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-2010/12

Microcontrôleurs sécurisés ATMEL AT90SC12872RCFT / AT90SC12836RCFT rev. M

Paris, le 29 avril 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

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

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

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-2010/12

Nom du produit

Microcontrôleurs sécurisés ATMEL AT90SC12872RCFT / AT90SC12836RCFT rev. M

Référence/version du produit

AT90SC12872RCFT / AT90SC12836RCFT, référence AT58803 révision M, avec la bibliothèque logicielle cryptographique Toolbox version 00.03.01.07

Conformité à un profil de protection

PP/9806

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur

ATMEL Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR - Ecosse, Royaume-Uni

Commanditaire

ATMEL Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR - Ecosse, Royaume-Uni

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 :

- La direction centrale 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 le microcontrôleur sécurisé AT90SC12872RCFT référence AT58803, en révision M. Ce microcontrôleur inclut une bibliothèque logicielle cryptographique stockée en ROM : Toolbox en version 00.03.01.07.
La référence AT90SC12836RCFT identifie différemment le même composant matériel pour des raisons commerciales.

Ce microcontrôleur appartient à la famille de produits AVR ASL4 développée par ATMEL Secure Products Division.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

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 au profil de protection [PP9806].

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 suivants :

- Nom du produit : AT90SC12872RCFT / AT90SC12836RCFT, et son numéro d'identification : AT58803. Cette information peut être vérifiée en utilisant le registre de numéro de série SN_0, qui contient la donnée hexadécimale 0x1F (cf. [GUIDES], « AT90SC12872RCFT Technical Data Sheet » section 23.1.1).
- Silicium révision M. Cette information peut être vérifiée en utilisant le registre de numéro de série SN_1, qui contient la donnée hexadécimale 0x0C (cf. [GUIDES], « AT90SC12872RCFT Technical Data Sheet » section 23.1.2).
- Bibliothèque logicielle Toolbox révision: 00.03.01.07. Cette information peut être vérifiée en utilisant la commande de la Toolbox « Selftest », dont la réponse doit être la valeur hexadécimale spécifiée dans le guide « Toolbox 3.x on AT90SCxxxxC Family with AdvX » section 4.1 (cf. [GUIDES]).
- Le produit lui-même peut être physiquement identifié par ses numéros de réticules identifiés dans le document « Patern and mask list » (cf. [CONF]), et visibles au microscope sur la surface métallique du produit.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- procédure d'entrée en mode « test » ;
- protection du contenu des mémoires en mode « test » ;
- désactivation du mode « test » ;
- test du produit ;
- détection des erreurs ;
- pare-feu ;
- audit d'évènements ;
- actions associées aux évènements ;
- non observabilité ;
- cryptographie ;
- procédure d'entrée en mode « diagnostic » ;
- protection du contenu des mémoires en mode « diagnostic ».

1.2.3. Architecture

Le microcontrôleur AT90SC12872RCFT / AT90SC12836RCFT est constitué des éléments suivants :

- processeur AVR Risc ;
- 128ko de mémoire ROM pour le stockage des programmes ;
- 72ko de mémoire EEPROM pour le stockage des programmes et des données avec 128 octets d'OTP (One Time Programmable) et 384 octets accessibles par bit ;
- 5ko de mémoire RAM statique utilisateur ;
- un accélérateur de calcul de checksum 32 bits ;
- un périphérique CRC-16/32 ;
- un générateur de nombres aléatoires ;
- un accélérateur de calcul cryptographique DES/3DES ;
- un coprocesseur cryptographique 32-bits (AdvX) incluant de façon optionnelle sa bibliothèque logicielle de 32ko en ROM (boîte à outils cryptographique) permettant en particulier d'accélérer les calculs RSA (avec et sans CRT), ECC (courbes elliptiques), de réaliser les fonctions SHA-1 et de générer des nombres premiers ;
- des détecteurs tension, fréquence, température ;
- un firewall protégeant l'accès à toutes les mémoires et tous les périphériques ;
- un régulateur de tension (le microcontrôleur fonctionne dans une gamme de tension de 3.0V à 5.0V) ;
- des périphériques, incluant 2 timers, 2 ports série avec une interface et un contrôleur conforme au standard ISO7816, 1 port RF, avec une interface et un contrôleur en mode sans contact conforme au standard ISO/IEC 14443 type A et B ;
- une structure de test dédiée, sciée lors de la mise en micro-module et accessible uniquement en mode test pour les tests de production.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

