PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2007/02

Carte IDOneClassIC : composant P5CT072VOP masqué par ID-One Cosmo 64 RSA v5.4 et embarquant l'application IDOneClassIC v1.0

Paris, le 29 janvier 2007,

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 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

2007/02

Nom du produit

Carte IDOneClassIC : composant P5CT072VOP masqué par ID-One Cosmo 64 RSA v5.4 et embarquant l'application IDOneClassIC v1.0

Référence/version du produit

Référence de l'application embarquée : IDOneClassIC, Version 1.0

Références du microcontrôleur : P5CT072VOP, ROM mask P5CT072EWE1/T0PB6311

Conformité aux profils de protection

PP SSCD type 2 [PP0005] et PP SSCD type 3 [PP0006]

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, AVA_MSU.3, AVA_VLA.4

Développeurs

Oberthur Card Systems

71-73 rue des Hautes Pâtures,
92726 Nanterre Cedex, France

Philips Semiconductors GmbH

Business Line Identification
PP Box 54 02 40
D-22502 Hamburg, Germany

Commanditaire

Oberthur Card Systems

71-73 rue des Hautes Pâtures, 92726 Nanterre Cedex, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France
Tél : +33 (0)5 57 26 08 64, mél : m.dus@serma.com

Accords de reconnaissance applicables

CCRA

Le produit est reconnu au niveau EAL4.

Les composants ADV_IMP.2, AVA_MSU.3, AVA_VLA.4 ne sont pas couverts par la reconnaissance.

SOG-IS

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 IDOneClassIC : composant P5CT072VOP masqué par la plate-forme ID-One Cosmo 64 RSA v5.4 (GOP ID MX 64) et embarquant l'application IDOneClassIC version 1.0, développé par Philips Semiconductors GmbH et Oberthur Card Systems.
Ce produit est une application de création de signature électronique, définie par :

- le microcontrôleur sous-jacent ;
- le système d'exploitation embarquant la machine virtuelle Java ;
- l'application Java de création de signature.

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.
Cette cible de sécurité est conforme aux profils de protection [PP0005] et [PP0006] (SSCD de type 2 et 3).

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 :

- identifiant du microcontrôleur, « Philips T023P », écrit à la surface du produit et visible au microscope ;
- identifiant du ROM code, « 0B6 », écrit à la surface du produit et visible au microscope ;
- identifiant de l'applet (AID), « A0 00 00 00 77 01 00 00 07 10 00 01 00 00 04 », saisi lors de son chargement.

1.2.2. Services de sécurité

Le produit évalué comprend les éléments suivants :

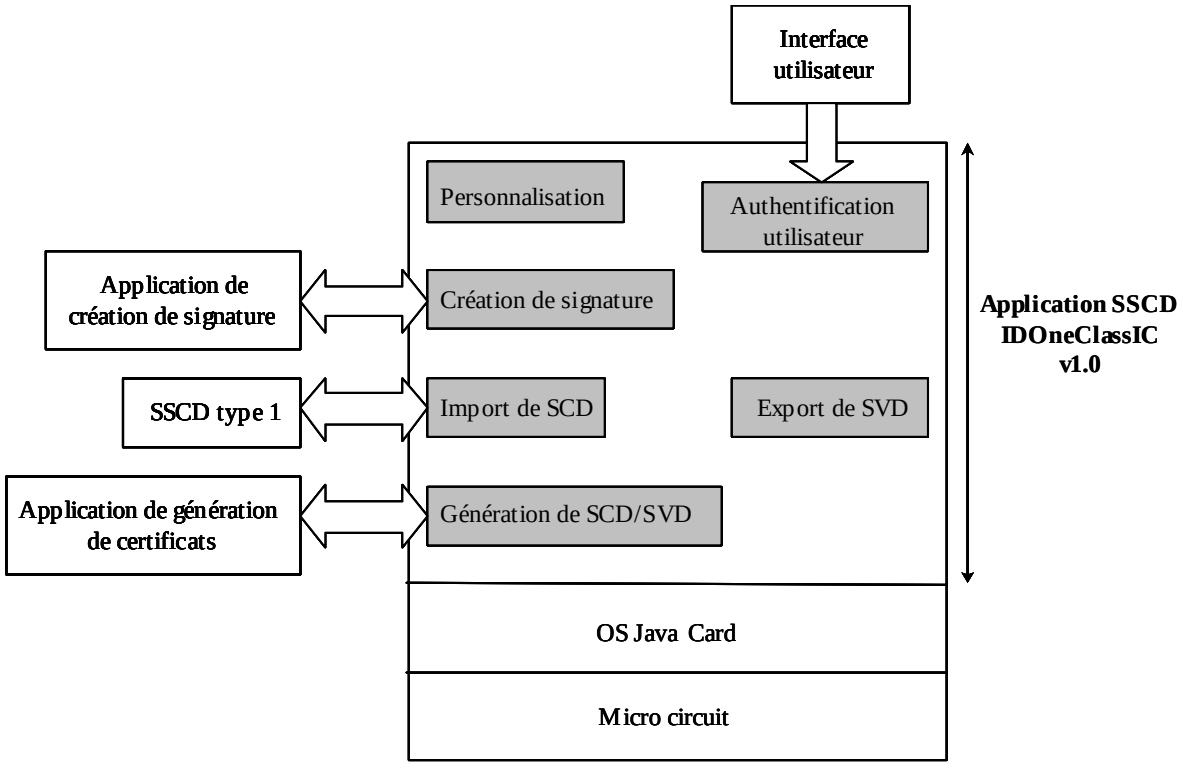
- un système d'exploitation, basé sur les technologies JavaCard et Global Platform, qui fournit les principaux services de sécurité suivants :
    - interface entre le microcontrôleur et l'applet IDOneClassIC ;
    - services basiques pour accéder aux mémoires et aux opérations cryptographiques requis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

- l'application IDOneClassIC, qui fournit les principaux services de sécurité suivants :
  - 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.

1.2.3. Architecture

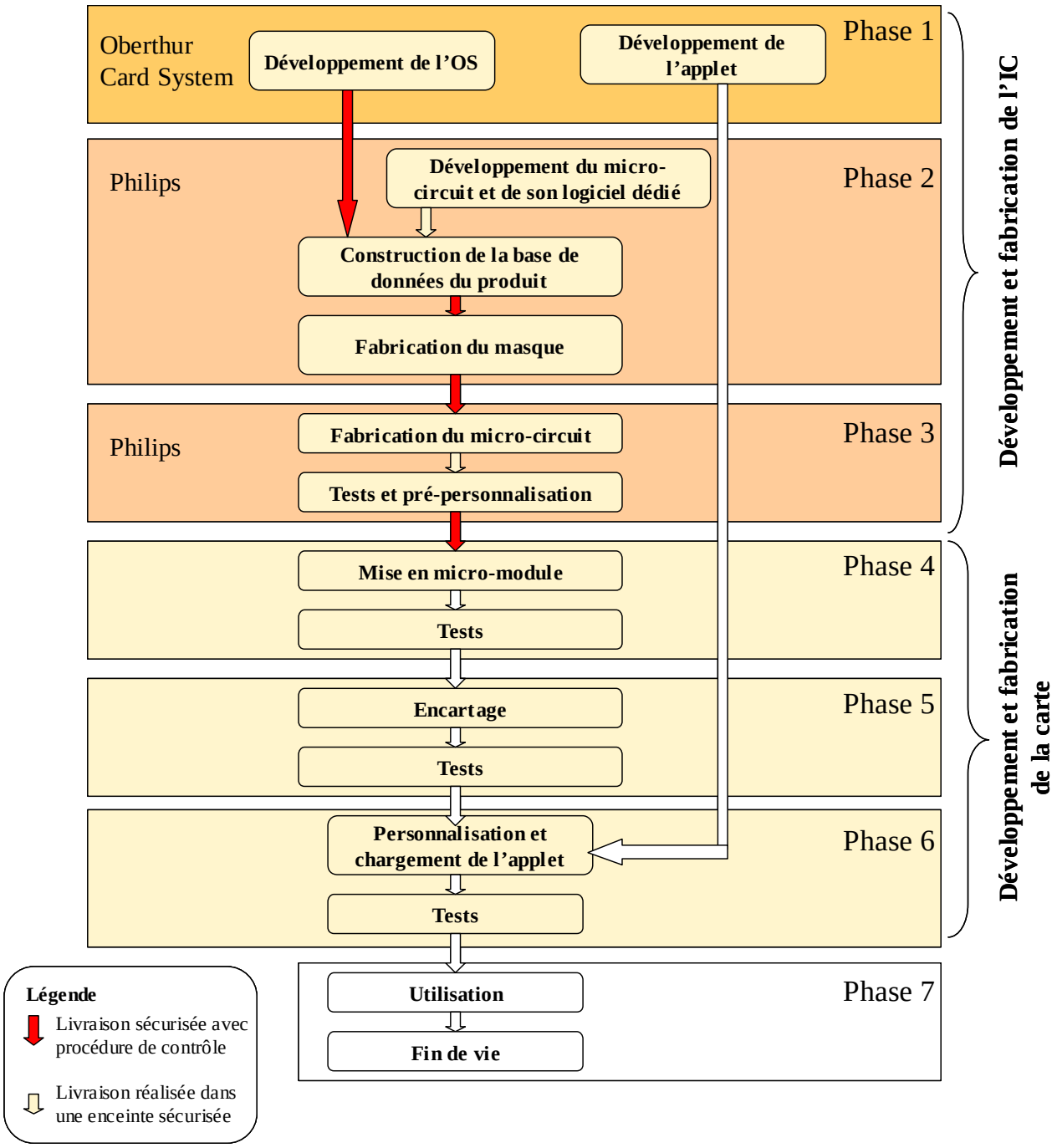
Le produit est constitué :

- du microcontrôleur P5CT072VOP, développé et fabriqué par Philips Semiconductors GmbH ;
- de l'OS JavaCard, développé par Oberthur Card Systems, constitué de :
  - la plateforme ID-One Cosmo 64 RSA v5.4 (GOP ID MX 64), masquée dans la ROM du microcontrôleur (BIOS/VM : ref. build33, Platform : ref. Platform RefV87, Resident application : ref. GOP64_20051014),
  - du code optionnel RSA SFM en EEPROM (version r1.0, ref. Liv20060310) ;
- de l'application SSCD IDOneClassIC, développée par Oberthur Card Systems, chargée au moment de la personnalisation de la carte (IDOneClassIC v1.0).



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur le site suivant :

Oberthur Card Systems
71-73, rue des Hautes Pâtures,
92726 Nanterre Cedex,
France

Le microcontrôleur, certifié par le BSI, a été développé et produit par Philips Semiconductors GmbH.

Pour l'évaluation, l'évaluateur a considéré comme « administrateurs du produit » les personnalisateurs des cartes et comme « utilisateurs du produit » les terminaux au travers desquels les signataires utilisent les cartes.

1.2.5. Configuration évaluée

Le produit évalué est le microcontrôleur et son logiciel embarqué identifié au §1.1.
Le certificat porte sur la configuration « fermée » du produit (blocage du chargement d'applets après le chargement de l'applet IDOneClassIC).
Le produit testé par le centre d'évaluation est représentatif du produit final.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [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, validées par la DCSSI et compatibles avec le document [AIS34], 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 a été réalisée en composition 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 P5CT072VOP au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 28 mars 2006 sous la référence BSI-DSZ-CC-0348-2006.

L'évaluation s'appuie sur les résultats d'évaluation du produit « Carte CNS : composant P5CT072VOP masqué par la plate-forme JavaCard GOP ID MX 64 et embarquant l'application CNS 1.0.7 » certifié le 15 septembre 2006 sous la référence 2006/13 [2006_13].

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 24 janvier 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 n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], 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 IDOneClassIC : composant P5CT072VOP masqué par ID-One Cosmo 64 RSA v5.4 et embarquant l'application IDOneClassIC v1.0» 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 1.2 du présent rapport de certification.

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

- 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 sécurisée –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 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 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	**1**	Indentification 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**	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 : - IDOneClassIC CARD Security Target, ref. FQR: 110 3517, édition 4, 16/01/07 Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IDOneClassIC CARD Public Security Target, ref. 110 36 45, version 1.0, 16/01/07
[RTE]	ANTERAK project: Evaluation Technical Report, ref. ANTERAK_ETR_V1.2, version 1.2 du 24/01/07
[CONF]	ANTERAK Configuration List, ref. FQR : 110 3580, édition 2 du 16/01/07
[GUIDES]	Guide d'installation, d'administration et d'utilisation du produit : - IDOneClassIC Guidance, ref. FQR : 110 3558, édition: 1 du 20/11/06 - Software Requirement Specification, ref. 066771 00 SRS, édition 1-AB du 23/11/06
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certifié sous la référence BSI-PP-0005-2002.*
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certifié sous la référence BSI-PP-0006-2002.*
[PP0002]	Protection Profile — Smart card IC Platform Protection Profile, Version: 1.0, July 2001. *Certifié sous la référence BSI-PP-0002-2001.*
[2006_13]	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, 15 septembre 2006 SGDN/DCSSI

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, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.0, 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.
[AIS34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004 Bundesamt für Sicherheit in der Informationstechnik