Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2011/01

Carte à puce ID-ONE Cosmo V7.0.1-a masquée sur composants standard et basic AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G

Paris, le 3 février 2011

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[Original signé]

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 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-2011/01

Nom du produit

Carte à puce ID-ONE Cosmo V7.0.1-a masquée sur composants standard et basic AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G

Référence/version du produit

Version V7.0.1-a

Conformité à un profil de protection

[PP/0304], version 1.0b

PP SUN Java Card™ System Protection Profile Collection, août 2003, certifié par l'ANSSI

Critères d'évaluation et version

Critères Communs V3.1

Niveau d'évaluation

EAL5

ALC_DVS.2, ADV_IMP.2, AVA_VAN.5

Développeur(s)

Oberthur Technologies

50 quai Michelet
92300 Levallois-Perret, France

Atmel Secure Products Division,

Scottish Technology Par,
G75 0QR East Kilbride, Scotland
Angleterre

Commanditaire

Oberthur Technologies

50 quai Michelet
92300 Levallois-Perret, France

Centre d'évaluation

THALES - CEACI (T3S – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.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 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

1.1. Présentation du produit

Le produit évalué est la carte à puce ID-One Cosmo V7.0.1-a, plate-forme Java Card ouverte, développée par Oberthur Technologies :

- compatible avec les spécifications de Java Card 2.2.2 et de VISA GlobalPlatform 2.1.1 ;
- masquée sur des variantes (par la taille mémoire et les interfaces offertes) d'une même famille de composants développées par ATMEL.

Ces différentes variantes du produit sont récapitulées dans le tableau ci-après :

Dénomination de la variante du produit	Version de la plate-forme Java Card	Référence commerciale de la variante du composant sur lequel le logiciel est masqué	Référence masque identifiant la variante du composant
Standard	V7.0.1.a	AT90SC 28872RCU Rev G	1A 01C3
Basic	V7.0.1.a	AT90SC 28848RCU Rev G	1A 01CF

1.2. Description du produit

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 [PP0304] .

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 :

L'identification est obtenue en analysant la réponse à la commande « GET DATA » pour le tag DF50 (voir [GUIDES]).
=> 80 CA DF 50 0E
<= DF 50 09 **30** 06 09 54 56 26 05 28 3B 90 00
La valeur du champ « Device Coding Byte » DC2, 0x30 en gras dans la réponse ci-dessus, identifie le composant AT90SC28872RCU.

La taille mémoire est obtenue en analysant la réponse à la commande « GET DATA » pour le tag DF52 (voir [GUIDES]).

```
=> 80 CA DF 52 00
<= DF 52 4C 01 01 C3 02 02 00 48 03 02 1A 01 04 00
   05 01 01 06 17 83 00 01 3F 3F FF F9 00 00 00 00
   00 00 00 00 96 01 FF FF FF FF FF FF 07 01 0F 08
   0B 00 31 C0 64 C3 1A 01 00 00 90 00 09 11 00 00
   00 00 00 00 00 00 00 B3 00 00 00 00 00 00 00
```

La valeur du tag 01, « C3 » ou « CF » en gras dans la réponse ci-dessus, identifie le composant.
La valeur du tag 01, « 1A01 » en gras dans la réponse ci-dessus, identifie la version du système d'exploitation.

Valeur du Tag03	Référence système d'exploitation
1A 01C3	ID-One Cosmo V7.0.1-a Standard
1A 01CF	ID-One Cosmo V7.0.1-a Basic

La valeur du tag 04, en gras dans la réponse ci-dessus, identifie les correctifs. Ici « 00 », pas de correctifs.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- les services de pré-personnalisation de la carte ;
- la personnalisation des applets avec la faculté de la charger, de l'installer, de la supprimer, grâce au gestionnaire GlobalPlatform Card Manager et au contrôleur de domaine de sécurité associé et du mécanisme DAP (*Data Authentication Pattern* - reconnaissance des données d'authentification) ;
- les interfaces au service des API dédiées aux applets et l'accès à ces API ;
- la gestion de GlobalPlatform ainsi que des clés de signature ;
- le pare-feu isolant les objets ou les applets ;
- les services standards GlobalPlatform comme le canal logique et le protocole de canal sécurisé (SCP01, SCP02), ainsi que le protocole de canal sécurisé propriétaire (SCP03).

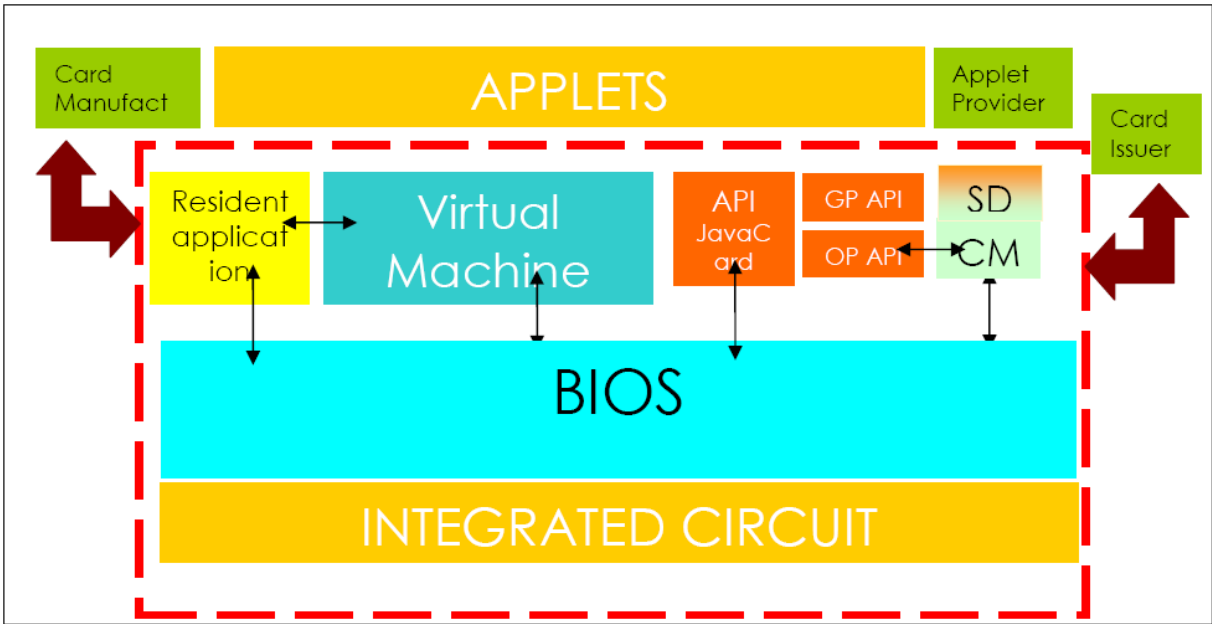
Une liste plus détaillée des services de sécurité est donnée dans [ST].

1.2.3. Architecture

Le produit est constitué :

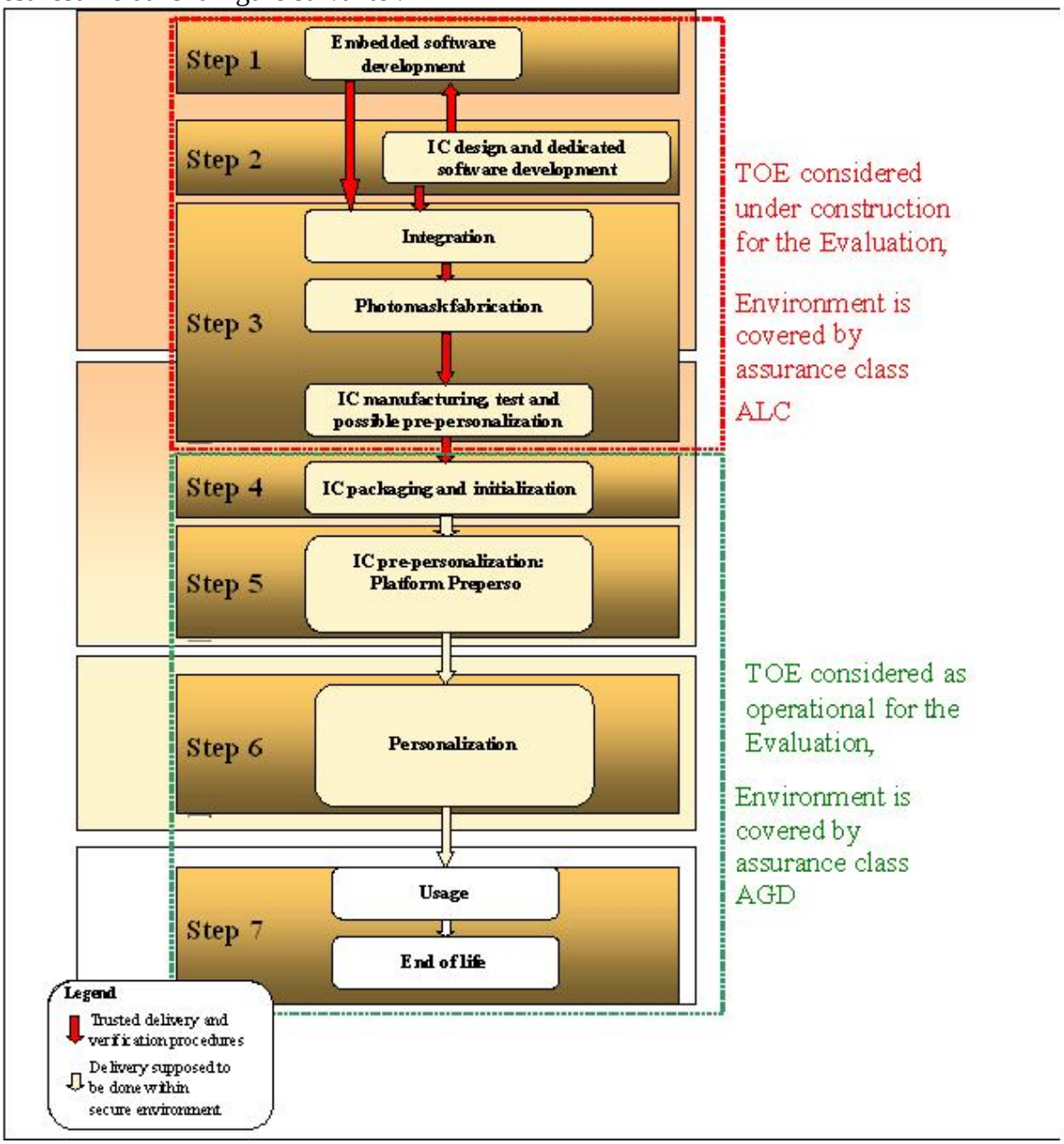
- du microcontrôleur, offrant les fonctionnalités matérielles, et de sa bibliothèque cryptographique ToolBox ;
- du BIOS assurant l'interface entre les applications natives, comme la machine virtuelle (*Virtual Machine*), et le matériel ;
- de la machine virtuelle interprétant le *byte code* des applets Java Card ;
- d'API offrant les interfaces de programmes aux applications comme la génération de clés, la négociation de clés, la signature, le chiffrement de messages ainsi que d'autres interfaces de programmes aux applications propriétaires (OCS API) ;
- de Common Open Platform, constitué du gestionnaire de la carte (*Card Manager*) et des API OPSystem and GPSystems ; il est implémenté en code natif et en Java (son *byte code* se trouve en ROM) ;
- de l'application résidente, en code natif, permettant de recevoir et de distribuer les commandes reçues par la carte.

Cette architecture est résumée dans la figure suivante :

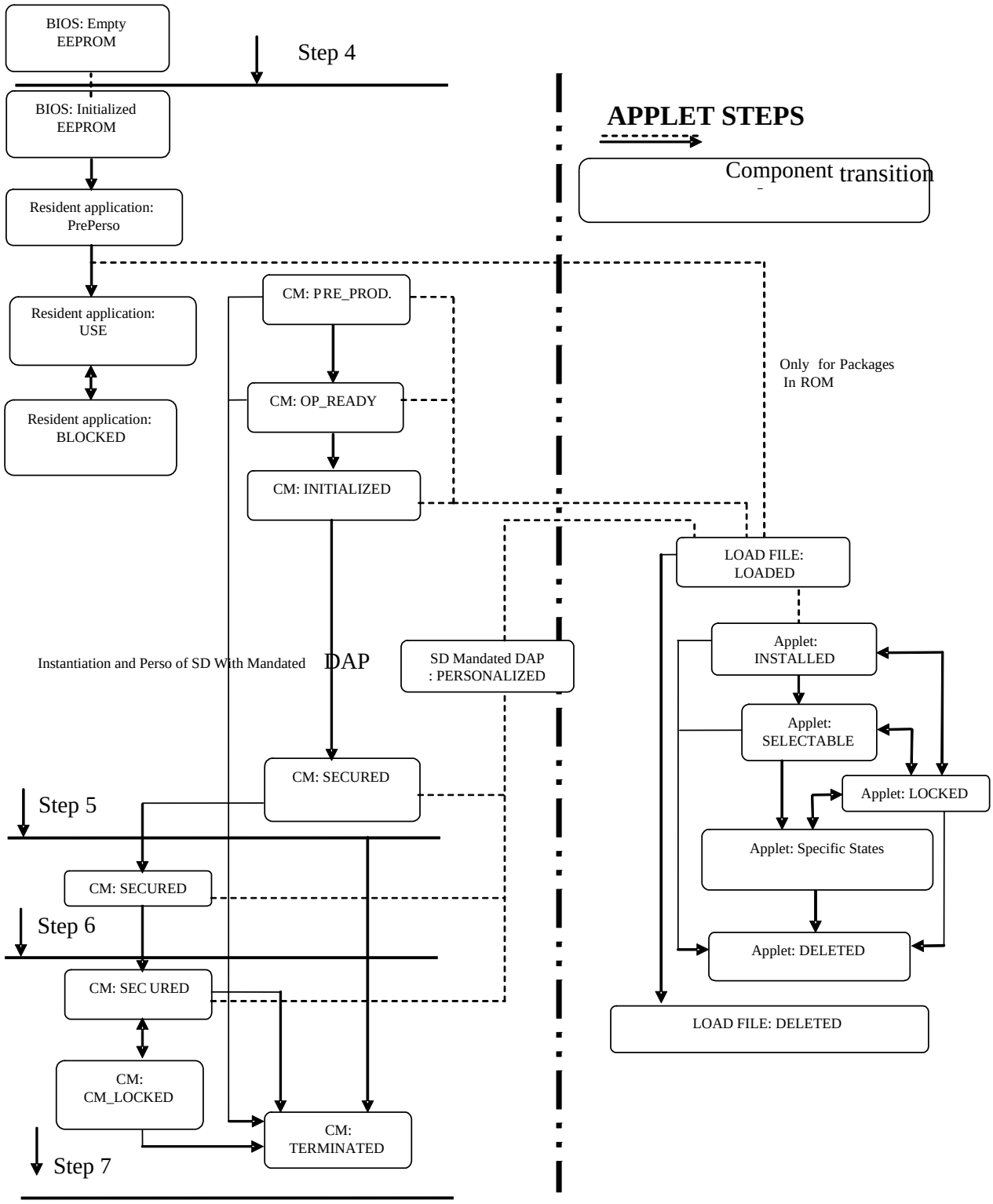


1.2.4. Cycle de vie

Le cycle de vie du produit est conforme au cycle de vie en sept étapes d'une carte à puce, il est résumé dans la figure suivante :



Cycle de vie du produit



États de la plate-forme à partir de la phase 4

L'évaluation a couvert la conception et le développement de la plate-forme qui sont effectués en phase 1. Les phases 2 et 3, jusqu'à la livraison, ont été couvertes par l'évaluation du composant. La fin de la phase 3 et les phases 4, 5 et 6 sont couvertes par des guides. Le produit évalué correspond à celui livré à l'utilisateur à partir de la phase 4.

Le produit a été développé sur les sites suivants :

Oberthur Technologies - Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies - Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies - Bordeaux

Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus - Porte 2
33 600 Pessac
France

Le microcontrôleur a été développé et fabriqué par Atmel sur ses sites (cf. BSI-DSZ-CC-0421-2008), dont le principal est :

Atmel Secure Products Division,

Scottish Technology Par,
G75 0QR East Kilbride, Scotland
Angleterre

1.2.5. Configuration évaluée

Le certificat porte sur la plate-forme Java Card seule, telle que présentée plus haut au paragraphe « 1.2.3 Architecture » et configurée conformément au guide de personnalisation (cf. [GUIDES]).

Les tests ont été effectués sur une plate-forme ID-ONE Cosmo V7.0.1-a Standard, sur composant AT90SC28872RCU.
Certains composants ont été livrés avec la machine d'état du « Card Manager » de la plate-forme dans l'état « Secure ». D'autres composants ont été livrés dans l'état de pré-personnalisation « Resident Application : PrePerso ».

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version V3.1** [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.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] 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 AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G au niveau EAL5 augmenté des composants [ALC_DVS.2, AVA_MSU.3, AVA_VLA.4], conforme au profil de protection [RBSI-PP-002-2001]. Ce microcontrôleur a été certifié le 4 décembre 2008 sous la référence BSI-DSZ-CC-0421-2008.

Le niveau de résistance du microcontrôleur a été confirmé le 19 novembre 2010 dans le cadre du processus de surveillance [BSI-DSZ-CC-0421-2008 Confirmation].

L'évaluation s'appuie sur les résultats d'évaluation du produit Carte à puce ID-One Cosmo V7.0-a en configuration Standard et Basic certifié le 19 novembre 2009 sous la référence ANSSI-CC-2009-46 [ANSSI-CC-2009-46].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 décembre 2010, 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à ses référentiels techniques [REF-CRY], [REF-KEY] et [REF-AUT]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu à la conclusion suivante :

- les mécanismes analysés permettent de proposer des applications conformes aux exigences du référentiel cryptographique de l'ANSSI (Cf. [REF-CRY]) ;

- les spécifications GlobalPlatform de la cible de sécurité [ST] auxquelles le développeur est contraint de se conformer apportent des faiblesses cryptographiques. Ces faiblesses concernent l'utilisation de taille de clé RSA de 1024 bits et de l'algorithme de hachage SHA-1.

Ces 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 visé.

2.4. Analyse du générateur d'aléas

Ce générateur d'aléas a fait l'objet d'une analyse par l'ANSSI [ANA-CRY].

Le produit est basé sur les composants AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G dont le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31], comme indiqué dans le certificat BSI-DSZ-CC-0421-2008. Le générateur atteint le niveau « P2 ». Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception.

Comme requis dans [REF-CRY], la sortie du générateur physique subit un retraitement de nature cryptographique. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu à la conclusion suivante :

- la génération de clé (RSA ou courbe elliptiques) doit se faire sous le contrôle de l'utilisateur.

Ces résultats ont été pris en compte dans l'analyse indépendante de vulnérabilité réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN 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 « Carte à puce ID-ONE Cosmo V7.0.1-a masquée sur composants standard et basic AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G », version V7.0.1-a soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 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].

3.3. Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale

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'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 semiformal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	TSF internal description
	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**	**2**	**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 : - TERPSICHORE ST ID-ONE cosmo V7.0.1-a AT90SC28872RCU/AT90SC28848RCU référence FQR 110 4889, version V2 du 19 avril 2010 éditée par Oberthur Technologies Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - TERPSICHORE ST Lite ID-ONE cosmo V7.0.1-a AT90SC28872RCU/AT90SC28848RCU référence FQR 110 5411, version V1 du 14 octobre 2010 éditée par Oberthur Technologies
[RTE]	Rapport technique d'évaluation : - Evaluation technical report Project TERPSICHORE référence TER_ETR, version V4.0 du 7 décembre 2010 édité par THALES SECURITY SOLUTIONS SERVICES Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Report lite Project TERPSICHORE référence TER_ETR_Lite_v1.0, version v1.0 de janvier 2011 édité par THALES SECURITY SOLUTIONS SERVICES
[ANA-CRY]	projet TERSICHORE référence 1684/ANSSI/ACE du 25 juin 2010 édité par ANSSI
[CONF]	- Configuration List Atmel référence FQR 110 4893, version V5 du 12 mai 2010, édité par Oberthur Technologies
[GUIDES]	Guide d'installation du produit : - PGD COP REF référence 071841 00 PGD/1AB, version V02.12 du 8 février 2010 édité par Oberthur Technologies Guide d'administration du produit : - GENERIC PREPERSONALISATION référence FQR : 110 4910, version V3 du 4 mai 2010 édité par Oberthur Technologies Guide d'utilisation du produit : - ID-One Cosmo V7.0.1 Reference Guide référence FQR 110 4911, version V3 du 12 mai 2010 édité par Oberthur Technologies
[ANSSI-CC-2009-46]	Certificat délivré par l'ANSSI le19 novembre 2009 pour le produit Carte à puce ID-One Cosmo V7.0-a en configuration Standard et Basic

[BSI-DSZ-CC-0421-2008]	Certificat délivré par le BSI le 4 décembre 2008 pour le produit AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G
[BSI-DSZ-CC-0421-2008 Confirmation]	Lettre de confirmation du produit émise par le BSI sous la référence BSI-DSZ-CC-0421-2008-Reassessment-Letter le 19 Novembre 2010
[PP0304]	Profile de protection SUN Java Card™ System Protection Profile Collection, août 2003, version 1.0b. *Certifié par l'ANSSI sous la référence PP/0304.*

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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr

[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)