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-2010/10

BULL TRUSTWAY PCI CRYPTOGRAPHIC CARD (version S709 - ECC)

Paris, le 26 mars 2010

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

Patrick Pailloux
[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.

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

Référence du rapport de certification

ANSSI-CC-2010/10

Nom du produit

BULL TRUSTWAY PCI CRYPTOGRAPHIC CARD (version S709 - ECC)

Référence/version du produit

Version matérielle : 76675628-220
Version logicielle : S709

Conformité à un profil de protection

[PP/0308]
Profil de protection CWA 14167-2:
Cryptographic Module for CSP Signing Operations with Backup,
version 0.28, 27 octobre 2003, certifié par l'ANSSI

Critères d'évaluation et version

Critères Communs version 2.3
conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté
ADV_IMP.2, ALC_FLR.3, AVA_CCA.1, AVA_VLA.4

Développeur(s)

Bull SAS
Rue Jean Jaurès – BP 68 - 78340 LES CLAYES SOUS BOIS - FRANCE

Commanditaire

Bull SAS
Rue Jean Jaurès – BP 68 - 78340 LES CLAYES SOUS BOIS - FRANCE

Centre d'évaluation

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France
Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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 :

- 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 la carte BULL TRUSTWAY PCI CRYPTOGRAPHIC CARD (version S709 - ECC) développée par Bull SAS.

Le détail de la version évaluée de la TOE (*Target Of Evaluation* – cible d'évaluation) est le suivant :

- référence de la carte (de type PCA2) : 76675628
- version *hardware/firmware :* 220
- version software : S709

La TOE est une carte cryptographique au format PCI (*Peripheral Component Interconnect* – interconnexion de composants périphériques) offrant des services de chiffrement et de signature, via l'interface standard PKCS#11, tout en assurant une haute sécurité du stockage et de la manipulation des clés. C'est un *token* (au sens PKCS#11 du terme) capable d'échanger des informations avec une application cliente.

Cette évaluation s'appuie sur les résultats de la précédente évaluation et certification par l'ANSSI de la carte (cf. [ANSSI-CC-2004/34]). Le changement majeur par rapport à la précédente version est l'ajout de services cryptographiques : AES, SHA-2, ECC. Pour effectuer ces ajouts, certains algorithmes (MD5, RC4) ont dû être supprimés. En revanche, le produit matériel n'a pas changé. La structure générale du code embarqué n'a pas non plus été modifiée.

1.2. Description du produit

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

Cette cible de sécurité est conforme au profil de protection [PP/0308] qui impose au produit de résister à un attaquant de potentiel d'attaque élevé. Ce niveau n'est pas atteint par le seul produit évalué : il doit être utilisé dans un environnement d'exploitation protégé, c'est-à-dire respectant les exigences de sécurité de l'environnement d'exploitation comme spécifiées dans la [ST] et rappelées dans les [GUIDES.

La TOE est constituée :

- d'éléments matériels :
  - la carte électronique PCA2 comprenant les composants (publics) montés en surface d'un circuit imprimé (conçu par le développeur) ;
  - un lecteur de carte à puce et des cartes à puce (personnalisées par le développeur) pour l'installation et l'administration de la carte PCA2 ;
- d'éléments logiciels : ce sont les codes (conçus par le développeur) chargés sur la carte, dans les mémoires non volatiles (Flash EPROM). On distingue un code *firmware* (noyau permettant entre autre de charger le code applicatif), un code applicatif et le code de configuration du composant programmable FCE (FPGA Crypto Engine - composant cryptographique programmé dans un circuit logique programmable).

1.2.1. 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 :

- l'étiquette collée sur la carte indique sa version (76675628-220 en l'occurrence) ;
- les versions obtenues avec l'outil d'administration de la carte [cf. GUIDES] :
  - version cryptographique : S709 ;
  - version logiciel CIP : 3007 ;
  - version logiciel IOP : 3005 ;
  - version Firmware : 5.5.