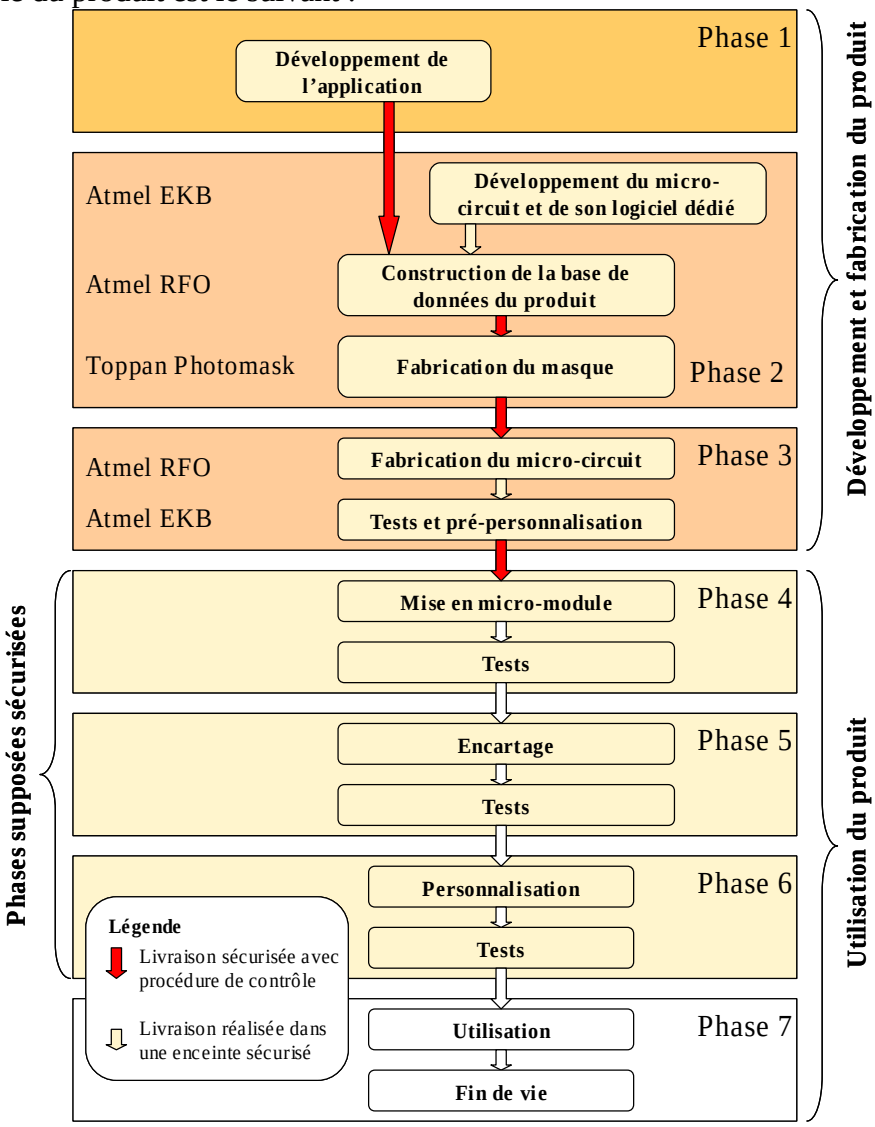

Figure 1 - Cycle de vie du produit

Le microcontrôleur est développé, testé et préparé par :

Atmel East Kilbride

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

La base de données de fabrication du masque du microcontrôleur ainsi que la fabrication du produit lui-même sont réalisées par :

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France

Les réticules du microcontrôleur sont fabriqués par :

Toppan Photomasks France

224, bd John Kennedy
91100 Corbeil Essonnes
France

Le microcontrôleur comporte trois modes d'utilisation :

- un mode « Test », dans lequel le microcontrôleur fonctionne sous le contrôle d'un logiciel de test écrit en mémoire EEPROM à l'aide d'une interface de test et utilisé sous le contrôle d'un système de test externe. Ce mode requiert une authentification de l'administrateur. Il n'est utilisable que par le personnel autorisé de l'équipe du développement. Après la phase de test, le mode « test » est inhibé de façon irréversible par découpage du « wafer ». L'interface de test n'est alors plus accessible ;
- un mode « utilisateur », dans lequel le microcontrôleur fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans ce mode ;
- un mode « diagnostic », utilisé lors du retour de pièces défectueuses et permettant d'effectuer des tests à l'aide d'une interface de test utilisée sous le contrôle d'un système de test externe. Lors de l'activation de ce mode, le contenu des mémoires est effacé. Ce mode n'est utilisable que par le personnel autorisé de l'équipe du développement.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur seul.
Toute application, éventuellement embarquée pour les besoins de l'évaluation, ne fait pas partie du périmètre d'évaluation.
En regard du cycle de vie, le produit évalué est celui qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).
Pour les besoins de l'évaluation, le microcontrôleur AT90SC12872RCFT / AT90SC12836RCFT a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié, dans un mode dit « ouvert[1] ».

[1] Mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables.

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]. 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

La présente réévaluation a été initiée par la mise à jour des guides du produit certifié [2008/05] suite à sa surveillance 2009, cf. [GUIDES, *Securing Cryptographic Operations on AT90SC Products with Toolbox 3x*]. Elle s'appuie également sur les résultats de réévaluation du produit « Bibliothèque cryptographique ATMEL Toolbox 00.03.01.07 pour la famille de microcontrôleur AT90SC » en cours de certification sous la référence ANSSI-2010/11 (cf. [2010/11]).

Le rapport technique d'évaluation [RTE] se compose du RTE correspondant à la certification initiale [2008/05], ainsi que du rapport de surveillance 2009, comme addendum, remis à l'ANSSI le 7 janvier 2010. Le [RTE] 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

Le produit évalué offre des services cryptographiques identifiés §1.2.3 mais qui ne peuvent cependant pas être analysés d'un point de vue cryptographique car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépend de leur emploi par l'application embarquée sur le microcontrôleur.

2.4. Analyse du générateur de nombres aléatoires

Ce générateur a fait l'objet d'une analyse par le CESTI suivant une méthodologie validée par l'ANSSI. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF-CRY] il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

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 microcontrôleur sécurisé ATMEL AT90SC12872RCFT / AT90SC12836RCFT rev. M soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit AT90SC12872RCFT / AT90SC12836RCFT à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

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], notamment :

- la communication entre un produit développé sur le microcontrôleur sécurisé et d'autres produits doit être sécurisée (en termes de protocole et de procédure) ;
- le système (terminal, communication,…) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

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'accord[1], 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 :

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 France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[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 5+	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	**3**	Development tools 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**	**3**	Semiformal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**3**	Semiformal high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**	**1**	Modularity
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**2**	Semiformal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**3**	Formal 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	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**2**	Standardised life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**2**	Testing: low-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	**1**	Covert channel analysis
	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

[2008/05]	Rapport de certification 2008/05 - Microcontrôleurs sécurisés ATMEL AT90SC12872RCFT / AT90SC12836RCFT rev. M, 27 février 2008, SGDN/DCSSI
[2010/11]	Rapport de certification ANSSI-CC-2010/11 - Bibliothèque cryptographique ATMEL Toolbox 00.03.01.07 pour la famille de microcontrôleur AT90SC, 2010, SGDSN/ANSSI
[ST]	Cible de sécurité de référence pour l'évaluation : - Cyclone Security Target, Référence : Cyclone_ST_V3.0_19Feb08, ATMEL Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - AT90SC12872RCFT / AT90SC12836RCFT Security Target Lite, Référence : TPG0129D_19Feb08 ATMEL
[RTE]	Rapport technique 2008 de l'évaluation initiale : - Evaluation Technical Report Project: Cyclone 5 rev M Re Evaluation, 14 février 2008, Référence: CYM_ETR_V2.0 CEACI Addedum 2010 : - Surveillance Evaluation Technical Report, Project : MARIEL 2009, 5 janvier 2010, CEACI - THALES ITSEF Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique 2010 pour la composition a été validé : - ETR LITE for composition Cyclone 5 rev M Re Evaluation, AT90SC12872RCFT & AT90SC12836RCFT MCU Device (AT58803), Référence : CYM_ETR_Lite_v2.0, 5 mars 2010, CEACI – THALES ITSEF
[CONF]	Liste de configuration du design : - Cyclone Design Configuration List, Référence : Cyclone_DCL_V1.1_12Oct07, ATMEL Liste de configuration de la fabrication : - Cyclone Rev M Manufacturing Configuration Liste, Référence : Cyclone Rev M _MCL_V1.0, ATMEL

	Liste des patterns et des masques : - Cyclone Process Stage Flow, Référence : Cyclone_RevM_PSF_10Oct07 ATMEL Liste de configuration de la librairie cryptographique : - Crypto Library Configuration List Library Version 00.03.01.07, Référence : TPR0150FX_01Oct07 ATMEL Liste des fournitures ATMEL : - Cyclone Rev M Deliverable list, Référence : Cyclone_EDL_RevM_23Apr10 ATMEL
[GUIDES]	Guidance of the product: - AT90SC AGD Interface Document, Référence : AT90SC_AGD_V2.0_22Sep05, ATMEL - AT90SC12872RCFT Technical Data Sheet, Référence : TPR0097A-23Dec04, ATMEL - AT90SC12872RCFT Errata - Full NVM Erase, Référence : TPG0137AX_19Oct06 ATMEL - Secure Hardware DES and Triple DES on AT90SC ASL4 Products, Référence : TPR0063IX_05Dec07. ATMEL - Security Recommendations for AT90SC ASL4 Products, Référence : TPR0066H_31Jan08. ATMEL - Checksum Accelerator use on the AT90SC ASL4 products, Référence : TPR0065A-02Jul02 ATMEL - AT90SC Addressing Modes and Instruction Set, Référence : 1323C-03May04 ATMEL - Using the supervisor and user modes on the AT90SC ASL4 products, Référence : TPR0095A-11Mar03 ATMEL - Generating unpredictable random numbers on the AT90SC family devices, Référence : 1573CX_SMIC_21mar03 ATMEL - Generation of Random Numbers with a Controlled Entropy on AT90SC, Référence : TPR0166BX_27Jun06. ATMEL - AdvX™ for AT90SC Family Datasheet,

	Référence : TPR0116BX-12Aug05 ATMEL - Toolbox 3.x on AT90SCxxxxC Family with AdvX™, Référence : TPR0133DX_01Aug06 ATMEL - Toolbox 00.03.01.xx Errata, Référence : TPR0163DX_10Jul07, ATMEL - Efficient use of AdvX for Implementing Cryptographic Operations, Référence : TPR0142CX_14Jun05 ATMEL - Securing Cryptographic Operations on AT90SC Products with Toolbox 3x, Référence : TPR0141FX_13Nov09. ATMEL - Wafer Saw Recommendations, Référence : TPG0079A_13Jun05 ATMEL
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certifié par la DCSSI sous la référence PP/9806.*

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]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[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-2007-04-001 version 2.3, revision 1, April 2007.
[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, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.

[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)