



PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

## **Rapport de certification ANSSI-CC-2009/46**

### **Carte à puce ID-One Cosmo V7.0-a en configuration Standard et Basic**

*Paris, le 19 novembre 2009*

*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 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 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 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](mailto:certification.anssi@ssi.gouv.fr)

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



<i>Référence du rapport de certification</i>	<b>ANSSI-CC-2009/46</b>
<i>Nom du produit</i>	<b>Carte à puce ID-One Cosmo V7.0-a en configuration Standard et Basic : plate-forme Java Card masquée sur composants Atmel Secure Microcontroller Solutions AT90SC 28872RCU Rev G and Rev E, 28848RCU Rev G and Rev E et masquée avec la version 00.03.11.05 de la bibliothèque cryptographique ToolBox d'Atmel Secure Microcontroller Solutions</b>
<i>Référence/version du produit</i>	<b>Version Plate-forme Java Card correspondant à toutes les configurations : 7.0-a Version patch Optional Code r1.0 High Secure correspondant à chaque configuration : 071771, 071781 Version patch CodopAuth r1.0 Platform Identification correspondant à chaque configuration : 071631, 071641 Version ToolBox correspondant à toutes les configurations : 00.03.11.05</b>
<i>Conformité à un profil de protection</i>	<b>[PP/0304] Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b, August 2003, certifié par l'ANSSI</b>
<i>Critères d'évaluation et version</i>	<b>Critères Communs version 3.1</b>
<i>Niveau d'évaluation</i>	<b>EAL5 augmenté ADV_IMP.2, ALC_DVS.2, AVA_VAN.5</b>
<i>Développeur(s)</i>	<b>Oberthur Technologies<sup>1</sup>                      ATMEL Secure Microcontroller 50 quai Michelet                              Solutions<sup>1</sup> 92300 Levallois-Perret, France              Maxwell Building - Scottish Enterprise technology Park East Kilbride, G75 0QR - Ecosse, Royaume-Uni</b>
<i>Commanditaire</i>	<b>Oberthur Technologies 50 quai Michelet, 92300 Levallois-Perret, France</b>
<i>Centre d'évaluation</i>	<b>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</b>
<i>Accords de reconnaissance applicables</i>	  <b>Le produit est reconnu au niveau EAL4.</b>

<sup>1</sup> : il s'agit des sites principaux.

## 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 :

- 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](http://www.ssi.gouv.fr).



# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Identification du produit</i> .....	7
1.2.2. <i>Services de sécurité</i> .....	7
1.2.3. <i>Architecture</i> .....	8
1.2.4. <i>Cycle de vie</i> .....	9
1.2.5. <i>Configuration évaluée</i> .....	10
<b>2. L’EVALUATION .....</b>	<b>11</b>
2.1. REFERENTIELS D’EVALUATION .....	11
2.2. TRAVAUX D’EVALUATION .....	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	11
<b>3. LA CERTIFICATION .....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS D’USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT .....	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	13
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>15</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>17</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la carte à puce ID-One Cosmo V7.0-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 Secure Microcontroller Solutions ;
- masquée avec la version 00.03.11.05 de la bibliothèque cryptographique ToolBox développée également par Atmel Secure Microcontroller Solutions ;
- patchée par deux patches intitulés Optional Code r1.0 High Secure et CodopAuth r1.0 Platform Identification, développés par Oberthur Technologies, dont la version dépend du composant sur lequel il est porté.

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	Version du patch Optional Code r1.0 High Secure	Version du patch CodopAuth r1.0 Platform Identification	Référence de la variante du composant sur lequel le logiciel est masqué	Version de la ToolBox
Standard	7.0-a	071771	071631	AT90SC 28872RCU révision G et E	00.03.11.05
Basic	7.0-a	071781	071641	AT90SC 28848RCU révision G et E	00.03.11.05

## 1.2. Description du produit

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/0304].



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

Ainsi, sur un produit utilisé lors de l'évaluation, la commande GET DATA pour le tag DF 52 a donné la réponse suivante :

- DF 52 3E 01 01 **C3** 02 02 00 48 03 02 **08 01** 04 10 **07 16 31 01** CE D1 94 BB **07 17 71 01** 73 4C AE 83 05 01 01 06 17 83 00 01 3F 3F FF F9 00 00 00 00 01 C8 80 C0 00 00 96 FF 69 FF 00 FF 07 01 0F 08 00.

Dans cette réponse, on lit les éléments d'identification suivants (caractères en gras) :

- le numéro du masque est **0801 C3** ce qui correspond à ID-One Cosmo V7.0-a Standard ;
- le numéro du patch CodopAuth r1.0 Platform Identification est **071631** en version **01** ;
- celui du Optional Code r1.0 High Secure est **071771** en version **01**.

