PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/16

Carte VITALE 2 - Application Adèle : Composant P5CC036V1 rév. D masqué par le logiciel SESAM VITALE P 2.2.0 (réf : P5CC036V1D/2.2.0)

Paris, le 27 octobre 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 la DCSSI, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2006/16

Carte VITALE 2 - Application Adèle : Composant P5CC036V1 rév. D masqué par le logiciel SESAM VITALE P 2.2.0 (réf : P5CC036V1D/2.2.0)

Développeurs : Philips Semiconductors GmbH, Sagem Défense Sécurité

Critères Communs version 2.2

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

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

Commanditaire : Sagem Défense Sécurité

Centre d'évaluation : CESTI-Leti

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 octobre 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, les Pays-Bas, la Norvège, l'Espagne et la Corée du Sud ; 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 VITALE 2 - Application Adèle : Composant P5CC036V1 rév. D masqué par le logiciel SESAM VITALE P 2.2.0** (réf : P5CC036V1D/2.2.0) développée par Philips Semiconductors GmbH et Sagem Défense Sécurité.

1.2. Développeurs

Philips France Semiconducteurs M & S

5-7, rue Salomon de Rotchschild
BP 317
92156 Suresnes Cedex
France

Sagem Défense Sécurité

Avenue du Gros Chêne
95610 Eragny sur Oise
France

1.3. Description du produit évalué

1.3.1. Architecture

Le produit est un composant masqué (référence : P5CC036V1D/2.2.0) destiné à être utilisé dans une carte à puce, il est constitué :

- d'un micro-circuit P5CC036V1-D, développé et fabriqué par Philips Semiconductors GmbH;
- d'un logiciel SESAM VITALE P 2.2.0 développé par Sagem Défense Sécurité constitué d'un code (réf. S_VITALE_P_2_2_0) masqué dans la mémoire ROM et dans la mémoire EEPROM du micro-circuit.

Le logiciel inclut les applications suivantes :

- l'application d'administration électronique Adèle (E-ADMINISTRATION) ;
- l'application de santé VITALE ,
- l'application AIP d'initialisation et de personnalisation.

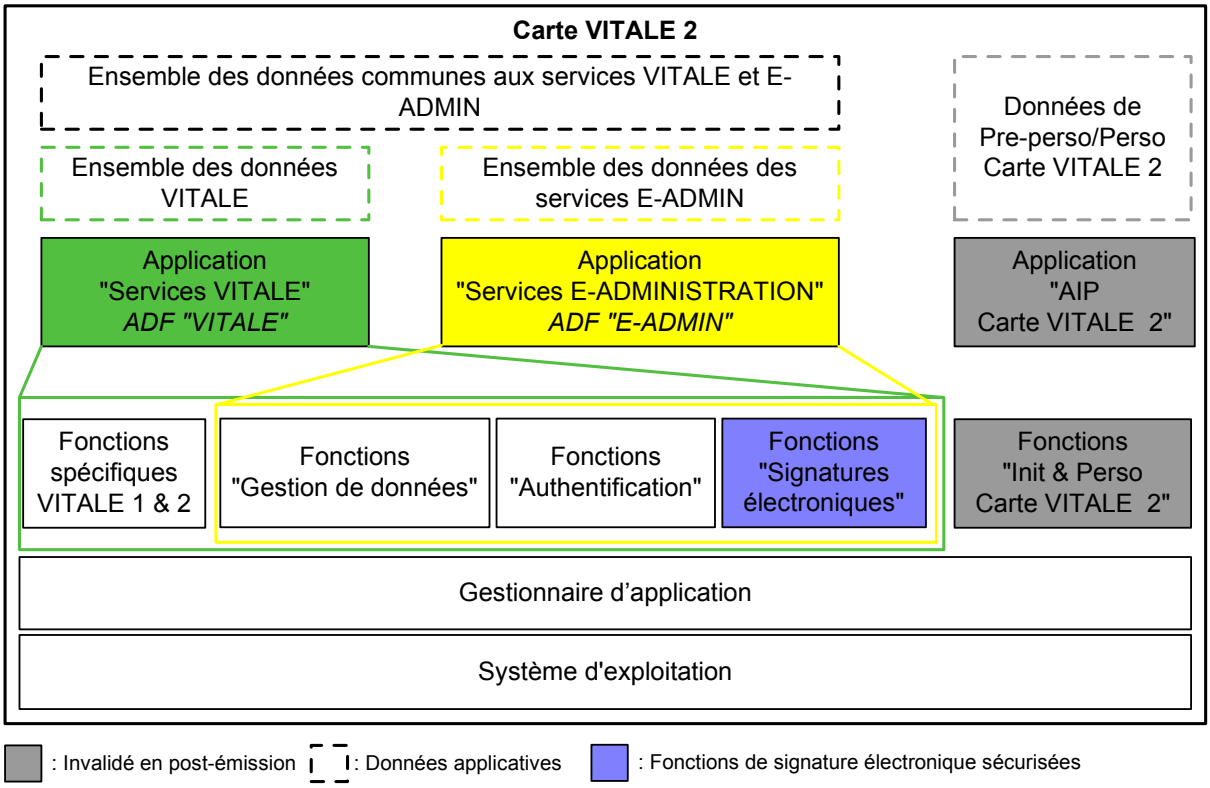

Figure 1 - Description de l'architecture de la carte VITALE 2

L'application Adèle (E-ADMINISTRATION) peut être instanciée plusieurs fois (le code de l'application est unique, seules les données traitées sont différentes pour chaque instance d'application).