L'évaluateur a pu obtenir ces informations sur les échantillons du produit soumis à l'évaluation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont (cf. pour plus de détails dans [ST] au §6.1 TOE security functions) :

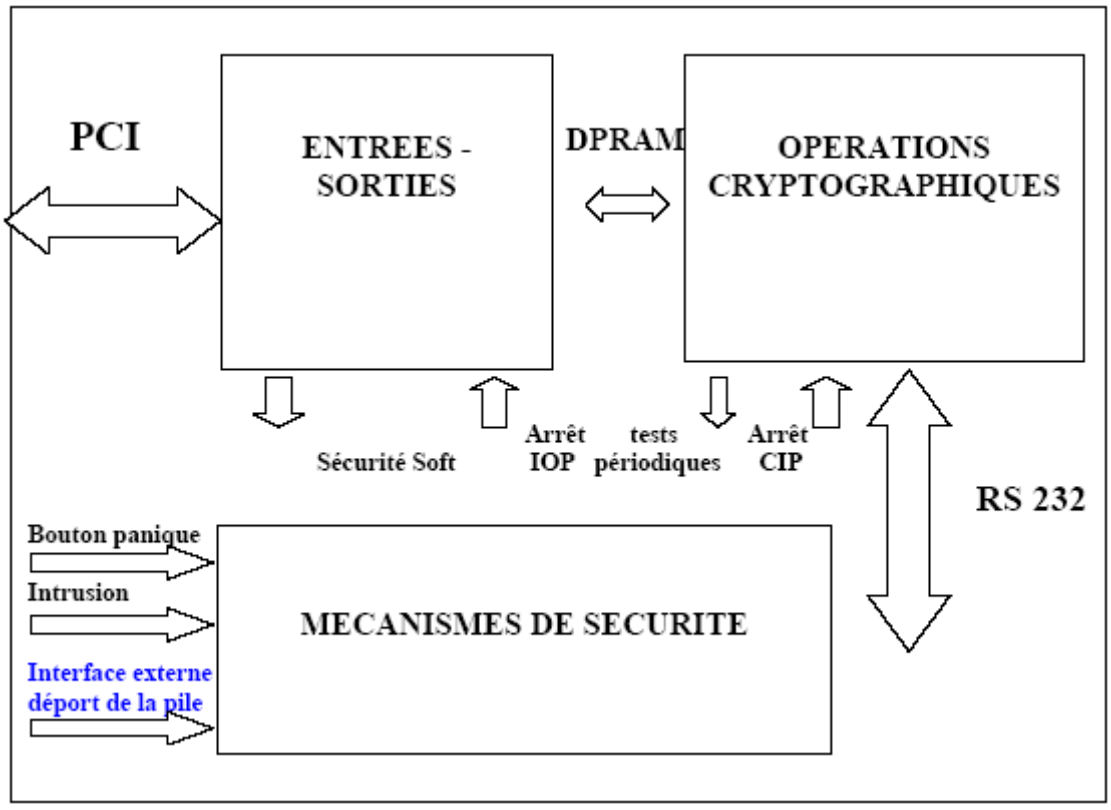
- SF.SL : *secure loading* – chargement sécurisé ;
- SF.SI : *secure installation* – installation sécurisée ;
- SF.keys_distribution : introduction de clés secrètes ;
- SF.CO : *cryptographic operation* – opération cryptographique ;
- SF.backup : sauvegarde ;
- SF.authentification : authentification ;
- SF.Access_Control : contrôle d'accès ;
- SF.audit : audit ;
- SF.SM : *security mechanisms* – mécanismes de sécurité.

1.2.3. Architecture

L'architecture technique de la TOE est représentée par le schéma bloc ci-après dans lequel on distingue les trois sous-systèmes :

- "entrées – sorties": il gère les échanges avec l'extérieur au travers du bus PCI et les échanges avec le sous-système "opérations cryptographiques" ;
- "opérations cryptographiques": il effectue essentiellement les opérations cryptographiques à la demande du sous-système "entrées-sorties" ;
- "mécanismes de sécurité»: il détecte les violations de sécurité et il agit sur les deux autres sous-systèmes pour préserver un état sûr de la TOE.

Du point de vue interfaces externes physiques, le seul changement par rapport à la structure du produit lors de l'évaluation initiale est l'ajout d'un déport de la pile (illustré en bleu sur le schéma bloc).



1.2.4. Cycle de vie

Le cycle de vie du produit compte cinq phases décrites dans le tableau ci-après (extrait du §2.2.2 de [ST]) :

Phase		***Phase Responsibility***	***Phase Environment***
Phase 1	*Token development*	***The engineering team (BULL Les Clayes)*** *is in charge of hardware design and embedded software development.*	*These phases are performed in the developer environment (developer responsibility)*
Phase 2	*Token manufacturing and testing*	***The manufacturer (SELCO)*** *is responsible for token manufacturing and testing.*	
Phase 3	*token personalisation*	***The personaliser (BULL ANGERS)*** *is responsible for the Token personalisation (customisation). The personaliser prepares the token by loading the embedded software.*	
Phase 4	*Token delivery*	***The issuer (BULL ANGERS)*** *is responsible for the token delivery to the end-user.*	
Phase 5a	*Secure installation and configuration*	*The secure installation and configuration are performed by* ***the end-user (administrator)****.*	*Theses phases are performed in the user environment (user responsibility)*
Phase 5b	*Embedded software update*	*If required, the secure software update of the token is performed by* ***the end-user (administrator)****.*	
Phase 5C	*Token use*	*Token final use is performed by* ***the end-user***	

Le périmètre du cycle de vie couvert par l'évaluation inclut les étapes de conception, de fabrication et de test (phases 1 à 4) ; le produit évalué correspond à celui délivré en phase 5C à l'utilisateur final. Les autres phases sont couvertes par des guides.

Le produit a été conçu et développé sur le site suivant :

BULL Les Clayes

Rue Jean Jaurès – BP 68
78340 LES CLAYES SOUS BOIS
FRANCE

Le produit a été fabriqué sur le site suivant :

SELCO (sous-traitant)

Le Val d'Ombrée
49520 COMBREE
FRANCE

Le produit a été personnalisé sur le site suivant :

BULL Angers

357 avenue Patton, BP 20845
49008 ANGERS
FRANCE

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit les rôles en charge des opérations d'administration décrites dans le guide d'administration du produit (cf. [GUIDES]) et comme utilisateur du produit les rôles utilisant les services décrits dans le guide d'utilisation du produit (cf. [GUIDES]).

1.2.5. Configuration évaluée

La TOE peut être configurée en usine suivant plusieurs "profils" qui dépendent de l'utilisation finale de la carte. Le profil « PCA2 OEM en 400 RSA/s » est le seul évalué (profil identifié comme « PMC T400-0000 » dans la documentation de personnalisation - cf. [GUIDES]).

L'entrée des secrets (nombre secret et secret d'authentification) peut se faire de deux façons différentes (cf. [GUIDES]) :
- directement par le clavier du lecteur de cartes à puce (mode "saisie"),
- avec un jeu de cartes à puce (mode "cartes à puce").

Seul le mode "saisie" a été évalué.

D'autre part, pour réaliser certaines exigences fonctionnelles de la [ST], les recommandations sécuritaires du développeur identifient la mise sous contrôle d'authentification d'un certain nombre d'opérations (cf. [GUIDES]). C'est uniquement cette configuration qui a été évaluée.

Ainsi, la seule configuration évaluée est le *token* tel que configuré :
- par le développeur suivant le profil « PCA2 OEM en 400 RSA/s » ;
- par le paramétrage initial fait par l'administrateur :
  - entrée des secrets en mode "saisie",
  - mise sous contrôle d'authentification de commandes en accord avec les recommandations du développeur.

Par ailleurs, lors de l'évaluation, l'évaluateur a pris comme hypothèse que la TOE était utilisée dans son environnement d'exploitation protégé.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par l'ANSSI et compatibles avec le document [AIS 34], ont été utilisées.

Bien que le produit ne soit pas une carte à puce, le guide [CC AP] a été appliqué.

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation de la version précédente du produit, qui a été certifiée par l'ANSSI en 2004 (cf. [ANSSI-CC-2004/34]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 mars 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à son référentiel technique [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu aux conclusions suivantes : le produit peut être conforme au [REF-CRY] sous réserve de respecter les recommandations spécifiées dans les [GUIDES].

Par ailleurs, les 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_VLA.4 visé.

2.4. Analyse du générateur d'aléas

Le produit offre un générateur d'aléas qui a fait l'objet d'une analyse par l'ANSSI. L'aléa généré est en fait un pseudo-aléa qui résulte d'un retraitement algorithmique de nature cryptographique d'un aléa issu d'un générateur d'aléas physique. L'algorithme de génération de pseudo-aléa mis en œuvre par le produit est reconnu conforme au [REF-CRY].

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 BULL TRUSTWAY PCI CRYPTOGRAPHIC CARD (version S709 - ECC) soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'évaluation a montré que la protection de la TOE par l'environnement d'exploitation, sur les plans technique, logique et organisationnel, est critique pour éviter l'exploitation des vulnérabilités identifiées.

L'utilisateur du produit certifié devra donc s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment aux §8.2 à §8.4 du manuel d'installation :

- dispositions sécuritaires concernant l'environnement d'exploitation, comprenant :
  - des mesures de protection physiques ;
  - des mesures devant s'appliquer au personnel interagissant avec le produit ;
  - des mesures devant s'appliquer à l'application pilotant le produit ;
- dispositions sécuritaires concernant la carte ;
- dispositions sécuritaires concernant l'utilisation de la carte.

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
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level 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_CCA					**1**	**2**	2	**1**	Covert channel analysis
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - BULL TrustWay PCI Cryptographic Card; réf. D00G008, version 3.9; Bull SAS.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation du projet R4C-2 ; réf. R4C-2_ETR_v1.0, version 1.0 ; Serma Technologies.
[ANA-CRY]	Rapport d'analyse cryptographique de l'ANSSI ; réf. N° 751/SGDN/DCSSI, daté du 30/03/2009.
[CONF]	Liste de Configuration de la carte PCA2 ; réf. D00P009, version 1.13
[GUIDES]	Guide d'installation du produit : - CryptoCard PCI Guide d'Installation (version française) ; réf. 86 F2 59ET, version 04 ; Bull SAS. - CryptoCard PCI Installation Guide (version anglaise) ; réf. 86 A2 59ET, version 04 ; Bull SAS. Guide d'administration du produit : - CryptoCard PCI API d'Administration (version française) ; réf. 86 F2 58ET, version 02 ; Bull SAS. - CryptoCard PCI Administration API (version anglaise) ; réf. 86 A2 58ET, version 02 Bull SAS. - CryptoCard PCI Outil d'Administration (version française) ; 86 F2 56ET, version 04 ; Bull SAS. - CryptoCard PCI Administration Tool (version anglaise) ; 86 A2 56ET, version 04 ; Bull SAS. Guide d'utilisation du produit : - CryptoCard PCI Guide d'Utilisation (version française) ; réf. 86 F2 57ET, version 06 ; Bull SAS. - CryptoCard PCI User's Guide (version anglaise) réf. 86 A2 57ET, version 06 ; Bull SAS.
[PP/0308]	Profil de protection CWA 14167-2:

	Cryptographic Module for CSP Signing Operations with Backup, version 0.28, 27 octobre 2003, certifié par l'ANSSI
[DCSSI - 2004/34]	Certificat ANSSI délivré le 26/11/2004 pour le produit « BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S302) »

Annexe 3. 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.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, référence 2741/SGDN/DCSSI/SDS/Crypto.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)