



*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-2012/82**

### **Athena IDProtect/OS755 avec application ICAO BAC sur composants SB23YR48/80B**

Athena IDProtect/OS755 Java Card on STMicroelectronics  
SB23YR80/48 Microcontrollers embedding ICAO BAC applet

*Paris, le 26 décembre 2012*

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

Patrick Pailloux  
[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](mailto:certification.anssi@ssi.gouv.fr)

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

Référence du rapport de certification

**ANSSI-CC-2012/82**

Nom du produit

**Athena IDProtect/OS755 avec application ICAO BAC sur  
composants SB23YR48/80B**

Référence/version du produit

- Athena IDProtect/OS755 Java Card : release date 0355, release level 0402
- Athena IDPass applet : version 3, correctif FA, build 2
- STMicroelectronics SB23YR48/80B: revision interne G
- STMicroelectronics NesLib: version 3.0

Conformité à un profil de protection

**BSI-CC-PP-0055-2009, [PP BAC], version 1.10**  
Machine Readable Travel Document with ICAO application, Basic Access Control

Critères d'évaluation et version

**Critères Communs version 3.1 révision 3**

Niveau d'évaluation

**EAL 4 augmenté**  
**ALC\_DVS.2**

Développeurs

**Athena Smartcard Solutions  
Inc.**  
20380 Town Center Lane – Suite 240  
Cupertino CA95014, U.S.A.

**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**  
30 avenue Gustave Eiffel, 33608 Pessac, 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
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> .....	7
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Cycle de vie</i> .....	9
1.2.5. <i>Configuration évaluée</i> .....	10
<b>2. L’EVALUATION .....</b>	<b>11</b>
2.1. REFERENTIELS D’EVALUATION .....	11
2.2. TRAVAUX D’EVALUATION .....	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LE REFERENTIEL TECHNIQUE DE L’ANSSI.....	11
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	11
<b>3. LA CERTIFICATION .....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS D’USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT .....	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	13
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>16</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la carte à puce « Athena IDProtect/OS755 avec application ICAO BAC sur composants SB23YR48/80B », développée par Athena Smartcard Solutions et STMicroelectronics.

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

- d'un des composants :
  - o SB23YR48/80B, révision interne G, développé par STMicroelectronics ;
- associés à la librairie cryptographique :
  - o NesLib, version 3.0, développée par STMicroelectronics ;
- embarquant le système d'exploitation :
  - o Athena IDProtect/OS755 Java Card, release date 0355, release level 0402, développé par Athena Smartcard Solutions ;
- et l'application :
  - o Athena IDPass applet, version 3, correctif FA, build 2 développée par Athena Smartcard Solutions.

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit mais ne sont pas actives dans la configuration évaluée.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à vérifier l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module ou d'inlay. Le produit final peut être un passeport, une carte plastique, etc.

## 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 au profil de protection [PP BAC]. Elle comprend la fonctionnalité additionnelle « *Active Authentication* ».

### 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 fabricant	2	'4750'
IC type	2	'0204' STM ST23YR80 '0205' STM ST23YR48
Operating system identifier	2	'8211'
Operating system release date	2	'0355' ('0' = 2010 + '355' = 21 December)
Operating system release level	2	'0402'
IC fabrication date	2	Test date (YDDD)
IC serial number	4	Serial number
IC batch identifier	2	Batch Number
IC module fabricant	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'

Après la sélection de l'applet IASECC, la commande GET DATA avec le tag '0003' (voir [GUIDES]) permet d'obtenir les éléments identifiant la version d'applet.

Les données renvoyées par le produit sont: 'FA030002', les valeurs 'FA03' et '0002' correspondant respectivement aux informations « *Applet version* » et « *Build number* ».

### 1.2.2. Services de sécurité

Les principaux services de sécurité évalués fournis par la TOE sont :

- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme BAC (« *Basic Access Control* ») ;
- la protection de l'intégrité et de la confidentialité des données lues à l'aide du mécanisme « *secure messaging* » ;
- l'authentification du microcontrôleur par le mécanisme optionnel AA (« *Active Authentication* »).

### 1.2.3. Architecture

L'architecture du produit est résumée par la figure ci-après.

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

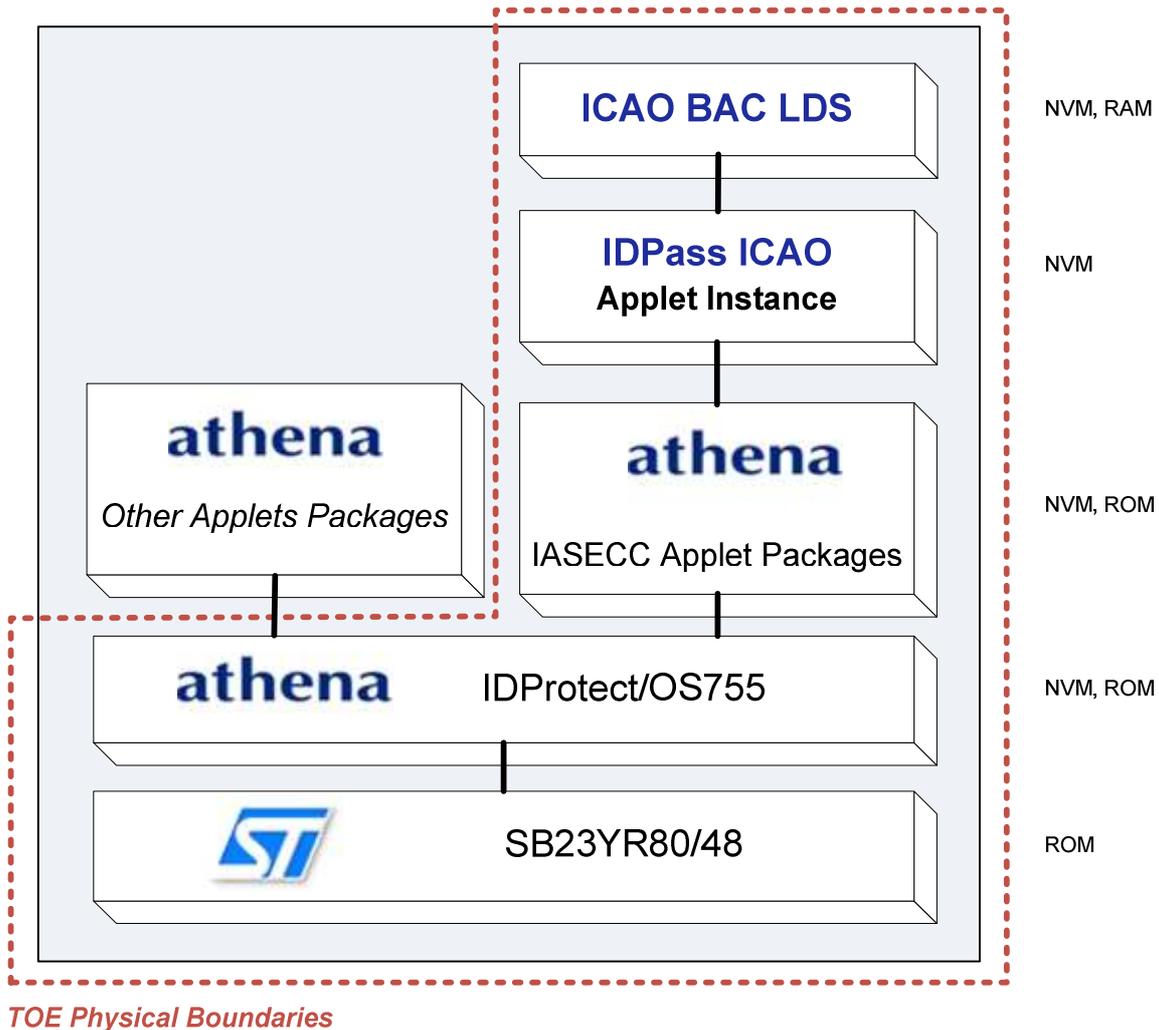


Figure 1 – Architecture du produit

Le produit est une carte à puce constituée :

- du microcontrôleur SB23YR48B ou SB23YR80B en révision interne G avec librairie cryptographique NesLib v3.0, développé et fabriqué par STMicroelectronics ;
- de la plateforme logicielle Java Card IDProtect/OS755 développée par Athena Smartcard Solutions et masquée dans la ROM du microcontrôleur ;
- du code correctif (« patch ») de la plateforme, développé par Athena Smartcard Solutions et chargé en EEPROM ;
- des packages de l'applet IASECC développés par Athena Smartcard Solutions et masqués dans la ROM du microcontrôleur ;
- du code correctif de l'applet IASECC, développé par Athena Smartcard Solutions et chargé en EEPROM ;
- de l'instance IDPass ICAO créée en EEPROM lors de la pré-personnalisation ;
- des données ICAO BAC LDS chargées en EEPROM lors de la personnalisation et temporairement en RAM lors de l'utilisation ;
- des packages d'autres applets masqués en ROM, situées en dehors du périmètre de l'évaluation et non actives dans la configuration évaluée.

### 1.2.4. Cycle de vie

Le cycle de vie du produit (figure 2) est basé sur celui du Profile de Protection référencé [PP BAC], mais raffiné dans la phase 2 « *Manufacturing* » par l'interversion des étapes 4 et 5 qui deviennent respectivement « *Pré-personnalisation* » et « *Packaging* ».

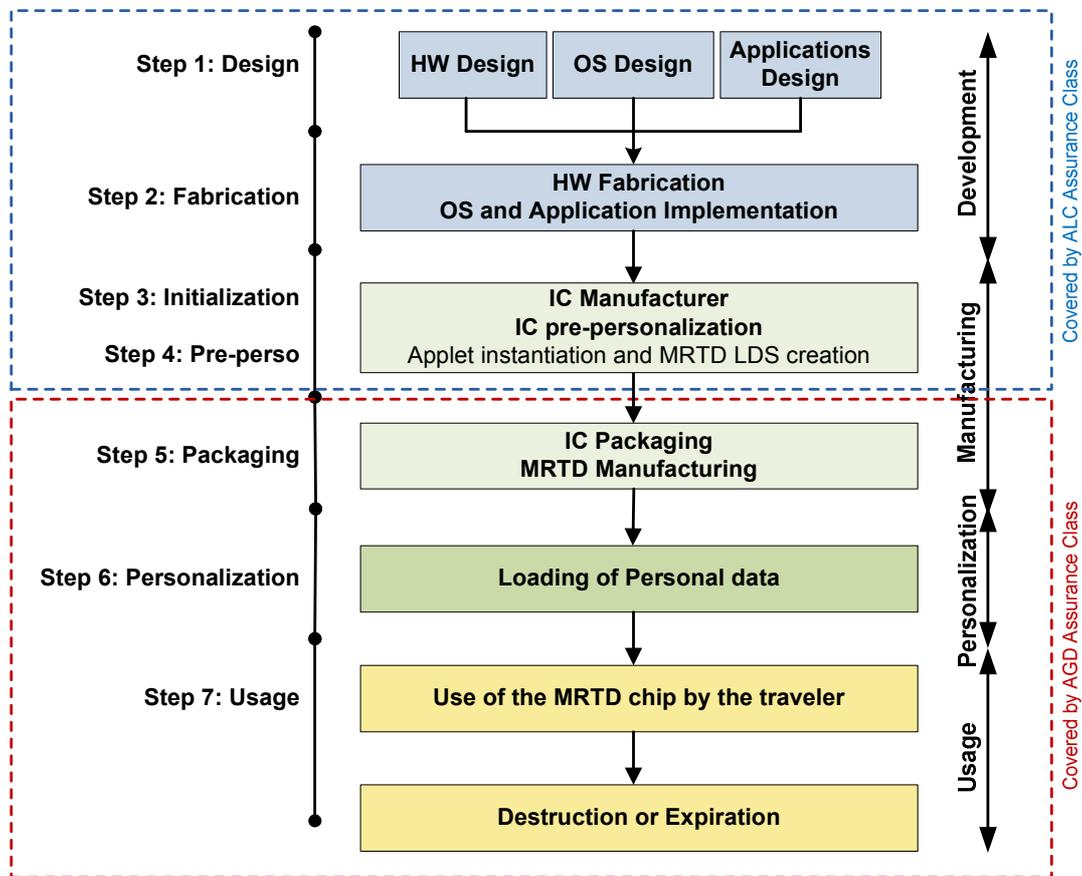


Figure 2 – Cycle de vie du produit

Le point de livraison est situé en fin de l'étape 4 « *Pré-perso* », marquant la fin de la construction 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.

Les codes correctifs de la plateforme et de l'applet sont chargés par STMicroelectronics lors de l'étape 2 « *Fabrication* ». La création de l'instance IDPass ICAO est réalisée par STMicroelectronics lors de l'étape 4 « *Pré-personnalisation* ».

Les étapes 6 « *Personalization* » et 7 « *Usage* » ont été prises en compte durant l'évaluation au travers des guides (au titre d'AGD). Les tests ont porté sur les fonctionnalités du produit disponibles lors des étapes 6 « *Personalization* » et 7 « *Usage* », (au titre des classes ATE et 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  
STMicroelectronics.**

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

Les composants sont développés et fabriqués par STMicroelectronics. Les sites de développement et de fabrication des puces STMicroelectronics sont détaillés dans le rapport de certification référencé [2010/02].

Les « administrateurs du produit » sont les nations ou organisations émettrices du document de voyage.

Les « utilisateurs du produit » sont les voyageurs et les systèmes d'inspection pendant la phase d'utilisation.

### ***1.2.5. Configuration évaluée***

Le certificat porte sur l'application IDPass en configuration ICAO BAC associée à la plateforme IDProtect/OS755, masquées sur le microcontrôleur SB23YR48B ou SB23YR80B en révision interne G avec librairie cryptographique NesLib v3.0 et telles que présentées plus haut, au paragraphe 1.2.3.

Le produit peut être personnalisé selon différentes configurations.

Le certificat porte sur la configuration suivante :

- mécanisme BAC activé ;
- mécanisme « *Active Authentication* » activé (ECC ou RSA).

Le produit évalué a été fourni au CESTI en mode développement, c'est-à-dire que le chargement des codes correctifs de la plateforme et de l'applet ainsi que l'instanciation de l'applet ont été réalisés par Athena Smartcard Solutions et non par STMicroelectronics. Athena Smartcard Solutions a fourni au CESTI le fichier de chargement EEPROM (codes correctifs) ainsi que les scripts de pré-personnalisation (instanciation de l'applet) livrés à STMicroelectronics.

## 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 [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 [2010/02]. Le niveau de résistance de ces microcontrôleurs, maintenus le 8 juillet 2010 sous la référence [2010/02-M02], a été confirmé dans le cadre de leur processus de surveillance le 27 septembre 2012.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 13 septembre 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] 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 IDProtect/OS755 avec application ICAO BAC 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 EAL 4 augmenté du composant ALC\_DVS.2.

### 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<sup>1</sup>, 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 :



---

<sup>1</sup> 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<sup>1</sup>, 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 :



---

<sup>1</sup> 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 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



<b>AVA</b> <b>Estimation des</b> <b>vulnérabilités</b>	AVA_VAN	1	2	2	3	4	5	5	3	Focused 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"> <li>- IDPass ICAO BAC - Security Target Athena IDProtect/OS755 Java Card on STMicroelectronics ST23YR48/80 Microcontroller embedding Athena IDPass applet, version 3.1, 06/09/2012, Athena Smartcard Solutions.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- IDPass ICAO BAC - Security Target Lite Athena IDProtect/OS755 Java Card on STMicroelectronics ST23YR48/80 Microcontroller embedding Athena IDPass applet, version 3.1, 06/09/2012, Athena Smartcard Solutions.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation technical report - Project: CASSIOPE2, version: 2.0, 13/09/2012, Serma Technologies.</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- Cassiope2 - Documents Configuration List, version 1.0, 6 September 2012, Athena Smartcard Solutions.</li> </ul>
[GUIDES]	<p>Guide de préparation du produit :</p> <ul style="list-style-type: none"> <li>- IDPass ICAO – Manufacturer Manual, version 2.1, 27 August 2012, Athena Smartcard Solutions.</li> <li>- IDPass ICAO BAC – Preparation Manual, version 3.1, 27 August 2012, Athena Smartcard Solutions.</li> </ul> <p>Guide d'opération du produit :</p> <ul style="list-style-type: none"> <li>- IDPass with corrective P4FA – ICAO BAC Operation manual, version 3.1, 27 August 2012, Athena Smartcard Solutions.</li> </ul>
[PP BAC]	<p>Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, 25 Mars 2009. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0055-2009.</i></p>
[PP0035]	<p>Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der</i></p>



	<i>Informationstechnik) sous la référence BSI-PP-0035-2007.</i>
[2010/02]	« Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » <i>Certifié par l'ANSSI le 10 février 2010 sous la référence ANSSI-CC-2010/02.</i>
[2010/02-M02]	Rapport de maintenance ANSSI-2010/02-M02, délivré le 8 juillet 2010, relatif au certificat ANSSI-CC-2010/02.

### Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</p>
[CC]	<p>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.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation :          Evaluation Methodology,          July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</p>
[JIWG AP]	<p>Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.</p>
[COMP]	<p>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.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF]	<p>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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p> <p>Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p> <p>Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_3), voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>