



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-2012/21

**Microcontrôleur RISC AT90SC28880RCV /
AT90SC28848RCV, Rev A**

Paris, le 12 juin 2012

*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 présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

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

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2012/21

Nom du produit

**Microcontrôleur RISC AT90SC28880RCV /
AT90SC28848RCV, Rev A**

Référence/version du produit

**Révision A pour le microcontrôleur
versions 00.03.12.00 / 00.03.11.08 / 00.03.10.02 / 00.03.14.03 pour la
bibliothèque cryptographique logicielle**

Conformité à un profil de protection

**[PP0035] : Security IC platform Protection Profile
Version 1.0**

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

**EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5**

Développeur

**Inside Secure
Maxwell Building – Scottish Enterprise Technology Park
East Kilbride – Glasgow G75 0QF - Ecosse
Tél : +44 1355 356668**

Commanditaire

**Inside Secure
Maxwell Building – Scottish Enterprise Technology Park
East Kilbride – Glasgow G75 0QF - Ecosse
Tél : +44 1355 356668**

Centre d'évaluation

**Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France**

Accords de reconnaissance applicables



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 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	9
1.2.5. <i>Configuration évaluée</i>	11
2. L’EVALUATION	12
2.1. REFERENTIELS D’EVALUATION.....	12
2.2. TRAVAUX D’EVALUATION	12
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	12
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	12
3. LA CERTIFICATION	13
3.1. CONCLUSION	13
3.2. RESTRICTIONS D’USAGE.....	13
3.3. RECONNAISSANCE DU CERTIFICAT	14
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	14
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	14
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	15
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	16
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	18

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « Microcontrôleur RISC AT90SC28880RCV / AT90SC28848RCV, Rev A » développé par Inside Secure.

Pour des raisons commerciales, ce produit est vendu sous les deux références AT90SC28880RCV et AT90SC28848RCV, la différence entre les deux réside uniquement dans la taille de mémoire proposée.

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, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est strictement conforme au profil de protection [PP0035].

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 :

- microcontrôleur : AT90SC28880RCV, **Revision A** ; la référence interne d'Inside Secure est AT59U12 ; celle-ci, ainsi que la lettre A de la révision sont marquées sur le composant ;
- librairie cryptographique logicielle : « **Toolbox 00.03.12.00 ou 00.03.11.08 ou 00.03.10.02 ou 00.03.14.03** » (de la version la plus complète à la moins complète, voir [ST] au chapitre 1.4.2.3 *Cryptographic Toolbox Software* et paragraphe suivant du présent rapport de certification).

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire EEPROM (non effaçable) :

- identification du microcontrôleur AT90SC28880RCV : **0x56** par lecture du registre SN_0 ;
- révision : **0x00** pour la **révision A** par lecture du registre SN_1 ;
- version de la bibliothèque cryptographique *Toolbox* disponible via la commande *SelfTest*. Les valeurs retournées devront être :

- 0x00031403 pour la version 00.03.14.03 incluant les fonctionnalités suivantes : *SefTest*, *AIS31OnlineTest*, *PrimeGen (Miller Rabin)*, *RSA without CRT* et *RSA with CRT* ;
- 0x00031002 pour la version 00.03.10.02 incluant les fonctionnalités précédentes ainsi que SHA-1, SHA-224 et SHA 256 ;
- 0x00031108 pour la version 00.03.11.08 incluant les fonctionnalités précédentes ainsi que *ECDSA over Zp* et *EC-DH over Zp* ;
- 0x00031200 pour la version 00.03.12.00 incluant toutes les fonctionnalités précédentes ainsi que *ECDSA over GF (2n)*, *EC-DH over GF (2n)*, SHA-384 et SHA-512.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par la TOE (*Target Of Evaluation* – cible d'évaluation) sont :

- la protection contre les attaques physiques, pour lesquelles la TOE dispose de mécanisme :
 - de surveillance de la tension ;
 - de surveillance de la fréquence ;
 - de surveillance de la température ;
 - de détection de *glitch* ;
 - de détection de sondes (*probing*) par la présence d'un bouclier actif ;
 - de détection de la lumière ;
 - de détection de violation d'EPO (*Enhanced Protection Object*) ;
 - de détection de perturbation (présence de registres redondés) ;
 - de vérification de *CStack* ;
- la gestion sécurisée de la mémoire ainsi qu'une protection des accès à cette mémoire.