1.3.2. Cycle de vie

Le cycle de vie du produit correspond à celui d'une carte à puce décrit dans le profil de protection PP/9911 [PP/9911], il est détaillé au chapitre 2.2 de la cible de sécurité [ST] et comprend les phases suivantes :

Phase	Description
Développement du produit	
Phase 1	Développement du logiciel embarqué de la carte à puce **Sagem Défense Sécurité** développe le logiciel intégré à la carte à puce et spécifie les exigences d'initialisation du circuit intégré.
Phase 2	Développement du composant masqué **Philips Semiconductors GmbH** conçoit le micro-circuit. A partir du micro-circuit et des données de **Sagem Défense Sécurité** sur le logiciel masqué, il construit la base de données du circuit intégré de la carte à puce.
Phase 3	Fabrication et test du circuit intégré **Philips Semiconductors GmbH** produit le circuit intégré qui se déroule en trois étapes principales : fabrication, test et initialisation du circuit intégré. **Philips Semiconductors GmbH** inclut le patch développé par **Sagem Défense Sécurité** dans le produit.
Exploitation du produit	
Phase 4	Encapsulation et test du circuit intégré Le constructeur de conditionnement du circuit intégré assure l'encapsulation et le test du circuit intégré.
Phase 5	Finition du produit carte à puce Le constructeur de la carte à puce assure la finition et le test de la carte à puce.
Phase 6	Personnalisation de la carte à puce Le personnalisateur assure la personnalisation de la carte à puce et des derniers tests.
Phase 7	Exploitation de la carte à puce L'émetteur de la carte à puce assure la livraison du produit à l'utilisateur final (porteur), ainsi que la fin du cycle de vie.

Figure 2 - Cycle de vie du produit

1.3.3. Périmètre et limites du produit évalué

Ce rapport de certification porte sur l'application Adèle (E-ADMINISTRATION) pour laquelle les aspects suivants ont été évalués :

- système d'exploitation,
- gestionnaire d'application,
- fonction de gestion des données,
- fonction de gestion des authentifications utilisateur,
- fonction de services de signature électronique sécurisée.

Les fonctions d'initialisation et de personnalisation de la carte VITALE 2 n'ont pas été évaluées.

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 pris en compte les résultats de l'évaluation du micro-circuit **Philips P5CC036V1D Secure Smart Card Controller with cryptographic library as IC Dedicated Support Software** au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [BSI-PP]. Ce micro-circuit a été certifié le 10 mars 2006 par le Bundesamt für Sicherheit in der Informationstechnik sous la référence BSI-DSZ-CC-0296-2006 [BSI-CC].

Une partie des verdicts de la présente évaluation s'appuie sur les résultats des travaux d'évaluation d'une version précédente du produit.

Le même projet d'évaluation a donné lieu au rapport de certification 2006/17 [2006/17] sur l'application VITALE.

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. Commanditaire

Sagem Défense Sécurité

Avenue du Gros Chêne
95610 Eragny sur Oise
France

2.4. Centre d'évaluation

CEA - LETI

17 rue des martyrs
38054 Grenoble Cedex 9
France

Téléphone : +33 (0)4 38 78 40 87

Adresse électronique : alain.merle@cea.fr

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 7 juin 2006 au 11 septembre 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].

Elle est également basée sur le profil de protection suivant :

- « Micro-circuit pour carte à puce avec un logiciel embarqué », PP/9911 [PP9911].

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 des exigences fonctionnelles de sécurité explicitement énoncées :

- FPT_EMSEC.1 issue des profils de protection PP SSCD type 2 et PP SSCD type 3 ;
- FCS_RND.1 issue du [BSI-PP] ;
- FCS_RND.2 et FPT_TST.2 issues du composant certifié [BSI-CC].

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
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_MSU.3	Analysis and testing for insecure state
+ AVA_VLA.4	Highly resistant

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

Sagem Défense Sécurité

Avenue du Gros Chêne
95610 Eragny sur Oise
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.

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

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.2	Sufficiency 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 :

- Potential violation analysis (FAU_SAA.1)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Quality metric for random numbers (FCS_RND.1)
- Random number generation (FCS_RND.2)
- Subset access control (FDP_ACC.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)
- Subset information flow control (FDP_IFC)
- Import of user data without security attributes (FDP_ITC.1)
- Basic internal (user data) transfer protection (FDP_ITT.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)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.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)
- Specification of management functions (FMT_SMF.1)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Abstract machine testing (FPT_AMT.1)
- TOE emanations (FPT_MSEC.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Basic internal TSF data transfer protection (FPT_ITT.1)
- Passive detection of physical attack (FPT_PHP.1)
- Resistance to physical attack (FPT_PHP.3)
- TSF domain separation (FPT_SEP.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TSF testing (FPT_TST.1)
- Subset TOE security testing (FPT_TST.2)
- Inter-TSF trusted channel (FTP_ITC.1)
- Limited fault tolerance (FRU_FLT.2)
- 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 et de ses constituants entre les différentes phases de son développement.

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, les différentes utilisations du produit ont été considérées :

Phase du cycle de vie	Rôle	Utilisation
4 et 5	Administrateur	Pré-personnalisateur
6	Administrateur	Personnalisateur
7	Administrateur	Autorité de domaine et émetteur
	Administrateur	Émetteur
	Utilisateur	Porteur

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 le développeur.

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 (identifiées dans la cible de sécurité ST) :

- authentification utilisateur par code PIN (FS_AUTH) ;
- production/vérification de cryptogrammes d'authentification (FS_CRYPTO, F.HW_DES, F.DES, F.SHA-1 et F.RSA) ;
- génération d'un checksum d'intégrité (FS_CHECKSUM) ;
- génération de clé (FS_SEC et F.RSA_KeyGen)

ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé 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 a été analysée par la DCSSI [COTATION] ; les mécanismes analysés sont cotés d'un niveau de robustesse standard (cf. [CRYPTO]) sous l'hypothèse de certaines conditions décrites dans le document.
Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

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] atteste que le produit satisfait au niveau d'évaluation décrit en 2.7.1 et 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 identifiés dans la cible de sécurité [ST] et résumés ci-dessous. Il devra suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] et respecter les conditions d'utilisation des mécanismes cryptographiques [COTATION].

Des objectifs de sécurité sur l'environnement sont issus du profil de protection PP/9911 [PP9911], en particulier :

- des procédures doivent assurer une livraison sûre du produit après son développement (phase 4 à 7) (O.DLV_PROTECT, O.DLV_AUDIT, O.DLV_RESP et O.DLV_DATA) ;
- des tests de fonctionnalité appropriés de la cible d'évaluation doivent être mis en œuvre aux phases 4 à 6 (O.TEST_OPERATE).

Des objectifs de sécurité sur l'environnement issus du profil de protection PP SSCD type 2 [SSCD2] concernent les aspect suivants :

- la correspondance entre SVD et SCD (OE.SCD_SVD_Corresp) ;
- le transfert sécurisé de SCD entre SSCD (OE.SCD_Transfer) ;
- l'unicité des données de création de signature (OE.SCD_Unique).

Des objectifs de sécurité sur l'environnement issus des profils de protection PP SSCD type 2 [SSCD2] et PP SSCD type 3 [SSCD3] concernent les aspects suivants :

- la génération de certificats qualifiés (OE.CGA_Qcert) ;
- la vérification de l'authenticité de la SVD par la CGA (OE.SVD_Auth_CGA) ;
- la protection des VAD (OE.HI_VAD) ;
- les données devant être signées (OE.SCA_Data_Intend).

Annexe 1. 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 2. Références documentaires du produit évalué

[CONF]	Carte VITALE 2, Fiche de livraison Logiciel 2.2.0, réf: SK 00000 32740 du 1/09/2006.
[GUIDES]	Guide administrateur carte VITALE 2. Référence : SK 0000024629 Version 1.10 du 29/06/06. Guide utilisateur carte VITALE 2. Référence : SK 0000024337 Version 1.4du 24/03/06.
[INSTALL]	Document d'installation, de génération et de démarrage. Référence : SK 0000027313 Version 1.5 du 24/02/06.
[RTE]	Projet CADUCEE, Rapport Technique d'Evaluation, réf : LETI.CESTI.CAD.RTE.005, version 1.0 du 11/09/2006.
[ST]	Cible de sécurité Carte VITALE 2: Application E-ADMINISTRATION - Composant Philips, Sagem Défense Sécurité, réf: SK – 00000 26 533, version 1.09 du 28/08/2006.
[COTATION]	Cotation des mécanismes cryptographiques du projet CADUCEE, N°3488/SGDN/DCSSI/SDS/Crypto du 12/12/2005.
[BSI-CC]	BSI-DSZ-0296-2006, Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software from Philips Semiconductors GmbH Business Line Identification, BSI, 10/03/2006.
[BSI-PP]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001, référence BSI-PP0002.
[2006/17]	Rapport de certification 2006/17 : Carte VITALE 2 - Application Adèle : Composant P5CC036V1 rev. D masqué par le logiciel SESAM VITALE P 2.2.0, DCSSI.
[SSCD2]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001
[SSCD3]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001.
[PP/9911]	Eurosmart Protection Profile, Smart Card Integrated Circuit With Embedded Software, PP/9911, v2.0, june 1999

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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard*, DCSSI, version 1.02 du 19/11/2004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[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