Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/18

Carte Morpho-Citiz 32 - Microcontrôleur P5CC036V1-D masqué par le logiciel Morpho-Citiz 32 (référence : MC32/P5CC036V1D/1.0.0)

Paris, le 24 septembre 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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 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

Référence du rapport de certification

DCSSI-2007/18

Nom du produit

Carte Morpho-Citiz 32 - Microcontrôleur P5CC036V1-D masqué par le logiciel Morpho-Citiz 32 (référence : MC32/P5CC036V1D/1.0.0)

Référence/version du produit

Version MC32/P5CC036V1D/1.0.0

Conformité à un profil de protection

PP-SSCD2, PP-SSCD3

Critères d'évaluation et version

Critères Communs version 2.2

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

Sagem Défense Sécurité

Avenue du Gros Chêne,
95610 Eragny sur Oise, France

NXP Semiconductors

Stresemannallee 101
D-22529 Hamburg, Germany

Commanditaire

Sagem Défense Sécurité

Avenue du Gros Chêne,
95610 Eragny sur Oise, France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

IT Security Certified

Le produit est reconnu au niveau EAL4

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, 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 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 Morpho-Citiz 32 - Microcontrôleur P5CC036V1-D masqué par le logiciel Morpho-Citiz 32 (référence : MC32/P5CC036V1D/1.0.0) » développée par Sagem Défense Sécurité et NXP (anciennement Philips).

Le produit est destiné à être utilisé dans le cadre de l'administration électronique. Il fournit l'application IAS-eGOV qui offre un ensemble de services, notamment de signature électronique répondant aux caractéristiques des dispositifs sécurisés de création de signature électronique (SSCD). Il permet en particulier la mise en œuvre de signatures électroniques présumées fiables au sens du décret n° 2001-272 du 30 mars 2001.

1.2. Description du produit évalué

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

La cible de sécurité s'inspire du profil de protection « Micro-circuit pour carte à puce avec un logiciel embarqué », PP/9911 [PP9911].

Cette cible de sécurité est conforme au profil de protection « Secure Signature-Creation Device Type 2 » [SSCD2] et « Secure Signature-Creation Device Type 3 » [SSCD3].

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 :
- nom commercial : Carte Morpho-Citiz 32 ;
- référence du produit : MC32/P5CC036V1D/1.0.0 ;
- référence du logiciel : OFFICIEL_S_MC32_P_1_0_0 ;
- référence du composant : NXP P5CC036V1- révision D.

Ces informations peuvent être vérifiées par la réponse de la carte à l'initialisation (ATR). Les octets d'identification sont disponibles dans le guide « Document d'installation, de génération et de démarrage » (cf. [GUIDES]) pour vérification.

1.2.2. Services de sécurité

Le produit propose un ensemble de services disponibles uniquement en phase utilisateur. L'accès à ces services dépend du rôle de l'utilisateur, de l'état de la carte Morpho-Citiz 32 et de l'état de l'application réalisant le service.

- Service de gestion de données de l'utilisateur. Ce service réalise l'ensemble des opérations de gestion de données et des secrets, accessibles à un utilisateur autorisé. Les données des instances de l'application IAS-eGOV sont cloisonnées, c'est-à-dire qu'une instance ne peut pas accéder aux données d'une autre instance (exception faite des données explicitement partagées).
- Service d'authentification des utilisateurs. Il est réalisé en faisant appel aux fonctions d'authentification :
    - vérification de code PIN/PUK ;
    - authentification mutuelle symétrique ;
    - authentification externe symétrique ;
    - authentification mutuelle asymétrique-DH ;
    - authentification externe asymétrique ;
    - authentification interne asymétrique.
- Service de signature électronique sécurisé. Il est réalisé en faisant appel aux :
    - fonctions de gestion des SCD/SVD ;
    - fonctions de signature.
- Service de confidentialité et d'intégrité. Il est réalisé en faisant appel aux :
    - fonctions de canal de confiance « Secure Messaging » ;
    - fonctions de confidentialité ;
    - fonction d'intégrité.

1.2.3. Architecture

Le produit est un composant masqué (référence : MC32/P5CC036V1D/1.0.0) destiné à être utilisé dans une carte à puce, il est constitué :

1. d'un micro-circuit P5CC036V1 révision D développé et fabriqué par NXP ;
2. d'un logiciel OFFICIEL_S_MC32_P_1_0_0 développé par Sagem Défense Sécurité constitué d'un code masqué dans la mémoire ROM et dans la mémoire EEPROM du micro-circuit (référence : MC32/P5CC036V1D/1.0.0).

Le code en ROM réalise les fonctionnalités suivantes :

- gestion des données (données utilisateur et secrets) ;
- gestion des authentifications utilisateur ;
- services de signature électronique sécurisée ;
- fonctions d'initialisation et de personnalisation de la carte Morpho-Citiz 32.

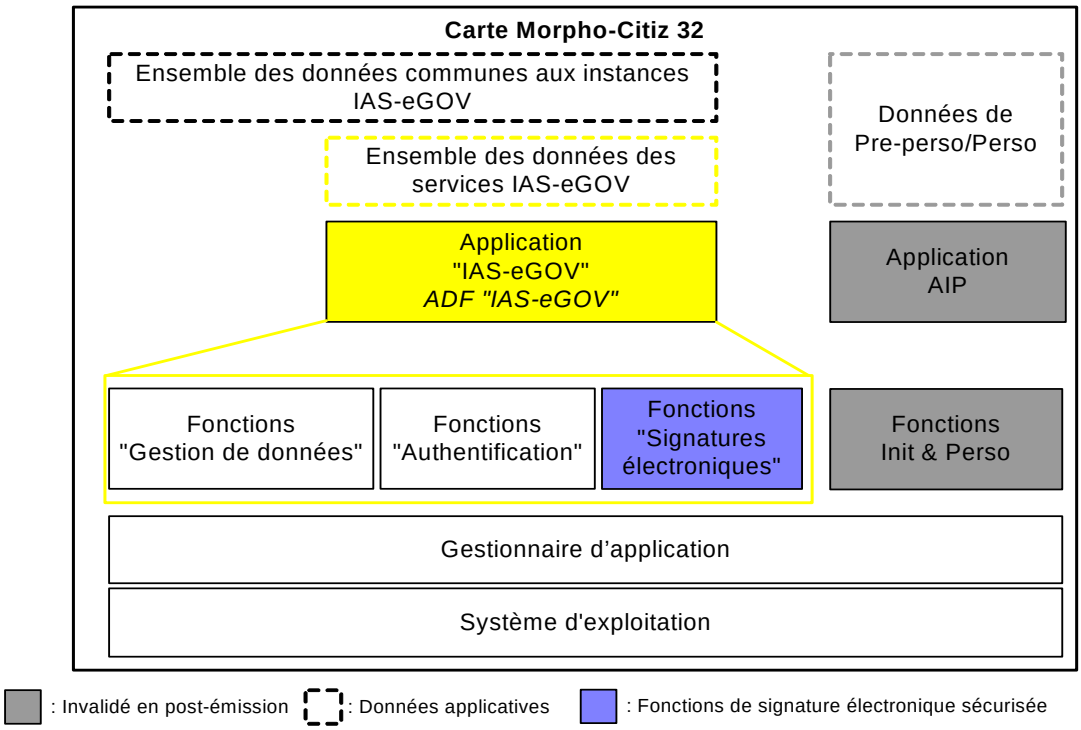
Ces fonctionnalités permettent de réaliser les applications suivantes :

- application d'initialisation et de personnalisation (invalidée en phase "USER"),
- application IAS-eGOV répondant aux besoins de l'administration électronique.

L'application IAS-eGOV peut être instanciée plusieurs fois (le code de l'application, en ROM, est unique, ce sont les données traitées qui sont différentes pour chaque instance d'application).

Le logiciel inclut les applications suivantes :

- l'application IAS-eGOV ;
- l'application AIP d'initialisation et de personnalisation.


Carte Morpho-Citiz 32
Ensemble des données communes aux instances IAS-eGOV
Ensemble des données des services IAS-eGOV
Application "IAS-eGOV" ADF "IAS-eGOV"
Données de Pre-perso/Perso
Application AIP
Fonctions "Gestion de données"
Fonctions "Authentification"
Fonctions "Signatures électroniques"
Fonctions Init & Perso
Gestionnaire d'application
Système d'exploitation
: Invalidé en post-émission
: Données applicatives
: Fonctions de signature électronique sécurisée

1.2.4. 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 **NXP** conçoit le microcontrôleur. A partir du microcontrôleur 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 **NXP** produit le circuit intégré en trois étapes principales : fabrication, test et initialisation du circuit intégré. **NXP** 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 les derniers tests.
Phase 7	Exploitation de la carte à puce L'émetteur de carte à puce assure la livraison du produit à l'utilisateur final (porteur), ainsi que la fin du cycle de vie.

Figure 1 - Cycle de vie du produit

Le produit a été développé sur le site suivant :

Sagem Défense Sécurité

Avenue du Gros Chêne, 95610 Eragny sur Oise, France

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

1.2.5. Configuration évaluée

Ce rapport de certification porte sur l'application IAS-eGOV dont les aspects suivants ont été évalués :

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

Les fonctions d'initialisation et de personnalisation (AIP) de la carte Morpho-Citiz 32 n'ont pas été évaluées ; ces fonctions sont invalidées après la personnalisation de la carte (Phase 6).

Au regard du cycle de vie, le produit évalué est celui qui sort de fabrication (phase 3).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.2** [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 centre d'évaluation et validées par la DCSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « **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].

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 9 mai 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

Les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de la DCSSI (cf. [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 par 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 « Carte Morpho-Citiz 32 - Microcontrôleur P5CC036V1-D masqué par le logiciel Morpho-Citiz 32 (référence : MC32/P5CC036V1D/1.0.0) » 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 2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation identifiés dans la cible de sécurité [ST] et résumés ci-dessous. Il devra suivre les recommandations de configuration et d'utilisation se trouvant dans les guides fournis [GUIDES] et respecter les conditions d'utilisation des mécanismes cryptographiques [ANA-CRY].

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 fonctionnels 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 aspects 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).

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance 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 :

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

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

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle-Zélande, la Norvège, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
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	**2**	Sufficiency of security measures
	ALC_FLR									
	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		
	AVA_MSU			**1**	**2**	2	**3**	3	**3**	Analysis and testing of insecure states
	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 : - Cible de sécurité Carte Morpho-Citiz 32 - Composant PHILIPS référence : SK - 00000 53753 V 1.3, du 03/05/07. Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cible de sécurité Carte Morpho-Citiz 32 - Composant PHILIPS Version publique référence : SK-0000053755 V 1.2
[RTE]	Rapport technique d'évaluation : - Rapport technique d'évaluation Référence : LETI.CESTI.DEM.RTE.002 - v1.0 - 09/05/07
[ANA-CRY]	Cotation des mécanismes cryptographiques, N°3488/SGDN/DCSSI/SDS/Crypto du 12/12/2005.
[CONF]	Projet MORPHO-CITIZ32 Fiche de Version du Logiciel OFFICIEL_S_MC32_P_1_0_0 Composant PHILIPS Référence : SK0000055238-1.2 V 1.2 du 05/04/07
[GUIDES]	Guide d'installation du produit : - Document d'installation, de génération et de démarrage. Référence : SK-0000051482 Version 1.2 du 07/11/06. Guide d'administration du produit : - Guide administrateur carte Morpho-Citiz 32. Référence : SK-0000051475 Version 1.1 du 25/07/06, Guide d'utilisation du produit : - Guide utilisateur carte Morpho-Citiz 32. Référence : SK-0000051481 Version 1.1 du 25/08/06, Guide de livraison du produit : - Procédures de livraison pour le composant PHILIPS P5CC036. Référence : SK-0000057043 Version 1.1 du 11/12/06.
[BSI-PP]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI sous la référence BSI-PP-0002-2001.*
[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.
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. *Certifié par la DCSSI sous la référence PP/9911.*
[SSCD2]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0005-2002.*

[SSCD3]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002.*

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.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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.
[REF-CRY]	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.