PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2009/11

Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05

Paris, le 30 Juin 2009

Le Directeur central 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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification

DCSSI-2009/11

Nom du produit

Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 pour la famille de microcontrôleur AT90SC

Référence/version du produit

Version 00.03.11.05

Conformité à un profil de protection

Néant

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 – Scotland, United Kingdom

Commanditaire

ATMEL Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR – Scotland, United Kingdom

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 la bibliothèque logicielle cryptographique « ATMEL Toolbox 00.03.11.05 » développée par ATMEL Secure Microcontroller Solutions pour la famille de microcontrôleur AT90SC.

Le produit correspond au sous-système cryptographique de type logiciel embarqué sur les microcontrôleurs de la famille AT90SC. Il offre une interface permettant aux applications également embarquées d'utiliser les accélérateurs cryptographiques matériels.

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.
La cible de sécurité est construite de façon à rendre possible la réutilisation des résultats de l'évaluation de la bibliothèque ou son évaluation en composition (cf. [COMP]) avec un microcontrôleur incluant la bibliothèque et se réclamant conforme au [PP0002].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit peut être identifiée en utilisant la commande « selftest() » de la bibliothèque, qui doit répondre avec l'identifiant : « 05 11 03 00 ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- tests [AIS31] ;
- génération et test des nombres premiers ;
- fonctions de hachage (SHA-1, SHA-224, SHA-256) ;
- RSA sans fonction CRT ;
- RSA avec fonction CRT ;
- DSA et ECDSA ;
- addition des points de courbes elliptiques ;
- doublement de points de courbes elliptiques ;
- multiplication de points de courbes elliptiques ;
- identification.

1.2.3. Architecture

La bibliothèque logicielle cryptographique permet l'exécution rapide de calculs cryptographiques (RSA, SHA-1, ECC, génération de nombres premiers…) sur la famille de microcontrôleurs AT90SC disposant d'accélérateurs cryptographiques matériels. Dans le but de faciliter le travail des développeurs de logiciels embarqués, la bibliothèque propose des

routines cryptographiques logicielles de base (multiplication totale, mise au carré, multiplication partielle, division) ainsi que des algorithmes de signature de données DSA et EC-DSA.
Cette bibliothèque logicielle a vocation à être embarquée sur les composants de la famille AT90SC et à cette fin, elle est intégrée au logiciel embarqué lors de la phase 2 du cycle de vie du produit (voir. §1.2.4).

1.2.4. Cycle de vie

Le cycle de vie de la bibliothèque Toolbox 00.03.11.05 s'intègre dans la phase 2 du cycle de vie standard d'une carte à puce, en tant que développement et intégration d'un logiciel dédié.

Les autres phases du cycle de vie standard d'une carte à puce (phase 1 pour le développement du code client et phase 3 à phase 6 pour le reste de la production) ne sont pas dans le périmètre de cette évaluation.

Le cycle de vie de la bibliothèque toolbox 00.03.11.05 peut alors être raffiné par les phases ci-dessous :

- développement :
  - spécification ;
  - conception ;
  - codage (C et Assembleur) ;
  - validation ;
- génération et intégration :
  - génération du code ROM toolbox ;
  - intégration (fusion du code ROM client avec le code ROM toolbox) et génération des données correspondantes pour la préparation des masques (fin de la phase 2 standard du cycle de vie d'une carte à puce).

La bibliothèque logicielle est développée par :

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

Elle est ensuite intégrée au logiciel embarqué en ROM par :

Atmel East Kilbride

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

1.2.5. Configuration évaluée

La bibliothèque logicielle peut être mise en œuvre dans deux modes différents :

- mode « test » : mode permettant de pouvoir tester tous les paramètres pour faciliter la phase de développement, et particulièrement d'analyser l'état des paramètres et des mémoires des coprocesseurs (Ram AdvX) ;
- mode « émission » : mode final d'utilisation permettant l'exécution rapide du code.

La configuration évaluée correspond au mode « émission ».

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 la DCSSI 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

Le rapport technique d'évaluation [RTE], remis par le CEACI à la DCSSI le 17 février 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ». Concernant les tâches liées au cycle de vie, le verdict à réussite a été établi par la DCSSI sur la base des rapports d'évaluation de l'environnement d'Atmel réalisés par un autre CESTI (Serma Technologies).

Au-delà des tâches de conformité et des tests sur émulateur, l'évaluateur a réalisé des tests de pénétration sur la bibliothèque 00.03.11.05 embarquée sur le composant **AT90SC28872RCU** de la famille AT90SC.

La version publique de ce rapport [RTE_Lite] a été remis à la DCSSI le 9 mars 2009 et pourra être utilisée dans le cadre d'une composition entre une puce de la famille AT90SC, par ailleurs certifiée, de la bibliothèque 00.03.11.05 et d'un logiciel embarqué (cf. §3.2).

L'évaluateur d'un produit composite, muni d'une puce spécifique de la famille AT90SC, pourra alors s'appuyer sur l'analyse de vulnérabilité décrite au sein du rapport [RTE_Lite] afin de construire sa propre analyse globale et son propre plan de tests de pénétration sur le produit composite, incluant éventuellement des tests sur les fonctions de la bibliothèque utilisées par le logiciel embarqué.

2.3. Analyse de la résistance des mécanismes cryptographiques

Le produit évalué offre les services cryptographiques identifiés au §1.2.2 de ce rapport. Ces services 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 qui utilise la bibliothèque évaluée.

3. La certification

3.1. Conclusion

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

Ce certificat atteste que la bibliothèque logicielle cryptographique « ATMEL Toolbox 00.03.11.05 » soumise 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 de la bibliothèque logicielle cryptographique à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet intégrant cette bibliothèque ne pourra être appréciée que par une évaluation de ce produit complet (cf. §2.2), laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

La présente certification ne garantit pas que les résultats obtenus sont valides pour tous les composants de la famille AT90SC. Néanmoins, au-delà des tâches de conformité et des tests sur émulateur, cette certification atteste (cf. §2.2) que lors de l'évaluation, des tests ont été réalisés sur une puce témoin (AT90SC28872RCU) de la famille AT90SC, permettant ainsi d'obtenir des résultats concrets à l'issue de l'analyse théorique élaborée pour la bibliothèque logicielle 00.03.11.05.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifié dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- le développeur de logiciels embarqués doit respecter les exigences des documents suivants pour garantir que la bibliothèque logicielle cryptographique est utilisée de façon sûre :
  - guides de la bibliothèque [GUIDES] ;
  - conclusions du rapport technique d'évaluation pour la composition [RTE-Lite] relatives au logiciel embarqué.
- les données utilisateurs critiques (particulièrement les clés cryptographiques) doivent être traitées par le logiciel embarqué conformément au besoin de sécurité relatif au contexte de l'application finale.
- la sécurité fournie par la plate-forme matérielle embarquant la bibliothèque doit être d'un niveau suffisant pour garantir la protection totale de la bibliothèque et de ses données sensibles. La sécurité de la plate-forme matérielle est particulièrement

importante lors de l'utilisation de la bibliothèque conjointement au générateur de nombres aléatoires matériel pour générer des clés cryptographiques. Le générateur de nombres aléatoires devra notamment avoir été testé selon une métrique reconnue.

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 CC RA [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

[ST]	Cible de sécurité de référence pour l'évaluation : - Atmel Toolbox 00.03.11.05 on the AT90SC Family of devices - Security Target, Référence : TBX_00.03.11.05_ST_V1.3_28Oct08 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 : - Atmel Toolbox 00.03.11.05 on the AT90SC Family of devices - Security Target Lite, Référence : TPG0177A_19Dec08 Atmel Secure Microcontroller Solutions
[RTE]	Evaluation Technical Report - Project: Toolbox 1104, Reference: TBX1104_ETR, V2.0 CEACI
[RTE-Lite]	Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR for composite evaluation – Toolbox 1104, Référence : TBX1104_ETR_Lite, V3.0 CEACI
[CONF]	La liste de configuration est constituée des documents suivants : - Toolbox 00.03.11.05 Source Code & Configuration List, Référence : TPR0371CX-SMIC, rev C, 9Sep08 Atmel Secure Microcontroller Solutions - TBX1104 deliverables list, Référence : TBX_00.03.11.05_EDL_V1.5_29Oct08 Atmel Secure Microcontroller Solutions
[GUIDES]	Les guides sont constituée des documents suivants : - AdvX for AT90SC Family, Référence: TPR0116CX_13Dec06, rev C Atmel Secure Microcontroller Solutions - AT90SC Enhanced Security Technical Datasheet, Référence : TPR0255CX_SPD_22Nov07 Atmel Secure Microcontroller Solutions - AT90SC Technical Datasheet, Référence : TPR0160BX_SMS_03Oct07, rev B Atmel Secure Microcontroller Solutions - AT90SC28872RCU Technical DataSheet, Référence : TPR0235CX_SPD_22Nov07 Atmel Secure Microcontroller Solutions - Generating Unpredictable Random Numbers with a controlled Entropy on the AT90SC family of Devices, Référence : TPR0166CX, rev C Atmel Secure Microcontroller Solutions

	- Securing Toolbox Operations using version 00.03.11.xx on ASL5, Référence : TPR0375BX_08Dec08, rev B 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.*

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)
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik