PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2013/16

Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual)

Paris, le 29 mars 2013

Le directeur général de l'agence nationale 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), 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 et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2013/16

Nom du produit

Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual)

Référence/version du produit

Version Plateforme JavaCard : 7.1-s

Conformité à un profil de protection

ANSSI-CC-PP-2010/03-M01 [PP JCS]

Java Card System – Open Configuration, version 3.0

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Oberthur Technologies

71-73 rue des Hautes Pâtures
92726 Nanterre Cedex
France

ST Microelectronics

Smartcard IC division
190 avenue Célestin Coq
13106 Rousset
France

Commanditaire

Oberthur Technologies

420 rue d'Estienne d'Orves, 92705 Colombes, France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

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 modifié. Ce décret indique que :

- L'agence nationale 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 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 7
1.2.4. Architecture 8
1.2.5. Cycle de vie 9
1.2.6. Configuration évaluée 10

2. L'EVALUATION 12

2.1. REFERENTIELS D'EVALUATION 12
2.2. TRAVAUX D'EVALUATION 12
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LE REFERENTIEL TECHNIQUE DE L'ANSSI 12
2.4. ANALYSE DU GENERATEUR D'ALEAS 13

3. LA CERTIFICATION 14

3.1. CONCLUSION 14
3.2. RESTRICTIONS D'USAGE 14
3.3. RECONNAISSANCE DU CERTIFICAT 15
3.3.1. Reconnaissance européenne (SOG-IS) 15
3.3.2. Reconnaissance internationale critères communs (CCRA) 15

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 16

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 17

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 19

1. Le produit

1.1. Présentation du produit

L'évaluation porte sur la plateforme ouverte JavaCard du produit « ID-One Cosmo V7.1-s » qui est une carte à puce pouvant être en mode contact, sans contact ou dual. Le produit est développé par la société Oberthur Technologies et masqué sur l'un des microcontrôleurs ST23YR80B (Standard Dual) ou ST23YR48B (Basic Dual) développés et fabriqués par la société ST Microelectronics.

La plateforme ouverte JavaCard est destinée à fournir des services de sécurité aux applets qui seront installées et chargées sur la carte.

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées sur le produit (voir [GUIDES]), notamment :
- l'application IAS ECC destinée à mettre en œuvre la signature électronique ;
- l'application LDS EAC, comportant le mécanisme SAC, qui réalise les fonctions de passeport électronique.

1.2. Description du produit

1.2.1. Introduction

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 au profil de protection [PP JCS]. Cette conformité est de type démontrable.

1.2.2. 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 présents dans la réponse que donne le produit suite à la commande GET DATA (voir [GUIDES]).

La commande GET DATA pour le tag ‘DF 52’, donne les réponses suivantes :

Nom de la TOE	**ID-One Cosmo V7.1-s Standard Dual**	**ID-One Cosmo V7.1-s Basic Dual**
Identification du microcontrôleur (tag ‘DF 52’, sous-tag ‘01’)	‘20’ : Standard Dual (ST23YR80B)	‘04’ : Basic Dual (ST23YR48B)
Identification du masque (tag ‘DF 52’, sous-tag ‘03’)	‘61 01’ ID-One Cosmo V7.1	‘61 01’ ID-One Cosmo V7.1
Identification du patch *Generic* (tag ‘DF 52’, sous-tag ‘04’) (obligatoire)	‘07 86 24’ Generic r4.0 (version 00)	‘07 89 12’ Generic r2.0 (version 00)
Identification du patch *SAC* (tag ‘DF 52’, sous-tag ‘04’) (optionnel)	‘07 92 12’ SAC r2 (version 02)	Ce patch n’est pas destiné à être chargé sur cette configuration.

Le patch *Generic*, chargé sur la carte en phase de pré-personnalisation (phase 5 du cycle de vie), apporte des corrections et des améliorations de sécurité à la plateforme.

Le patch *SAC*, qui est chargé de manière optionnelle sur la carte en phase de pré-personnalisation (phase 5 du cycle de vie) à la demande du client, apporte des corrections fonctionnelles au mécanisme SAC (en dehors de l’évaluation). Lorsque le patch *SAC* est chargé sur la carte, le mécanisme SAC est opérationnel.

La commande GET DATA pour les tags ‘DF 66’ et ‘DF 67’, donne les réponses suivantes :

Tag ‘DF 66’ Version Commerciale du produit	**Tag ‘DF 67’ Version Interne du produit**
‘076651FF 07010000 0000’	‘01010F00’

La commande GET DATA pour le tag ‘9F 7F’, donne la réponse suivante :
- *IC Fabricator* : ST Microelectronics ‘**47 50**’;
- *IC Type* : ST23YRxxB (où “xx” vaut “80” ou “48”) : ‘**B2 14**’ ;
- *Operating System Identifier* : ‘**82 31**’ ;
- *Operating System Release Date* : ‘**B1 5E**’;
- *Operating System Release Level* : ‘**00 75**’.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- les services de pré-personnalisation de la carte ;
- l’authentification du porteur de la carte par code PIN ou données biométriques ;
- le chargement, l’installation, la suppression, l’extraction et la vérification en intégrité et en authenticité d’applets ;
- la fourniture de mécanismes de chiffrement et de déchiffrement ;
- la fourniture d’un mécanisme de génération et de vérification de signature électronique ;
- la fourniture d’un générateur de nombres aléatoires ;
- la gestion des clés contenues dans la carte (chargement, génération, utilisation, mise à jour, suppression, distribution, désactivation de l’usage d’une clé, accès sécurisé, fourniture d’un protocole d’échange) ;

- la protection des clés, du code PIN, des données biométriques et du code patché à l'aide d'une valeur d'intégrité ;
- le traitement sécurisé des opérations ;
- la fourniture d'un *Runtime Verifier* assurant des opérations de contrôle supplémentaire pendant l'exécution des applets ;
- la gestion de la mémoire EEPROM ;
- le pare-feu isolant les objets ou les applets ;
- les services standards GlobalPlatform comme le canal logique et les canaux sécurisés (SCP02, SCP03), ainsi que le canal sécurisé propriétaire (SCPF3).

Une liste détaillée des services de sécurité est donnée dans [ST].

Les principaux services offerts par les microcontrôleurs sont :

- l'initialisation de la plateforme matérielle et des attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- les tests du produit ;
- la gestion mémoire (*firewall*) ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité ;
- le support au chiffrement cryptographique ;
- le support à la génération de nombres non prédictibles.

1.2.4. Architecture

La plateforme JavaCard de la carte à puce « ID-One Cosmo V7.1-s » est constituée des éléments suivants :

- du microcontrôleur, offrant les fonctionnalités matérielles (gestion de la mémoire et gestion des entrées/sorties), et sa bibliothèque cryptographique ;
- du BIOS, assurant l'interface entre les applications natives, comme la machine virtuelle, et le microcontrôleur ;
- de l'application résidente, en code natif, permettant de recevoir les commandes de la carte et de les distribuer aux applications ;
- de la machine virtuelle (*Virtual Machine*) interprétant le *byte code* des applets Java ;
- d'APIs, offrant des interfaces aux applications pour la génération de clés, la négociation de clés, la signature, le chiffrement de messages ainsi que d'autres interfaces de programmation propriétaires (OT API) ;
- du gestionnaire de la carte (*Card Manager*) et du domaine de sécurité (*Security Domain*).

Cette architecture est résumée dans la figure suivante :

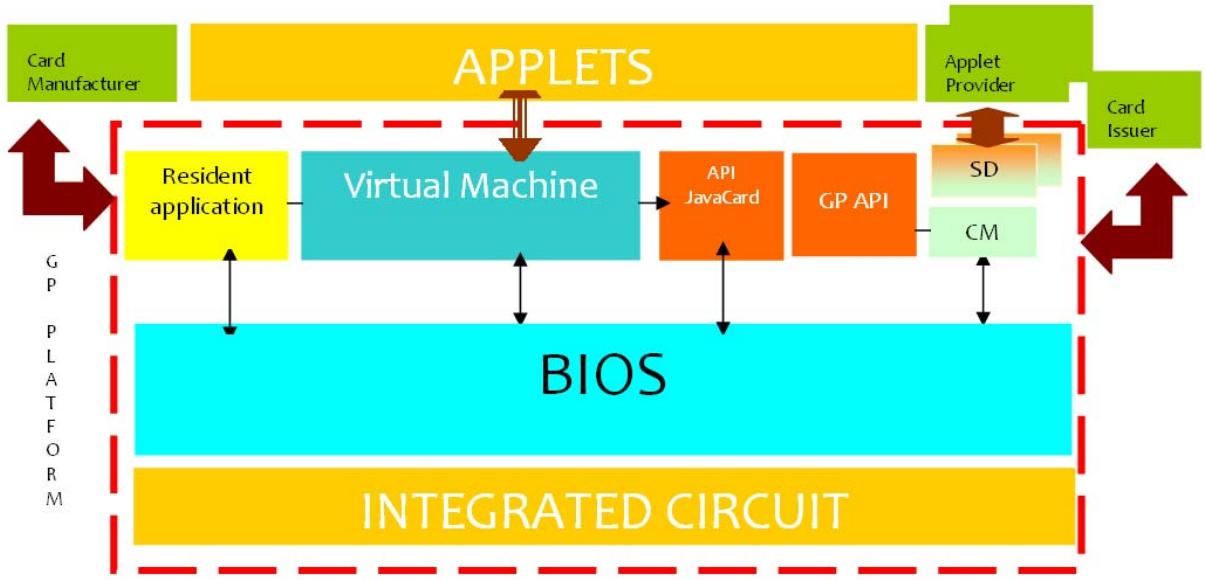

Figure 1 - Architecture et périmètre de la TOE

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

Phase	Nom de la phase	Sites de développement et de fabrication
Phase 1	Développement du logiciel embarqué	- Oberthur Technologies (*Levallois-Perret, Nanterre, Pessac*). - ID3 (*Le Fontanil-Cornillon*).
	Développement du patch *Generic* et du patch *SAC*	Oberthur Technologies (*Levallois-Perret, Nanterre*).
Phase 2	Développement du microcontrôleur	ST Microelectronics.
Phase 3	Fabrication du microcontrôleur	ST Microelectronics.
Phase 4	Packaging de la plateforme JavaCard	
Phase 5	Intégration du produit composite Chargement du patch *Generic* (obligatoire) et du patch *SAC* (optionnel)	
Phase 6	Personnalisation	
Phase 7	Phase d'utilisation	

Périmètre d'évaluation

Figure 2 - Cycle de vie de la plateforme JavaCard

En regard du cycle de vie, le produit évalué est celui qui sort de la phase de production (phase 3). Les phases 4, 5, 6 et 7 sont couvertes par les guides du produit (voir [GUIDES]).

Le produit est développé sur les sites suivants :

Oberthur Technologies

71-73 rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies

4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

ID3 (développeur de la fonction Match On Card)

5 rue de la Verrerie
38120 Le Fontanil-Cornillon
France

Les microcontrôleurs sont développés et fabriqués par ST Microelectronics. Les sites de développement et de fabrication des puces ST23YR80B et ST23YR48B sont détaillés dans le rapport de certification dont la référence est [ANSSI-CC-2010/01].

1.2.6. Configuration évaluée

Le certificat porte sur la plateforme ouverte JavaCard seule, telle que présentée plus haut, au paragraphe « 1.2.4 Architecture », et configurée conformément au guide de personnalisation (voir [GUIDES]).

Le mécanisme de chargement de patch a été évalué. Ce mécanisme permet de charger un patch fonctionnel jusqu'à la phase 5 du cycle de vie si et seulement si ce patch n'a pas d'impact sur les mécanismes d'autoprotection du produit. Aucun patch ne pourra être chargé après la phase 5, le mécanisme de chargement de patch étant désactivé.

Les applets embarquées sur la plateforme ont été analysées dans le cadre de cette évaluation au titre de l'environnement de la cible de sécurité. Elles ne dégradent pas la sécurité de la plateforme.

Le mécanisme *Match-on-Card* est intégré au produit et permet l'authentification du porteur de la carte à l'aide d'empreinte digitale. La résistance de ce mécanisme a été évaluée pour les valeurs de seuil par défaut :

- *JavaCardX Security API* : 7143 (FAR = 10^{-5}) ;
- *OTPinBio* : 10000 (FAR = 10^{-7}).

L'évaluation a montré qu'il est recommandé de modifier la valeur du seuil d'*OTPinBio* en la diminuant tout en la laissant à un niveau acceptable, la valeur minimale du seuil devant être 4672 (correspondant à un FAR de $3x10^{-4}$).
Les valeurs acceptables du seuil sont donc :

FAR (*False Acceptance Rate* – Taux de fausse acceptance)	**Valeur minimale du seuil**
0,03 % = 3×10^{-4}	4672
0,01 % = 10^{-4}	6000
0,001 % = 10^{-5}	7143
0,0001 % = 10^{-6}	8671
0,00001 % = 10^{-7}	10000 (valeur par défaut de *OTPinBio*)

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, le guide [JIWG AP] a été appliqué. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

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.

Les microcontrôleurs ST23YR48B et ST23YR80B ont été certifiés au niveau EAL6 augmenté du composant ALC_FLR.1, conformément au profil de protection [BSI-PP-0035-2007], le 1er février 2010, sous la référence [ANSSI-CC-2010/01].

Le niveau de résistance des microcontrôleurs ST23YR48B et ST23YR80B a été confirmé le 27 septembre 2012 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 décembre 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu aux conclusions suivantes :

- les mécanismes analysés permettent de proposer des applications conformes aux exigences du référentiel cryptographique de l'ANSSI (voir [REF]) ;
- les spécifications GlobalPlatform de la cible de sécurité [ST] auxquelles le développeur est contraint de se conformer apportent des faiblesses cryptographiques. Ces faiblesses concernent les mécanismes de protection des données sensibles échangées sur les canaux sécurisés SCP02 et SCP03 supportés par le produit. Ces

faiblesses sont également applicables au protocole propriétaire SCPF3 supporté par le produit.

Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- lors du chargement sécurisé d'applets sur la carte une signature RSA, utilisant des clés de 2048 bits et l'encodage PSS (*Probabilistic Signature Scheme*) avec la fonction de hachage SHA-256, doit être utilisée ;
- le nombre maximum de blocs traités dans le cadre du canal sécurisé SCP02 avec la même clé doit être inférieur à 2^{27} ;
- lorsque des éléments sensibles sont échangés au cours d'une session de communication sécurisée, le niveau de sécurité le plus haut du canal sécurisé doit être utilisé (voir [GUIDES]).

Quoi qu'il en soit, les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation des microcontrôleurs (voir [ANSSI-CC-2010/01]).
Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature crytographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

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 pour 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 « Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES]. Les recommandations des chapitres « 1.2.6 Configuration évaluée » et « 2.3 Cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI » du présent rapport devront également être mises en œuvre.

Plus particulièrement, toutes les applications qui seront chargées sur la carte (qu'elles soient certifiées ou non) devront satisfaire l'ensemble des contraintes et exigences relatives aux propriétés de cloisonnement d'applications, imposées par la plateforme, avant leur installation effective (voir [GUIDES]).

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 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé 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 CCRA [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'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, 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
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular 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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - TOUTATIS – Security Target, Référence : FQR 110 6070, version 5 du 10/12/2012, Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cosmo v7.1-s – TOUTATIS – Java Card Open Platform – Public Security Target, Référence : FQR 110 6155, version 1, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report, Référence : LETI.CESTI.TOU.RTE.001, version 1.0 du 21/12/2012, CEA-LETI.
[ANA-CRY]	Cotation des mécanismes cryptographiques, Référence : LETI.CESTI.TOU.RT.001, version 1.0 du 16/11/2012, CEA-LETI.
[CONF]	TOUTATIS – Configuration List Référence : FQR 110 6164, version 2 du 10/12/2012 Oberthur Technologies.
[GUIDES]	- ID-One Cosmo V7.1 – Pre-Perso Guide, Référence : FQR 110 6027, version 3 du 12/12/2012, Oberthur Technologies. - ID-One Cosmo V7.1 – Reference Guide, Référence : FQR 110 6028, version 3 du 12/12/2012, Oberthur Technologies. - ID-One Cosmo V7.1 – Security Recommendations, Référence : FQR 110 6029, version 2 du 29/11/2012, Oberthur Technologies. - ID-One Cosmo V7.1 – Application Loading Protection Guidance, Référence : FQR 110 6267, version 1 du 15/11/2012, Oberthur Technologies. - Applications on ID-ONE COSMO V7.1, Référence : FQR 110 6268, version 1 du 24/09/2012, Oberthur Technologies.

	- All Applications on ID-One Cosmo V7.1, Référence : FQR 110 6319, version 1 du 25/09/2012, Oberthur Technologies.
[PP JCS]	"Java Card Protection Profile – Open Configuration", version 3.0 du 18 mai 2012. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01*.
[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 august 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[ANSSI-CC-2010/01]	Certificat délivré par l'ANSSI le 1er février 2010 pour les produits « *Microcontrôleurs sécurisés ST23YR48B et ST23YR80B* ».

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.