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-2014/92

Athena IDProtect/OS755 (release 0355, level 0802, correctif P8) avec application IAS-ECC (version 03, build 02, correctif FA) sur composants SB23YR48/80B

Paris, le 5/01/2015

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

Guillaume POUPARD
[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-2014/92

Nom du produit

Athena IDProtect/OS755 avec application IAS-ECC sur composants SB23YR48/80B

Référence/version du produit

Athena IDProtect/OS755 : release 0355, level 0802, correctif P8
Application IAS-ECC : version 03, build 02, correctif FA
STMicroelectronics SB23YR48/80B: revision interne G
STMicroelectronics NesLib: version 3.0

Conformité à un profil de protection

[PP0005] : SSCD Type 2, version 1.04
[PP0006] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.
16615 Lark Ave, Suite 202
Los Gatos CA 95032
United States of America

STMicroelectronics
190 Avenue Célestin Coq, ZI de Rousset, BP2,
13106 Rousset Cedex, France

Commanditaire

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

Serma Technologies
14 rue Galilée, CS 10055, 33615 Pessac Cedex, 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 la carte à puce « Athena IDProtect/OS755 (release 0355, level 0802, correctif P8) avec application IAS-ECC (version 03, build 02, correctif FA) sur composants SB23YR48/80B », développée par Athena Smartcard Solutions et STMicroelectronics.

La cible d'évaluation est une application de la carte à puce destinée à être utilisée dans le cadre de l'administration électronique. Elle répond aux caractéristiques des dispositifs sécurisés de création de signatures électroniques (SSCD - *Secure Signature Creation Device*), dont les fonctionnalités applicatives sont offertes par IAS ECC (*Identification Authentication Signature / European Citizen Card* - identification authentification signature / carte du citoyen européen).

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme aux profils de protection [PP0005] et [PP0006], adaptés dans la cible à la version 3.1 des CC (ces PP ayant été rédigés selon la version 2.1 des 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 ci-après, qui sont renvoyés par le produit suite à la commande GET DATA avec le tag **'0003'** (voir [GUIDES]) :

- IDProtect OS release identifier : 0355h ;
- IDProtect OS release level : 0802h (le premier octet spécifie le correctif P8) ;
- IDPass Applet version : FA03h (le premier octet spécifie le correctif FA) ;
- IDPass Applet build : 0002h.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la création de signature : le produit signe les données devant être signées (DTBS – *Data To Be Signed*) au moyen de la clé privée de signature (SCD – *Signature Creation Data*) ;
- l'identification et l'authentification des utilisateurs : le produit gère l'identification et l'authentification du signataire et de l'administrateur. Il met également en œuvre un mécanisme de séparation des rôles ;
- le contrôle des accès : le produit vérifie que, pour chaque opération initiée par un utilisateur, les attributs de sécurité, correspondant aux autorisations accordées à l'utilisateur et à la communication des données, sont corrects ; les opérations typiques

du SSCD, telles que la signature électronique, la génération des clés, l'import/export de SCD/SVD (*Signature Creation Data / Signature Verification Data*, clé privée / clé publique de signature) et la vérification du RAD/PUK (*Reference Authentification Data / PIN Unblocking Key*, code PIN d'authentification / code PIN de déblocage) sont soumises à ces vérifications ;

- le canal sécurisé : le produit peut mettre en place un canal de communication sécurisé entre lui et le dispositif externe qui interagit avec lui ; les opérations typiques du SSCD, telles que la signature électronique, l'import/export de SCD/SVD et la vérification du RAD/PUK, sont soumises à l'établissement du canal sécurisé ;
- un ensemble de moyens cryptographiques nécessaires à toutes les autres fonctions de sécurité (en particulier, DES/TDES, RSA, RNG, génération de nombres premiers) ;
- la protection des données et des fonctionnalités : le produit protège les données utilisateur (*user data*), les données des fonctionnalités de sécurité (*TSF data*) et les fonctionnalités de sécurité (*TSF*) contre le dysfonctionnement, la perturbation et l'observation grâce aux autotests, à la gestion des pannes, aux tests d'intégrité, à la réinitialisation sécurisée, aux contre-mesures prévenant les fuites. Ce service de sécurité assure également la terminaison du chargement du contenu de la carte, de son installation, du chargement du correctif et le blocage du mécanisme de chargement.

1.2.4. Architecture

Le produit, présenté figure 1, est constitué des éléments suivants :

- des composants « SB23YR48/80B, révision interne G », développés par STMicroelectronics. Les deux versions du composant peuvent être utilisées, elles diffèrent uniquement par la taille mémoire ;
- de la librairie cryptographique « NesLib, version 3.0 », développée par STMicroelectronics ;
- du système d'exploitation « Athena IDProtect/OS755 Java Card, release 0355, level 0802, correctif P8 » développé par Athena Smartcard Solutions ;
- de l'application « Athena IAS-ECC applet, version 03, build 02 correctif FA » développée par Athena Smartcard Solutions ;
- de *packages* d'autres applications inactives dans la configuration évaluée.

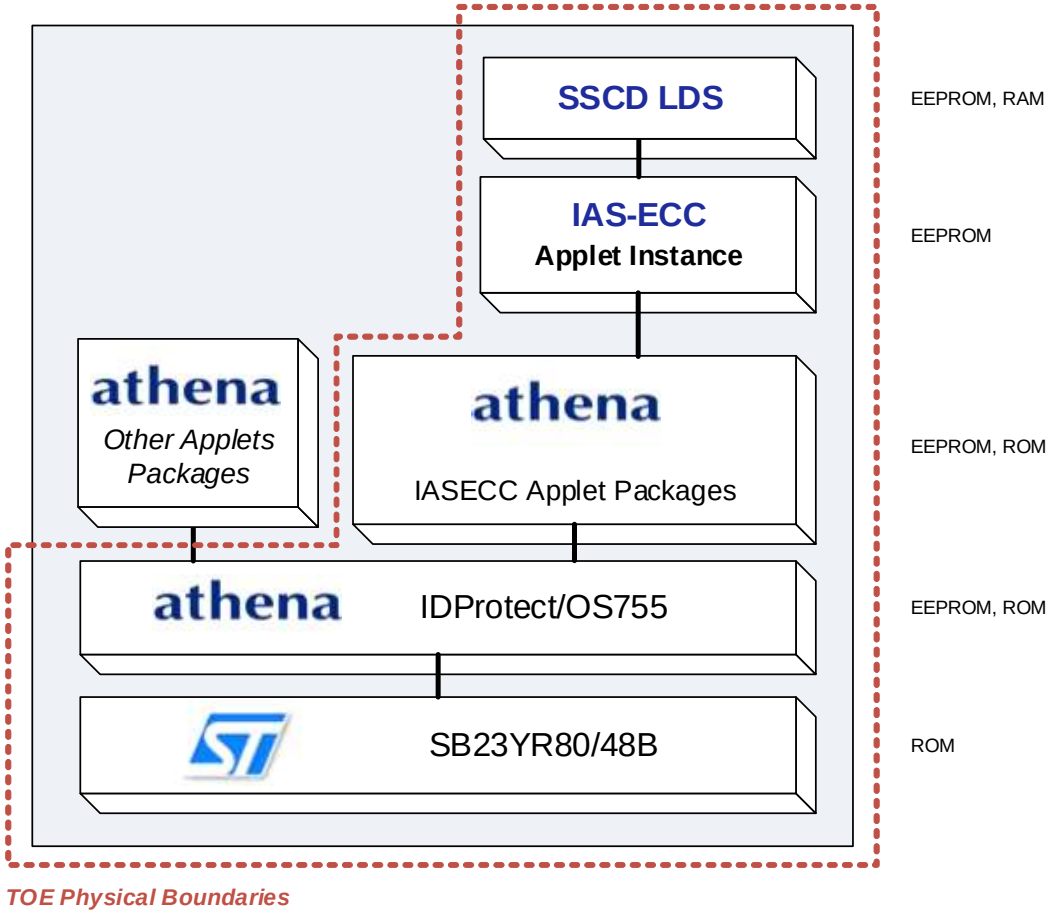

Figure 1 – Architecture du produit (configuration évaluée)

Le système d'exploitation et l'application IASECC sont chargés en mémoire ROM. Le correctif P8 et le correctif FA sont chargés en mémoire EEPROM.

1.2.5. Cycle de vie

Le cycle de vie du produit est basé sur celui de la carte à puce, tel que décrit dans les profils de protection [PP0005] et [PP0006].

Il est illustré par la figure 2.

Le point de livraison est situé en fin de l'étape « *Initialisation* ».

Toutes les étapes qui précèdent ce point de livraison ont été couvertes par la présente évaluation (au titre d'ALC), le cas échéant, en réutilisant les résultats obtenus lors de l'évaluation du composant sous-jacent.

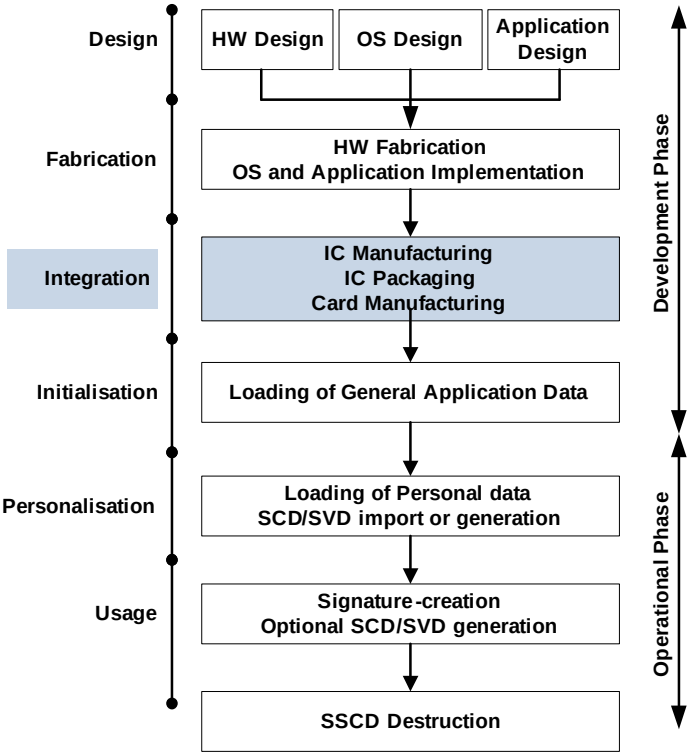

Figure 2 – Cycle de vie du produit

Les tests ont porté sur les fonctionnalités du produit disponibles en phase opérationnelle (au titre d'ATE et d'AVA).

Le produit a été développé et fabriqué sur les sites suivants :

Site n°1 de développement du logiciel
Athena Smartcard Inc.

16615 Lark Avenue – Suite 202
Los Gatos CA95032
United States of America

Site n°2 de développement du logiciel
Athena Smartcard Ltd.

The Alba Centre
Livingston EH54 7EG
Scotland - United Kingdom

Les composants sont développés et fabriqués par STMicroelectronics. Les sites de développement et de fabrication des composants STMicroelectronics sont détaillés dans le rapport de certification référencé [ANSSI-CC-2010/02] et les rapports de maintenance référencés [ANSSI-CC-2010/02-M01] et [ANSSI-CC-2010/02-M02].

1.2.6. Configuration évaluée

Ce certificat ne porte que sur la configuration du produit où les applications en dehors du périmètre de cette évaluation (nommées « *other applets packages* » dans la figure 1) sont toutes inactivées.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.
Pour répondre aux spécificités des cartes à puce, 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 le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation des microcontrôleurs « Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0035]. Ces microcontrôleurs ont été certifiés le 10 février 2010 sous la référence [ANSSI-CC-2010/02]. Le niveau de résistance de ces microcontrôleurs, maintenus le 19 mars 2010 sous la référence [ANSSI-CC-2010/02-M01] et le 8 juillet 2010 sous la référence [ANSSI-CC-2010/02-M02], a été confirmé dans le cadre de leur processus de surveillance le 20 novembre 2014.

L'évaluation s'appuie sur les résultats d'évaluation du produit « Athena IDProtect/OS755 avec application IASECC sur composants SB23YR48/80B » certifié le 26 juillet 2013 sous la référence [ANSSI-CC-2013/54].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 décembre 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 selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit a été analysé au titre de l'évaluation des composants (voir [ANSSI-CC-2010/02]).

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 « Athena IDProtect/OS755 avec application IAS-ECC sur composants SB23YR48/80B » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 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].

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 :

[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.

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[1], 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 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.

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 TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	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 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	**4**	Problem tracking 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	**1**	Well-defined development tools
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**	**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**	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 : - Athena IDPass SSCD – Security Target version 3.3, 10/12/2014, Athena Smartcard Solutions. Pour les besoins de publication, la cible de sécurité suivante a été fournie dans le cadre de cette évaluation : Athena IDPass SSCD – Security Target Lite version 3.3, 10/12/2014, Athena Smartcard Solutions.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: PERSEUS3, reference PERSEUS_ETR_V3.2, version 3.2, 16/12/2014, Thalès.
[CONF]	Liste de configuration du produit : - Perseus_3 - Docs Configuration List, version 2.3, 10/12/2014, Athena Smartcard Solutions.
[GUIDES]	Guide de préparation du produit : - Athena IDPass SSCD – Preparation Manual, version 2.0, 26/01/2014, Athena Smartcard Solutions. Guide d'opération du produit : Athena IDPass SSCD - Operation manual, version 2.0, 26/03/2014, Athena Smartcard Solutions.
[PP-0005]	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-0005-2002T.*
[PP-0006]	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-2010/02]	« Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB ». Certifié par l'ANSSI le 10 février 2010 sous la référence ANSSI-CC-2010/02.
[ANSSI-CC-2010/02-M01]	Rapport de maintenance ANSSI-CC-2010/02-M01, délivré le 19 mars 2010, relatif au certificat ANSSI-CC-2010/02.

[ANSSI-CC-2010/02-M02]	Rapport de maintenance ANSSI-CC-2010/02-M02, délivré le 8 juillet 2010, relatif au certificat ANSSI-CC-2010/02.
[ANSSI-CC-2013-54]	Rapport de certification ANSSI-CC-2013/54, délivré le 26 juillet 2013 pour le produit « Athena IDProtect/OS755 (release 0355, level 0602, correctif P6) avec application IAS-ECC (version 03, build 02, correctif FA) sur composants SB23YR48/80B ».

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[JIWG 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, July 2014.
[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.

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