Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2009/33

Microcontrôleur sécurisé ATMEL AT90SC320288RCT/AT90SC144144CT - Rév. D

Paris, le15 octobre 2009

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.

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

Référence du rapport de certification

ANSSI-CC-2009/33

Nom du produit

AT90SC320288RCT/AT90SC144144CT

Référence/version du produit

référence AT58888, révision D

Conformité à un profil de protection

PP/9806

Critères d'évaluation et version

Critères Communs version 2.2

(avec les interprétations couvrant les évolutions jusqu'à la version 2.3)

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, 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

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

IT Security Certified

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

1.1. Présentation du produit

Le produit évalué est le microcontrôleur sécurisé AT90SC320288RCT, de référence AT58888 en révision D. Ce microcontrôleur inclut une bibliothèque logicielle cryptographique optionnelle, stockée en mémoire ROM : Toolbox 3.x en version 00.03.01.04.

La référence AT90SC144144CT identifie le même composant matériel, mais qui embarque un logiciel de configuration en mémoire ROM : « Embedded ROM Rev. 1.0 ». Il peut alors être considéré comme un composant « flash », le logiciel embarqué étant alors chargé après fabrication en mémoire EEPROM.

Ce microcontrôleur appartient à la famille de produits AVR RISC AT90SC ASL4 développée par ATMEL Secure Microcontroller Solutions.

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 : AT90SC320288RCT ou AT90SC144144CT et son numéro d'identification : AT58888. Cette information peut être vérifiée en utilisant le registre de numéro de série SN_0, qui contient la donnée hexadécimale 0x1B (cf. [GUIDES], en particulier le document intitulé : « AT90SC320288RCT/AT90SC144144CT Technical Data Sheet » au § 21.1.1) ;
- silicium en révision D. Cette information peut être vérifiée en contactant ATMEL. Les clients annoncent à ATMEL les informations contenues dans les registres SN_2 à SN_8 et ATMEL répond avec l'information d'identification requise concernant la révision du silicium et celle du *Flash loader*. Cette procédure est une alternative à ce qui est habituellement proposé au sein du document « Technical Data Sheet » via la vérification du registre SN_1, ce dernier n'ayant pas été mis à jour par ATMEL ;

- révision de la bibliothèque cryptographique *Toolbox* : 00.03.01.04. Cette information est vérifiable en utilisant la commande « Selftest » de la *Toolbox* 3.x dont la réponse doit être la valeur hexadécimale 0x00030104 ;
- révision du logiciel *Flash loader* : Embedded ROM V1.0. Cette information est vérifiable en utilisant la fonction ROM « bGetVersion » qui doit retourner la valeur 0x10.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- tests du produit et contrôle d'accès au mode « test » ;
- protection du contenu des mémoires en mode « test » ;
- désactivation du mode « test » ;
- génération physique de nombres aléatoires ;
- détection des erreurs (intégrité des données) ;
- pare-feu (contre les adresses, accès et opcodes illégaux) ;
- audit d'évènements (détection et contrôle des conditions environnementales contre les attaques par injection de fautes) ;
- actions associées aux évènements critiques ;
- non observabilité (protection contre la fuite d'informations, contre les attaques par canaux auxiliaires : régulateur de tension, brouillage des bus, horloge variable, …) ;
- cryptographie ;
- tests réduits du produit et contrôle d'accès au mode « diagnostic » ;
- protection du contenu des mémoires en mode « diagnostic ».

1.2.3. Architecture

Le microcontrôleur AT90SC320288RCT / AT90SC144144CT est constitué des éléments suivants :
- un CPU AVR Risc ;
- 320ko de mémoire ROM pour le stockage des programmes (*Toolbox*, code client) et 288ko de mémoire EEPROM pour le stockage des programmes et des données, en configuration « classique » (AT90SC320288RCT) ;
- 320ko de mémoire ROM pour le stockage des programmes (*Toolbox*, *Flash loader*), 144ko de mémoire Flash pour le stockage des programmes (code client) et 144ko de mémoire EEPROM pour le stockage des programmes et des données, en configuration « flash » (AT90SC144144CT) ;
- la mémoire EEPROM (288ko, dans les deux configurations) comprend 128 octets d'OTP (mémoire inscriptible, non effaçable en mode « utilisateurs », pour stocker les données sensibles par exemple, ou servir de verrous sur les phases du cycle de vie notamment) et 384 octets accessibles par bit ;
- 8ko de mémoire RAM statique ;
- un accélérateur de calcul de somme de contrôle 32 bits (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un périphérique CRC-16/32 (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un générateur de nombres aléatoires ;
- un accélérateur de calcul cryptographique DES/3DES ;
- un coprocesseur cryptographique 32-bits (AdvX) permettant d'accélérer les calculs RSA (avec et sans CRT), SHA-1 et de générer des nombres premiers ;

- des détecteurs tension, fréquence, température et lumière ultraviolette ;
- un *firewall* protégeant l'accès à toutes les mémoires et tous les périphériques, comportant cinq modes d'utilisation ;
- un régulateur de tension (le microcontrôleur fonctionne dans une gamme de tension de 3.0V à 5.0V) ;
- deux Timers ;
- un port série SPI et un port série avec une interface et un contrôleur conforme au standard ISO7816 ;
- 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 :

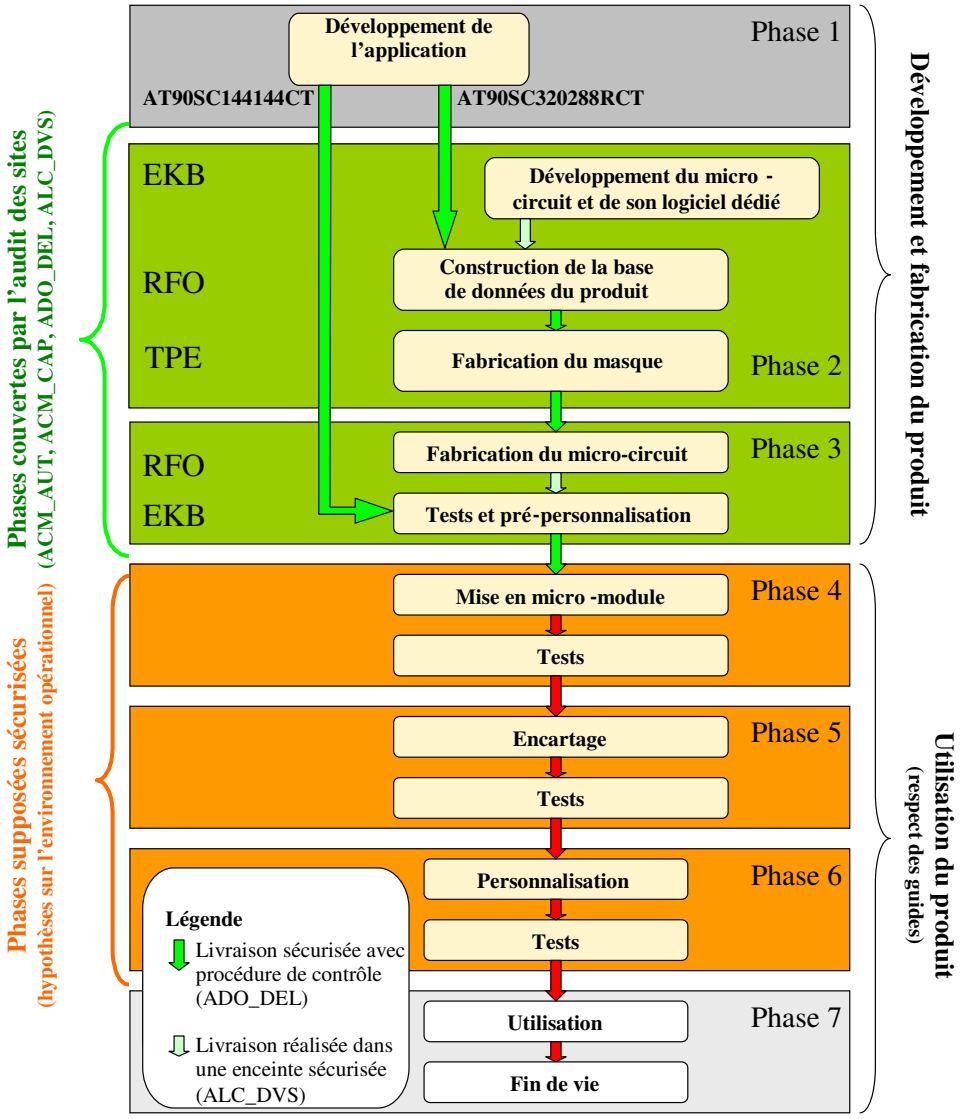

Figure 1 - Cycle de vie du produit

Le microcontrôleur est conçu et testé par :

Atmel East Kilbride (EKB)

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

La base de données de fabrication du masque et la fabrication du microcontrôleur sont réalisées par :

Atmel Rousset (RFO)

Z.I. Rousset Peynier
13106 Rousset Cedex
France

Les réticules du microcontrôleur sont fabriqués par :

Toppan Photomasks Europe (TPE)

Sites de Corbeil Essonnes et Rousset en France ainsi que Hamburg et Dresden en Allemagne.

Le cycle de vie du microcontrôleur met en exergue trois modes possibles :

- Un mode « test » (*Test Mode*), 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 » (*User Mode*), 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 » (*Package Mode*), 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 tel qu'identifié dans le périmètre d'évaluation défini au sein de sa cible de sécurité [ST].

La bibliothèque cryptographique logicielle (*Toolbox* 3.x), développée par Atmel, peut en option être chargée en CRYPTO ROM, l'alternative étant de charger une bibliothèque propriétaire d'un développeur de cartes à puce. Cette bibliothèque (*Toolbox*) permet de fournir une implémentation rapide de fonctions cryptographiques (opérations de type RSA, SHA, génération de nombres premiers, etc.) basée sur l'accélérateur cryptographique AdvX. La version 00.03.01.04 de cette bibliothèque a été prise en compte lors de l'évaluation du microcontrôleur, de manière à garantir que sa présence n'introduit aucune vulnérabilité. De plus, les fonctions de la *Toolbox* 00.03.01.04, lorsque celle-ci est utilisée, ont été évaluées.

Toute autre 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). Les modes « utilisateur » et « diagnostic » sont couverts par l'évaluation ; le mode « test » a seulement été pris en compte pour assurer l'impossibilité de son utilisation à partir des deux autres modes. Pour les besoins de l'évaluation, le microcontrôleur AT90SC320288RCT (AT58888) en révision D a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié, dans un mode dit « ouvert[1] ».

Ce microcontrôleur comporte une spécificité en configuration « flash » (AT90SC144144CT) : le logiciel applicatif n'est pas embarqué en mémoire ROM (cas où le logiciel est figé lors de la phase de fabrication) mais en mémoire Flash. Il peut donc être chargé ultérieurement à la phase de fabrication du microcontrôleur. Pour la présente évaluation, il est considéré que le logiciel applicatif est embarqué dans le microcontrôleur dans les locaux d'Atmel et sous sa responsabilité.

[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 2.2** [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.

Un ensemble d'interprétations des Critères Communs version 2.2 également pris en compte lors de l'évaluation fait que celle-ci peut être considérée comme conforme aux Critères Communs version 2.3. C'est d'ailleurs la CEM en version 2.3 qui a été utilisée.

2.2. Travaux d'évaluation

Cette évaluation fait suite à une demande de maintenance faite par Atmel concernant le produit certifié sous le numéro DCSSI-2006/20. L'analyse du rapport d'analyse d'impact sur la sécurité [SIA] faite par l'ANSSI a conclu à un impact majeur sur la sécurité et a conduit à la présente réévaluation. Cette réévaluation EAL4+ a pris en compte les résultats de l'évaluation du microcontrôleur sécurisé ATMEL AT90SC320288RCT / AT90SC144144CT, de référence AT58807 en révision G, au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP9806]. Ce microcontrôleur a été certifié sous la référence DCSSI-2006/20 (cf. [2006/20]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 avril 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

Le produit évalué offre des services cryptographiques, identifiés au §1.2.3. Ces services ne peuvent cependant pas être analysés vis-à-vis des référentiels techniques de l'ANSSI [REF-CRY], [REF-CLE] et [REF-AUT] car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépendra de leur emploi par l'application embarquée sur le microcontrôleur qui utilisera éventuellement les fonctions de la librairie *Toolbox* 00.03.01.04, si celle-ci est présente.

2.4. Analyse du générateur d'aléas

La qualité du générateur physique d'aléas (tests statistiques) n'a pas été analysée. Ce générateur physique d'aléas a néanmoins fait l'objet de tests de pénétration au titre de l'analyse de vulnérabilité.

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 AT90SC320288RCT/ AT90SC144144CT, de référence AT58888 en révision D, 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 et donne une appréciation de la résistance du produit AT90SC320288RCT/ AT90SC144144CT 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].

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 :

[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.

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[1], 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	**2**	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	**2**	Sufficiency 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

[ST]	Cible de sécurité de référence pour l'évaluation : - Longbow Security Target, Référence : Longbow_ST v1.5 Atmel Secure Microcontroller Solutions Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - AT90SC320288RCT-AT90SC144144CT Security Target Lite, Référence : TPG0132D Atmel Secure Microcontroller Solutions
[SIA]	Analyse d'impact sur la sécurité : - Longbow SIA, Référence : Longbow_SIA v2.5 Atmel Secure Microcontroller Solutions
[2006/20]	Rapport de certification : - Rapport de certification AT90SC320288RCT/AT90SC144144CT (AT58807) Rév. G, Référence : DCSSI-2006/20 (16 novembre 2006) DCSSI
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – LONGBOW project Référence : LETI.CESTI.LON.RTE.003, V2.0, 29 avril 2009 CEA LETI Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite LONGBOW, Référence: LETI.CESTI.LON.RTE.004 V2.0 CEA LETI
[CONF]	Liste de configuration du design : - Longbow Design Configuration List, Référence : Longbow_DCL v1.5 Atmel Secure Microcontroller Solutions Liste de configuration de la fabrication : - Longbow Manufacturing Configuration List, Référence : Longbow_MCL_v2.3 Atmel Secure Microcontroller Solutions Liste des patterns et des masques : - Longbow Pattern and Mask list, Référence : Longbow_PML_v2.1

	Atmel Secure Microcontroller Solutions Liste des fournitures ATMEL : - Longbow Deliverables list, Référence : LongbowRevD_EDL v1.3 Atmel Secure Microcontroller Solutions
[GUIDES]	- Security Recommendations for AT90SC ASL4 Products, Référence : TPR0066HX Atmel Secure Microcontroller Solutions - Secure Hardware DES/TDES on AT90SC ASL4 Products, Référence : TPR0063IX Atmel Secure Microcontroller Solutions - Generating Random Numbers with a Controlled Entropy on AT90SC, Rev C Référence : TPR0166CX Atmel Secure Microcontroller Solutions - Generating unpredictable random numbers on the AT90SC family devices, Référence : 1573CX_SMIC Atmel Secure Microcontroller Solutions - AdvX™ for AT90SC Family Datasheet, Référence : TPR0116CX Atmel Secure Microcontroller Solutions - Efficient use of AdvX for Implementing Cryptographic Operations, Rev D Référence : TPR0142DX Atmel Secure Microcontroller Solutions - Securing cryptographic operations on AT90SC products with the Toolbox 3.x, Rev A Référence : TPR0141EX Atmel Secure Microcontroller Solutions - Toolbox 3.0 on AT90SCxxxxC Family with AdvX, Référence : TPR0133DX Atmel Secure Microcontroller Solutions - AT90SC320288RCT Technical Datasheet, Référence : TPR0115AX_03Jun04 Atmel Secure Microcontroller Solutions

	- AT90SC320288RCT Errata Sheet, Référence : TPR0151BX_30May05 Atmel Secure Microcontroller Solutions - AT90SC144144CT Configuration of AT90SC320288CT, Référence : TPR0143BX Atmel Secure Microcontroller Solutions - Full NVM Erase Errata (AT90SC320288RCT/ AT90SC144144RCT), Référence : TPR0254AX Atmel Secure Microcontroller Solutions - Using the supervisor and user modes on the AT90SC ASL4 products, Rev B Référence : TPR0095BX Atmel Secure Microcontroller Solutions - AT90SC Addressing Modes and Instruction Set, Référence : 1323C Atmel Secure Microcontroller Solutions - Checksum Accelerator use on the AT90SC ASL4 products, Référence : TPR0065AX Atmel Secure Microcontroller Solutions - Wafer Saw Recommendations, Référence : TPG0079A Atmel Secure Microcontroller Solutions
[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certifié par le centre de certification français sous la référence 9806. *Document publié sur le site : www.ssi.gouv.fr*

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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[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.
[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, version 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-CLE]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[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)