



PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2009/41

Carte ASEPCOS-TS/CNS DI Système d'exploitation ASEPCOS avec application de signature électronique TS/CNS embarqué sur le microcontrôleur AT90SC12872RCFT

Paris, le 6 octobre 2009

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

[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 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-2009/41	
Nom du produit	Carte ASEPCOS-TS/CNS DI	
Référence/version du produit	ASEPCOS Version 1.80 Build 003 sur AT90SC12872RCFT référence AT58803 rev. M avec la bibliothèque Toolbox Version 00.03.11.05	
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 2.3 conforme à la norme ISO 15408:2005	
Niveau d'évaluation	EAL 4 augmenté AVA_MSU.3, AVA_VLA.4	
Développeurs	Athena Smartcard Solutions, Inc. Regus House, 10 Lochside Place, Edinburgh Park, Edinburgh, EH12 9RG, Ecosse, Royaume-Uni	ATMEL Secure Products Division Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR - Ecosse, Royaume-Uni
Commanditaire	Athena Smartcard Solutions, Inc. 1-14-16, Motoyokoyama-cho, Hachioji-shi, Tokyo, 192-0063, Japon	
Centre d'évaluation	CEACI (Thales Security Systems – CNES) 18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France Tél : +33 (0)5 61 28 16 51, mél : ceaci@cnes.fr	
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, publié au Journal officiel de la République française. 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 EVALUE	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>	8
1.2.5. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION.....	10
2.2. TRAVAUX D’EVALUATION	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	10
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE.....	11
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	12
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte ASEPCOS-TS/CNS, constituée d'une part du composant AT90SC12872RCFT rev. M pourvu de la bibliothèque logicielle *Toolbox* version 00.03.11.05, développé par ATMEL Secure Products Division, et d'autre part du système d'exploitation « ASEPCOS » avec application de signature électronique « TS/CNS », développé par Athena Smartcard Solutions, Inc. La référence du logiciel embarqué est ASEPCOS-TS/CNS version 1.80 Build 003.

Le produit est une carte à puce destinée à être utilisée comme dispositif sécurisé de création de signature électronique (SSCD) de type 2 et 3. Elle est munie d'une interface contact ISO/IEC 7816 et d'une interface sans-contact ISO/IEC 14443.

1.2. Description du produit évalué

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 suivants :

- « Secure Signature-Creation Device Type 2 Version: 1.04 » de référence BSI-PP-0005-2002 (cf. [PP0005]) ;
- « Secure Signature-Creation Device Type 3 Version: 1.05 » de référence BSI-PP-0006-2002 (cf. [PP0006]).

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 en utilisant la commande « Get Data ». Les informations d'identification sont les suivantes :

- Système d'exploitation ASEPCOS avec l'application TS/CNS, version 1.80 Build 003 :
 - o *Operating system identifier*: 9108 1768 AC62 7FC7 D5B6 ;
 - o *Operating system version number*: 0x0180 ;
 - o *Operating system build number*: 0x3003.
- Composant : AT90SC12872RCFT rev. M :
 - o *Chip platform fabricator*: 0x1F
 - o *Chip platform type*: 0x001F ;
 - o *IC information (version/date/batch/serial number)* dont le premier octet 0x0C identifie la révision M du composant ;
 - o *Crypto HW & library (toolbox) version*: 0000 0101 0003 1105.

Les valeurs assignées à ces identifiants sont définies dans les guides utilisateurs et administrateurs du produit (Cf. [GUIDES]).



1.2.2. Services de sécurité

Le produit ASEPCOS-TS/CNS met en œuvre les fonctions de sécurité requises au titre de la signature électronique et propose leur usage uniquement au travers de canaux de communication sécurisés. Le logiciel implémente la fonction de « dispositif sécurisé de création de signatures » (SSCD) qui permet la génération et l’importation de données de création de signatures (SCD), de vérification de signatures (SVD) et la création de signatures électroniques qualifiées. Le produit protège les SCD et restreint leur usage aux seuls signataires autorisés.

1.2.3. Architecture

Le produit est une carte à puce constituée :

- du composant AT90SC12872RCFT rev. M avec sa bibliothèque logicielle cryptographique ;
- du système d’exploitation ASEPCOS ;
- de l’application de signature électronique TS/CNS avec ses données ;
- d’autres commandes en dehors du périmètre de l’évaluation.

