnelles afin de prévenir toute modification du produit. Ces mesures doivent restreindre l'accès aux personnes autorisées uniquement (O.ENV_Protect_Access) ;
- des plans et procédures de recouvrement doivent permettre d'assurer la confidentialité et l'intégrité des biens du produit évalué en cas de problème majeur (par exemple, blocage du produit, discontinuité de service ou détection d'altération physique) (O.ENV_Recovery) ;
- des procédures sur l'environnement du produit doivent être définies, permettant de configurer et d'initialiser le produit de manière sécurisée. Ceci inclut la génération et l'importation de clés et des biens concernant les rôles et utilisateurs (O.ENV_Secure_Init) ;
- des procédures sur l'environnement du produit doivent être définies, permettant d'opérer le produit avec le système d'une autorité de certification répondant aux exigences de la directive européenne et de la politique de l'autorité de certification émettant les certificats qualifiés (O.ENV_Secure_Oper).

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le produit BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302) identifié au paragraphe 1.1 et décrit au paragraphe 1.3 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Visite du site BULL (Les Clayes sous Bois)

Le site de développement de BULL – TrustWay situé rue jean Jaurès, BP 68, 78340 Les Clayes sous Bois, a fait l'objet, dans le cadre de l'évaluation du produit BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302), d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- le support au cycle de vie : **ALC** (ALC_DVS.1).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site. Le rapport de visite se trouve sous la référence [Visite].

Annexe 2. Visite du site BULL (Angers)

Le site de développement de BULL S.A. situé 357 avenue Patton, BP 20345, 49008 Angers, a fait l'objet, dans le cadre de l'évaluation du produit BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302), d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.1).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site. Le rapport de visite se trouve sous la référence [Visite].

Annexe 3. Visite du site SELCO

Le site de développement de SELCO situé à Le Val d'Ombrée, 49520 Combrée, a fait l'objet, dans le cadre de l'évaluation du produit BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302), d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- le support au cycle de vie : **ALC** (ALC_DVS.1).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site. Le rapport de visite se trouve sous la référence [Visite].

Annexe 4. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

- Quality metrics for random numbers (FCS_RND.1)
- Backup and recovery (FDP_BKP.1)

Class FAU	**Security audit**
Security audit data generation	
FAU_GEN.1	*Audit data generation* Ce composant définit le niveau des événements auditables et spécifie la liste des données que chaque enregistrement doit contenir.
FAU_GEN.2	*User identity association* Le produit doit associer les événements auditables aux identités des utilisateurs individuels.
Security audit event storage	
FAU_STG.2	*Guarantees of audit data availability* Le produit doit maintenir des garanties (spécifiées dans le document [ST]) sur les données d'audit malgré l'apparition d'une condition non souhaitée.
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basées sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.2	*Cryptographic key distribution* Le produit doit distribuer des clés cryptographiques conformément à une méthode de distribution spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.1	*Subset access control*

	Chaque règle de contrôle d'accès identifiée doit être mise en place pour un sous-ensemble des opérations qu'il est possible d'effectuer sur un sous-ensemble des objets du produit.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Export to outside TSF control	
FDP_ETC.1	*Export of user data without security attributes* Le produit doit appliquer les règles de sécurité appropriées lors de l'exportation de données de l'utilisateur à l'extérieur. Les données de l'utilisateur exportées par cette fonction le sont sans les attributs de sécurité qui leur sont associés.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'informations.
Information flow control functions	
FDP_IFF.4	*Partial elimination of illicit information flows* Le produit doit couvrir l'élimination de certains flux d'information illicites (mais pas nécessairement de tous).
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
Authentication failures	
FIA_AFL.1	*Authentication failure handling* Le produit doit être capable d'arrêter le processus d'établissement d'une session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
Specification of secrets	
FIA_SOS.1	*Verification of secrets* Le produit doit vérifier que les secrets répondent à des métriques de qualité définies.
User authentication	
FIA_UAU.1	*Timing of authentication*

	Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.
User identification	
FIA_UID.1	*Timing of identification* Le produit autorise les utilisateurs à exécuter certaines actions, identifiées dans la cible de sécurité [ST], avant d'être identifiés.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.2	*Secure security attributes* Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
Specification of Management Functions	
FMT_SMF.1	*Specification of Management Functions* Le produit doit fournir les fonctions de gestion de la sécurité spécifiées dans la cible de sécurité [ST].
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).
Class FPT	**Protection of the TSF**
Underlying abstract machine test	
FPT_AMT.1	*Abstract machine testing* Ce composant définit la façon de tester la machine abstraite sous-jacente.
Fail secure	
FPT_FLS.1	*Failure with preservation of secure state* Le produit doit préserver un état sûr dans le cas de défaillances identifiées.
Confidentiality of exported TSF data	
FPT_ITC.1	*Inter-TSF confidentiality during transmission* Le produit doit garantir que les données transmises vers un produit TI de confiance distant sont protégées contre une divulgation pendant leur transit.
Integrity of exported TSF data	
FPT_ITI.1	*Inter-TSF detection of modification* Le produit doit avoir l'aptitude de détecter une modification des données du produit pendant leur transmission entre le produit et un produit TI de confiance distant, dans l'hypothèse où le produit TI de confiance distant a connaissance du mécanisme utilisé.
TSF physical protection	
FPT_PHP.2	*Notification of physical attack*

	Le produit doit notifier automatiquement l'intrusion physique sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusions physiques (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
Trusted recovery	
FPT_RCV.1	*Manual recovery* Le produit ne doit fournir que des mécanismes qui impliquent une intervention humaine pour retourner à un état sûr.
Time stamps	
FPT_STM.1	*Reliable time stamps* Le produit doit fournir un horodatage fiable.
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.
Class FTP	**Trusted path/channels**
Trusted path	
FTP_TRP.1	*Trusted path* Un chemin de confiance entre le produit et un utilisateur doit être fourni pour un ensemble d'événements défini. Soit l'utilisateur soit le produit initie le chemin de confiance.

Annexe 5. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 6. Références documentaires du produit évalué

[ADM]	Manuel d'installation et d'utilisation carte TrustWay PCI Référence D00U003 Version 4.3 Octobre 2004 BULL TrustWay API d'administration de la carte TrustWay PCI Référence D00U001 Version 4.4 Septembre 2004 BULL TrustWay
[DEL]	Dispositions sécuritaires pour l'intégration des cartes PCA2 Référence PCABILS-01 révision 03 Octobre 2003 BULL TrustWay
[FLR]	Environnement de développement de la carte PCA2 Chapitre 5 Référence D00P002 Version 6.0 BULL TrustWay
[IGS]	Manuel d'installation et d'utilisation carte TrustWay PCI Référence D00U003 Version 4.3 Octobre 2004 BULL TrustWay
[LGC]	Liste de configuration de la carte PCA2 Référence D00P009 Version 1.4 BULL TrustWay
[PP/0308]	Profil de protection CWA14167-2 Cryptographic Module for CSP Signing Operations with Backup version 0.28 27 octobre 2003 Rapport de certification DCSSI PP/0308
[RTE]	Rapport Technique d'Evaluation Référence R4C_ETR Version 1.2 Serma Technologies

[ST]	BULL TrustWay PCI Cryptographic Card Security Target Version 3.2 7 octobre 2004 BULL TrustWay
[Visite]	Rapport d'évaluation des classes ACM, ADO et ALC Annexe B, C et D Version 3.0 Serma Technologies
[USR]	Interface PKCS#11 de la carte TrustWay PCI version 1.0 BULL TrustWay Cryptographic Token Interface Standard Version 2.10

Annexe 7. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, DCSSI.
[CRY/I/01]	Instruction CRY/I/01 Analyse des mécanismes cryptographiques, DCSSI.
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, August 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, August 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, August 1999, version 2.1, réf: CCIMB-99-033. Le contenu des Critères Communs version 2.1 est identique à celui de la Norme Internationale ISO/IEC 15408:1999, comportant les trois documents suivants : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model ; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements ; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, August 1999, version 1.0, ref CEM- 99/045.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr