PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-2009/24

Microcontrôleur sécurisé ATMEL AT90SC24036RCU - Rév. B

Paris, le 21 août 2009

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

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

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

Référence du rapport de certification

ANSSI-2009/24

Nom du produit

AT90SC24036RCU

Référence/version du produit

référence AT58U48, révision B

Conformité à un profil de protection

PP BSI-PP-0002-2001

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

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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 ATMEL AT90SC24036RCU, de référence AT58U48 en révision B. Ce microcontrôleur appartient à la famille de produits AVR RISC AT90SC ASL5 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 [PP0002] et contient quelques exigences supplémentaires issues du document [AUG].

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 : AT90SC24036RCU et son numéro d'identification : AT58U48, cette information peut être vérifiée en utilisant le registre de numéro de série SN_0, qui contient la donnée hexadécimale 0x37 (cf. [GUIDES], « AT90SC24036RCU Technical Data Sheet » ;
- silicium en révision B, cette information peut être vérifiée en utilisant le registre de numéro de série SN_1, qui contient la donnée hexadécimale 0x01 (cf. [GUIDES], « AT90SC24036RCU Technical Data Sheet ».

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 AT90SC24036RCU est constitué des éléments suivants :

- un processeur AVR Risc Low power HCMOS core ;
- un contrôleur ISO7816 ;
- un générateur de nombres aléatoires ;
- un accélérateur de calcul cryptographique DES/3DES ;
- un coprocesseur cryptographique 32-bits (AdvX) pour les opérations à clé publique de type RSA, DSA, ECC, Diffie-Hellman ;
- 208ko de mémoire ROM pour le stockage des programmes et 32ko dédiés à la cryptographie (CRYPTO ROM) pour embarquer une bibliothèque cryptographique d'Atmel (*toolbox*) basée sur l'AdvX ;
- 36ko de mémoire EEPROM pour le stockage des programmes et des données dont 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) ainsi que 384 octets accessibles par bit ;
- 4ko de mémoire RAM statique utilisateur et 2ko dédiés à la cryptographie (CRYPTO RAM) ;
- un contrôle d'accès aux mémoires, suivant trois modes au cours du cycle de vie ;
- un accélérateur de calcul de checksum 32 bits ;
- un module de signature de code ;
- un périphérique CRC-16/32 ;
- des oscillateurs internes programmables ;
- des protections contre les attaques physiques :
    - contrôleurs de tension, fréquence et température ;
    - détecteurs (*glitch* et laser) ;
    - grille de protection (*active shield*) ;
    - duplication de registres ;
    - vérification du compteur ordinal et pile ;
    - protection avancée des objets : « EPO » (double lecture en EEPROM avec vérification) ;
- une structure de test dédiée, sciée lors de la mise en micro-module et accessible uniquement en mode « test » pour les tests de production (cf. §1.2.4).

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

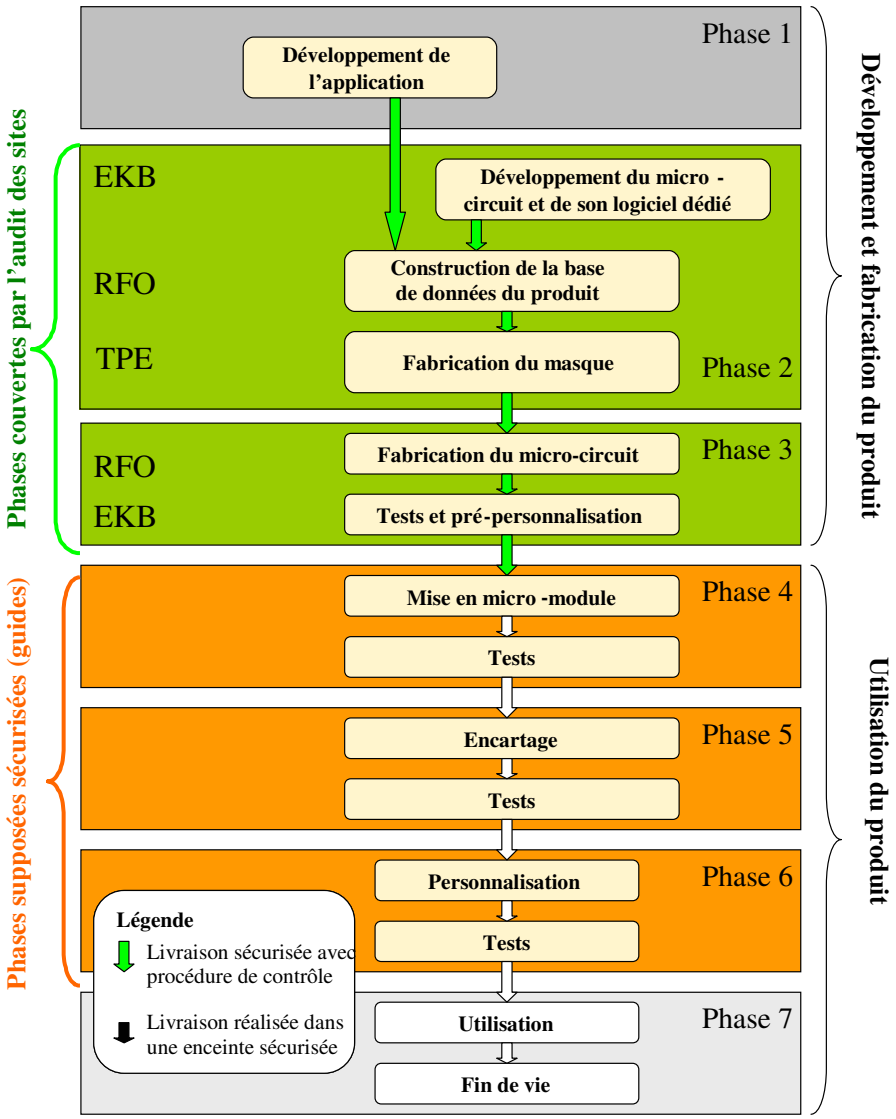

Figure 1 - Cycle de vie du produit

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 (t*oolbox*), 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. Les versions de cette bibliothèque 00.03.10.00 (version complète) et 00.03.13.00 (version partielle, ne contenant que les tests AIS31 pour le RNG) ont été prises en compte lors de l'évaluation du microcontrôleur AT90SC24036RCU, de manière à garantir que leur présence n'introduit aucune vulnérabilité. De plus, les fonctions de la *toolbox* 00.03.10.00, 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 tandis que le mode « test » a néanmoins été pris en compte de manière à assurer l'impossibilité de son utilisation à partir des deux autres modes. Pour les besoins de l'évaluation, le microcontrôleur AT90SC24036RCU a été fourni au centre d'évaluation (5 DIL-48 et 15 micromodules) 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 [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

Cette évaluation EAL5+ a pris en compte les résultats de l'évaluation du microcontrôleur sécurisé ATMEL AT90SC20818RCU rév. C au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur est en cours de certification sous la référence ANSSI-2009/22 (cf. [2009/22]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 juillet 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

L'ANSSI n'a pas réalisé la cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY], [REF-CLE] et [REF-AUT]. Le produit évalué offre des services cryptographiques, identifiés au §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 qui utilise éventuellement les fonctions de la librairie *toolbox* 00.03.10.00, si celle-ci est présente.

2.4. Analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas qui peut être utilisé par le logiciel embarqué.
Ce générateur physique (TRNG) de nombres aléatoires a fait l'objet d'une évaluation par le centre d'évaluation selon la méthodologie [AIS 31]. Le générateur est de classe « P2 – *SOF-high* » selon l'[AIS31].

Un registre à décalage avec rétroaction linéaire (LFSR) de 65 bits fournit un post-traitement du TRNG. Néanmoins, dans le cas où le générateur d'aléas serait utilisé à des fins cryptographiques, il est obligatoire de le combiner à un mécanisme algorithmique de génération de pseudo-aléa, de nature cryptographique, afin de fournir des données aléatoires cryptographiquement satisfaisantes, comme énoncé dans le document [REF-CRY].

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 AT90SC24036RCU rév. B 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 AT90SC24036RCU 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 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

[ST]	Cible de sécurité de référence pour l'évaluation : - Custodian Security Target, Référence : Custodian_ST v1.2 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 : - AT90SC24036RCU EAL5+ Custodian Security Target Lite, Rev A Référence : TPG0187A Atmel Secure Microcontroller Solutions
[2009/22]	Rapport de certification : - Rapport de certification AT90SC20818RCU Rév. C (EAL5+) Référence : ANSSI-2009/22 ANSSI
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - CUSTODIAN project Référence : CUSTODIAN_ETR_v1.1 / 1.1, 17 juillet 2009 Serma Technologies
[CONF]	Liste de configuration du design : - Custodian_Design Configuration List, Référence : Custodian_DCL v1.0 Atmel Secure Microcontroller Solutions Liste de configuration de la fabrication : - Custodian Manufacturing Configuration List, Référence : 58U48RB_MCL Rev B Atmel Secure Microcontroller Solutions Liste des patterns et des masques : - Custodian Pattern and Mask list, Référence : 58U48B_PML Rev B Atmel Secure Microcontroller Solutions Liste des fournitures ATMEL : - Custodian Deliverables list, Référence : Custodian_EDL v1.3 Atmel Secure Microcontroller Solutions
[GUIDES]	- AT90SC CC Guidance Documentation Référence : AT90SC_AGD_0.15 / V1.1 Atmel Secure Microcontroller Solutions - AT90SC24036RCU Technical Datasheet, Rev A Référence : TPR0359AX Atmel Secure Microcontroller Solutions

	- AT90SC Enhanced Security Technical Datasheet, Rev B Référence : TPR0255BX Atmel Secure Microcontroller Solutions - RISC Instruction Set, Rev C Référence : 1323C Atmel Secure Microcontroller Solutions - Using the supervisor and user modes on the AT90SC ASL4 products, Rev B Référence : TPR0095BX Atmel Secure Microcontroller Solutions - Security Recommendations for AT90SC, Rev D Référence : TPR0267DX Atmel Secure Microcontroller Solutions - Code Signature Module, Rev B Référence : TPR0252BX Atmel Secure Microcontroller Solutions - Secure Hardware DES and Triple DES on AT90SC ASL5 Products (0.15µm), Rev B Référence : TPR0396BX Atmel Secure Microcontroller Solutions - Generation of Random Numbers with a Controlled Entropy on AT90SC, Rev C Référence : TPR0166CX Atmel Secure Microcontroller Solutions - Efficient use of AdvX for Implementing Cryptographic Operations, Rev D Référence : TPR0142DX Atmel Secure Microcontroller Solutions - AdvX™ for AT90SC Family Datasheet, Référence : TPR0116CX Atmel Secure Microcontroller Solutions - Securing Toolbox Operations using version 00.03.10.xx on ASL5 products, Rev H Référence : TPR0260HX Atmel Secure Microcontroller Solutions - Securing Toolbox Operations using version 00.03.13.xx on ASL5 products, Rev G Référence : TPR0290GX Atmel Secure Microcontroller Solutions - Using Toolbox 00.03.10.x, Rev C

	Référence : TPR0259CX Atmel Secure Microcontroller Solutions - Using Toolbox 00.03.13.x on AT90SCxx, Rev C Référence : TPR0289CX Atmel Secure Microcontroller Solutions - Toolbox 00.03.10.x Errata Sheet, Rev A Référence : TPR0344AX_SPD Atmel Secure Microcontroller Solutions - Toolbox 00.03.13.x Errata Sheet, Rev A Référence : TPR0345AX_SPD Atmel Secure Microcontroller Solutions - Wafer Sawing Recommendations, Référence : TPG0079A Atmel Secure Microcontroller Solutions
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*
[AUG]	Smartcard Integrated Circuit Platform Augmentations, version 1.0, mars 2002. *Développé par Atmel, Hitachi Europe, Infineon Technologies et Philips Semiconductors et édité par le BSI (Bundesamt für Sicherheit in der Informationstechnik).*

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.
[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.
[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 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)
[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)