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-2012/23

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Paris, le 31 mai 2012

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-2012/23

Nom du produit

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Référence/version du produit

- **Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005**
- **Athena IAS-ECC applet : version 3, correctif F9, build 2**
- **Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G**
- **Inside Secure Toolbox version: 00.03.11.05**

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 révision 3

Niveau d'évaluation

EAL 4 augmenté

AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.

1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Inside Secure S.A.

Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom

Commanditaire

Athena Smartcard Solutions Inc.

1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

THALES (TCS – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse 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 la carte à puce «Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU», développée par Athena Smartcard Solutions et Inside Secure.

La cible d'évaluation ou TOE (*Target Of Evaluation*) est constituée :

- du composant :
  - AT90SC28872RCU Microcontroller : AT58U07, révision G, développé par Inside Secure ;
- adjoint de la librairie crypto :
  - Toolbox, version 00.03.11.05, développée par Inside Secure ;
- embarquant le système d'exploitation :
  - Athena IDProtect/OS755 v6 Java Card, release date 0352, release level 0005, développé par Athena Smartcard Solutions ;
- et l'application :
  - Athena IAS-ECC applet, version 3, correctif F9, build 2 développée par Athena Smartcard Solutions.

Ce produit est destiné à être utilisé dans le cadre d'applications mettant en œuvre la signature électronique.

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 strictement conforme aux profils de protection [BSI-PP-0005-2002] et [BSI-PP-0006-2002] (SSCD types 2 et 3).

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 du tableau ci-après, qui sont renvoyés par le produit suite à la commande GET DATA avec le tag 9F7F (voir [GUIDES]) :

Donnée d'identification de la plateforme	Lg	Contenu et interpretation
IC fabricator	2	'4180'
IC type	2	'010B' AT90SC28872RCU
Operating system identifier	2	'8211'
Operating system release date	2	'0352' ('0' = 2010 + '352'= 18 December)
Operating system release level	2	'0005'

Donnée d'identification de la plateforme	Lg	Contenu et interpretation
IC fabrication date	2	Test date (YDDD)
IC serial number	4	Serial number
IC batch identifier	2	Batch Number
IC module fabricator	2	'0000'
IC module packaging date	2	'0000'
ICC manufacturer	2	'0000'
IC embedding date	2	'0000'
IC pre-personalization data	8	'0000000000000000'
IC personalization data	8	'0000000000000000'

Ainsi, à titre d'illustration, on donne ci-après le constat effectué par l'évaluateur sur un échantillon qu'il a testé :

- commande SELECT avec l'identifiant ISD (« *Issuer Security Domain* ») envoyée:
  - 00A4040C A0000001510000 00 ;
- données renvoyées par le produit :
  - 6F0F8407A0000001510000A5049F6501FF ;
- commande GET DATA avec tag **9F7F** envoyée :
  - 00CA**9F7F**00 ;
- données renvoyées par le produit :
  - 4180 010B 8211 **0352 0005** 0A54 00123819 6947 0000 0000 0000 0000 0000000000000000 0000000000000000.

Dans ces données, on retrouve bien, en particulier, les valeurs **0352** et **0005** (correspondant aux champs « *Operating system release date* » et « *Operating system release level* » dans le tableau précédent).

Par ailleurs, la commande GET DATA avec le tag 0046 permet d'obtenir les éléments identifiant le composant. Ainsi, sur l'échantillon testé, on a :

- commande GET DATA avec tag **0046** envoyée :
  - 00CA**0046**00 ;
- données renvoyées par le produit :
  - **3006**0A546947123819.

La valeur **30** donne l'identification du composant correspondant à la valeur du registre matériel SN_0 (soit AT90SC28872RCU), tandis que la valeur **06** donne la révision du composant correspondant à la valeur du registre matériel SN_1 (soit révision G).

L'applet IAS-ECC est sélectionnée grâce à son identifiant :

- commande SELECT avec Applet AID (« *Applet Identifier* ») envoyée:
  - 00A4040C 4941534543435F53534344 ;

Après la sélection de l'applet IAS-ECC, la commande GET DATA avec le tag 0003 permet d'obtenir les éléments identifiant la version d'applet. Ainsi, sur l'échantillon testé, on a :

- commande GET DATA avec tag **0003** envoyée :
  - 00CB**0003**04 ;
- données renvoyées par le produit :
  - **F9030002.**

On obtient les valeurs **F903** et **0002** correspondant aux informations « *Applet version* » et « *Build number* ».

1.2.2. 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 ;
- la cryptographie : le produit offre des moyens cryptographiques 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, etc. ; ce service de sécurité assure également la terminaison du chargement du contenu de la carte, de son installation, du chargement du correctif et du mécanisme de terminaison.

1.2.3. Architecture

La TOE correspond à une carte à puce. Le composant sous-jacent AT90CS28872RCU fournit l'interface matérielle ISO 7816.

La TOE n'a pas d'autre interface externe.

Le système d'exploitation et l'application sont masqués dans la ROM, seul le correctif de l'application est chargé en EEPROM.

Le périmètre de la TOE est illustré dans la figure 1 (contours en pointillé rouge).

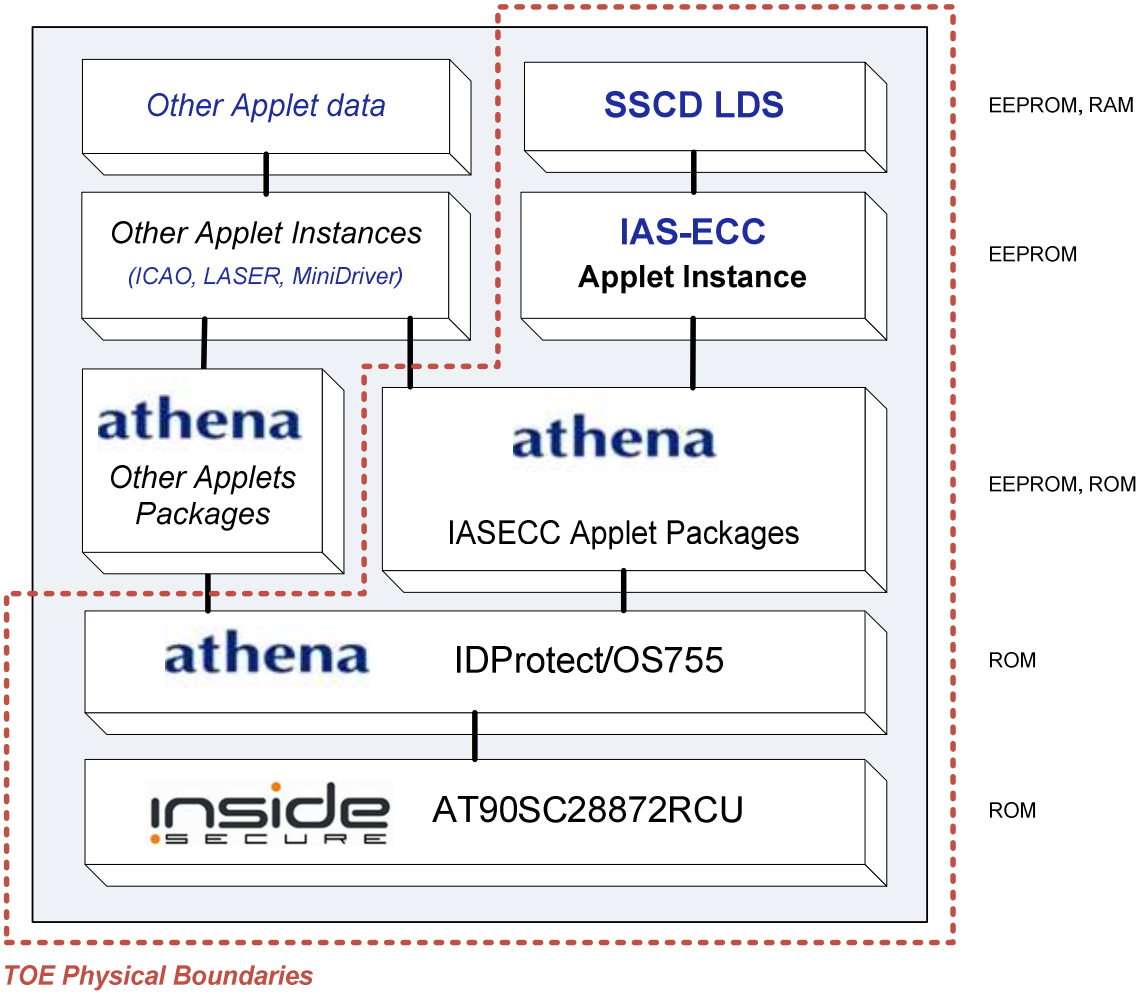