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

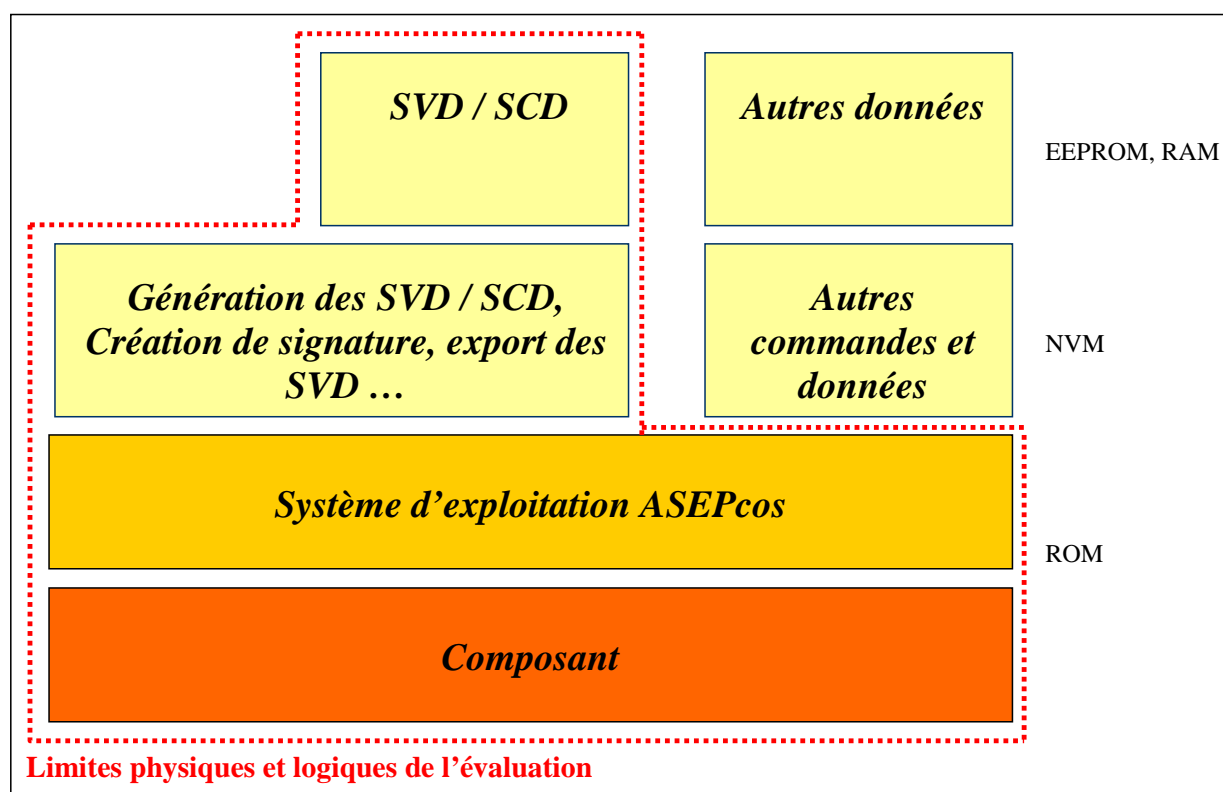


Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

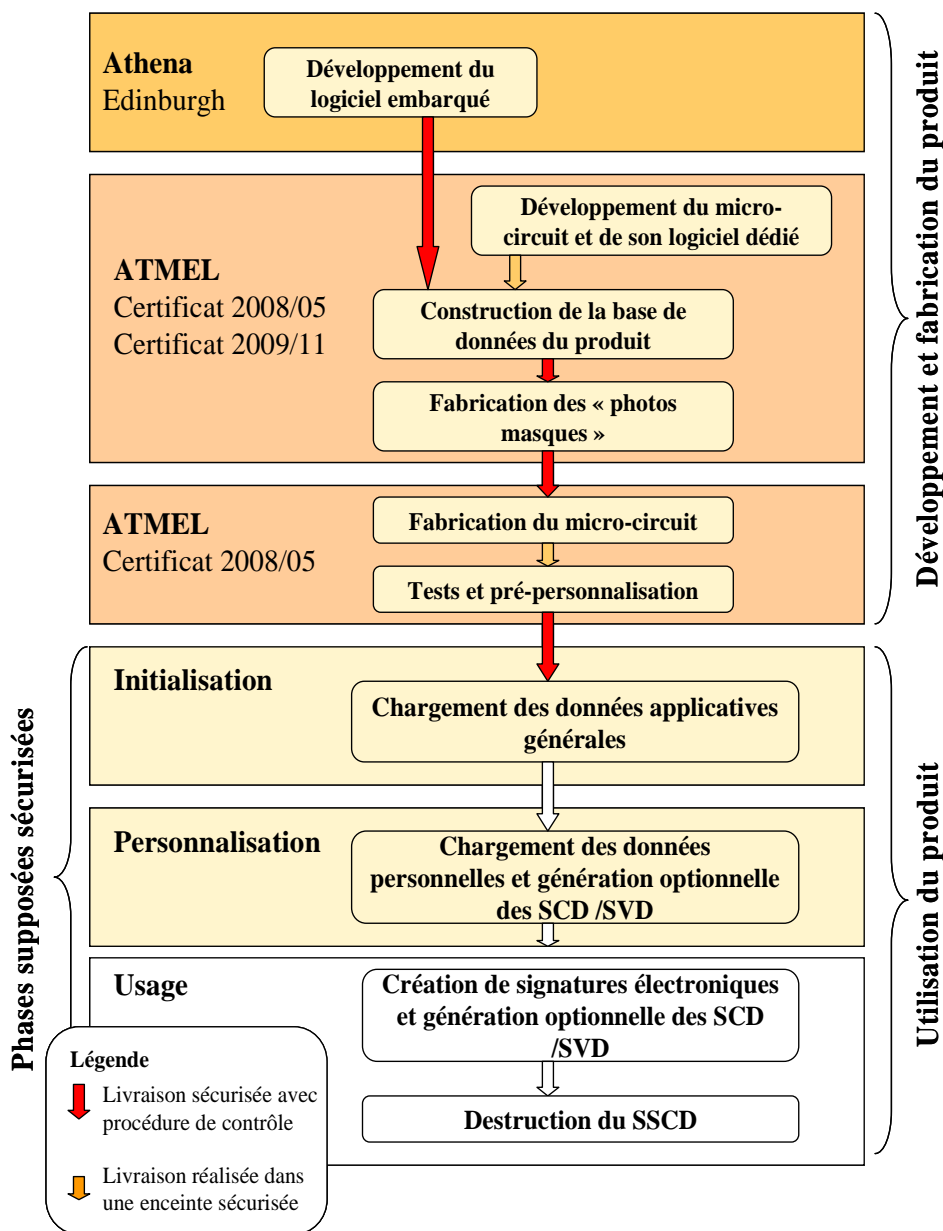


Figure 2 – Cycle de vie du produit

Le logiciel embarqué a été développé sur le site d’Athena Smartcard Solutions à Edimbourg :

Athena Smartcard Solutions

Regus House, 10 Lochside Place, Edinburgh Park,
Edinburgh, EH12 9RG,
Ecosse, Royaume-uni



Le composant et sa bibliothèque logicielle cryptographique ont été développés par Atmel Secure Products Division :

Atmel Secure Products Division

Maxwell Building, Scottish Enterprise technology Park, East Kilbride
Glasgow G75 0QR,
Ecosse, Royaume-uni

1.2.5. Configuration évaluée

Le certificat porte sur les fonctionnalités suivantes du produit :

- contrôle d'accès ;
- identification et authentification ;
- création de signatures ;
- communications sécurisées (*secure messaging*) ;
- implémentation de la cryptographie ;
- protection des biens sensibles.

En regard du cycle de vie, le produit évalué est celui qui sort de la phase de fabrication, tests et pré-personnalisation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par l'ANSSI et compatibles avec le document [AIS 34], 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 muni de sa bibliothèque cryptographique, tous deux déjà certifiés par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « AT90SC12872RCFT rev M » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP9806]. Ce microcontrôleur a été certifié le 27 février 2008 sous la référence DCSSI-2008/05 (cf. [2008/05]). Une surveillance de ce composant a également été réalisée avec succès en novembre 2008.

Les résultats de l'évaluation indépendante de la bibliothèque cryptographique *Toolbox* en version 00.03.11.05, qui ont conduit à la certification de référence DCSSI-2009/11 (cf. [2009/11]), ont aussi été pris en compte.

L'évaluation s'appuie également sur les résultats d'évaluation du produit ASEPCos-CNS/CIE en version 1.72 Build 004 certifié le 26 mars 2009 sous la référence DCSSI-2009/04 (cf. [2009/04]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 septembre 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY], [REF-CLE] et [REF-AUT] n'a pas été réalisée par l'ANSSI.

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 « Carte ASEPCOS-TS/CNS DI » 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.

Les conclusions de l'évaluation (cf. §8 du rapport technique d'évaluation [RTE]) mettent en garde l'administrateur du produit évalué au regard de la configuration créée qui doit être conforme à la configuration évaluée, par le respect des guides d'administration, en particulier vis-à-vis des choix de certains paramètres liés à la sécurité qui sont choisis durant la personnalisation.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation 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 1999 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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'Espagne, la Finlande, la France, la Grèce, 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 signataires¹, 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
ACM Gestion de configuration	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	2	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	1	1	1	2	3	3	4	2	Fully defined external interfaces
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	1	Subset of the implementation of the TSF
	ADV_INT					1	2	3		
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	1	Informal correspondence demonstration
	ADV_SPM				1	3	3	3	1	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Support au cycle de vie	ALC_DVS			1	1	1	2	2	1	Indentification of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	1	Testing: high-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annexe 2. Références documentaires du produit évalué

[2009/11]	Rapport de certification DCSSI-2009/11 – Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05, 30 juin 2009, SGDN/DCSSI
[2009/04]	Rapport de certification DCSSI-2009/04 - Carte ASEPCOS-CNS/CIE : composant AT90SC12872RCFT masqué par le logiciel ASEPCOS-CNS/CIE avec application de signature électronique, 26 mars 2009, SGDN/DCSSI
[2008/05]	Rapport de certification DCSSI-2008/05 - Microcontrôleurs sécurisés ATMEL AT90SC12872RCFT / AT90SC12836RCFT rev. M, 27 février 2008, SGDN/DCSSI
[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - ASEPCOS-TS/CNS DI Security Target, Version 0.3, Athena Smartcard Solutions <p>Une version publique a été fournie et validée au cours de l'évaluation :</p> <ul style="list-style-type: none"> - ASEPCOS-TS/CNS DI Public Security Target, Version 0.4, Athena Smartcard Solutions
[RTE]	Evaluation Technical Report - Project: AURORA_CRS, Référence : ACRS_ETR, revision 1.0 CEACI
[CONF]	<p>La liste de configuration est constituée des documents suivants :</p> <ul style="list-style-type: none"> - ASEPCOS-CNS (ROM) Source Configuration List, Version 1.8, 13 Mai 09 Athena Smartcard Solutions - ASEPCOS-CNS (ROM) Scripts Configuration List, Version 1.9, 12 Jui. 09 Athena Smartcard Solutions - ASEPCOS-TS/CNS DI Document Configuration List, Version 1.9, 3 Sep. 09 Athena Smartcard Solutions - ASEPCOS-CNS (ROM) Binary Configuration List, Version 1.8, 13 Mai 09 Athena Smartcard Solutions - ASEPCOS-TS/CNS DI Configuration Management, Version 0.1, Athena Smartcard Solutions



[GUIDES]	Guide d'administration du produit : <ul style="list-style-type: none">- ASEPCOS-TS/CNS DI Administrator Guidance - Part 1: Generic Guidance, Version 0.4 Athena Smartcard Solutions- ASEPCOS-TS/CNS DI Administrator Guidance - Part 2: Dedicated guidance, Version 0.1 Athena Smartcard Solutions Guide d'utilisation du produit : <ul style="list-style-type: none">- ASEPCOS-TS/CNS DI User Guidance, Version 0.1 Athena Smartcard Solutions
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. <i>Certifié par la DCSSI sous la référence PP/9806.</i>
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002.</i>
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002.</i>

Annexe 3. Références liées à la certification

	Décret 2002-535 du 18 avril 2002 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]	<p>Common Criteria for Information Technology Security Evaluation :</p> <p>Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001;</p> <p>Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002;</p> <p>Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003.</p> <p>Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.</p> <p>Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.</p>
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.



[REF-CLE]	Gestion de clés - Règles et recommandations concernant La gestion des clés utilisées dans les mécanismes cryptographiques de niveau de robustesse standard, v1.0 du 28 mars 2006, réf: 724/SGDN/DCSSI/SDS/AsTeC.
[REF-AUT]	Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, v0.13 du 12 avril 2007, réf: 729/SGDN/DCSSI/SDS.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)