La commande GET DATA pour le tag DF 50 a donné la réponse suivante :

- DF 50 09 **30 04 08 52 43 55 04 41 0A**.

Dans cette réponse-ci, on lit les éléments d'identification suivants (caractères en gras) :

- **30** identifie le composant, ici c'est AT90SC 28872RCU ;
- **04** donne la révision du composant, soit la révision G ;
- **08** indique l'année de production ;
- **52** indique l'identifiant usine et le trimestre de production ;
- **43 55** indique le numéro du lot ;
- **04** indique le numéro du wafer ;
- **41 0A** indique le numéro du dé.

### 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).

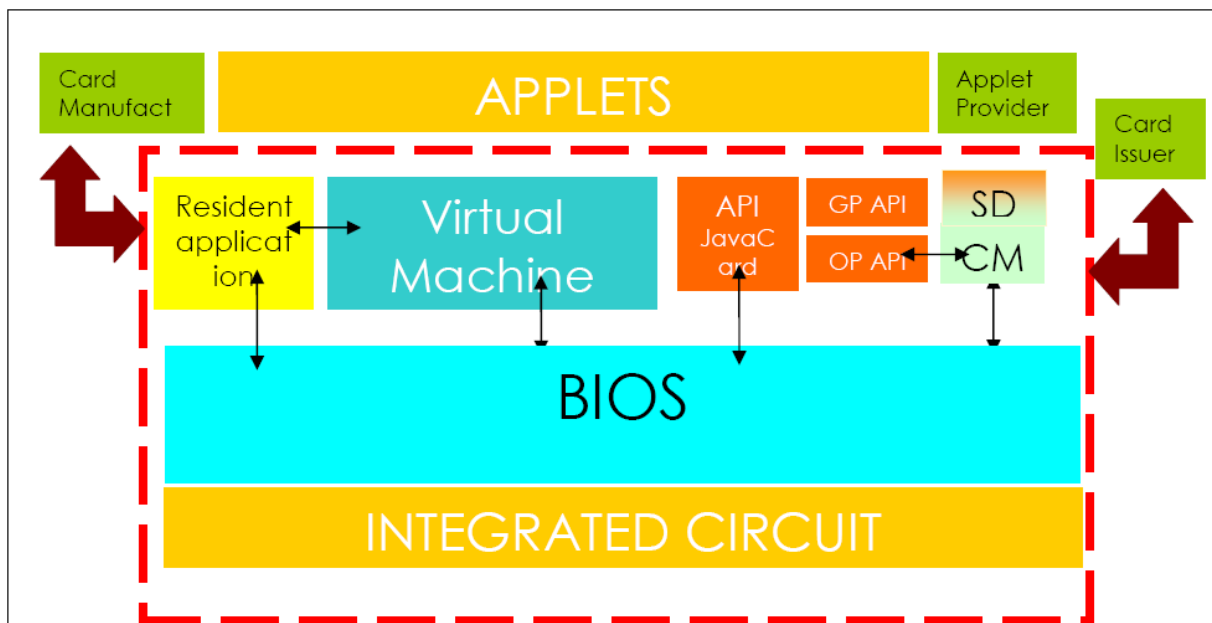
Une liste plus détaillée des services de sécurité est donnée dans [ST].

### 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 carte reçues.

Cette architecture est résumée dans la figure suivante :

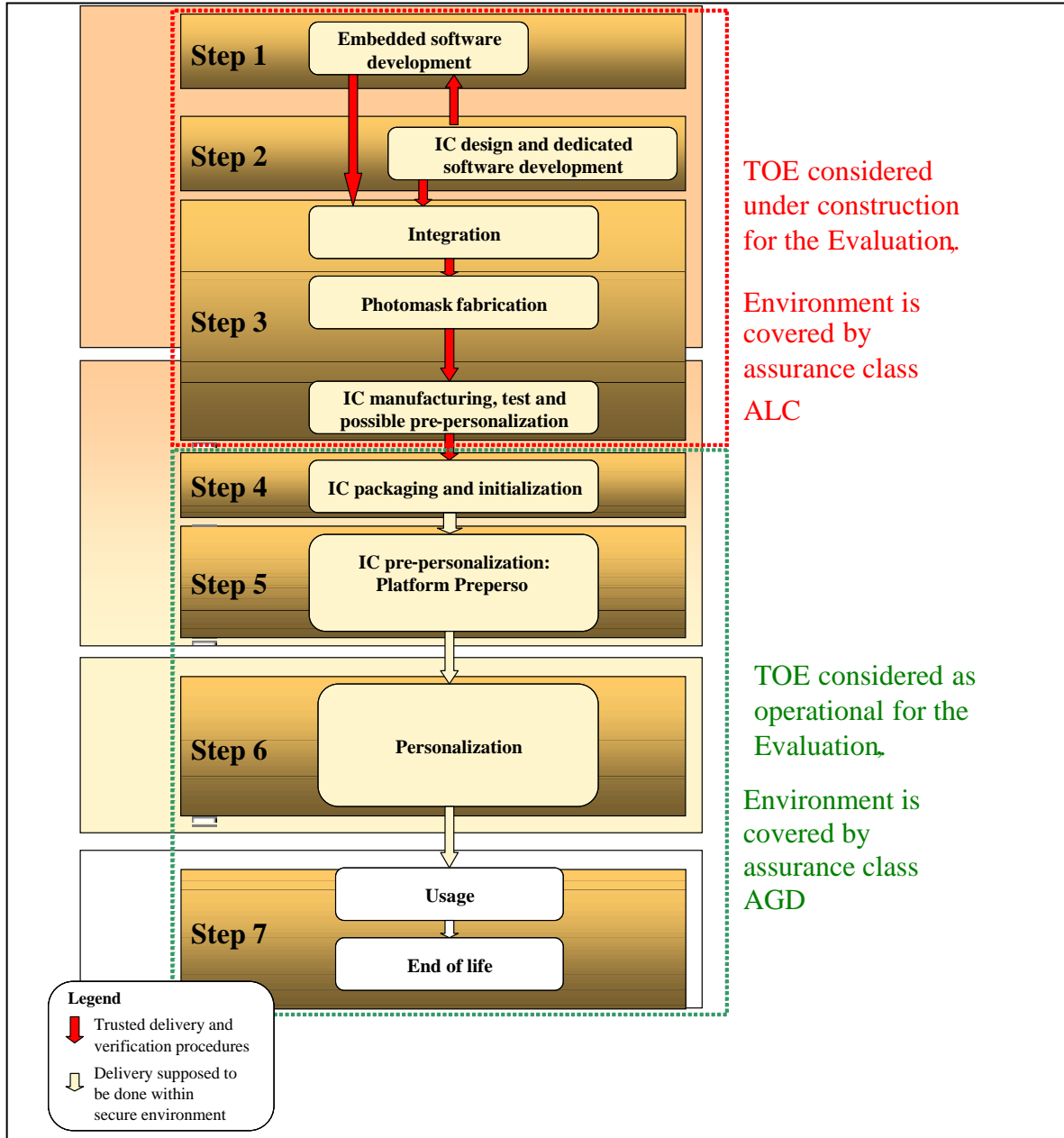






### 1.2.4. Cycle de vie

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 :



L'évaluation a couvert la conception et le développement de la plate-forme qui sont effectués en étape 1. Les étapes 2 et 3, jusqu'à la livraison, ont été couvertes par l'évaluation du composant. La fin de l'étape 3 et les étapes 4, 5 et 6 sont couvertes par des guides. Le produit évalué correspond à celui livré à l'utilisateur à l'étape 7.

La plate-forme a été développée par Oberthur Technologies 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 Secure Microcontroller Solutions sur ses sites (cf. [BSI-DSZ-CC-0421-2008-MA-02]), dont le principal est :

**ATMEL Secure Microcontroller Solutions**

Maxwell Building - Scottish Enterprise technology Park  
East Kilbride, G75 0QR – Ecosse  
Royaume-Uni

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré-personnalisateur, le personnalisateur et le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateurs du produit les développeurs des applications à charger dans la plate-forme.

***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]).



## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC], 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, 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 et de la bibliothèque cryptographique dans le microcontrôleur. La bibliothèque et le microcontrôleur étaient déjà certifiés.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation :

- du microcontrôleur sécurisé ATMEL - AT90SC 28872RCU / AT90SC 28848RCU rev. G et E 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 puis maintenu par le BSI (cf. [BSI-DSZ-CC-0421-2008-MA-02]) ;
- de la bibliothèque cryptographique ATMEL - Toolbox 00.03.11.05 au niveau EAL5 augmenté des composants ALC\_DVS.2, AVA\_MSU.3 et AVA\_VLA.4 ; cette bibliothèque a été certifiée par l'ANSSI (cf. [DCSSI-2009/11]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 septembre 2009, 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 n'a pas été réalisée par l'ANSSI.

## 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 la carte à puce ID-One Cosmo V7.0-a, décrite au chapitre 1.1 du présent rapport de certification, soumise 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

#### 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<sup>1</sup>, 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 CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires<sup>2</sup>, 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 :



---

<sup>1</sup> 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 Royaume-Uni et la Suède.

<sup>2</sup> 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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedure
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ADO_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claim
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended component definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specifications
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independant testing, sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis



## Annexe 2. Références documentaires du produit évalué

<p>[ST]</p>	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"><li>- ID-ONE COSMO V7.0 - CLIO SECURITY TARGET For AT90SC28872RCU / AT90SC28848RCU Référence FQR: 110 4626 - issue 1 - 22/06/2009 Oberthur Technologies.</li></ul> <p>Cible de sécurité pour la composition avec les composants :</p> <ul style="list-style-type: none"><li>- ID-ONE COSMO V7.0 - CLIO SECURITY TARGET COMPATIBILITY For ATMEL IC Référence FQR: 110 4622 - issue 1 - 22/06/2009 Oberthur Technologies.</li></ul> <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"><li>- ID-ONE COSMO V7.0 - CLIO Security Target Lite For AT90SC28872RCU / AT90SC28848RCU Référence FQR: 110 4777 - issue 1 Oberthur Technologies.</li></ul>
<p>[RTE]</p>	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"><li>- Evaluation technical report - Project: CLIO Référence CLIO_ETR_1 - révision 2.0 – 04/09/2009 THALES-CEACI.</li></ul> <p>Pour le besoin des évaluations en composition avec cette plate-forme, un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"><li>- Evaluation technical report lite - Project: CLIO ETR LITE for composition Référence CLIO_ETR Lite_1 – révision 2.0 – 04/09/2009 THALES-CEACI.</li></ul>
<p>[CONF]</p>	<p>Liste de configuration du produit</p> <ul style="list-style-type: none"><li>- CLIO - CONFIGURATION LIST AT90SC288xxRCU Référence FQR : 110 4616 - issue: 3 – 09/02/2009 Oberthur Technologies.</li></ul>
<p>[GUIDES]</p>	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"><li>- COP REF V02.12 - PRODUCT GENERATION DESCRIPTION – PGD 069241 00 PGD – issue 1 AA, 10/06/2008 Oberthur Technologies</li><li>- ID-One Cosmo V7.0-a Applets - PRODUCT GENERATION DESCRIPTION - PGD 069671 00 PGD – issue 1 AA, 23/10/2008 Oberthur Technologies</li><li>- Optional Code r1.0 Authenticate on ID-One Cosmo V7.0-a Platform 72k - PRODUCT GENERATION DESCRIPTION - PGD 071631 00 PGD – issue 1 AA, 02:06/2009</li></ul>

	<p>Oberthur Technologies</p> <ul style="list-style-type: none"> <li>- Optional Code r1.0 Authenticate on ID-One Cosmo V7.0-a Platform 48k - PRODUCT GENERATION DESCRIPTION - PGD 071641 00 PGD – issue 1 AA, 15/05/2009 Oberthur Technologies</li> <li>- Optional Code r1.0 High Secure on ID-One Cosmo V7.0-A Platform 72k - PRODUCT GENERATION DESCRIPTION - PGD 071771 00 PGD – issue 1 AA, 15/06/2009 Oberthur Technologies</li> <li>- Optional Code r1.0 High Secure on ID-One Cosmo V7.0-A Platform 48k - PRODUCT GENERATION DESCRIPTION - PGD 071781 00 PGD – issue 1 AA, 15/06/2009 Oberthur Technologies</li> </ul> <p>Guide d’administration du produit :</p> <ul style="list-style-type: none"> <li>- ID-One Cosmo V7.0 - Pre-Perso Guide FQR : 110 4379 – issue 6, 26/06/2009 Oberthur Technologies</li> <li>- ID-One Cosmo V7.0 - Security recommendations FQR 110 4730 – issue 1, 02/09/2009 Oberthur Technologies</li> </ul> <p>Guide d’utilisation du produit :</p> <ul style="list-style-type: none"> <li>- ID-One Cosmo V7.0 - Reference Guide FQR 110 4483, issue 5 Oberthur Technologies</li> </ul>
[PP/0304]	<p>Profil de protection ANSSI certifié le 30 septembre 2003 sous le titre : Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b, August 2003.</p>
[BSI-DSZ-CC-0421-2008-MA-02]	<p>Rapport de maintenance BSI délivré le 6 avril 2009 pour le microcontrôleur sécurisé ATMEL - AT90SC28872RCU / AT90SC28848RCU rev G.</p>
[DCSSI-2009/11]	<p>Certificat ANSSI délivré le 30 juin 2009 pour la bibliothèque cryptographique ATMEL - Toolbox 00.03.11.05.</p>
[PP0002]	<p>Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.</i></p>





### 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-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.