



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2007/16

Carte COSMOS V1.1: composant P5CT072VOP masqué par la plate-forme COSMO 64 RSA D v5.4 et embarquant l'application IDOne IAS v1.01 (configuration SSCD)

Paris, le 29 août 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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.



Référence du rapport de certification

2007/16

Nom du produit

Carte COSMOS V1.1: composant P5CT072VOP masqué par la plate-forme COSMO 64 RSA D v5.4 et embarquant l'application IDOne IAS v1.01 (configuration SSCD)

Référence/version du produit

Référence de l'application embarquée : IDOne IAS (IDOne V3), Version 1.01
Références du microcontrôleur : P5CT072VOP, ROM mask P5CT072EWE1/T0PB6311

Conformité à un profil 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 5 augmenté

ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeurs

Oberthur Card Systems

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

NXP

**Stresemannallee 101
22505 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, e.francois@serma.com**

Accords de reconnaissance applicables

CCRA



SOG-IS



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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT EVALUE	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	9
1.2.5. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	14
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	15
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	17

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte COSMOS V1.1 : composant P5CT072VOP masqué par la plate-forme Cosmo 64 RSA v5.4 (GOP ID MX 64) et embarquant l'application IDOne IAS (IDOne V3) version 1.01 en configuration SSCD , développé par NXP et Oberthur Card Systems.

L'applet IDOne IAS est aussi appelée IDOne V3.

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 types 2 et 3).

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version de chaque composant logiciel de la version certifiée du produit peut être vérifiée, en phase d'utilisation finale, par la commande *Get Data* (voir [AGD_JCP] et [SRS]). Cette commande renvoie les données suivantes :

- Pour la plate-forme, Tag 'DF52':
 - o 00 02 **e9 10** 01 06 41 07 11 30 42 36 02 05 **00 00 f9 00 ff** 03 06 **06 58 81** 01 23
e9 04 01 77 05 01 0f 90 00
 - identifiant du masque : **E910** ;
 - identifiant de la carte: **00 00 f9 00 ff** ;
 - identifiant du code optionel : **065881** ;
- pour l'application ID One V3 et les APIs, Tag '61':
 - o 61 20 53 02 **d0 14** 53 02 **a0 04** 53 02 **a0 08** 53 02 **a0 0d** 53 02 **a0 09** 53 02 36
40 53 02 02 19 53 02 02 19 90 00
 - application ID One V3 : **D014** ;
 - utilitaires : **A004** ;
 - système de fichiers : **A008** ;
 - secure messaging : **A00D** ;
 - sécurité : **A009**.

1.2.2. Services de sécurité

Le produit évalué comprend les éléments suivants :

- Une plate-forme JavaCard qui fournit les principaux services de sécurité suivants :
 - o interface entre le microcontrôleur et l'applet IDOne V3 ;
 - o services basiques pour accéder aux mémoires et aux opérations cryptographiques requis par l'applet IDOne V3 ;
 - o gestion de la carte (chargement, installation et suppression d'applets) et contrôle des services de sécurité de la carte (intégrité des données et contre-mesures relatives aux attaques physiques) ;
 - o mécanisme de blocage du chargement d'applets après le chargement de l'applet IDOne V3 (ainsi aucune nouvelle applet ne pourra être chargée après que le statut de JCP ait été positionné à SECURED).

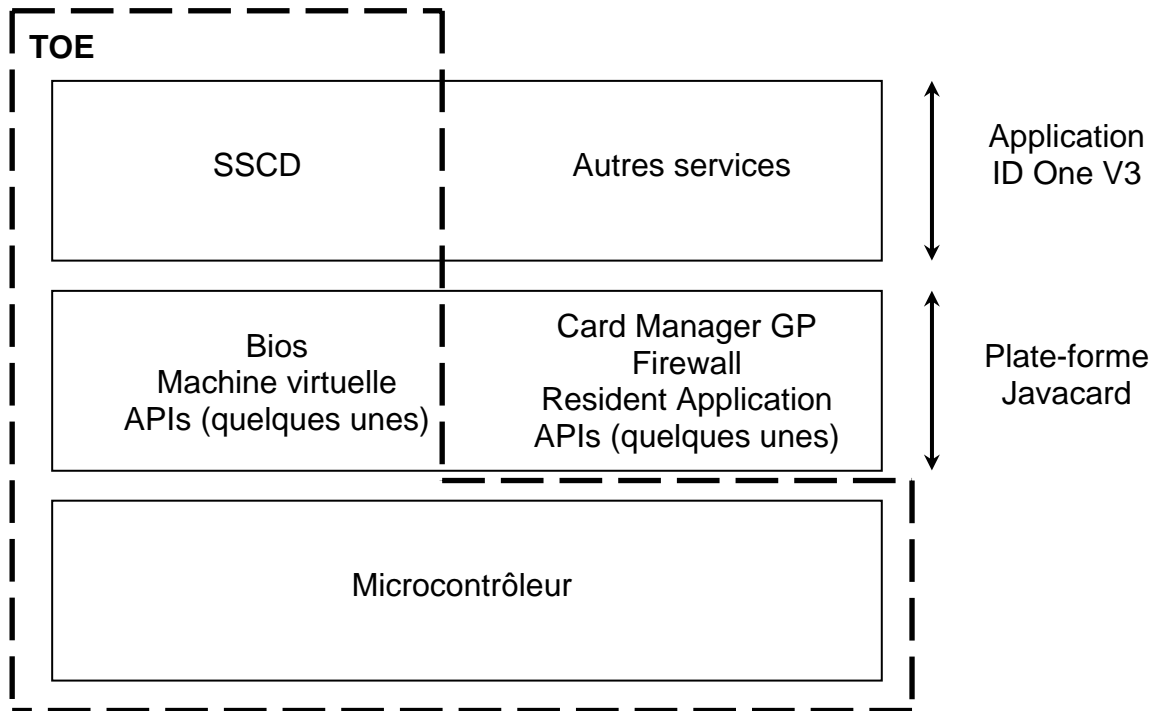
- L'application IDOne V3 (dont le nom commercial est IDOne IAS) qui fournit les principaux services de sécurité suivants :
 - o génération de clés privées et publiques de signature (SCD et SVD) ;
 - o protection des clés privées de signature ;
 - o import de clés privées et publiques de signature ;
 - o export de clés publiques de signature ;
 - o création de signature ;
 - o administration des PIN ;
 - o authentification du signataire par un PIN ;
 - o authentification externe d'un administrateur ;
 - o implémentation d'un chemin de confiance avec le dispositif en interface avec les utilisateurs.

Cette application fournit également les fonctionnalités IAS qui sont hors du périmètre de cette évaluation.

1.2.3. Architecture

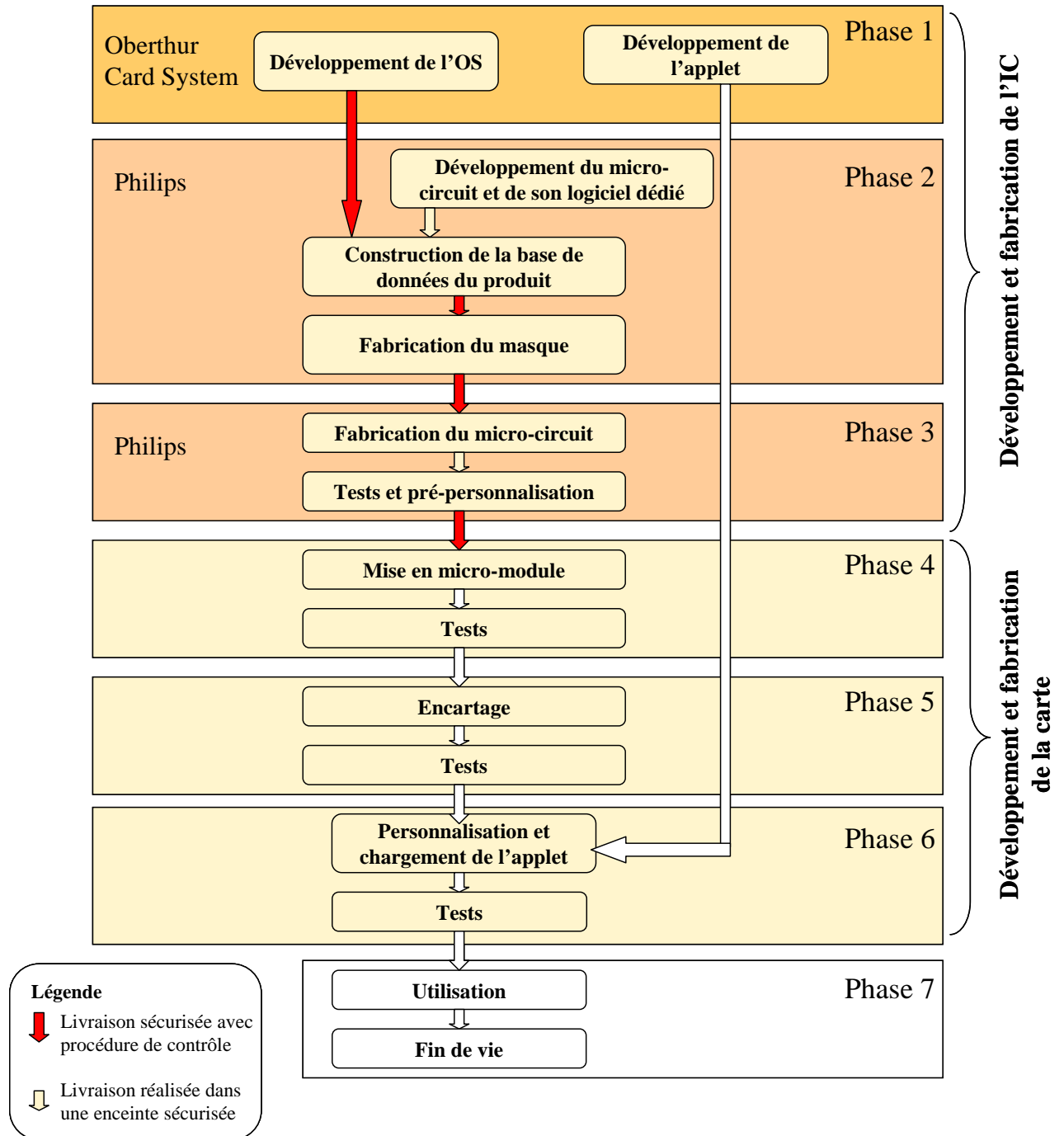
Le produit est constitué :

- du microcontrôleur P5CT072VOP, développé et fabriqué par NXP ;
- de l'OS JavaCard, développé par Oberthur Card Systems, constitué de :
 - o la plate-forme 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),
 - o du code optionnel RSA SFM en EEPROM (version r1.0, ref. Liv20060310) ;
- de l'application IDOne V3, développée par Oberthur Card Systems, chargée au moment de la personnalisation de la carte (v1.01).



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 NXP (précédemment connu en tant que 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

Ce certificat ne s'applique qu'à la configuration SSCD du produit : les fonctionnalités IAS ne sont pas disponibles dans la configuration étudiée (i.e. les objets mis en œuvre par les fonctionnalités IAS ne sont pas créés dans la phase de pré-personnalisation de l'application IDOne V3). Toutes les opérations de personnalisation sont décrites dans le document [PEP].

Le certificat porte sur la configuration « fermée » du produit (blocage du chargement d'applets après le chargement de l'applet IDOne V3).

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.

Le niveau de résistance du microcontrôleur a été confirmé le 6 août 2007, par le schéma allemand, dans le cadre du processus de surveillance.

L'évaluation s'appuie sur les résultats d'évaluation des cartes CNS et IDOneClassIC, certifiées par la DCSSI respectivement le 15 septembre 2006 et le 29 janvier 2007, sous les références 2006/13 [2006_13] et 2007/02 [2007_02].

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 8 juin 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 du rapport [ANA-CRY] qui établit que les mécanismes analysés atteignent, jusqu'en 2008, le niveau standard défini dans le référentiel cryptographique de la DCSSI (cf. [REF-CRY]). Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

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 COSMOS V1.1: composant P5CT072VOP masqué par la plate-forme COSMO 64 RSA D v5.4 et embarquant l'application IDOne IAS v1.01 (configuration SSCD)» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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'accord¹, 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 signataires², 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 5+	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	3	Development tools 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	3	Semiformal functional specification
	ADV_HLD		1	2	2	3	4	5	3	Semiformal high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3	1	Modularity
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	2	Semiformal correspondence demonstration
	ADV_SPM				1	3	3	3	3	Formal 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	2	Standardised life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	2	Testing: low-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					1	2	2	1	Covert channel analysis
	AVA_MSU			1	2	2	3	3	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]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - ID ONE V3 Security Target, ref. FQR: 110 2963, édition 6, 16/05/07 <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Oberthur Card System - Cosmos Security Target Lite, ref UDD 064471 02, édition 1-AA
[RTE]	<p>Rapports techniques d'évaluation :</p> <ul style="list-style-type: none"> - COSMOS project: Evaluation Technical Report, ref. COSMOS_ETR_V1.1.fm, version 1.1, 08/06/07 - Addendum to Evaluation Technical Report, ref. Add_COSMOS_ETR_v1.1_V1.0.fm, version 1.0, 28/08/07
[ANA-CRY]	<p>Cotation de mécanismes cryptographiques - Projet COSMOS, ref. N° 1479/SGDN/DCSSI/SDS/Crypto du 06 Juillet 2006</p>
[CONF]	<p>COSMOS Configuration List, ref. FQR : 110 3217, édition 2, 30/01/07</p>
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> - [PEP]: ID One IAS PERSONNALISATION ref. 065421 00 PEP, édition 1-AB, 01/12/06 <p>Guide d'administration et d'utilisation du produit :</p> <ul style="list-style-type: none"> - [AGD_JCP] : IDOne Cosmo 64 RSA D v5.4, ref. 064471 01 UDD AA - [SRS]: ID One V3 Applet SRS, ref. 063253 00 SRS, édition 3-AA, 30/01/07 - COSMOS AGD_USR/AGD_ADM, ref. FQR : 110 3597, édition 1, 01/12/06
[PP0005]	<p>Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0005-2002T.</i></p>
[PP0006]	<p>Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002T.</i></p>
[PP0002]	<p>Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0002-2001.</i></p>
[2006_13]	<p>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 September 2006, SGDN/DCSSI</p>



[2007_02]	Rapport de certification - Carte IDOneClassIC : composant P5CT072VOP masqué par ID-One Cosmo 64 RSA v5.4 et embarquant l'application IDOneClassIC v1.0, 29 january 2007, 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 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]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.



[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004 Bundesamt für Sicherheit in der Informationstechnik
----------	--