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-2010/36

Carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration Large Dual, Large et Standard Dual

Paris, le 29 juin 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

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-2010/36

Nom du produit

Carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration Large Dual, Large et Standard Dual

Référence/version du produit

Version applet 1121

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Oberthur Technologies
50 quai Michelet
92300 Levallois-Perret, France

Atmel Secure Microcontroller Solutions
Maxwell Building - Scottish Enterprise technology Park
East Kilbride, G75 0QR - Ecosse, Royaume-Uni

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, 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.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration Large Dual, Large et Standard Dual. L'applet et la plate-forme sont développées par Oberthur Technologies, le composant est développé par Atmel Secure Microcontroller Solutions.

La cible d'évaluation (TOE : *Target Of Evaluation* – cible d'évaluation) est un logiciel sécurisé s'exécutant sur un microcontrôleur, pouvant être mis, par exemple, dans une carte à puce ou un *inlay*, et destinée à être utilisée dans le cadre de projets mettant en œuvre de la signature électronique. Elle répond aux caractéristiques des dispositifs sécurisés de création de signature électronique (SSCD - *Secure Signature Creation Device*) comme défini dans la directive Européenne 1999/93/CE (Annexe III). Ses fonctionnalités applicatives sont offertes par l'application ID-One IAS-ECC v1.0.1 R1 qui s'exécute sur la plateforme JavaCard ouverte d'Oberthur Technologies ID-One Cosmo V7.0-a en configuration Large Dual, Large et Standard Dual sur composant Atmel Secure Microcontroller Solutions (plateforme certifiée par l'ANSSI, cf. [ANSSI-CC-2009_36]).

A ce titre, la TOE permet de réaliser des signatures électroniques avancées, et des signatures électroniques dites qualifiées (article 2 & article 5 de la directive Européenne 1999/93/CE).

L'application ID-One IAS-ECC v1.0.1 R1 couvre les domaines de l'identité, de la signature électronique, des services électroniques et du stockage de données ; elle est compatible avec les spécifications [IASECC].

Elle offre les deux principales fonctions attendues des produits SSCD type 2 et type 3 :
- génération et import de SCD / SVD (*Signature Creation Data / Signature Verification Data* – données de création de signature (la clé secrète) / données de vérification de signature (la clé publique)) ;
- création de signature.

Les autres fonctionnalités complémentaires notables sont :
- gestion de plusieurs paires de SCD/SVD ;
- re-génération et re-import de SCD/SVD ;
- configuration du mode de fonctionnement de l'application (par un administrateur ad hoc) ;
- authentification et établissement de canaux de confiance avec des entités distantes ;
- authentification des administrateurs ;
- protection de l'anonymat et des données échangées lors de l'utilisation en mode sans contact ;
- réalisation de services électroniques ;
- stockage de données.

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 démontre sa conformité au profil de protection [BSI-PP-0005-2002] – SSCD type 2 - et [BSI-PP-0006-2002] - SSCD type 3. Cette conformité est choisie de type démontrable par la [ST] car les [CC] ont évolué entre le moment où les profils de protection ont été écrits - en CCv2.1 - et la [ST] - écrite en CCv3.1.

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. [CONF]). Ces éléments identifient la plateforme ID-One Cosmo V7.0-a ainsi que l'application ID-One IAS-ECC v1.0.1 R1. On ne donne ci-après que les éléments relatifs à l'application ID-One IAS-ECC v1.0.1 R1 (pour l'identification de la plateforme sous-jacente, voir [ANSSI-CC-2009_36]) :

- commande GET DATA pour le tag (étiquette) DF 66 : DF 66 02 **11 21**.

Dans cette réponse, **11 21** est la version de l'application ID-One IAS-ECC v1.0.1 R1.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit, accessibles en mode « contact » et « sans contact », sont constitués de ceux fournis par :

- la partie plateforme sous-jacente (cf. [ANSSI-CC-2009_36]) incluant en particulier :
  - les interfaces au service des API dédiées aux applets et l'accès à ces API ;
  - 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) ;
- l'application ID-One IAS-ECC v1.0.1 R1 (cf. [ST] pour plus de détails, notamment les §2.1.4 et § 4.1.1) :
  - SF.PIN_MGT : gestion du PIN afin d'authentifier le signataire ou l'administrateur ;
  - SF.SIG : fourniture d'une signature électronique conformément aux exigences des profils de protection [BSI-PP-0005-2002] – SSCD type 2 - et [BSI-PP-0006-2002] - SSCD type 3 ;
  - SF.DEV_AUTH : authentification mutuelle et ouverture d'un canal de confiance avec les entités externes (SCA, CGA, SSCD type 1) ; les mécanismes cryptographiques utilisés peuvent alors être de type symétrique ou asymétrique ;
  - SF.ADM_AUTH : authentification externe des administrateurs ; les mécanismes cryptographiques utilisés peuvent alors être de type symétrique ou asymétrique ;

- SF.SM : gestion du canal de confiance avec les entités externes (SCA, CGA, SSCD type 1) assurant l'intégrité, la provenance, la destination et la confidentialité des échanges ;
- SF.KEY_MGT : gestion des clés (SCD, SVD, clés d'authentification et clés dédiées pour les services électroniques) ;
- SF.CONF : gestion de la configuration de la TOE (choix du lieu de hashage, du type de cryptographie pour l'authentification, du type de protocole d'échange) ;
- SF.ESERVICE : réalisation de services électroniques (authentification client/serveur, déchiffrement de clés de chiffrement, vérification de certificats) ;
- SF.EAVESDROPPING_PROTECTION : protection contre la capture au vol de données sensibles échangées en mode sans contact ;
- SF.SAFESTATE_MGT : garantie d'états internes sûrs ;
- SF.PHYS : protection contre les attaques physiques.

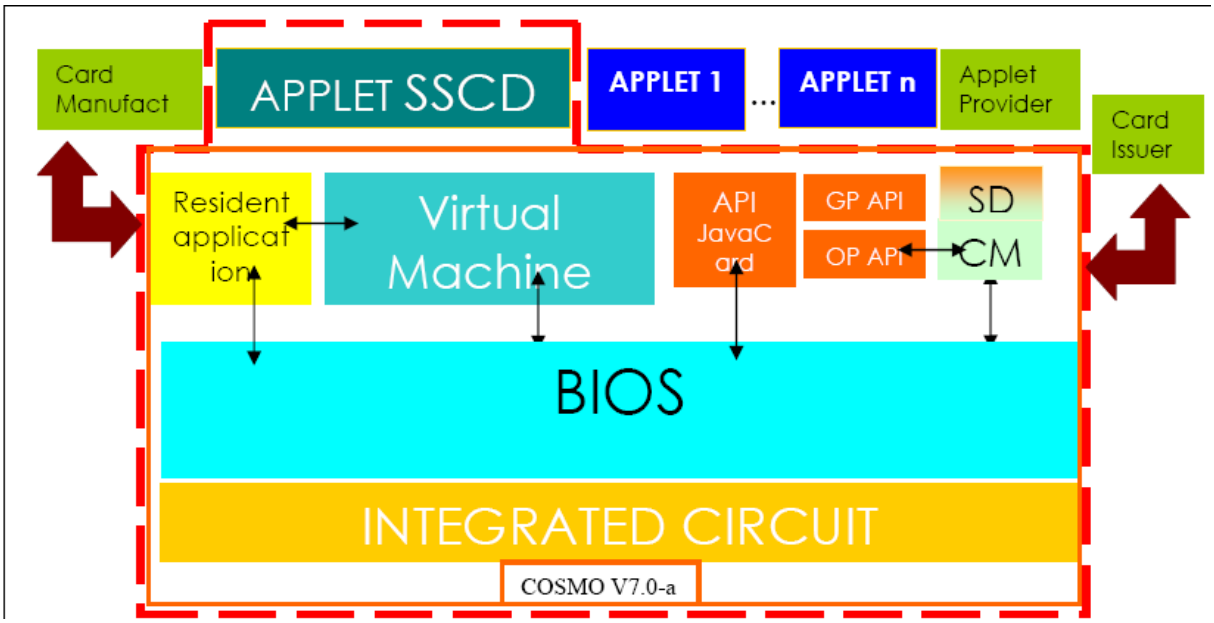
1.2.3. Architecture

Le produit est constitué de :

- l'applet SSCD nommée ID-One IAS-ECC v1.0.1 R1, version 1121 ;
- la plateforme nommée ID-One Cosmo V7.0-a sous-jacente (dont le détail des blocs est donné dans [ANSSI-CC-2009_36]) ;
- le composant sous-jacent correspondant à la plateforme, soit AT90SC256144RCFT rev F ou AT90SC256144RCFT rev F (antenne non montée) ou AT90SC25672RCFT rev F.

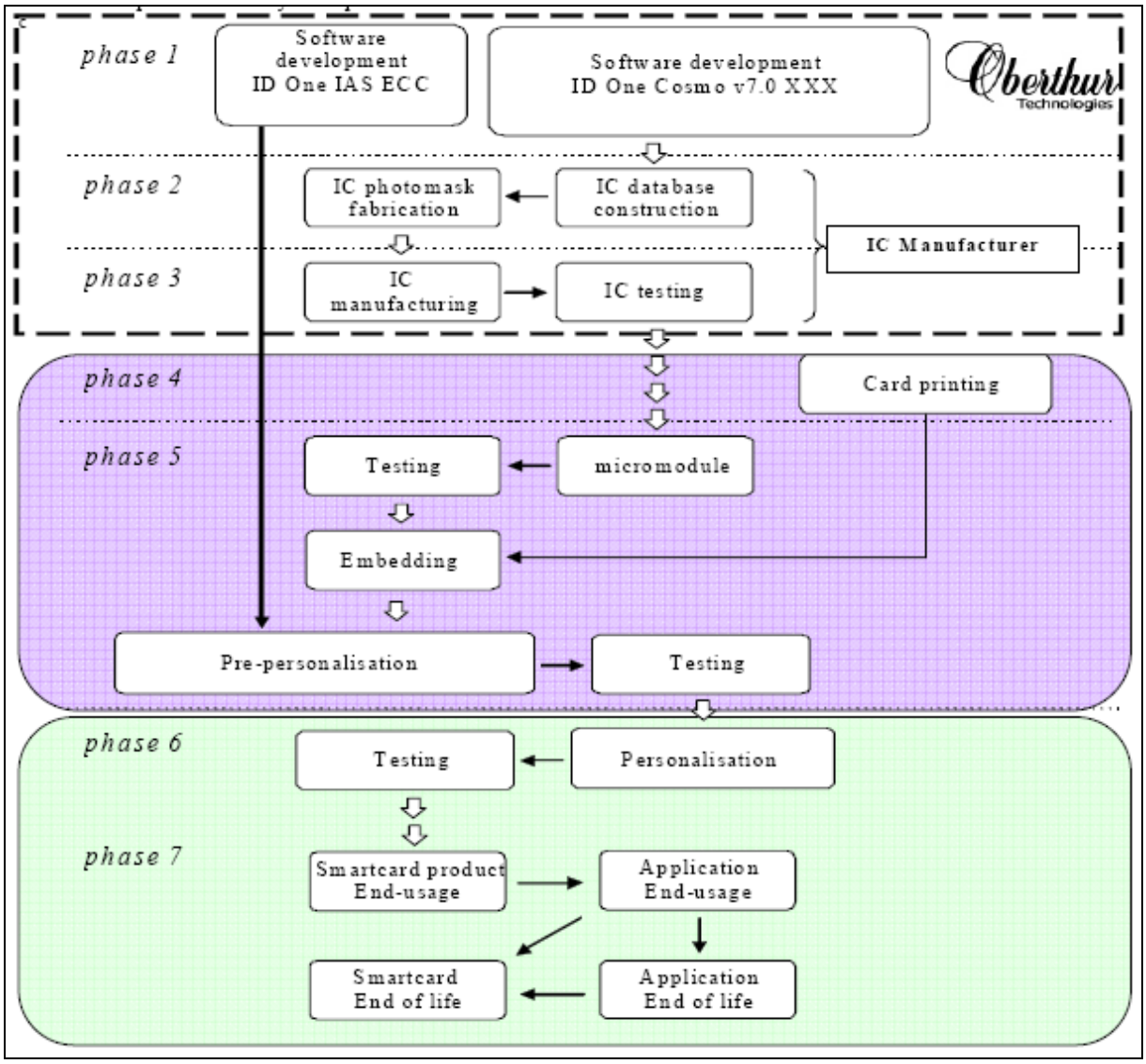
Le code de l'applet est interprété par la machine virtuelle de la plateforme JavaCard ouverte.

Cette architecture est résumée dans la figure suivante :



1.2.4. Cycle de vie

Le cycle de vie du produit comporte sept étapes et est résumé dans la figure suivante :



L'évaluation a couvert la conception et le développement de l'applet qui sont effectués en phase 1, ainsi que son chargement sur la plateforme effectué en phase 5. 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 sont par ailleurs couvertes par des guides de la plateforme, la phase 6 est également couverte par des guides de la plateforme complétés par des guides spécifiques à l'applet. Le produit évalué correspond à celui livré à l'utilisateur à la phase 7.

On notera que dans le cas présent, comme indiqué dans la figure ci-dessus, la composition étant faite sur une plateforme ID-One Cosmo V7.0-a, le code de l'applet a été chargé sur la plateforme sous-jacente en phase 5 suivie de son instanciation en phase 6. En tant qu'applet JavaCard gérée selon Global Platform, le détail de son cycle de vie est schématisé dans la figure suivante :

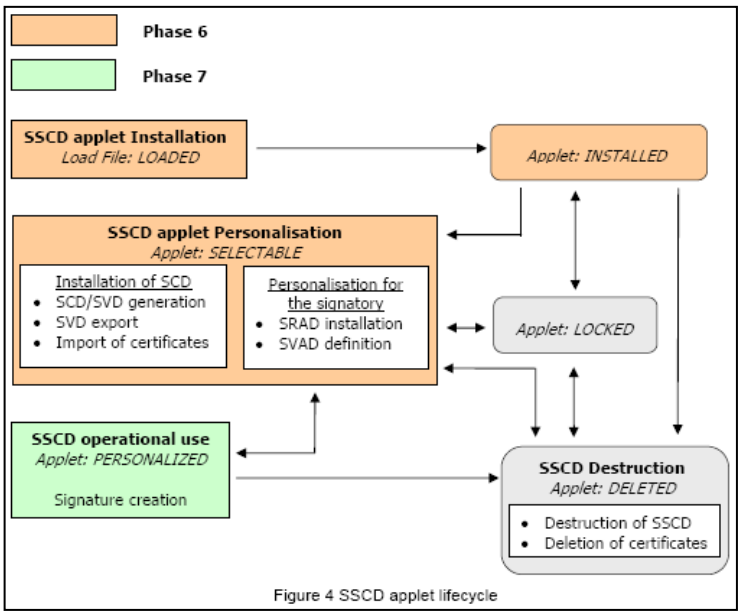


Figure 4 SSCD applet lifecycle

Le produit a été développé sur les sites suivants :

Oberthur Technologies – Levallois (pour la phase 1)

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies – Nanterre (pour la phase 1)

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Pessac (pour la phase 1)

Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus - Porte 2
33600 Pessac
France

Oberthur Technologies – Vitré (pour la phase 5)

La Haye Robert - Avenue d'Helmesdt – BP 36
35503 VITRE Cedex
France

La plateforme sous-jacente ID-One Cosmo V7.0-a a été développée et fabriquée par Oberthur Technologies et ATMEL Secure Microcontroller Solutions sur leurs sites respectifs (cf. [ANSSI-CC-2009_36]).

Pour l'évaluation, l'évaluateur a considéré trois types d'administrateurs du produit :

- le **personnalisateur de l'application** intervenant en phase de personnalisation (phase 6) du produit ; il est en charge de sa personnalisation ainsi que des autres fonctions d'administration telles que :
  - personnalisation du RAD (*Reference Authentication Data*, soit le PIN stocké) ;
  - génération ou import du SCD ;
  - export du SVD ;
  - génération, import ou export des clés d'authentification et de services électroniques ;
  - gestion des verrous applicatifs (choix du lieu de hashage, du type de cryptographie pour l'authentification, du type de protocole d'échange) ;
  - identification de la version de l'application ID-One IAS-ECC v1.0.1 R1 ;
  - passage de la TOE en phase d'utilisation ;
- l'**administrateur** intervenant en phase d'utilisation (phase 7) du produit ; il est en charge de sa personnalisation ainsi que des autres fonctions d'administration telles que :
  - personnalisation du RAD ;
  - génération ou import du SCD ;
  - export du SVD ;
  - génération, import ou export des clés d'authentification et de services électroniques ;
- l'**administrateur de la TOE**, appelé « TOE_Administrator » dans [ST], intervenant en phase d'utilisation du produit (phase 7) ; il est en charge en charge de la gestion de la configuration des verrous applicatifs et il possède les droits pour obtenir la version de l'application ID-One IAS-ECC v1.0.1 R1.

L'évaluateur a considéré comme utilisateur du produit son **détenteur final**, c'est-à-dire celui disposant des secrets lui permettant d'effectuer les opérations de signatures avec la carte. Il peut, en phase d'utilisation :

- modifier le RAD ;
- générer ou importer le SCD ;
- exporter le SVD ;
- réaliser des services électroniques ;
- générer, importer et exporter les clés d'authentification et de services électroniques.

1.2.5. Configuration évaluée

Le développeur a fourni, à l'évaluateur, la TOE décrite ci-après en configuration de test :

- applet ID-One IAS-ECC v1.0.1 R1, version 1121, chargée dans la plateforme JavaCard ouverte ID-One Cosmo v7.0-a Large Dual sur composant Atmel Secure Microcontroller Solutions (le composant était alors AT90SC256144RCFT) ;
- applet configurée suivant le profil SSCD1 (cf. [GUIDES]) ;
- état de l'applet positionné à SECURED (au sens GlobalPlatform), c'est-à-dire telle que livrée à l'utilisateur final (phase 7 du cycle de vie) ;
- le protocole de canal sécurisé SCP01 configuré.

D'autres applications étaient présentes dans la ROM de la carte et n'étaient pas instanciées. Comme indiqué au §1.2.3 Architecture, elles ne font pas partie du périmètre de la TOE.

La plateforme a été configurée conformément à son guide de pré-personnalisation (cf. [ANSSI-CC-2009_36]). L'applet a été configurée suivant [GUIDES].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 R2** [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, 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 pris en compte les résultats de l'évaluation de la plateforme sous-jacente intitulée « carte à puce ID-One Cosmo V7.0-a en configuration Large Dual, Large et Standard Dual » au niveau EAL5 augmenté des composants ADV_IMP.2, ALC_DVS.2, et AVA_VAN.5, conforme au profil de protection [PP/0304]. Cette plateforme a été certifiée par l'ANSSI (cf. [ANSSI-CC-2009_36]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 juin 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 au référentiel technique [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY].

Les mécanismes analysés sont conformes aux exigences du référentiel cryptographique de l'ANSSI (cf. [REF-CRY]) sous réserve du complet respect des guides (cf. [GUIDES]. En particulier, en vue de la qualification[1] du produit, ces [GUIDES] demandent que :

[1] Le processus de qualification d'un produit de sécurité, utilisé dans le schéma français, est décrit sur le site de l'ANSSI (cf. http://www.ssi.gouv.fr/site_article39.html)

- pour le paramétrage d'échange de clé Diffie-Hellman, la taille du *Prime* p soit égale à 2048 bits, l'ordre q soit divisible par un nombre premier de longueur au moins égal à 200 bits et que sa taille soit de 256 bits ;
- la taille des modules RSA employés pour les signatures soit égale à 2048 bits ;
- pour la signature électronique, les clés soient dédiées et que ce soit le SHA-256 qui soit utilisé ;
- la génération des clés RSA soit effectuée juste après avoir effectué un test complet du générateur d'aléas ;
- les fonctionnalités d'authentification client/serveur et de déchiffrement de clés de chiffrement ne soient pas utilisées.

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 produit offre un générateur de pseudo-aléas. Ces pseudo-aléas sont obtenus à partir d'un retraitement algorithmique de nature cryptographique de la sortie du générateur d'aléas matériel du composant sous-jacent.

Ce générateur a fait l'objet d'une analyse par l'ANSSI. La génération d'aléas du produit n'est pas conforme au référentiel [REF-CRY], ce qui impacte la génération des clés asymétriques. Toutefois, une mise en œuvre conforme aux recommandations mentionnées dans les [GUIDES] du produit est reconnue conforme au référentiel [REF-CRY] (cf. le résumé de cette recommandation dans le paragraphe précédent : « […] la génération des clés RSA soit effectuée juste après avoir effectué un test complet du générateur d'aléas »).

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 ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration Large Dual, Large et Standard Dual, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

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

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'Espagne, la Finlande, la France, 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 4+	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**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic 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 procedure
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	**4**	Problem tracking CM coverage
	ADO_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	**1**	Well-defined development tools
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant 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 : - Euterpe – Security target ; référence 110 4472, version 12 ; Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Euterpe – IAS ECC v1.0.1 R1 – public Security target ; référence 4773, version 3; Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: EUTERPE; référence EUT_ETR, version 4; Thales-CEACI.
[ANA-CRY]	Rapport d'analyse cryptographique de l'ANSSI : Cotation de mécanismes cryptographiques - Qualification EUTERPE, N° 722/ANSSI/ACE/LCC, 25 mars 2010
[CONF]	Liste de configuration du produit : - Euterpe - Diffusion List ; référence 110 4470, version 10 ; Oberthur Technologies.
[GUIDES]	Guide d'administration (personnalisation) du produit : - Euterpe – AGD_PRE ; référence 110 4511, version 8 ; Oberthur Technologies. Guide d'utilisation du produit : - Euterpe – AGD_OPE ; référence 110 4527, version 7 ; Oberthur Technologies.
[IASECC]	Spécifications IAS ECC v1.0.1 : - EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS - IAS ECC v1.0.1 – GIXEL – 21/03/2008; http://www.gixel.fr/includes/cms/_contenus/bibliotheque/file/CAP%20/IAS%20ECC%20v1_0_1UK.pdf
[BSI-PP-0005-2002]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. Certifié par le BSI sous la référence BSI-PP-0005-2002T.
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. Certifié par le BSI sous la référence BSI-PP-0006-2002T.

[ANSSI-CC-2009_36]	Certificat ANSSI délivré le 29 septembre 2009 pour le produit : carte à puce ID-One Cosmo V7.0-a en configuration Large Dual, Large et Standard Dual
[PP/0304]	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

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 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr