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-2010/60

Carte ASEPCOS-TS/CNS, version 1.82, build 0003

Paris, le 8 décembre 2010

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

Signé : Patrick Pailloux, Directeur général de l'ANSSI

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-2010/60

Nom du produit

Carte ASEPCOS-TS/CNS, version 1.82, build 0003

Référence/version du produit

- **Système d'exploitation ASEPCOS, avec application de signature électronique TS/CNS : v1.82, build 0003**
- **Microcontrôleur ST23YR48/ST23YR80 : révision B, configuration SB**
- **Librairie cryptographique NesLib : v3.0**

Conformité à un profil de protection

[BSI-PP0005-2002]: SSCD Type 2 Version 1.04

[BSI-PP0006-2002]: SSCD Type 3 Version 1.05

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

AVA_VAN.5

Développeur(s)

Athena Smartcard Ltd.
Westpoint, 4 Redheughs Rigg, South Gyle, Edinburgh EH12 9DQ, Ecosse, Royaume-Uni

STMicroelectronics
Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Commanditaire

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

Centre d'évaluation

THALES - CEACI (T3S – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.com

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 ASEPCOS-TS/CNS, version 1.82, build 0003 ». Il est constitué du microcontrôleur de STMicroelectronics STST23YR48/ST23YR80, révision B, configuration SB avec la librairie cryptographique NesLib, v3.0. Ce microcontrôleur embarque le système d'exploitation « ASEPCOS » avec l'application de signature électronique « TS/CNS », version 1.82, build 0003, développé par Athena Smartcard Ltd.

La cible d'évaluation (ou TOE pour « *Target Of Evaluation* ») est une carte à puce destinée à être utilisée comme dispositif sécurisé de création de signature électronique (SSCD) de types 2 et 3. Elle est munie des interfaces suivantes :

- interface contact ISO/IEC 7816 ;
- interface sans-contact ISO/IEC 14443 ;
- interface SOIC-8 compatible avec ISO 9141 ;
- interface QNF-44 compatible avec JEDEC.

1.2. Description du produit

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

Sa conformité par rapport au profil de protection [BSI-PP-0005-2002] – SSCD type 2 – et [BSI-PP-0006-2002] - SSCD type 3 est de type « démontrable ». En effet, la cible a été écrite en suivant les règles des CCv3.1 alors que les profils de protection sont écrits en suivant les règles des CC V2.1.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Les valeurs permettant d'identifier la version certifiée du produit sont définies dans les guides utilisateurs et administrateurs du produit (Cf. [GUIDES], en particulier au §3.1.2 de [SAG_AGD_Gen] et §2.1 de [SAG_AGD_USR].

Tag	Donnée	Longueur	Valeur
011B	Fabriquant du microcontrôleur	1	0x02
	Type de microcontrôleur	2	0xB214 (Product ID)
0118	Identifiant du système d'exploitation	10	0x910C 2568 EC62 7FCF D4B7
0116	Numéro de version du système d'exploitation	2	0x0182
0117	Numéro de construction du système d'exploitation	2	0x3003

Il est également possible d'identifier la librairie cryptographique de STMicroelectronics embarquée dans la carte (Neslib V3.0) via le tag 0x011F. La valeur attendue est 0000000000001300.

1.2.2. Services de sécurité

Les principaux services de sécurité[1] fournis par le produit sont (voir [ST] pour plus de détails) :

- le contrôle des droits lors des opérations (SF.Access Control) ;
- l'identification et l'authentification des utilisateurs (SF.Identification and Authentication) ;
- la création de la signature (SF.Signature Creation) ;
- le canal de communication sécurisé (SF.Secure Messaging) ;
- le service cryptographique (SF.Crypto) ;
- la protection des données utilisateurs et des fonctionnalités sécuritaires de la TOE (SF.Protection).

[1] La définition des services de sécurité de la TOE provient de la version 2.3 des Critères Communs qui a été utilisée lors des évaluations des précédentes versions de la carte.

1.2.3. Architecture

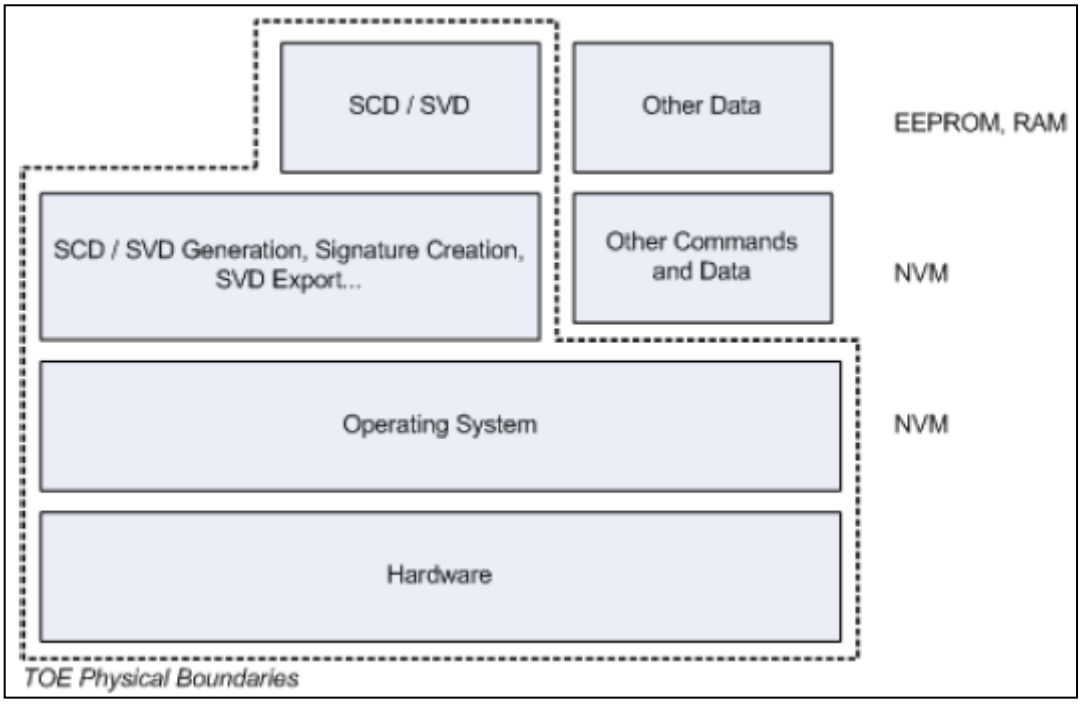
Le produit est une carte à puce constituée :

- du matériel :
  - le microcontrôleur de STMicroelectronics STST23YR48/ST23YR80, révision B, configuration SB ;
  - la librairie cryptographique NesLib, v3.0.
- du logiciel embarqué :
  - le système d'exploitation « ASEPCOS » ;
  - l'application de signature électronique « TS/CNS », version 1.82, build 0003, développé par Athena Smartcard Ltd. ;
  - les données correspondantes telles que SCD/SVD (données de création et de vérification de signature) ;
  - d'autres commandes et données associées mais qui sont en dehors du périmètre de l'évaluation.

Le produit propose les interfaces suivantes :

- une interface contact ISO/IEC 7816 ;
- une interface sans-contact ISO/IEC 14443 ;
- une interface SOIC-8 compatible avec ISO 9141 ;
- une interface QNF-44 compatible avec JEDEC.

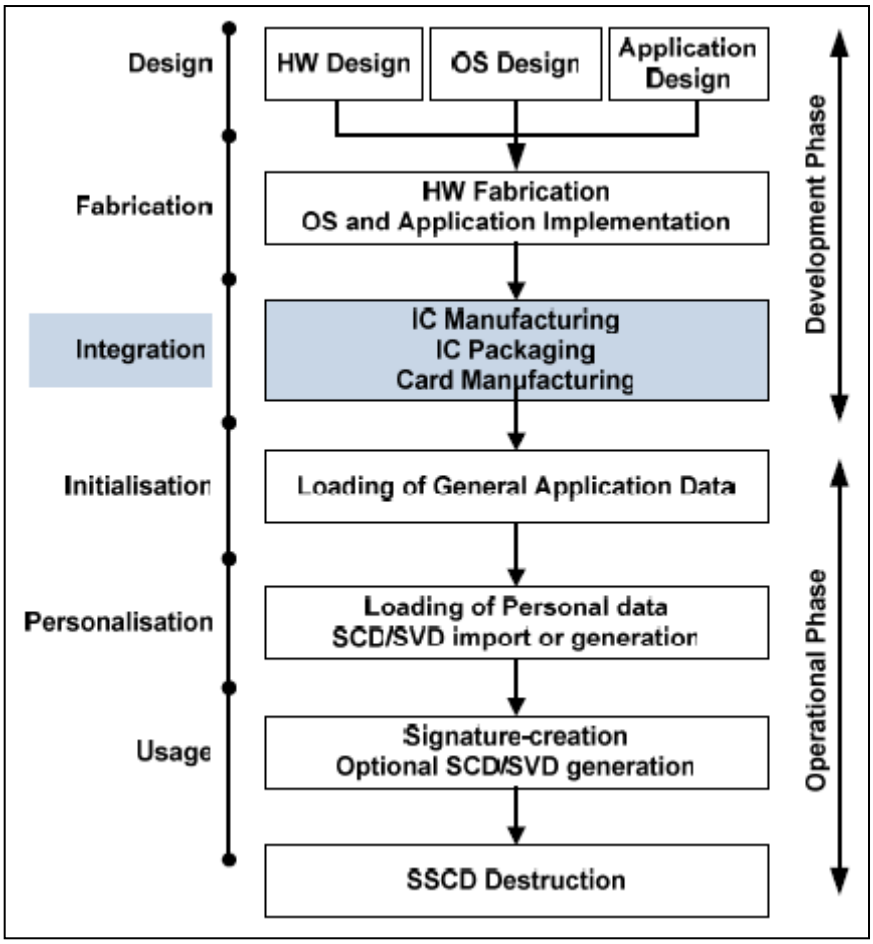
L'architecture du produit est résumée dans la figure suivante :



1.2.4. Cycle de vie

Le cycle de vie du produit est basé sur celui général de la carte à puce tel que décrit dans les profils de protection visés par la [ST], un raffinement a été effectué pour préciser que la phase d'intégration est couverte par les [GUIDES] du produit.

La figure suivante présente une vue globale de ce cycle de vie :



L'évaluation a couvert les phases de conception et de fabrication de la TOE, en réutilisant les résultats de l'évaluation du microcontrôleur pour ce qui concerne ses phases de conception et de fabrication.

Une fois que la TOE a été fabriquée, elle met en œuvre ses mécanismes d'autoprotection pour assurer la sécurité de la phase de transport.

Les phases d'intégration, d'initialisation et de personnalisation ont été évaluées au travers des [GUIDES] du produit.

Le produit testé est celui livré en phase d'utilisation.

Le produit a été développé sur le site suivant :

Athena Smartcard Ltd. (développement du logiciel embarqué)

Westpoint, 4 Redheughs Rigg, South Gyle
Edinburgh EH12 9DQ, Ecosse
Royaume-Uni

STMicroelectronics, Smartcard IC division (développement du microcontrôleur)

190 Avenue Célestin Coq
13106 Rousset Cedex
France

Pour l'évaluation, l'évaluateur a considéré comme :

- « administrateur du produit », le rôle d'administrateur décrit dans les guides. Il est en charge d'initialiser et de personnaliser le produit, ou d'exécuter des fonctions d'administration sur le produit ;
- « utilisateur du produit », le signataire et porteur du produit décrit dans les guides.

Les guides [GUIDES / SAG_AGD_Gen et SAG_AGD_Ded] sont dédiés à l'administrateur du produit, tandis que le guide [GUIDES / SAG_AGD_USR] est dédié à l'utilisateur.

1.2.5. Configuration évaluée

Le certificat porte sur la configuration personnalisée de la TOE qui est obtenue en suivant les guides administrateur [GUIDES / SAG_AGD_Gen et SAG_AGD_Ded], notamment ce second guide (SAG_AGD_Ded) qui décrit toutes les options de personnalisation qui doivent être sélectionnées pour obtenir la configuration évaluée.

D'autres options de configuration sont également décrites, en particulier dans le premier guide (SAG_AGD_Gen) ; cependant, elles ne correspondent pas à la configuration évaluée. Par exemple, des commandes biométriques y sont décrites mais elles ne sont pas dans le périmètre de l'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [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.

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 « 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 [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié par l'ANSSI (cf. [ANSSI-CC-2010_02]).

Par ailleurs, l'évaluation a également réutilisé les résultats d'évaluation de la version précédente du produit intitulée «Carte ASEPCOS-TS/CNS DI, Version 1.81, Build 003 Système d'exploitation ASEPCOS avec application de signature électronique TS/CNS embarqué sur le microcontrôleur AT90SC12872RCFT», qui a été certifié par l'ANSSI (cf. [ANSSI-CC-2010_05]) et dont le certificat a fait l'objet d'une maintenance par l'ANSSI (cf. [ANSSI-CC-2010-05-M01]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 septembre 2010, 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 par rapport aux référentiels techniques de l'ANSSI (cf. [RGS]) n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités exploitables pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

La conformité du générateur d'aléas du produit par rapport aux référentiels techniques de l'ANSSI (cf. [RGS]) n'a pas été vérifiée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités exploitables pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que la « carte ASEPCOS-TS/CNS, version 1.82, build 0003», développée par Athena Smartcard Ltd. et soumise 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 :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la Grèce, l'Italie, la France, 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**	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 : - ASE / ASEPCOS-TS/CNS STMicroelectronics Security Target version 1.1 Athena Smartcard Ltd. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ASEPCOS-TS/CNS STMicroelectronics Public Security Target version 1.1
[RTE]	Rapport technique d'évaluation : - SAG_ETR version: 1.0, 15/09/2010 Thales CEACI (T3S-CNES)
[CONF]	Liste de configuration : - ASEPcos-CNS (ROM) Binary Configuration List version 2.0 Athena Smartcard Ltd. - ASEPcos-CNS (ROM) Scripts Configuration List version 2.0 Athena Smartcard Ltd. - ASEPcos-CNS (ROM) Source Configuration List version 2.1 Athena Smartcard Ltd. - ASEPCOS-TS/CNS STMicroelectronics Document Configuration List version 2.3 Athena Smartcard Ltd.
[GUIDES]	Guide de préparation du produit : - ASEPCOS-TS/CNS STMicroelectronics V1.82 Card Reference Manual: o Part 1: Generic Guidance version 1.1 o Part 2: Dedicated Guidance version 1.0 Athena Smartcard Ltd. Guide d'opération du produit : - ASEPCOS-TS/CNS STMicroelectronics V1.82 User Guidance version 1.1 Athena Smartcard Ltd.
[BSI-PP0005-2002]	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.*

[BSI-PP0006-2002]	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-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[ANSSI-CC-2010_02]	Certificat ANSSI délivré le 10 février 2010 pour le produit : « Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB »
[ANSSI-CC-2010_05]	Certificat ANSSI délivré le 15 janvier 2010 pour le produit : » Carte ASEPCOS-TS/CNS DI, Version 1.81, Build 003 Système d'exploitation ASEPCOS avec application de signature électronique TS/CNS embarqué sur le microcontrôleur AT90SC12872RCFT »
[ANSSI-CC-2010-05-M01]	Rapport de maintenance ANSSI délivré le 8 mars 2010 pour le produit : » Carte ASEPCOS-TS/CNS DI, Version 1.81, Build 003.A Système d'exploitation ASEPCOS avec application de signature électronique TS/CNS embarqué sur le microcontrôleur AT90SC12872RCFT »

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.
[RGS]	Référentiel Général de Sécurité (RGS), version 1.0 – Documents concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité. voir www.ssi.gouv.fr.