



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-2011/46**

### **Microcontrôleur RISC AT90SC28880RCFV, Rev G**

*Paris, le 26 OCT. 2011*

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

[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](mailto:certification.anssi@ssi.gouv.fr)

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

Référence du rapport de certification	<b>ANSSI-CC-2011/46</b>
Nom du produit	<b>Microcontrôleur RISC AT90SC28880RCFV, Rev G</b>
Référence/version du produit	
Conformité à un profil de protection	<b>[PP0035] : Security IC platform Protection Profile Version 1.0</b>
Critères d'évaluation et version	<b>Critères Communs version 3.1 révision 3</b>
Niveau d'évaluation	<b>EAL 5 augmenté ALC_DVS.2, AVA_VAN.5</b>
Développeur(s)	<b>Inside Secure</b> Maxwell Building – Scottish Enterprise Technology Park East Kilbride – Glasgow G75 0QF - Ecosse Tél : +44 1355 356668
Commanditaire	<b>Inside Secure</b> Maxwell Building – Scottish Enterprise Technology Park East Kilbride – Glasgow G75 0QF - Ecosse Tél : +44 1355 356668
Centre d'évaluation	<b>CEA - LETI</b> 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	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;"><b>CCRA</b> </div><div style="text-align: center;"><b>SOG-IS</b> </div></div> <p><b>Le produit est reconnu au niveau EAL4.</b></p>

# 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
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
<b>2. L’EVALUATION .....</b>	<b>12</b>
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
<b>3. LA CERTIFICATION .....</b>	<b>13</b>
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
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>15</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>16</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le « Microcontrôleur RISC AT90SC28880RCFV, Rev G » développé par Inside Secure.

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 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 : **AT59U05, Revision G** ;
- bibliothèques logicielles : « *Toolbox 00.03.1x.xx*<sup>1</sup> ».

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

- identification du microcontrôleur : **0x3E** pour AT59U05 par lecture du registre SN\_0 à l'adresse 0x000060 ;
- révision : **06** pour la **révision G** 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 :
  - o 0x00031403 pour la version 00.03.14.03 incluant les fonctionnalités suivantes : *SelfTest, AIS31 tests, PrimeGen, RSA without CRT* et *RSA with CRT* ;
  - o 0x00031002 pour la version 00.03.10.02 incluant les fonctionnalités précédentes ainsi que SHA-1, SHA-224 et SHA 256 ;
  - o 0x00031108 pour la version 00.03.11.08 incluant les fonctionnalités précédentes ainsi que *ECDSA over Zp* et *EC-DH over Zp* ;

---

<sup>1</sup> 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.

- 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.

Ces éléments ont été vérifiés par l'évaluateur.

### 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<sup>1</sup> ;
- 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

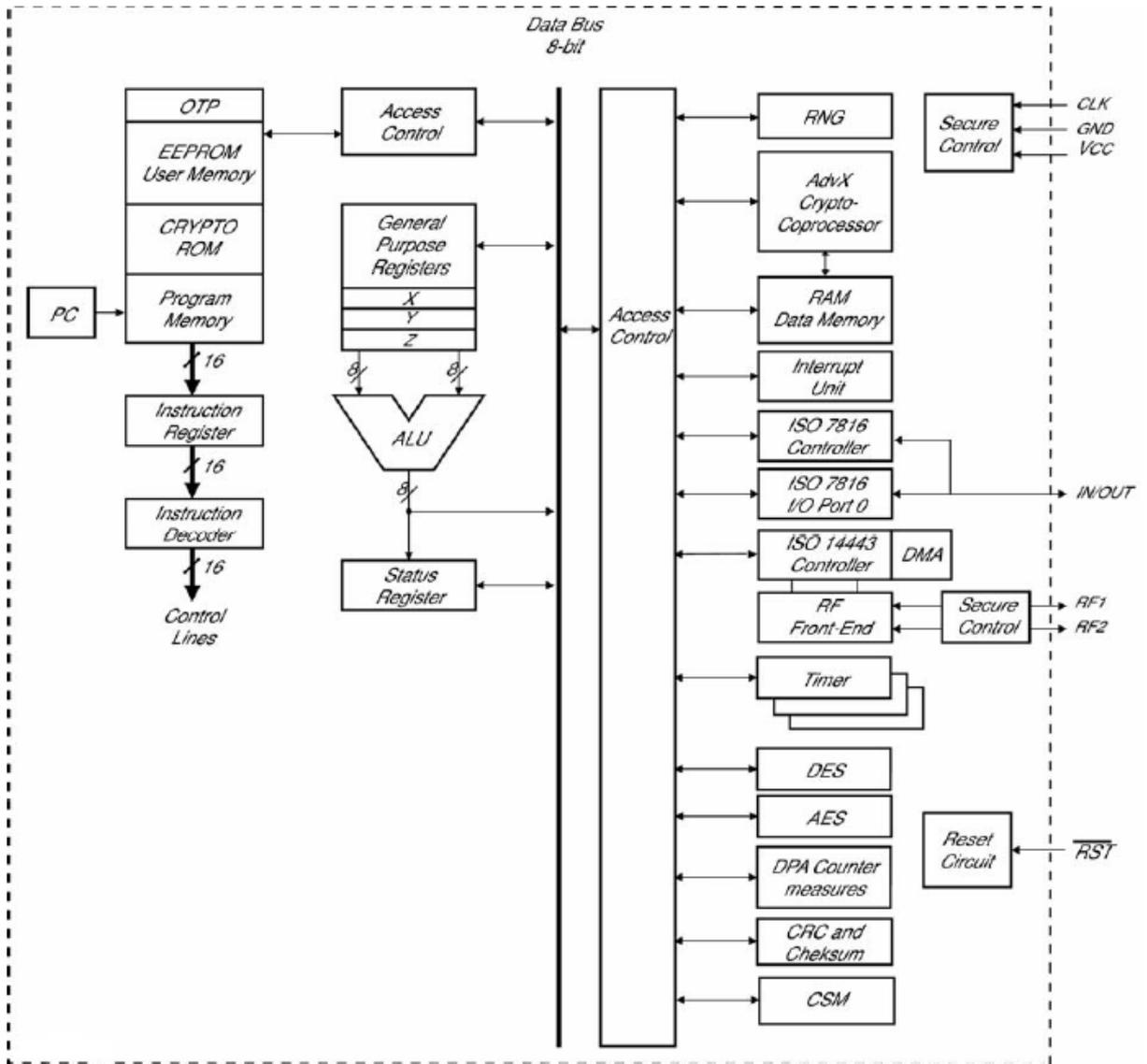
Le microcontrôleur AT90SC28880RCFV est constitué des éléments suivants :

- une partie matérielle composée en particulier :
  - d'un processeur 8-/16-bit RISC CPU ® Core Enhanced;
  - de mémoires :
    - 80 Ko (dont 128 octets d'OTP) de mémoire EEPROM ;
    - 288 Ko de mémoire ROM pour le stockage des programmes utilisateurs ;
    - 8 Ko de mémoire RAM dont 2Ko partagées entre le coprocesseur cryptographique et le processeur ;
  - de modules de sécurité : gestion de mémoire sécurisé (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) et *contactless* (ISO 14443 type B), générateurs de nombres aléatoires, crypto-processeurs DES/3DES et AES ainsi qu'un accélérateur cryptographique 32-bit Ad-X 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.

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

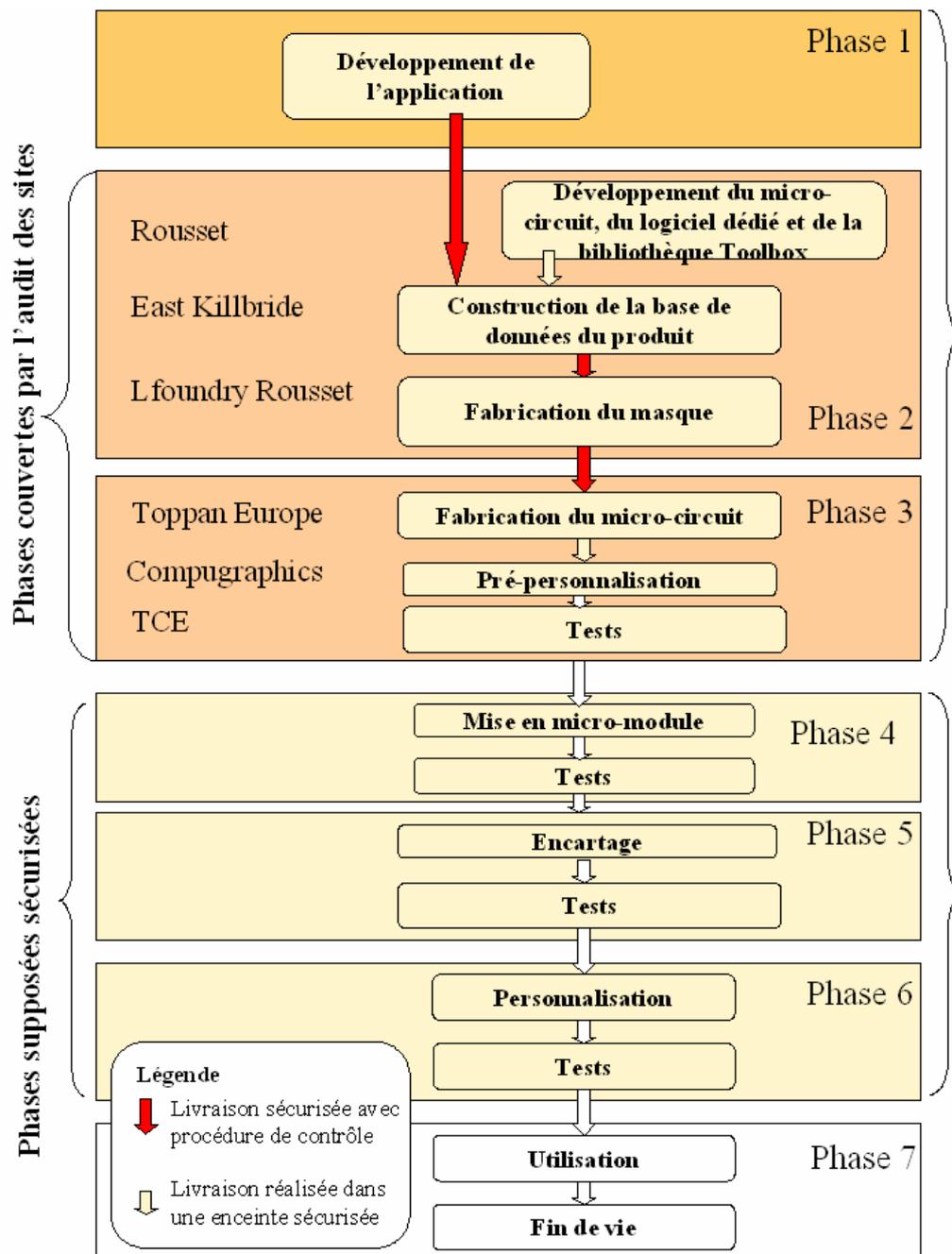
---

<sup>1</sup> *Target Of Evaluation* ou cible d'évaluation



### 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 wafer

**Lfoundry**

Lfoundry Rousset,  
Zone Industrielle  
13106 Rousset Cedex  
France

- pour ce qui concerne le reste de la fabrication :

**Toppan Europe**

Toppan Photomaks Europe,  
01109 Dresden  
Allemagne

**Toppan Europe**

Toppan Photomaks Europe,  
91105 Corbeil Essonne Cedex,  
France

**Compugraphics International Limited**

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

**TCE**

Toppan Chengwa Electronics,  
1127-3 Hopin Road  
Padeh City  
Taoyuan  
Taïwan 300

- pour ce qui concerne les tests :

**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 » : 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 routines embarquées 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 du cycle de vie.

Pour les besoins de l'évaluation, le produit fourni au centre d'évaluation est le microcontrôleur AT90SC28880RCFV (en révision G), de 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 16 septembre 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

Le générateur d'aléas a été évalué par le CESTI.

Le générateur d'aléas TRNG (*RDWDR output*) est construit directement à partir du support matériel et il a subi des tests statistiques de la part du CESTI.

Dans le cas où le TRNG 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 produit « Microcontrôleur RISC AT90SC28880RCFV, Rev G » 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 AT90SC28880RCFV, Rev G » 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, 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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> 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.

<sup>2</sup> 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> <p>Security Target AT90SC28880RCFV (Helium), version 1.6, reference HELIUM_ST_V1.7, 20<sup>th</sup> september 2011, Inside Secure ;</p> <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"> <li>- Security Target Lite AT90SC28880RCFV, reference TGP0210A, 22<sup>th</sup> September 2011, Inside Secure.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- <i>HELIUM Evaluation Technical Report, reference LETI.CESTI.HLM.RTE.001 - v1.3 -20 septembre 2011, CEA-LETI ;</i></li> </ul> <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"> <li>- <i>Evaluation Technical Report for composition (ETR_lite), reference LETI.CESTI.HLM.RTE.002_v1.0 -20 septembre 2011, CEA-LETI</i></li> </ul>
[CONF]	<p>Liste de configuration du produit</p> <ul style="list-style-type: none"> <li>- <i>Liste de configuration de la conception Design Configuration List, reference HELIUM_DCL_v1.1, version 1.1, 5<sup>th</sup> january 2011, Inside Secure ;</i></li> <li>- <i>Liste de configuration de la fabrication Manufacturing Configuration Liste, reference 59U05_DESIGN_G_MASK_ORDER.htm, 17<sup>th</sup> may 2009, Inside Secure ;</i></li> <li>- <i>Toolbox 3.x Crypto Library Software Development Tools configuration List, reference TPR153EX-SMS-16 Aug 10, 16<sup>th</sup> august 2010, Inside Secure ;</i></li> <li>- <i>Liste des fournitures Helium Deliverable List, reference Helium_EDL_V1.6_07Apr11.xls, Inside Secure.</i></li> </ul>
[GUIDES]	<ul style="list-style-type: none"> <li>- <i>SmartACT 's User, reference TPR0134DX, 18<sup>th</sup> February 2011,, Inside Secure ;</i></li> <li>- <i>Code Entry Customer Option Form, reference COF/FORM/Qpulse rev0, revision 3.5, Inside Secure ;</i></li> <li>- <i>AT90SC28880RCFV Die Dimensions and Bonding Pad Coordinates, reference TPG0203B-06Aug10, 6<sup>th</sup> august 2010, Inside Secure ;</i></li> <li>- <i>Technical Datasheet (Preliminary) AT90SCV28880RCFV, TPR0397FX, 25<sup>th</sup> january 2011, Inside Secure ;</i></li> <li>- <i>Application note Toolbox 00.03.1.x.xx on AT90SCV28880RCFV, TPR0454CX, 23<sup>rd</sup> february 2011, Inside Secure ;</i></li> <li>- <i>Wafer Saw Recommendations, TPG0079BX, reference TPG0079 revision B, 10 février 2011, Inside Secure ;</i></li> <li>- <i>Security recommendations for 0,13 µm products -2, TPR0456CX, 28<sup>th</sup> january 2011, Inside Secure ;</i></li> </ul>



	<p>- <i>Secure use of Tbx 00.03.lx.xx on AT90SC, TPR0455CX, 24<sup>th</sup> february 2011, Inside Secure.</i></p>
[PP0035]	<p><i>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.</i></p>

### 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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .