PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/13

Carte CNS : composant P5CT072VOP masqué par la plate-forme JavaCard GOP ID MX 64 et embarquant l'application CNS 1.0.7

Paris, le 15 septembre 2006,

Le Directeur central 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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2006/13

Carte CNS : composant P5CT072VOP masqué par GOP ID MX 64 et embarquant l'application CNS 1.0.7

Développeurs : Oberthur Card Systems, Philips

Critères Communs version 2.3
(norme internationale ISO/IEC 15408:2005)

EAL4 Augmenté
(ADV_IMP.2, AVA_MSU.3, AVA_VLA.4)

conforme aux profils de protection PP SSCD type 2 et PP SSCD type 3

Commanditaire : Oberthur Card Systems

Centre d'évaluation : Serma Technologies

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :
ADV_IMP.2, AVA_MSU.3, AVA_VLA.4

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 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 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 septembre 2006, 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, le Japon, la Norvège, les Pays-Bas, la Corée du Sud et l'Espagne ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Suède, la Turquie, la République Tchèque, Singapour, l'Inde et le Danemark.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la carte CNS : composant P5CT072VOP masqué par la plate-forme JavaCard GOP ID MX 64 et embarquant le code optionnel RSA FSM et l'application CNS 1.0.7, développé par les sociétés Oberthur Card Systems et Philips.

1.2. Développeurs

La plate-forme et l'application sont développées par :

Oberthur Card Systems

71-73, rue des Hautes Pâtures,

92726 Nanterre Cedex

France

Le micro-circuit est développé par :

Philips France Semiconducteurs M & S

5-7, rue Salomon de Rotchschild

BP 317

92156 Suresnes Cedex

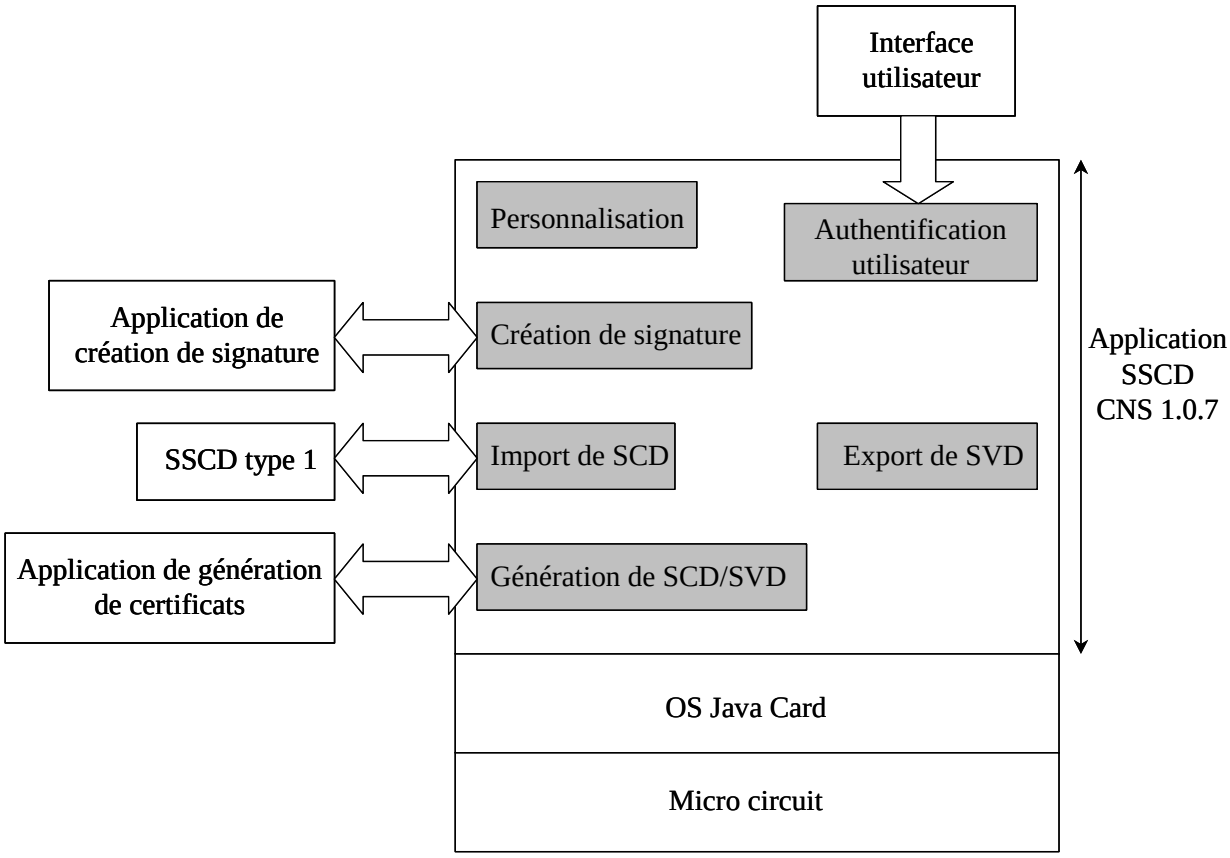
France

1.3. Description du produit évalué

1.3.1. Architecture

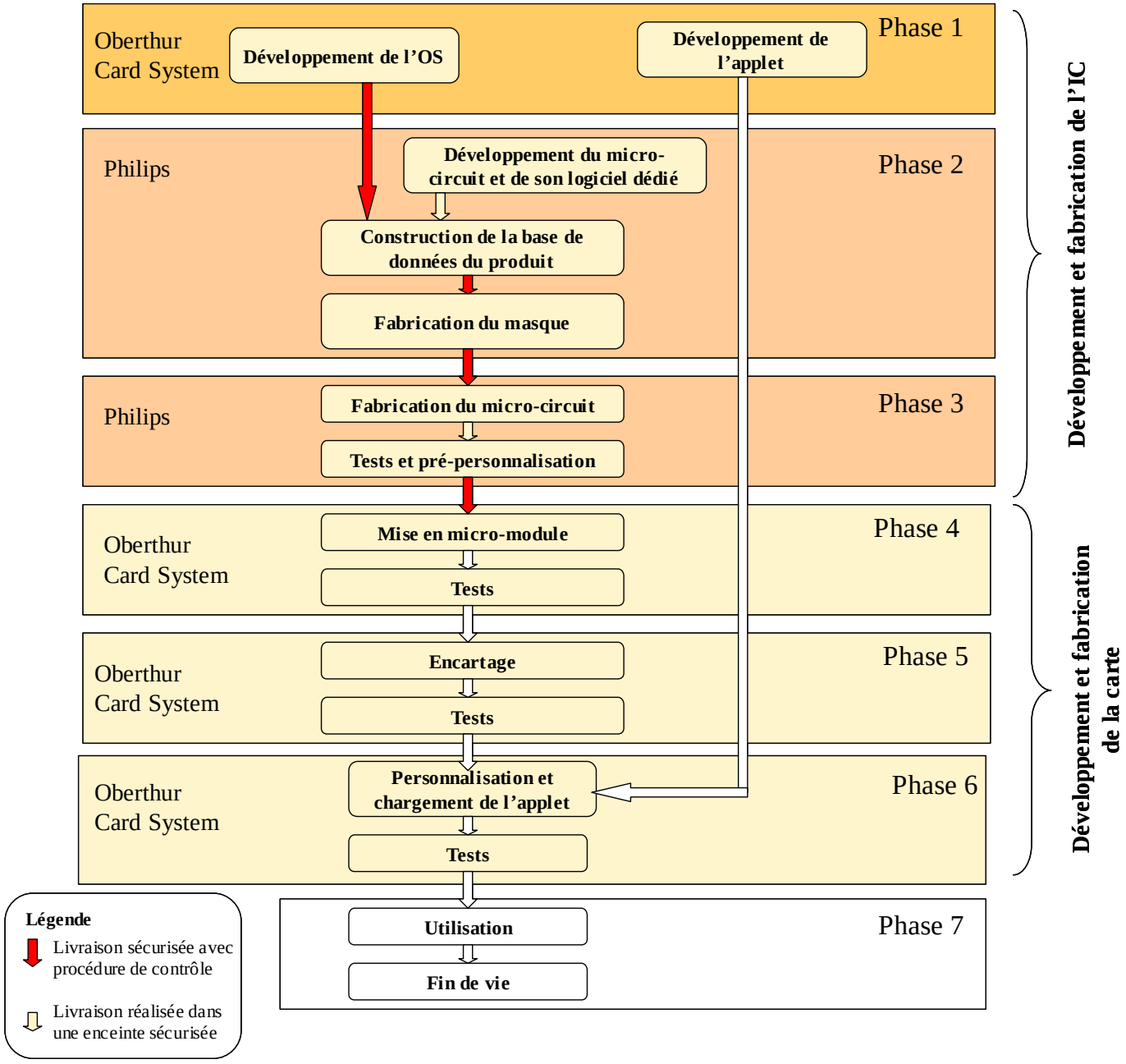
Le produit est constitué :

- du micro-circuit P5CT072VOP développé et fabriqué par Philips ;
- de l'OS JavaCard développé par Oberthur Card Systems constitué de :
  - la plateforme GOP ID MX 64, masqué dans la ROM du micro-circuit (BIOS/VM : ref. build33, Platform : ref. RefV87, Resident application : ref. GOP64_20051014)
  - du code optionnel RSA FSM en EEPROM (version r1.0, ref. Liv20060310) ;
- de l'application SSCD CNS (Carta Nazionale dei Servici) développée par Oberthur Card Systems, chargée au moment de la personnalisation de la carte (CNS 1.0.7).


Interface utilisateur
Personnalisation
Authentification utilisateur
Application de création de signature
Création de signature
Application SSCD CNS 1.0.7
SSCD type 1
Import de SCD
Export de SVD
Application de génération de certificats
Génération de SCD/SVD
OS Java Card
Micro circuit

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :



1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend les éléments suivants :

- Un système d'exploitation basé sur les technologies JavaCard et Global Platform, qui fournit :
  - l'interface entre le micro-circuit et l'applet CNS ;
  - les services basiques pour accéder aux mémoires et aux opérations cryptographiques requis par l'applet CNS ;
  - la gestion de la carte (chargement, installation et suppression d'applets) et les services de sécurité de la carte (intégrité des données et contre mesure relatives aux attaques physiques) ;
  - un mécanisme de blocage du chargement d'applets après le chargement de l'applet CNS (ainsi aucune nouvelle applet ne pourra être chargée après l'applet CNS).

- L'application CNS, qui fournit les fonctionnalités de :
  - génération de clés privées et publiques RSA de signature (SCD et SVD) ;
  - import de clés privées de signature RSA (SCD) ;
  - export de clés publiques de signature RSA (SVD) ;
  - création de signature ;
  - authentification du signataire par un PIN.

2. L'évaluation

2.1. Contexte

L'évaluation a été effectuée selon le schéma de composition défini dans le document [COMP]. La composition consiste à réaliser l'évaluation d'un composant masqué en évaluant d'une part le micro-circuit, et d'autre part la partie logicielle en vérifiant qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur le micro-circuit.
Cette évaluation a été réalisée sur la base des résultats de l'évaluation du micro-circuit P5CT072VOP au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection BSI-PP-0002-2001. Ce micro-circuit a été certifié le 28 mars 2006 sous la référence BSI-DSZ-CC-0348-2006.

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].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au CESTI validées par la DCSSI et compatibles avec le document [AIS34] ont été utilisées.

2.3. Commanditaire

Oberthur Card Systems

71-73, rue des Hautes Pâtures,

92726 Nanterre Cedex

France

2.4. 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

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 22 décembre 2005 au 29 août 2006.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité est conforme aux profils de protection suivants :

- module de création de signature sécurisée type 2, PP SSCD type 2 [SSCD2],
- module de création de signature sécurisée type 3, PP SSCD type 3 [SSCD3].

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
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

La cible de sécurité contient l'exigence fonctionnelle de sécurité explicitement énoncée :

- FPT_EMSEC.1 issue des profils de protection PP SSCD type 2 et PP SSCD type 3.

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ AVA_MSU.3	Analysis and testing for insecure state
+ AVA_VLA.4	Highly resistant

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

Oberthur Card Systems

71-73, rue des Hautes Pâtures,

92726 Nanterre Cedex

France

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de Nanterre. (cf Annexe 1)

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.1	Identification of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après 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 (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Subset access control (FDP_ACC.1)
- Security attributes based access control (FDP_ACF.1)

- Export of user data without security attributes (FDP_ETC.1)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Basic data exchange confidentiality (FDP_UCT.1)
- Data exchange integrity (FDP_UIT.1)
- Authentication failures handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.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 TOE security functions data (FMT_MTD.1)
- Security management roles (FMT_SMR.1)
- Abstract machine testing (FPT_AMT.1)
- TOE Emanation (FPT EMSEC.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Passive detection of physical attack (FPT_PHP.1)
- Resistance to physical attack (FPT_PHP.3)
- TSF testing (FPT_TST.1)
- Inter-TSF trusted channel (FTP_ITC.1)
- Trusted Path (FTP_TRP.1)

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre Philips et Oberthur Card Systems.
Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

L'installation du produit correspond à la phase 6 de personnalisation. Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme « administrateurs du produit » les personnalisateurs des cartes et comme « utilisateurs » les terminaux au travers desquels les signataires utilisent les cartes.
L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.
L'évaluateur a réalisé ses tests fonctionnels indépendants sur des échantillons fournis par les développeurs.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
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

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Les fonctions suivantes (décrites dans [ST]) :
- authentification de l'utilisateur (SF.USER_AUTH) ;
- secure messaging (SF.SM) ;
- génération de clés RSA (SF.KEYGEN).

ont fait l'objet d'une estimation du niveau de résistance intrinsèque des mécanismes. Le niveau de résistance de ces fonctions est coté élevé : SOF-high.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur les échantillons fournis par le développeur.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à un attaquant ayant un potentiel d'attaque de niveau **élevé**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.3	Analysis and testing for insecure state	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (Art. 8 du décret 2002-535).

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous (décrits dans [ST])
Il devra également suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES]
Les objectifs de sécurité sur l'environnement sont issus des profil de protection PP SSCD type 2 [SSCD2] et PP SSCD type 3 [SSCD3] ; ils concernent les aspects suivants :

- la correspondance entre la clé publique de vérification d'une signature électronique –SVD- et la clé privée de création de cette signature électronique –SCD- (OE.SCD_SVD_Corresp) ;
- le transfert sécurisé des clés privées de création de signature électronique –SCD- entre modules de création de signature sécurisé –SSCD- (OE.SCD_Transfer) ;
- l'unicité des données de création de signature (OE.SCD_Unique).
- la génération de certificats qualifiés (OE.CGA_Qcert) ;
- la vérification de l'authenticité de la clé publique de vérification de signature électronique –SVD- par l'application de génération de certificats –CGA- (OE.SVD_Auth_CGA) ;
- la protection des données de vérification de l'authentification –VAD- (OE.HI_VAD) ;
- les données devant être signées (OE.SCA_Data_Intend).

3.3. Reconnaissance européenne (SOG-IS)

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

3.4. 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_MSU.3, AVA_VLA.4.

Annexe 1. Visite du site de développement de la société Oberthur Card Systems à Nanterre

Le site de développement de la société Oberthur Card Systems situé à Nanterre, a fait l'objet d'une visite par l'évaluateur le 18 mai 2006 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison.

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_AUT.1 et ACM_CAP.4 ;
- ADO_DEL.2.

Un rapport de visite [Visite] a été émis par l'évaluateur dans le cadre d'un autre projet similaire à celui-ci.

Annexe 2. 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 3. Références documentaires du produit évalué

[CONF]	EVARISTE configuration list, référence : FQR : 110 3452, version 1 Draft 2 du 27/07/06
[GUIDES]	CNS Guidance, référence : FQR : 110 3344, version 1 Draft 4 du 26/07/06
[INSTALL]	Instructions de génération du logiciel, référence : 063787 00 PGD, version 7 - AB du 01/06/06
[RTE]	EVARISTE project - Evaluation Technical Report, Référence : EVARISTE_ETR_V1.1, version 1.1 du 29/08/06
[ST]	Cible de référence pour l'évaluation : • CNS Card Security Target, référence : FQR 110 3119, version 1 Draft 6 du 27/07/06 Pour les besoins de la reconnaissance internationale, la cible publique suivante a été fournie et validée dans le cadre de cette évaluation : • CNS CARD – Public Security Target, édition : 1 du 27/07/2006
[Visite]	COSMOS project - Evaluation report Classes ACM, ADO, ALC Référence : Référence COSMOS_ACM-ALC-ADO_v2.0, version 2.0 du 15/06/06
[SSCD2]	Secure Signature Creation Device Protection Profile Type 2 v1.04, EAL4+, référence : BSI -PP-0005-2002, d'avril 2002
[SSCD3]	Secure Signature Creation Device Protection Profile Type 3 v1.05, EAL4+, référence : BSI -PP-0006-2002 , d'avril 2002

Annexe 4. 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[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
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr