



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-2012/43

**Athena IDProtect/OS755 Key version 9.1.2 avec
application IDSign sur composant AT90SC25672RCT-USB**

Paris, le 10 août 2012

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

Capitaine de vaisseau Dominique RIBAN
[ORIGINAL SIGNE]



Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense 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

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

Référence du rapport de certification

ANSSI-CC-2012/43

Nom du produit

**Athena IDProtect/OS755 Key version 9.1.2 avec application
IDSign sur composant AT90SC25672RCT-USB**

Référence/version du produit

- Athena IDProtect/OS755 Java Card : release date 0113, release level 2109
- Inside Secure AT90SC25672RCT-USB : AT58829, révision D
- Inside Secure Toolbox : version 00.03.11.05
- Athena IDSign : version 3.0, build 001, classe AID A0 00 00 01 64 49 44 53 69 67 6E 01

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

Développeur(s)

Athena Smartcard Inc.
20380 Town Center Lane – Suite 240
Cupertino CA95014, Etats-Unis

Inside Secure S.A.
Maxwell Building - Scottish Enterprise
technology Park, East Kilbride, G75 0QR,
Scotland, Grande-Bretagne

Commanditaire

Athena Smartcard Solutions
1-14-16, Motoyokoyama-cho, Hachioji-shi
Tokyo, 192-0063, Japon

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414
31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables



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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	8
1.2.3. <i>Architecture</i>	8
1.2.4. <i>Cycle de vie</i>	9
1.2.5. <i>Configuration évaluée</i>	11
2. L’EVALUATION	12
2.1. REFERENTIELS D’EVALUATION	12
2.2. TRAVAUX D’EVALUATION	12
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	13
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	13
3. LA CERTIFICATION	14
3.1. CONCLUSION.....	14
3.2. RESTRICTIONS D’USAGE.....	14
3.3. RECONNAISSANCE DU CERTIFICAT	15
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	15
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	15
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	16
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	17
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	19

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Athena IDProtect/OS755 Key version 9.1.2 avec application IDSign sur composant AT90SC25672RCT-USB ». Le produit est développé par la société Athena Smartcard Solutions et embarqué sur le microcontrôleur AT90SC25672RCT-USB développé par la société Inside Secure. Il peut prendre la forme d'une carte à puce ou d'une clé USB. Il 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 conforme aux profils de protection certifiés sous les références [BSI-PP-0005-2002] et [BSI-PP-0006-2002], adaptés à la version 3.1 des Critères Communs [CC] (ces PP ayant été rédigés selon la version 2.1).

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 du tableau ci-après, qui sont renvoyés par le produit suite à la commande GET DATA avec le tag 9F7F (voir [GUIDES], aux §2.5 et §2.6 du guide de préparation et au §1.1 du guide d'opération) :

Data Element	Length	Chip Serial Number or default
IC fabricator	2	'4180'
IC type	2	'0106'
Operating system identifier	2	'8211'
Operating system release date	2	'0113'
Operating system release level	2	'2109'
IC fabrication date	2	IC production date (SIH_2 & SIH_3)
IC serial number	4	Die number ('00'+ SIH_6 + SIH_7 + SIH_8)
IC batch identifier	2	Lot number (SIH_4 & SIH_5)
IC module fabricator	2	'0000'
IC module packaging date	2	'0000'
ICC manufacturer	2	'0000'
IC embedding date	2	'0000'
IC pre-personalizer	2	'00000000000000000000'
IC pre-personalization date	2	
IC pre-personalization equipment identifier	4	
IC personalizer	2	'00000000000000000000'
IC personalization date	2	
IC personalization equipment identifier	4	

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

- commande GET DATA avec tag **9F7F** envoyée :
 - o 00CA**9F7F**00 ;
- données renvoyées par le produit :
 - o 4180 0106 8211 **0113 2109** 0954 00233904 6598 0000 0000 0000 0000
 0000000000000000 0000000000000000

Dans ces données, on retrouve bien, en particulier, les valeurs **0113** et **2109** (correspondant aux champs « *Operating system release date* » et « *Operating system release level* » dans le tableau précédent). Ces éléments correspondent à l'ensemble du logiciel embarqué comprenant le système d'exploitation Athena ID Protect et l'application Athena ID Sign.

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

- commande GET DATA avec tag **0046** envoyée :
 - o 00CA**0046**00 ;
- données renvoyées par le produit :
 - o **2303**09546598231909

La valeur **23** donne l'identification du composant correspondant à la valeur du registre matériel SN_0 (soit AT90SC25672RCT-USB). Tandis que la valeur **03** donne la révision du composant correspondant à la valeur du registre matériel SN_1 (soit révision D).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- 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*) ;
- identification et authentification : 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 ;
- 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 (*Secure Signature Creation Device*), telles que la signature électronique, la génération des clés, l'import/export de SCD/SVD (*Signature Creation Data / Signature Verification Data*, soit les clé privée / clé publique de signature) et la vérification du RAD/PUK (*Reference Authentication Data / PIN Unblocking Key*, soit le code PIN et le code de déblocage du produit), sont soumises à ces vérifications ;
- 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 ;
- cryptographie : le produit offre des moyens cryptographiques à toutes les autres fonctions de sécurité (en particulier, DES/TDES, RSA, RNG, génération de nombres premiers) ;
- protection : le produit protège les données des fonctionnalités de sécurité, les données utilisateur et les fonctionnalités de sécurité 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. Le service de protection est également en charge d'assurer la terminaison du processus de chargement et d'installation du contenu de la carte ainsi que le chargement du correctif et sa terminaison.

1.2.3. Architecture

Le produit final peut prendre soit la forme d'une carte à puce, soit celle d'une clé USB, le composant sous-jacent AT90CS25672RCT-USB fournissant des interfaces matérielles ISO 7816 et USB.

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

Le logiciel applicatif est masqué dans la ROM, seuls des correctifs du système d'exploitation sont chargés en EEPROM.

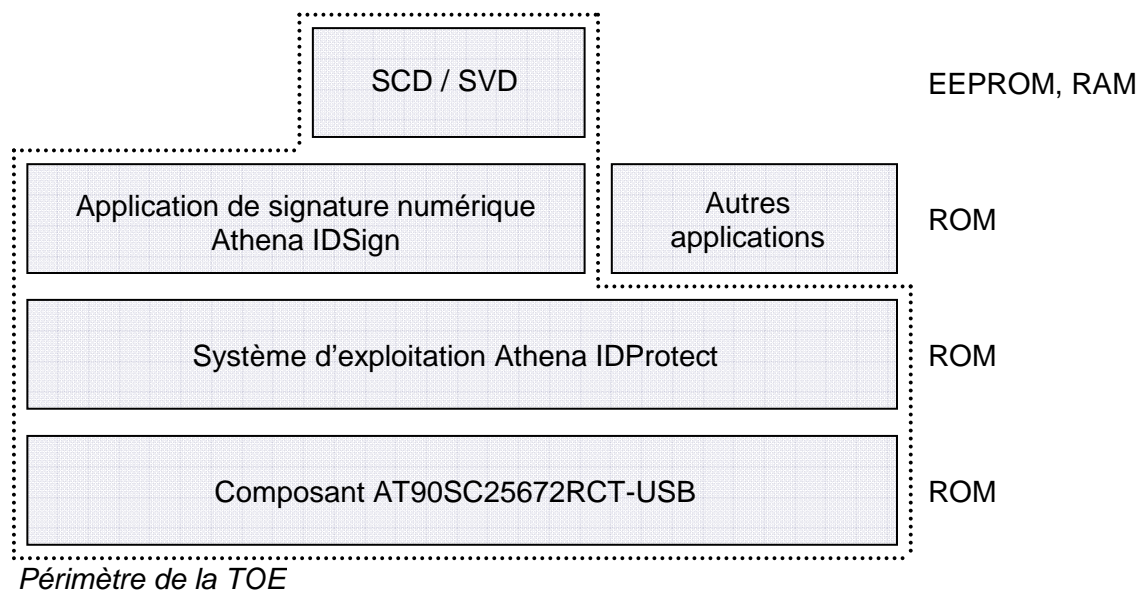
La TOE (*Target Of Evaluation* – cible d'évaluation) est constituée :

- du composant :
 - o INSIDE Secure AT90SC25672RCT-USB Microcontroller : AT58829, révision D, développé par Inside Secure ;
- adjoint de la bibliothèque cryptographique :
 - o INSIDE Secure Toolbox, version 00.03.11.05, développée par Inside Secure S.A. ;

- embarquant le système d'exploitation :
 - o Athena IDProtect 9.1.2, release Date '0113', release Level '2109', ROM code release Level '0109', EEPROM code Patch Level '2xxx' includes patches: PID01 to PID07, développé par Athena Smartcard ;
- et l'application :
 - o Athena IDSign, Applet class AID = A0 00 00 01 64 49 44 53 69 67 6E 01, version 3, Build 001, développée par Athena Smartcard.

Les autres applications ne sont pas instanciées et sont supprimées avant la phase de personnalisation.

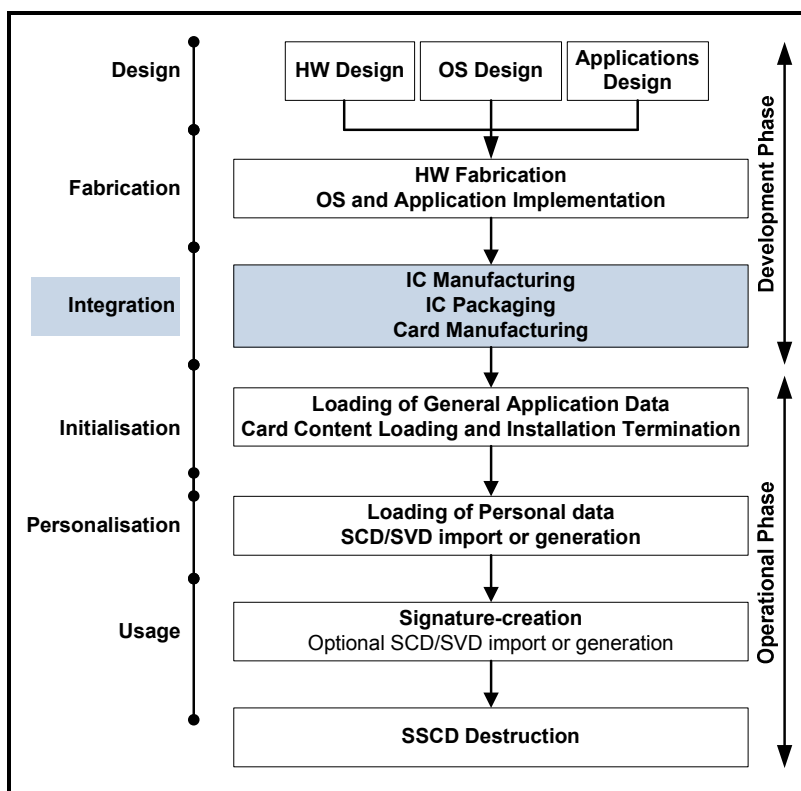
Le périmètre de la TOE est illustré par la figure suivante (contours en pointillé) :



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], mais raffiné par l'ajout de l'étape « *Integration* ».

Le cycle de vie du produit est illustré par la figure suivante :



Le point de livraison est situé en fin de l'étape « Intégration », 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.

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

- **Sites de développement du logiciel :**
 - **Athena Smartcard Ltd.**
Westpoint - 4 Redheughs Rigg - South Gyle
Edinburgh EH12 9DQ
Scotland – Grande Bretagne
 - **Athena Smartcard Inc.**
20380 Town Center Lane – Suite 240
Cupertino CA95014
Etats-Unis

- **Site de développement et fabrication du microcontrôleur**
 - **Inside Secure S.A.**
Maxwell Building
Scottish Enterprise technology Park,
East Kilbride, G75 0QR
Scotland – Grande Bretagne

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 (voir [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].

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 « Microcontrôleur sécurisé ATMEL AT90SC25672RCT-USB rev. D » au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection (voir [PPCR98_06]). Ce microcontrôleur a été certifié par l'ANSSI (voir [DCSSI-CC-2006_30]) le 19 décembre 2006.

Le niveau de résistance du microcontrôleur a été confirmé par l'ANSSI le 16 janvier 2012 dans le cadre du processus de surveillance (voir [SUR_IC]).

Cette évaluation a également pris en compte les résultats de la surveillance de la bibliothèque cryptographique « Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 » qui a été initialement certifiée au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 (voir [ANSSI-CC-2009_11] et [SUR_Biblio]).

Enfin, cette évaluation a pris en compte les résultats de l'évaluation des deux versions précédentes du produit. Cela avait donné lieu aux certificats [ANSSI-CC-2011_03] et [ANSSI-CC-2011_45].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 juillet 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 les référentiels techniques 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

L'analyse du générateur d'aléas du produit selon les référentiels techniques de l'ANSSI était en dehors du périmètre de l'évaluation et elle n'a pas été effectuée.

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 Key (Smartcard or USB token) version 9.1.2 - Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 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'accord¹, 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 signataire², 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 4+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedure
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	1	Identification of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claim
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended component definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specifications
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independant testing, sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none">- Athena IDProtect Key – Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB embedding IDSign applet Security Target, version 1.1, 02/12/2011, Athena Smartcard. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none">- Athena IDProtect Key – Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB embedding IDSign applet - Security Target Lite, version 1.1, 02/12/2011, Athena Smartcard.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- Evaluation technical report - Project: BOREALIS_M02, version: 2.0, 23/07/2012, Thales-CEACI.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none">- Borealis_M02 - Documents Configuration List – Borealis Project, version 2.0, 02/12/2011 Athena Smartcard.
[GUIDES]	<p>Guide de préparation du produit :</p> <ul style="list-style-type: none">- Preparative Procedures, Athena IDProtect Key version 1.0, 02/12/2011, Athena Smartcard.- Athena IDProtect Key, Card Administrator Manual, version 1.0, 02/12/2011, Athena Smartcard.- Athena IDProtect Transport Key Application Note version 0.2, 29/06/2010 Athena Smartcard. <p>Guide utilisateur :</p> <ul style="list-style-type: none">- Operational User Guidance, Athena IDProtect Key version 1.0, 02/12/2011, Athena Smartcard.

[BSI-PP-0005-2002]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0005-2002T.</i>
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002T.</i>
[PPCR98_06]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. <i>Certifié par l'ANSSI sous la référence PP/9806.</i>
[DCSSI-CC-2006_30]	Certificat ANSSI délivré le 19 décembre 2006 pour le produit : « Microcontrôleur sécurisé ATMEL AT90SC25672RCT-USB rev. D ».
[SUR_IC]	Lettre de poursuite de la surveillance émise par l'ANSSI le 16 janvier 2012 pour le produit : « Microcontrôleur sécurisé ATMEL AT90SC25672RCT-USB, rev. D » initialement certifié par l'ANSSI (voir [ANSSI-CC-2006_30]).
[ANSSI-CC-2009_11]	Certificat ANSSI délivré le 30 juin 2009 pour l'évaluation de la bibliothèque : « Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 ».
[SUR_Biblio]	Lettre de poursuite de la surveillance émise par l'ANSSI le 18 mars 2011 pour la bibliothèque : « Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 » initialement certifiée par l'ANSSI (voir [ANSSI-CC-2009_11]).
[ANSSI-CC-2011_03]	Certificat ANSSI délivré le 4 mars 2011 pour le produit : « SafeNet eToken (Smartcard or USB token) Version 9.1 - Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller embedding IDSign applet ».
[ANSSI-CC-2011_45]	Certificat ANSSI délivré le 22 Septembre 2011 pour le produit: « SafeNet eToken (Smartcard or USB token) Version 9.1.2 - Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet ».

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 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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr .