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-2011/65

Microcontrôleur RISC AT90SC20818RCV/AT90SC20812RCV, Rev C

Paris, le 19 décembre 2011

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

[ORIGINAL SIGNE]

Patrick Pailloux

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 et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/65

Nom du produit

Microcontrôleur RISC
AT90SC20818RCV/AT90SC20812RCV, Rev C

Référence/version du produit

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(s)

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

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 37 78, mél : elisabeth.crochon@cea.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 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

1.1. Présentation du produit

Le produit évalué est le « Microcontrôleur RISC AT90SC20818RCV/AT90SC20812RCV, Rev C» développé par Inside Secure. Pour raisons commerciales, ce microcontrôleur a les deux dénominations, AT90SC20818RCV et AT90SC20812RCV, mais il s'agit bien du même produit.

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

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 référence : AT90SC20818RCV/AT90SC20812RCV[1]**, *Revision* C** ;
- librairies logicielles : « ***Toolbox 00.03.1x.xx*** [2] ».

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire EEPROM (non effaçable) :
- identification du microcontrôleur : **0x54** pour 59U13 par lecture du registre SN_0 à l'adresse 0x000060 ;
- révision : **02** pour la **révision C** par lecture du registre SN_1 à l'adresse 0x000061 ;
- 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*, *AIS31 tests*, *PrimeGen*, *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 ;

[1] dont la référence interne Inside Secure est **59U13**
[2] 00.03.1x.xx décrivant les différentes valeurs possibles 00.03.14.03, 00.03.10.02, 00.03.11.08 ou 00.03.12.00 décrites plus bas dans ce même paragraphe.

- 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 le produit sont :

- la protection en intégrité et en confidentialité des données utilisateurs, dont les logiciels embarqués, que ce soit en exécution ou lorsqu'ils sont stockés dans les différentes mémoires de la TOE[1] ;
- la bonne exécution de services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles.

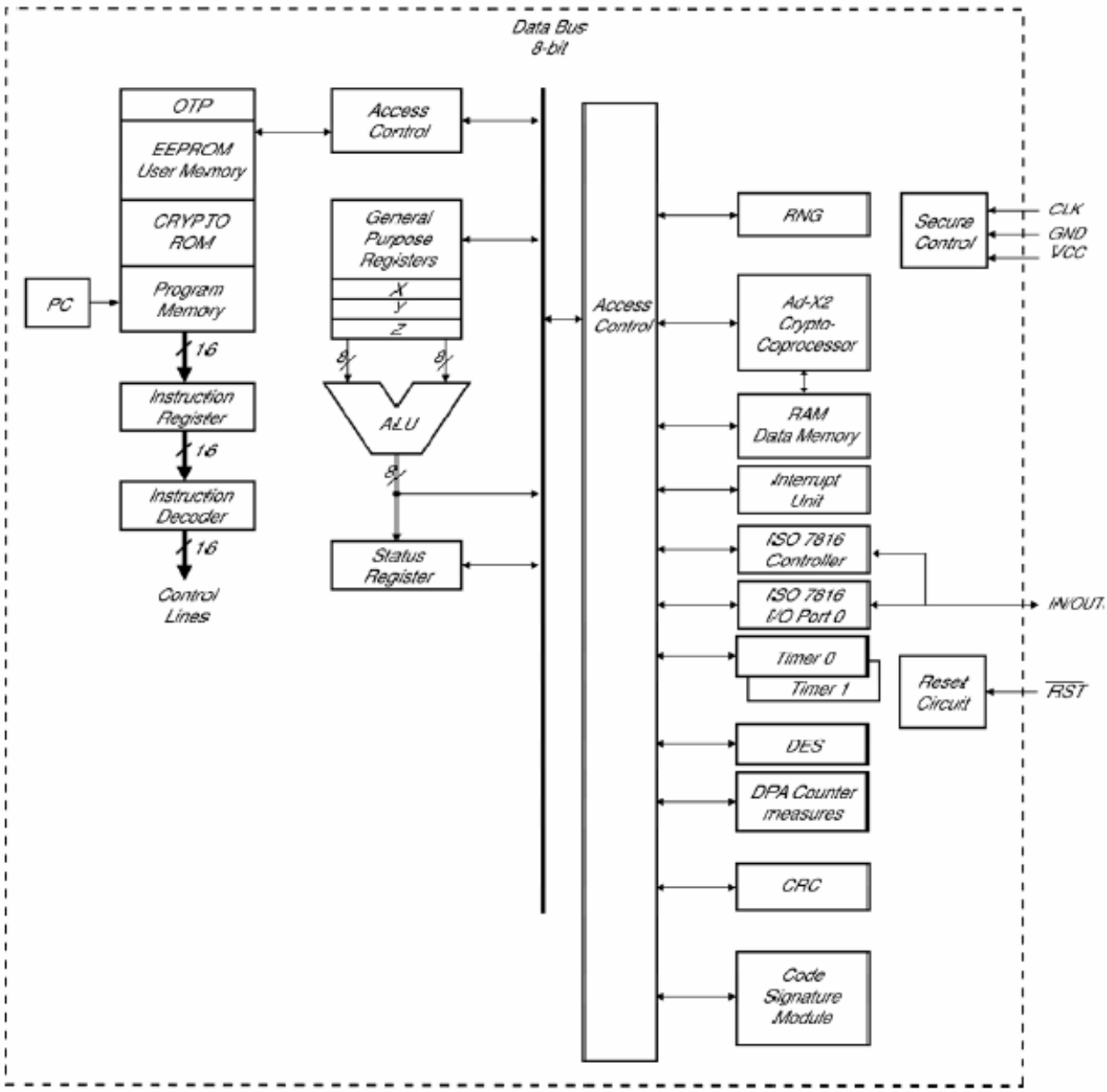
1.2.3. Architecture

Le microcontrôleur AT90SC20818RCV/AT90SC20812RCV, Rev C est constitué des éléments suivants :

- une partie matérielle composée en particulier :
  - d'un processeur 8-/16-bit RISC CPU ® *Core Enhanced RISC Architecture* ;
  - de mémoires :
    - 18 Ko (dont 128 octets d'OTP) de mémoire EEPROM ;
    - 176 Ko de mémoire ROM pour le stockage des programmes utilisateurs y compris la librairie cryptographique *Toolbox* d'Inside ;
    - 6 Ko de mémoire RAM dont 2Ko partagée entre le coprocesseur cryptographique *Ad-X2* et le processeur ;
  - de modules de sécurité : gestion de mémoire sécurisée (SMM), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes ;
  - de modules fonctionnels : gestion des entrées/sorties en mode contact (IART ISO 7816), générateurs de nombres aléatoires, crypto-processeurs DES/3DES ainsi qu'un accélérateur cryptographique 32-bit *Ad-X2* pour le support des algorithmes cryptographiques à clé publique.
- 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 cible d'évaluation (TOE) ;
  - en ROM, la librairie cryptographique *Toolbox* appartenant à la famille 00.03.1x.xx décrite ci-dessus. La librairie fait partie intégrante de la TOE.

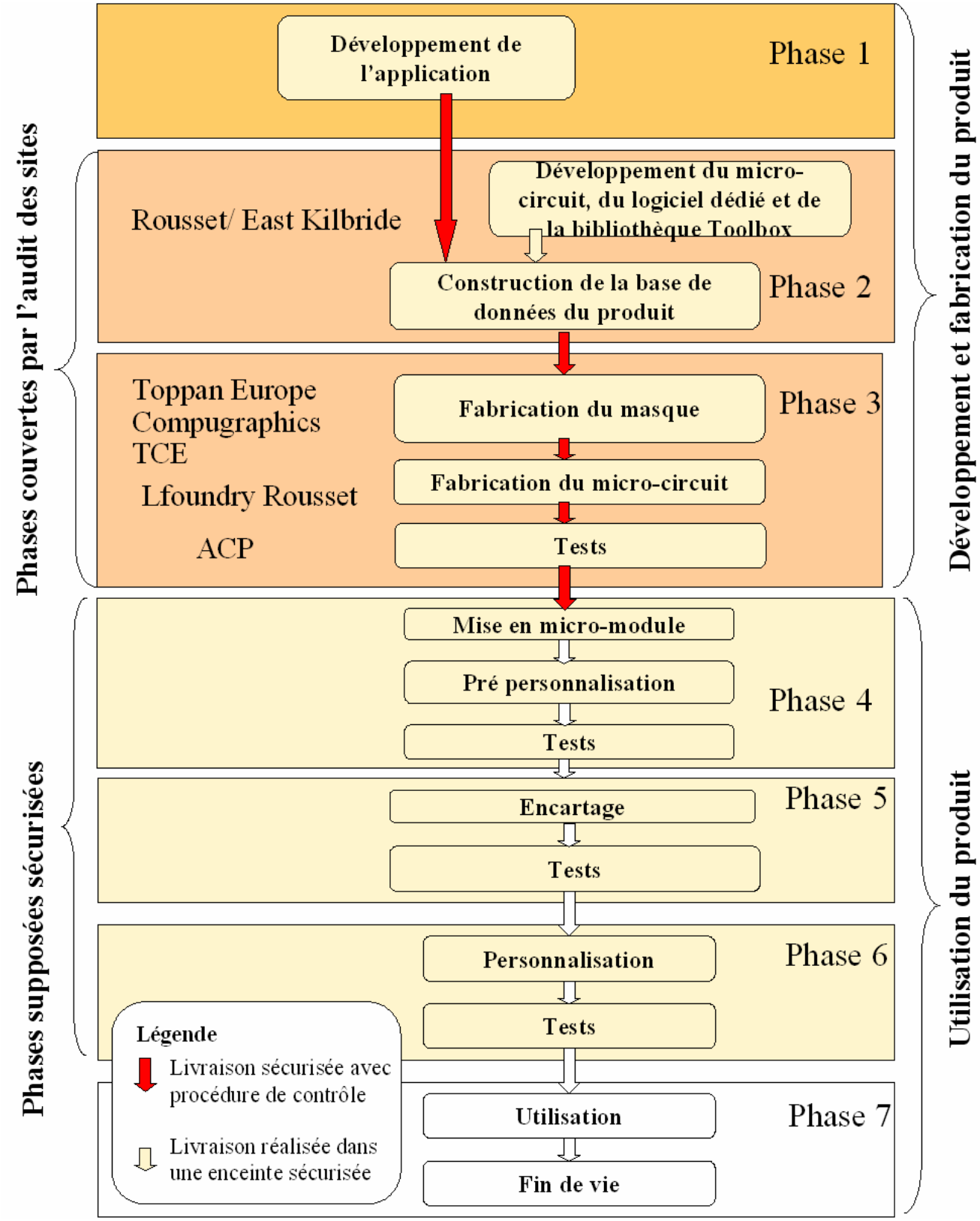
[1] *Target Of Evaluation* ou cible d'évaluation

L'architecture matérielle du microcontrôleur 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 :

- pour ce qui concerne la conception :

  Inside East Kilbride

  Scottish Technology Park
  East Kilbride
  G75 0QF

  Ecosse
  Royaume Uni

  Inside Rousset

  Site de Rousset
  Zone Industrielle
  13106 Rousset Cedex

  France

- pour ce qui concerne la fabrication des masques :

  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

  TCE

  Toppan Chengwa Electronics,
  1127-3 Hopin Road
  Padeh City
  Taoyuan

  Taïwan 334

- pour ce qui concerne la fabrication des *wafer* :

  Lfoundry

  Lfoundry Rousset,
  Zone Industrielle
  13106 Rousset Cedex

  France

- pour ce qui concerne les tests :

  Atmel Test Centre (ACP)

  102 Accuracy Drive Corner Excellence Avenue,
  Cametray Indstrial 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 » : le microcontrôleur peut être utilisé avec des logiciels et des outils spécifiques de test. Il n'est disponible qu'aux personnels autorisés de l'équipe de développement et utilise des protocoles de communications non-ISO. Ce mode est désactivé lors du découpage des *wafer* ;
- mode « diagnostic » (encore appelé *package mode*) : mode utilisable durant tout le cycle de vie du microcontrôleur. Il permet aux personnels autorisés de l'équipe de développement d'effectuer différents tests ;
- mode « utilisateur » : mode final d'utilisation du microcontrôleur.