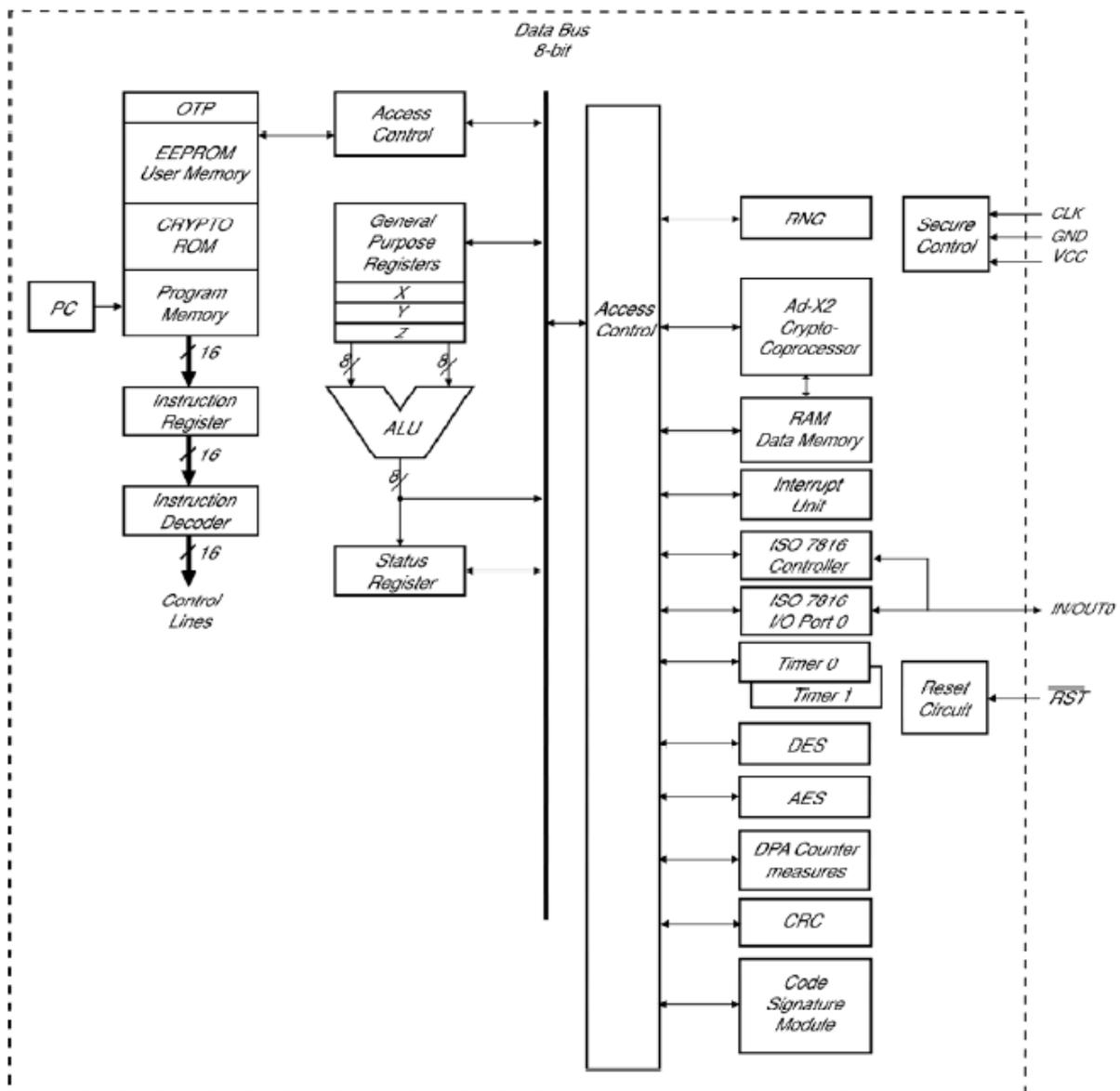
1.2.3. Architecture

Le produit est constitué des éléments suivants :

- une partie matérielle composée en particulier :
 - d'un processeur 8/16 bits RISC CPU ® *Core Enhanced RISC Architecture*, fabriqué en technologie 0.13 μm ;
 - d'un accélérateur cryptographique 32-bits *Ad-X2* pour les opérations à clé publique ;
 - d'un moteur CRC 16 et 32 conforme à l'ISO/IEC 3309 ;
 - d'un module de signature de code ;
 - d'un composant AES matériel ;
 - de composants DES et TDES matériels ;
 - d'un contrôleur d'interruptions à deux niveaux ;
 - d'un générateur d'aléa physique ;
 - de deux *timers* 16 bits ;
 - d'un oscillateur interne programmable (jusqu'à 30 MHz pour *Ad-X2* et pour les horloges internes) ;
 - d'un contrôleur ISO 7816 (jusqu'à 625 kbps à 5 MHz) et supportant les protocoles T=0 et T=1 ;
 - d'un port I/O ;

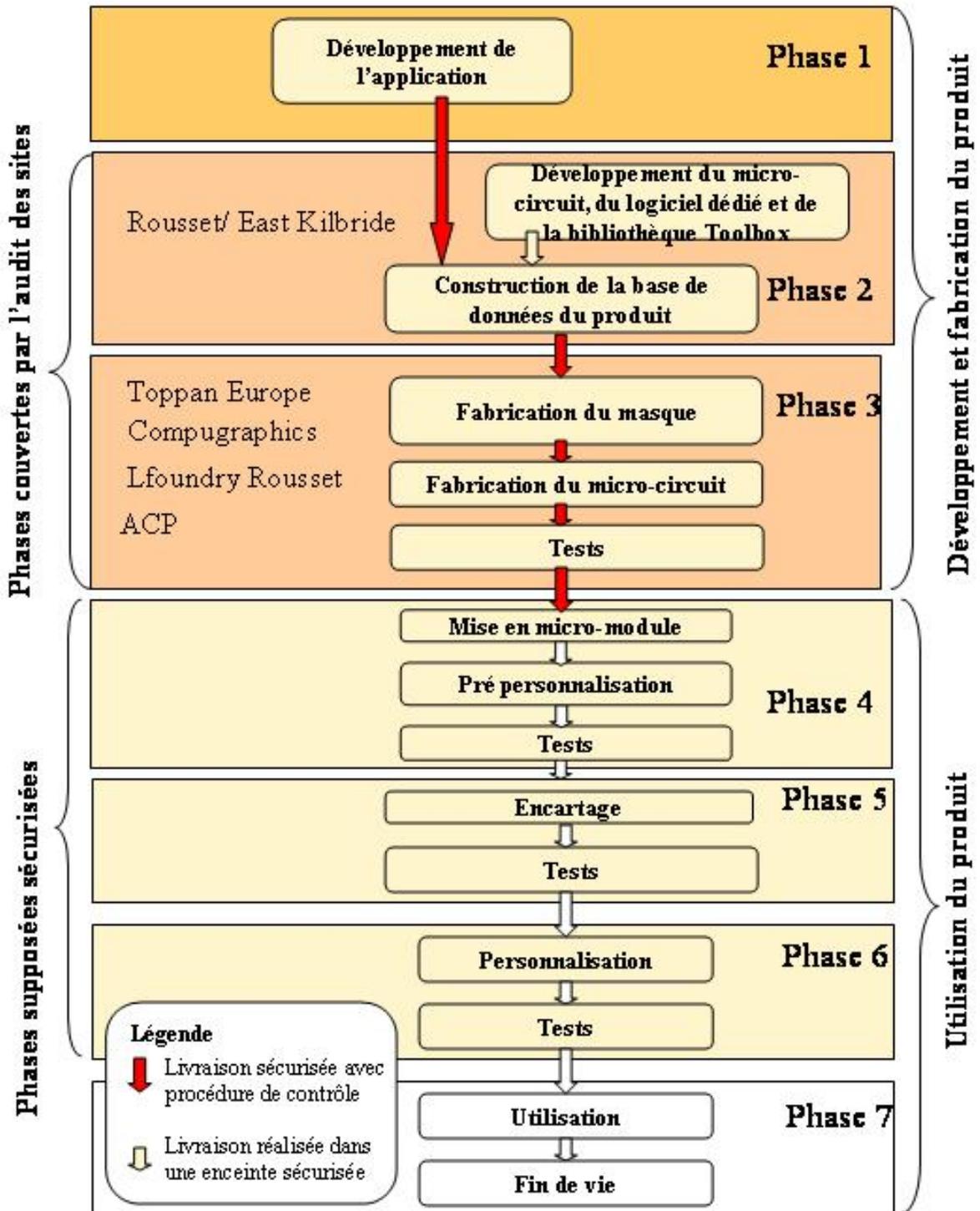
- de mémoires :
 - 288 Ko de ROM dont 32 Ko pour la *Toolbox* ;
 - 80 Ko d'EEPROM incluant 128 octets d'OTP et 384 octets adressables par bit ;
 - 8 Ko de mémoire RAM dont 2Ko de mémoire partagée entre le coprocesseur cryptographique *Ad-X2* et le processeur ;
- une partie logicielle comprenant :
 - en ROM et en EEPROM, des logiciels de test du microcontrôleur. Ces logiciels sont embarqués pour les besoins de l'évaluation et ne font pas partie de la TOE ;
 - en ROM, la librairie cryptographique *Toolbox* décrite au paragraphe 1.2.1. La librairie fait partie de la TOE.

L'architecture matérielle du produit peut être représentée de la façon suivante :



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants :

- la conception est assurée sur les sites :

Inside East Kilbride

Scottish Technology Park
East Kilbride
G75 0QF
Ecosse
Royaume Uni

Inside Rousset

Site de Rousset
Zone Industrielle
13106 Rousset Cedex
France

- la fabrication des masques est assurée sur les sites :

Toppan Europe

Toppan Photomaks Europe
01109 Dresden
Allemagne

Toppan Europe

Toppan Photomaks Europe,
91105 Corbeil Essonne Cedex
France

Compugraphics International Limited

Newark Road North,
Eastfield Industrial Estate
KY7 4NT
Ecosse
Royaume Uni

- la fabrication des *wafer* est assurée sur le site :

Lfoundry

Lfoundry Rousset
Zone Industrielle
13106 Rousset Cedex
France



- les tests sont assurés sur le site :

Atmel Test Centre (ACP)

102 Accuracy Drive Corner Excellence Avenue
Cametray Industrial Park 1
Canlubang City
4028 Laguna
Philippines

Le produit comporte lui-même une gestion de son cycle de vie, prenant la forme de trois modes :

- mode « *Test* », qui permet à l'administrateur de tester la TOE, de l'initialiser avec les paramètres de l'utilisateur et de la verrouiller en mode « *User* » ou mode « *Package* » ;
- mode « *User* », qui permet à l'utilisateur (développeur de l'application) de charger son code en EEPROM ; c'est aussi le mode final d'utilisation du microcontrôleur par le porteur du produit final ; le produit a été évalué dans ce mode ;
- mode « *Package* », qui est utilisé pour diagnostiquer le produit s'il se trouve défaillant ; dans ce mode, les droits d'accès à la TOE sont restreints et l'application de l'utilisateur chargée en EEPROM est automatiquement effacée.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et à la bibliothèque cryptographique. Toute autre application éventuellement embarquée, notamment les logiciels de test du microcontrôleur embarqués pour les besoins de l'évaluation, ne fait donc pas partie du périmètre d'évaluation.

Au regard du cycle de vie, le produit évalué est le produit qui sort de la phase 3 (au titre d'ALC) du cycle de vie.

Pour les besoins de l'évaluation, le produit fourni au centre d'évaluation est le microcontrôleur AT90SC28880RCV en révision A incluant la bibliothèque cryptographique *Toolbox* en version complète 00.03.12.00. Enfin, pour les besoins de l'évaluation, une application de test d'Inside Secure présente en ROM mais ne faisant pas partie de la TOE a été livrée.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 avril 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF-CRY] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

La TOE embarque un générateur d'aléas physique (TRNG - *True Random Number Generator*). Le générateur alimente un registre à décalage (LFSR - *Linear Feedback Shift Register*) de façon à fournir une valeur aléatoire. Celle-ci est alors rendue disponible pour l'application dans un registre. Ce générateur a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation : il atteint le niveau « P2 – SOF High ».

Par ailleurs, les quatre variantes de la Toolbox comprennent des routines d'autotest pour le TRNG.

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 produit « Microcontrôleur RISC AT90SC28880RCV / AT90SC28848RCV, Rev A » 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 « Microcontrôleur RISC AT90SC28880RCV / AT90SC28848RCV, Rev A » 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 de ce 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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- la vérification d'un point de validité pour ECC (« *Check a point's validity* »), qui est indiquée comme « obligatoire » au §5.5.7.2 du document référencé TPR0455EX version E dans [GUIDES] ;
- la vérification de l'intégrité des calculs DES (« *Check computation integrity* ») indiquée au §3.7 du document référencé TPR0400FX version F dans [GUIDES] ;
- la vérification de l'intégrité des calculs AES (« *Check computation integrity* ») indiquée au §3.6 du document référencé TPR0428DX version D dans [GUIDES] ;
- la vérification de la primalité des nombres devant être premiers (« *Primality checking* »), qui est indiquée obligatoire au §3.6.7.2 du document référencé TPR0455EX version E dans [GUIDES] ;
- les points à prendre en compte par l'application (« *Mandatory running considerations* ») qui sont indiqués comme obligatoires au §4.1.1 du document référencé TPR0456DX version D dans [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 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé 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 signataires², 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'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	3	3	Testing modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - KIBERIA Security Target, référence Kiberia_ST_V1.4, version 1.4, Inside Secure. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite AT90SC28880RCV / AT90SC28848RCV, référence TPG0219B, version B Inside Secure.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report KIBERIA project, référence KIBERIA_ETR_v1.2/ v1.2, Serma Technologies. <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"> - ETR Lite for Composition - KIBERIA project, référence KIBERIA_ETR_Lite_v1.1 / v1.1, Serma Technologies.
[CONF]	<p>Liste de configuration du produit</p> <ul style="list-style-type: none"> - Kiberia document list, référence Kiberia_EDL, version 1.2, Inside Secure.
[GUIDES]	<p>Guide du produit :</p> <ul style="list-style-type: none"> - AT90SC28880RCV Technical Datasheet, référence TPR0459CX, version C, Inside Secure ; - AT90SC Enhanced Security Technical Datasheet, référence TPR0447DX, version D, Inside Secure ; - AD-X2 Technical Datasheet, référence TPR0452CX, version C, Inside Secure ; - The Code Signature Module, référence TPR0409CX, version C Inside Secure ; - Secure Hardware DES/TDES on AT90SC 0.13µm products, référence TPR0400FX, version F Inside Secure ; - Security Recommendations for 0.13µm Products, référence TPR0456DX, version D Inside Secure ; - Toolbox 00.03.1x.xx on AT90SCxxxxC, référence TPR0454CX, version C Inside Secure ;



	<ul style="list-style-type: none">- Secure use of Tbx 00.03.1x.xx, référence TPR0455EX, version E Inside Secure ;- Efficient use of Ad-X2, référence TPR0463BX, version B, Inside Secure ;- Generating Random numbers to known standards for 0.13µm products, référence TPR0468CX, version C Inside Secure ;- Secure Hardware AES for 0.13µm products, référence TPR0428DX, version D, Inside Secure;- Customer Option Form, référence PNL/FORMxx, version 4.6.2, Inside Secure ;- SmartACT_Users_Manual, référence TPR0134DX, version D, Inside Secure ;- Wafer Saw Recommendations, référence TPG0079BX, version B Inside Secure.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007 certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.

Annexe 3. Références liées à la certification

<p>Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</p>
[CC IC]	<p>Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.</p>
[CC AP]	<p>Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF-CRY]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.</p>
[AIS31]	<p>Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).</p>