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-2014/41

Application IAS ECC v2 avec confidentialité en sans-contact, sur ID-One Cosmo v7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual)

Paris, le 11 juin 2014

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

[Original signé]

Guillaume Poupard

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-2014/41

Nom du produit

Application IAS ECC v2 avec confidentialité en sans-contact, sur ID-One Cosmo v7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual)

Référence/version du produit

Application : version D0010209
Plateforme : version 7.1-s

Conformité à un profil de protection

SSCD Type 2, version 1.04
SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

Oberthur Technologies
420 rue d'Estiennes d'orves, 400008 CS,
92705 Colombes Cedex, France

STMicroelectronics
190 avenue Celestin Coq, ZI de Rousset, B.P. 2,
13106 ROUSSET, France

Commanditaire

Oberthur Technologies
420 rue d'Estiennes d'orves, 400008 CS, 92705 Colombes Cedex, 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

1.1. Présentation du produit

Le produit évalué est l' « Application IAS ECC v2 avec confidentialité en sans-contact[1], sur ID-One Cosmo v7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual) ». L'application ainsi que la plateforme sont développées par Oberthur Technologies. Le composant est développé par ST Microelectronics.

La cible d'évaluation (Target of Evaluation – TOE) est un logiciel sécurisé s'exécutant sur un microcontrôleur et pouvant être embarquée dans une carte à puce.
Ses fonctionnalités applicatives sont offertes par l'application IAS ECC v2.

La TOE est destinée à être utilisée comme dispositif de création de signature électronique en conformité avec la directive européenne 1999/93/CE. A ce titre elle permet de réaliser des signatures électroniques avancées, et des signatures électroniques dites « qualifiées » (articles 2 et 5 de la directive précitée).

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 démontre sa conformité au profil de protection [PP0005] et [PP0006]. Cette conformité est choisie de type démontrable par la [ST] car les CC ont évolué entre la rédaction des profils de protection (selon la version 2.1 des CC) et celle de la [ST] (écrite selon la version 3.1 des CC) [CC].

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 :

- pour l'application IAS ECC avec le tag (étiquette) DF67 : la valeur de retour doit être D0010209 ;
- pour la plateforme ID-One Cosmo:
    - avec le tag (étiquette) DF52, en mode contact : la valeur de retour doit être conforme aux informations « identification du produit maintenu » indiquées dans [ANSSI-CC-2013/16-M01] ;

[1] La confidentialité en sans-contact protège l'accès aux données d'identification du porteur de la carte par une entité non autorisée.

- avec le tag DF6A (étiquette), en mode contact : la valeur de retour doit être « xxxxxx1x » (chaîne de bits), en mode sans contact le mot d'état doit être « 6985 ».

1.2.3. 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, avec en particulier :
  - 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) [1], ainsi que le canal sécurisé propriétaire (SCPF3) ;
- le microcontrôleur, sous-jacent à la plateforme, avec en particulier :
  - 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 ;
- l'application IAS-ECC v2 (voir [ST] pour plus de détails, notamment le §2.1.5) :
  - la génération et l'import de SCD[2]/SVD[3] ;
  - la création de signature basique, avancée et qualifiée telle que spécifiée dans les profils de protection [PP0005] et [PP0006] ;

[1] Le protocole de canal sécurisé propriétaire (SCP03), conformément aux guides, ne doit pas être utilisé.
[2] *Signature Creation Data* ou données de création de signature.
[3] *Signature Verification Data* ou données de vérification de signature.

- l'authentification du titulaire de la carte basée sur la vérification du PIN ou des données biométriques ;
- le déblocage du PIN ou des données biométriques du titulaire ;
- l'authentification d'un ou plusieurs administrateur(s) ;
- l'établissement de canaux de confiance, protégés en intégrité et confidentialité, avec des entités distantes ;
- la création de droits particuliers pour administrer la fonction de création de signature, le mode de communication et le type de mécanismes cryptographiques à utiliser pour un administrateur particulier ;
- l'utilisation de plusieurs SCD par le titulaire pour signer des documents ;
- la génération et/ou l'import, à n'importe quel moment du cycle de vie de la TOE, de une ou plusieurs paires de SCD/SVD et autres objets cryptographiques ;
- la signature numérique en mode contact et/ou sans contact ;
- la réalisation de services tels que : authentification client/serveur, chiffrement et déchiffrement de clefs ;
- la protection contre le pistage en mode sans contact.

1.2.4. Architecture

Le produit est constitué de :

- l'application SSCD nommée « IAS-ECC v2 », version D0010209 ;
- la plateforme javacard ouverte nommée ID-One Cosmo V7.1-s sous-jacente ;
- le composant sous-jacent correspondant à la plateforme, ST23YR80B (Standard Dual) ou ST23YR48B (Basic Dual) ;
- des applications connues au moment de l'évaluation de la plateforme présentes sur le produit, en dehors de la TOE et identifiées dans [GUIDE_PLT_App].

La figure suivante illustre cette architecture.

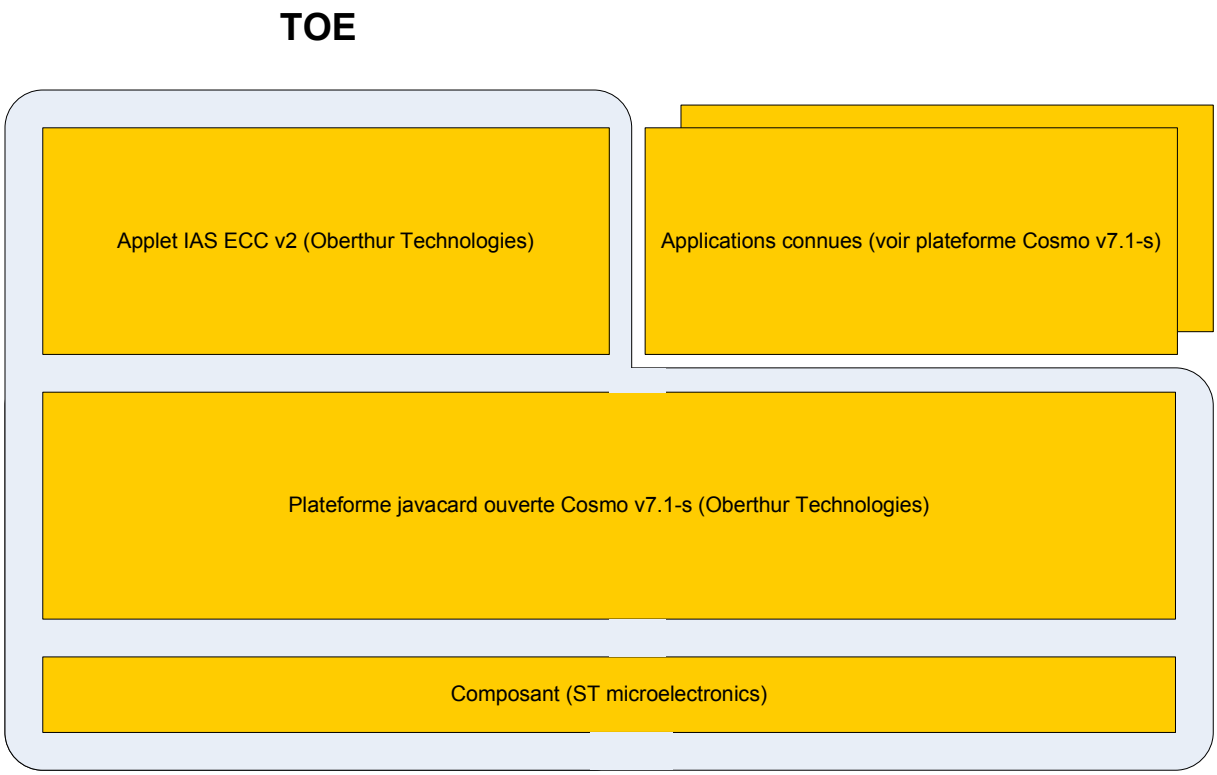

Figure 1 : Architecture de la TOE

1.2.5. Cycle de vie

Le cycle de vie du produit comporte sept phases, résumées dans la figure 2.

L'évaluation a couvert la conception et le développement de l'application 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 sont 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'application. Le produit évalué correspond à celui livré à l'utilisateur dans les phases 6 et 7.

Le service de confiance assurant la protection contre la traçabilité en mode sans contact (voir §1.2.3) est activé au cours de la phase 6. En particulier l'objet de données 'DF6A' pour la plateforme ID-One Cosmo est positionné à la valeur « xxxxxx1x » (chaîne de bits, voir §1.2.2).

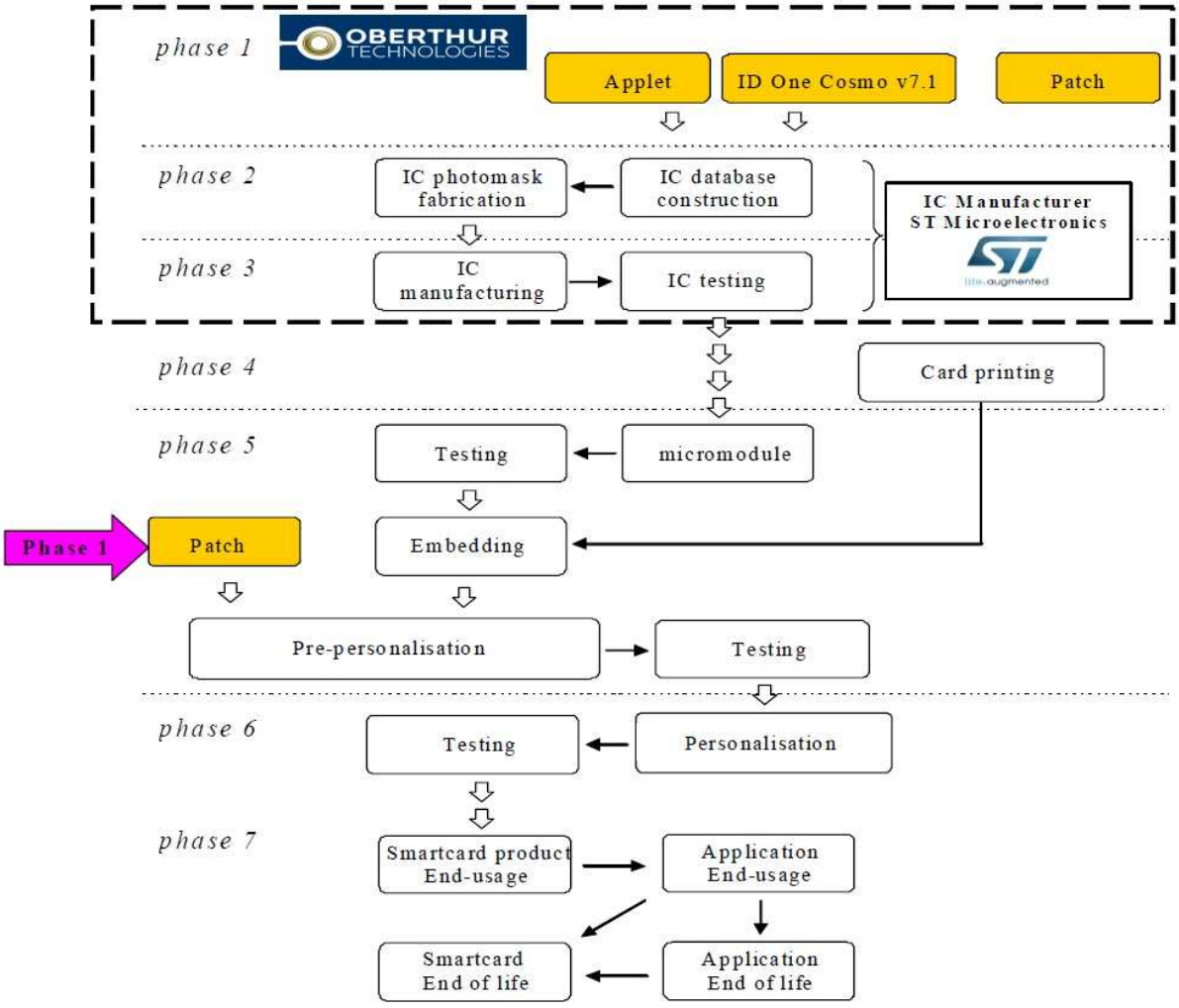

Figure 2 : Cycle de vie de la TOE

L'application a été développée sur les sites suivants :

Oberthur Technologies – Site de Colombes

420 rue d'Estiennes d'orves
400008 CS
92705 Colombes Cedex
France

Oberthur Technologies – Site de Vitré

Av. d'Helmstedt - BP90308
35503 VITRE Cedex
France

Oberthur Technologies – Site de Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Site de Levallois

50 quai Michelet
92300 Levallois-Perret
France

Les sites de développement et de fabrication de la plateforme et du microcontrôleur sont décrits dans les rapports de certification [ANSSI-CC-2013/16] et [ANSSI-CC-2010/01].

1.2.6. Configuration évaluée

Le certificat porte sur le produit tel que décrit plus haut au paragraphe 1.2.4 Architecture et configuré conformément aux [GUIDES].
La configuration ouverte du produit a été évaluée conformément à [ANSSI-CC-NOTE.10]. Ainsi tout chargement de nouvelles applications conforme aux contraintes exposées au chapitre 3.2 ne remet pas en cause le présent rapport de certification.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 [JIWG IC] et [JIWG AP] ont été appliqués. 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 la plateforme et les microcontrôleurs déjà certifiés par ailleurs.

Les microcontrôleurs ST23YR48B et ST23YR80B ont été certifiés au niveau EAL6 augmenté du composant ALC_FLR.1, conformément au profil de protection [PP0035], le 1er février 2010, sous la référence [ANSSI-CC-2010/01].

Le niveau de résistance des microcontrôleurs ST23YR48B et ST23YR80B a été confirmé le 4 décembre 2013 dans le cadre du processus de surveillance.

La « Plateforme JavaCard de la carte à puce ID-One Cosmo v7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual) » a été certifiée le 29 mars 2013 sous la référence [ANSSI-CC-2013/16] et maintenue sous la référence [ANSSI-CC-2013/16-M01].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 janvier 2014, 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. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que l'ensemble des mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations du guide [GUIDES_Reco_CRY] doivent être appliquées.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI, voir [RTE]. 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.5 visé si les recommandations contenues dans [GUIDES] sont correctement appliquées.

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 cryptographique.
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 « Application IAS ECC v2 avec confidentialité en sans-contact, sur 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], en particulier [GUIDES_Reco_CRY]. En complément, la réalisation et l'intégration d'applications supplémentaires sur la plateforme hébergeant la TOE doit s'accompagner des recommandations de [GUIDES_PLT], notamment celles relatives aux applications qui stipulent que :

- les développeurs d'applications « sensibles » doivent :
  - respecter dans leurs implémentations les recommandations se trouvant dans le guide [AGD_OPE_PLT] ;
  - respecter les [GUIDES] suivant la sensibilité de ces applications ;
- les applications « basiques » doivent être contrôlées par le « *Byte Code Verifier* » avant leur chargement et respecter les recommandations des guides de la plateforme [GUIDES_PLT] ;
- le chargement de ces applications doit être protégé :
  - si le chargement s'effectue après l'émission de la carte (« *post-issuance* »), conformément à la configuration « *Mandated DAP* », toutes les applications doivent être signées (typiquement, par une CA (*Controlling Authority* - autorité de contrôle comme définie dans [ST_PLT]), ce qui assure leur authenticité et leur intégrité jusqu'au chargement dans la carte. La vérification par la VA (*Verification Authority* – autorité de vérification comme définie dans [ST_PLT]) de ces signatures sera un préalable pour leur chargement effectif dans la carte ;
  - si le chargement s'effectue avant l'émission de la carte (« *pre-issuance* »), les [GUIDES_PLT] indiquent les mesures organisationnelles à mettre en place, en particulier pour s'assurer de l'intégrité et de l'authenticité des applications basiques à charger.

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 : - *Security target, IAS ECC v2 with privacy on contactless on ID-One Cosmo V7.1-s Card (Standard Dual and Basic Dual),* référence 110 6507 Ed4, 6 décembre 2013, Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Public security target, IAS ECC v2 with privacy on contactless on ID-One Cosmo V7.1-s Card (Standard Dual and Basic Dual),* référence 110 6878 Ed1, 8 décembre 2013, Oberthur Technologies.
[ST_PLT]	Cible de sécurité de référence pour l'évaluation de la plateforme sous-jacente maintenue (voir [ANSSI-CC-2013/16-M01]) : - *TOUTATIS – Security Target,* référence FQR 110 6070, version 7 du 31/03/2014, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - *Evaluation technical report,* LETI.CESTI.SUC.RTE.001 - v1.1, 6 janvier 2014, CEA-LETI.
[ANSSI-CC-2010/01]	*Rapport de certification ANSSI-CC-2010/01, Microcontrôleurs sécurisés ST23YR48B et ST23YR80B,* 1 février 2010, ANSSI.
[ANSSI-CC-2013/16]	*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),* 29 mars 2013, ANSSI.
[ANSSI-CC-2013/16-M01]	*Rapport de maintenance ANSSI-CC-2013/16-M01, Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual),* 13 mai 2014, ANSSI
[ANA-CRY]	*Cotation des mécanismes cryptographiques,* LETI.CESTI.SUC.RT.001 –v2.0, 5 novembre 2013, CEA-LETI.
[CONF]	Liste de configuration du produit : - *Configuration list,* référence : FQR 110 6870 Ed3, 9 décembre 2013, Oberthur Technologies.
[GUIDES]	- Sucellos AGD_PRE, référence 110 6816 Ed3, 2 décembre 2013, Oberthur Technologies ; - Sucellos AGD_OPE, référence 110 6863 Ed2, 2 décembre 2013, Oberthur Technologies ; - [GUIDES_Reco_CRY] *Recommandations pour la compatibilité avec le référentiel de qualification renforcée,* référence 110 6688 Ed3, 21 novembre 2013, Oberthur Technologies.

[GUIDES_PLT]	Voir [ANSSI-CC-2013/16], en particulier - ID-One Cosmo v7.1, security recommendations, référence 110 6029 Ed2, 29 novembre 2012, Oberthur Technologies ; - [GUIDE_PLT_App] All Applications on ID-One Cosmo V7.1, Référence : FQR 110 6319, version 1 du 25/09/2012.
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002.*
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP]*	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[COMP]	Mandatory Technical Document – 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.
[ANSSI-CC-NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.