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 AT90SC20818RCV/AT90SC20812RCV (en révision C) incluant la bibliothèque cryptographique *Toolbox* en version complète 00.03.12.00. Enfin, pour les besoins de l'évaluation, une application de test INSIDE 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].
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.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 novembre 2011, 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 les référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT] 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

Les générateurs d'aléas *RNGDAS*[1] et *RDWDR*[2] sont des *TRNG*[3] et ont été évalués par le CESTI.
Le générateur d'aléas *RNGDAS* est construit directement à partir du support matériel. Le générateur d'aléas *RDWDR* est construit à partir de *RNGDAS* associé à un *LFSR*[4]. Ces deux générateurs ont fait l'objet de tests statistiques de la part du CESTI.
L'utilisation du générateur *RDWDR* est préconisée. Dans le cas où ce générateur est 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 selon le référentiel [REF-CRY].

[1] *Random Number Generator Digitized Analog Source*
[2] *RanDom WorD Register*
[3] *True Random Generator*
[4] *Linear Feedback Shift Register*

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 AT90SC20818RCV/AT90SC20812RCV, Rev C » 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 AT90SC20818RCV/AT90SC20812RCV, Rev C » 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 microcontrôleur 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 de l'application des mesures précisées en 2.4 ainsi que du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre scrupuleusement les recommandations et contre-mesures 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 2010 permet la reconnaissance, par les pays signataires de l'accord[1], 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 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'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**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**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**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**3**	Testing modular 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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target AT90SC20818RCV/AT90SC20812RCV (Dakala), version 1.6, reference Dakala_ST_V1.6, 25th November 2011,* Inside Secure ; Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Lite AT90SC20818RCV/AT90SC20812RCV, reference TGP0212C-VIC, 19th October 2011,* Inside Secure.
[RTE]	Rapport technique d'évaluation : - DAKALA Rapport Technique d'Evaluation, référence LETI.CESTI.DAK.RTE.001 v2.1 -28 Novembre 2011, CEA-LETI ; Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report for composition (ETR_lite), reference* LETI.CESTI.DAK.RTE_lite.002 v2.0 – 15 décembre 2011, CEA LETI.
[CONF]	Liste de configuration du produit - Liste de configuration de la fabrication *Manufacturing Configuration Liste, reference 59U13_DESIGN_C_MASK_ORDER.htm, 12th May 2011,* Inside Secure ; - *Toolbox 3.x Crypto Library Software Development Tools Configuration List, reference TPR153EX-SMS-16 Aug 10, 16th August 2010,* Inside Secure ; - Liste des fournitures Dakala *Deliverable List, reference Dakala_EDL_V1.4 – 25th November 2011,* Inside Secure.
[GUIDES]	- *SmartACT 's User, reference TPR0134DX-VIC, 18th February 2011,* Inside Secure ; - *Ad-X2 Datasheet, reference TPR0452CX-VIC, 15th June 2011,* Inside Secure ; - *Efficient use of Ad-X2, reference TPR0463BX-VIC, 2nd February 2011,* Inside Secure ; - *The Code Signature Module for 0.13µm Products, reference TPR0409CX-VIC, 28th January 2011,* Inside Secure ; - *Secured Hardware DES/TDES for 0.13µm Products, reference TPR0400FX, 7h April 2011,* Inside Secure ; - *Generating Random numbers to known standards for 0.13µm products, reference TPR0468CX-VIC, 14h March 2011,* Inside Secure ; - *Code Entry Customer Options Form, reference COF_4_6.pdf, revision 4.6,* Inside Secure ; - *Technical Datasheet (Preliminary) AT90SC 0.13µm products, reference TPR0447DX-VIC, 20th June 2011*, Inside Secure ; - *Technical Datasheet (Preliminary) AT90SC20818RCV,*

	reference TPR0458BX-VIC, 2nd February 2011, Inside Secure ; - *Toolbox 00.03.1.x.xx on AT90SCXXXXC*, *TPR0454CX-VIC, 23rd February 2011*, Inside Secure ; - *Wafer Saw Recommendations, TPG0079BX, reference TPG0079BX, 10th February 2011*, Inside Secure ; - *Security recommendations for 0,13 µm products -2, TPR0456CX, 28th January 2011,* Inside Secure ; - *Secure use of TBX 00.03.1x.xx on AT90SC, TPR0455CX, 24th February 2011,* Inside Secure.
[PP0035]	*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

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.	
[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, 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	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.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, February 2009.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	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.
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.