Figure 1 – Architecture du produit

1.2.4. 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 [BSI-PP-0005-2002] et [BSI-PP-0006-2002].

Il est illustré par la figure 2.

Le point de livraison est situé en fin de l'étape « *Integration* », marquant la fin de la phase de développement du produit.

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.

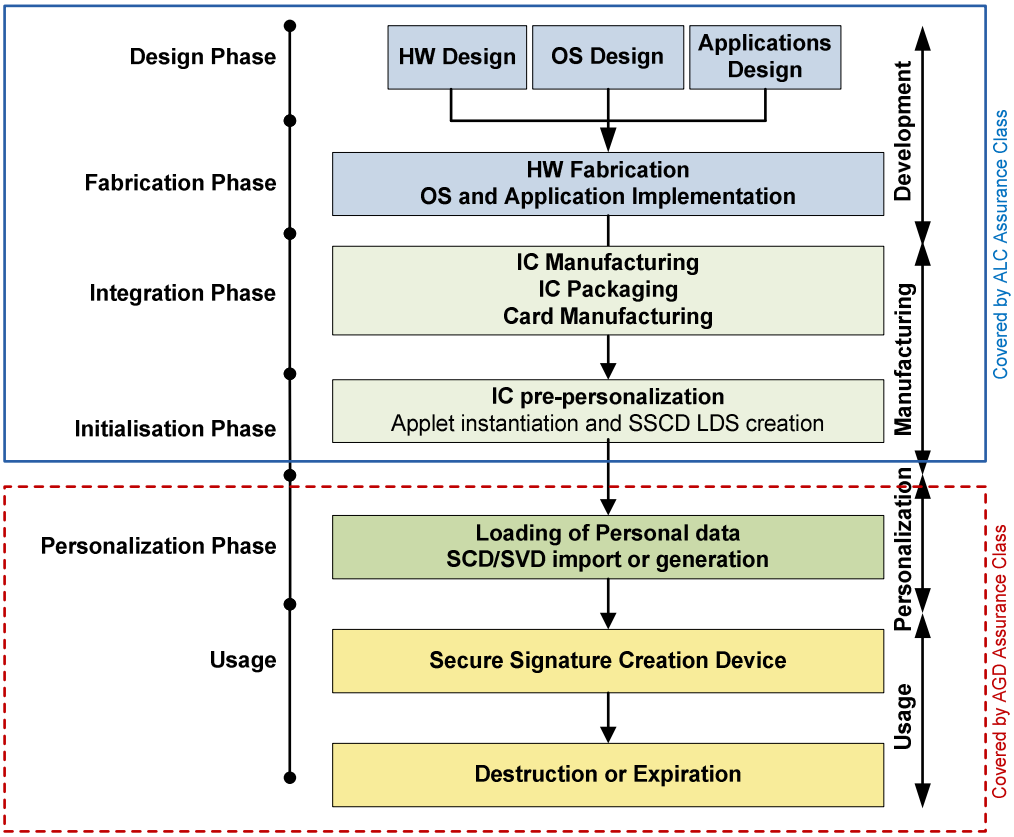

Figure 2 – Cycle de vie du produit

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.

20380 Town Center Lane – Suite 240
Cupertino CA95014
United States of America

Site n°2 de développement du logiciel (depuis le 11 janvier 2012)
Athena Smartcard Ltd.

The Alba Centre
Livingston EH54 7EG
Scotland - United Kingdom

Site n°3 de développement du logiciel (fermé au 11 janvier 2012)
Athena Smartcard Ltd.

Westpoint - 4 Redheughs Rigg - South Gyle
Edinburgh EH12 9DQ
Scotland - United Kingdom

Site de développement et fabrication du microcontrôleur Inside Secure.

Maxwell Building
Scottish Enterprise technology Park,
East Kilbride, G75 0QR
Scotland - United Kingdom

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le rôle « Administrateur » (« S.Admin ») et comme utilisateur du produit le rôle « Signataire » (« S.Signatory »), voir [ST] au §4.2 Subjects.

1.2.5. Configuration évaluée

Le certificat porte sur la configuration de la TOE obtenue en suivant le guide de préparation (cf. [GUIDES]). Ce guide décrit les options de personnalisation qui doivent être choisies afin d'obtenir la configuration évaluée de la TOE. D'autres options de personnalisation sont possibles mais ne correspondent pas à la configuration évaluée.

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 [CC IC] et [CC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC 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 du microcontrôleur « Atmel Smartcard ICs AT90SC28872RCU/AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [BSI-PP-0002-2001]. Ce microcontrôleur a été certifié le 4 décembre 2008 sous la référence [BSI-DSZ-CC-0421-2008] et maintenu le 8 janvier 2009 et le 4 avril 2009 sous les références respectives [BSI-DSZ-CC-0421-2008-MA-01] et [BSI-DSZ-CC-0421-2008-MA-02]. Le niveau de résistance de ce microcontrôleur a été confirmé dans le cadre de son processus de surveillance ;
- les résultats de l'évaluation 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, certifiée le 30 juin 2009 sous la référence [DCSSI-2009/11]. Le niveau de résistance de ce logiciel a été confirmé le 26 juillet 2011 dans le cadre de son processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 mars 2012, 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 le référentiel technique de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF-CRY] 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 était en dehors du périmètre de l'évaluation et n'a pas été analysé.

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 OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU » 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, 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. 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
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification 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 : - Athena OS755/ IDProtect v6 Java Card on Inside Secure AT90SC28872RCU Microcontroller embedding Athena IAS-ECC applet - Security Target, version 1.2, 22/03/2012, Athena Smartcard Solutions. Pour les besoins de publication, la cible de sécurité suivante a été fournie dans le cadre de cette évaluation : - Athena OS755/ IDProtect v6 Java Card on Inside Secure AT90SC28872RCU Microcontroller embedding Athena IAS-ECC applet – Public Security, version 1.2, 22/03/2012, Athena Smartcard Solutions.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: ATALANTE, version: 1.0, 30/03/2012, Thales.
[CONF]	Liste de configuration du produit : - Atalante - Documents Configuration List, version 0.3, 29/03/2012, Athena Smartcard Solutions.
[GUIDES]	Guide de préparation du produit : - IDProtect v6 – Manufacturer Manual, version 1.1, 26 March 2012, Athena Smartcard Solutions. - IDProtect v6 SSCD – Preparation Manual, version 1.2, 19 March 2012, Athena Smartcard Solutions. Guide d'opération du produit : - IDProtect v6 – IAS-ECC SSCD Operation manual, version 1.2, 19 March 2012, Athena Smartcard Solutions.
[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.*

[BSI-PP-0002-2001]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*
[BSI-DSZ-CC-0421-2008]	Certification report BSI-DSZ-CC-0421-2008 for Atmel Smartcard ICs AT90SC28872RCU/AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 from Atmel Corporation. *Certifié par le BSI le 4 décembre 2008.*
[BSI-DSZ-CC-0421-2008-MA-01]	Assurance Continuity Maintenance Report BSI-DSZ-CC-0421-2008-MA-01 for Atmel Smartcard ICs AT90SC28872RCU /AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 from Atmel Corporation. *Maintenu par le BSI le 8 janvier 2009.*
[BSI-DSZ-CC-0421-2008-MA-02]	Assurance Continuity Maintenance Report BSI-DSZ-CC-0421-2008-MA-02 for Atmel Smartcard ICs AT90SC28872RCU /AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 from Atmel Corporation. *Maintenu par le BSI le 6 avril 2009.*
[DCSSI-2009/11]	Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05. *Certifié par la DCSSI le 30 juin 2009 sous la référence DCSSI-2009/11.*

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.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr