Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2013/59

Microcontrôleur AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04

Paris, le 24 décembre 2013

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

[Original signé]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

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-2013/59

Nom du produit

Microcontrôleur AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04

Référence/version du produit

Révision C (microcontrôleur), version 00.03.22.04 (bibliothèque cryptographique)

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 4

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

Commanditaire

Inside Secure

Maxwell Building – Scottish Enterprise Technology Park

East Kilbride – Glasgow G75 0QF - Ecosse

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

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 AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04 » 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

1.2.1. Introduction

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].

1.2.2. 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 :

- identification du microcontrôleur : AT90SC28880RCFV2, *Revision* C ; la référence interne Inside Secure est AT59U21 ; celle-ci, ainsi que la lettre C de la révision sont marquées sur le composant ;
- librairie cryptographique logicielle : « *Toolbox 00.03.22.04* » ; celle-ci constitue la variante la plus complète en termes de primitives cryptographiques offertes, elle inclut les 3 autres variantes 00.03.21.03; 00.03.20.02 et 00.03.24.02 constituées de sous-ensembles de primitives cryptographiques offertes (voir [ST] au chapitre 1.4.2.3 « *Cryptographic Toolbox Software* »).

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire EEPROM et écrits en phase de test (non effaçables) :

- identification du microcontrôleur AT90SC28880RCFV2 : 0x61 par lecture du registre SN_0 ;
- révision : 0x82 pour la révision C par lecture du registre SN_1 ;
- version de la bibliothèque cryptographique « *Toolbox* » disponible via la commande « *SelfTest* ». Les valeurs retournées sont :

- 0x00032402 pour la version 00.03.24.02 incluant les fonctionnalités suivantes : *SefTest, AIS31OnlineTest, PrimeGen (Miller Rabin), RSA without CRT* et *RSA with CRT* ;
- 0x00032002 pour la version 00.03.20.02 incluant les fonctionnalités précédentes ainsi que SHA-1, SHA-224 et SHA-256 ;
- 0x00032103 pour la version 00.03.21.03 incluant les fonctionnalités précédentes ainsi que *ECDSA over Zp* et *EC-DH over Zp* ;
- 0x00032204 pour la version 00.03.22.04 incluant toutes les fonctionnalités précédentes ainsi que *ECDSA over GF (2n), EC-DH over GF (2n)*, SHA-384 et SHA-512.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par la TOE[1] sont :

- la protection contre les attaques physiques, pour lesquelles la TOE dispose de mécanismes :
  - de surveillance de la tension ;
  - de surveillance de la fréquence ;
  - de surveillance de la température ;
  - de détection de signaux transitoires (« *glitch* ») ;
  - de détection de sondage (« *probing* », 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 la pile (« *CStack* ») ;
  - de détection d'erreurs de parité ;
  - d'horloge interne ;
- la gestion sécurisée de la mémoire ainsi qu'une protection des accès à cette mémoire ;
- la cryptographie, grâce aux processeurs DES[2] et AES ainsi qu'à l'accélérateur matériel Ad-X2 pour la cryptographie asymétrique ;
- la génération de nombres aléatoires.

1.2.4. Architecture

Le produit est constitué des éléments suivants :

- une partie matérielle composée en particulier :
  - d'un processeur 8-/16-bit « *Enhanced RISC Architecture CPU*» ;
  - d'un accélérateur cryptographique 32-bit 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 ;
  - de composants DES[2] et AES matériels conçus pour résister à la DPA / DMA ;
  - d'un contrôleur d'interruption à 2 niveaux ;
  - d'un générateur d'alea physique ;
  - de trois *timers* 16 bit ;
  - d'un oscillateur interne programmable ;

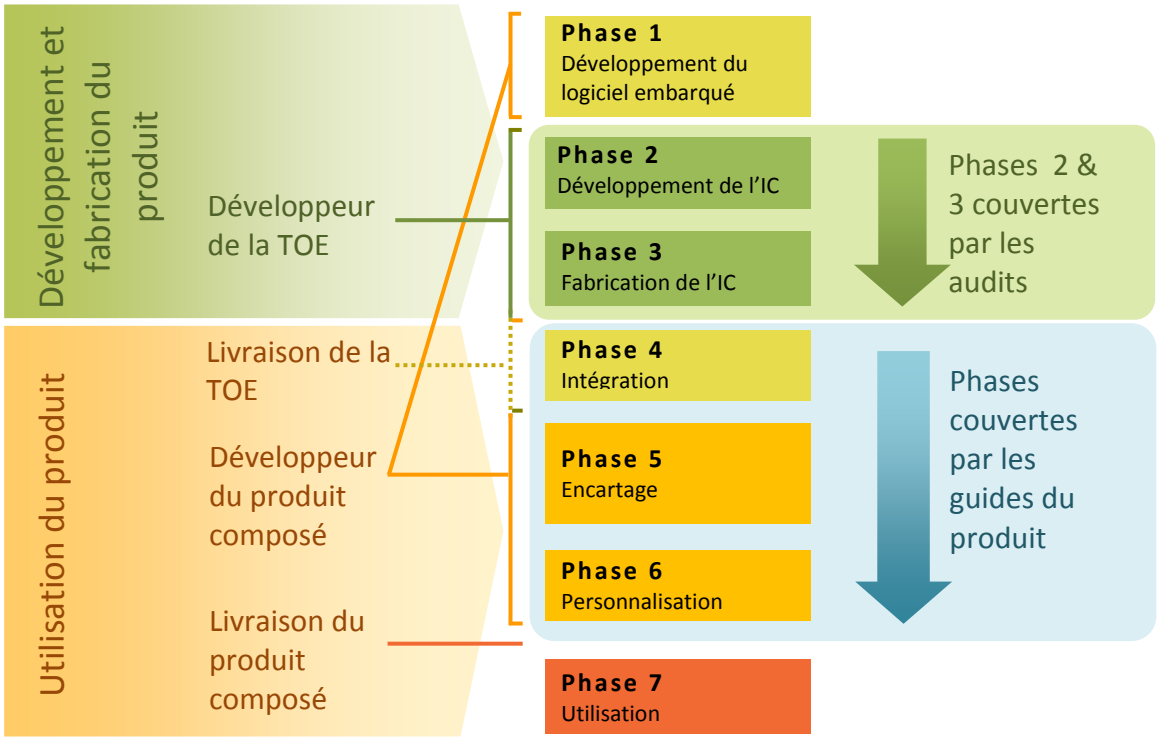
[1] *Target Of Evaluation* ou cible d'évaluation.
[2] Seul l'usage du chiffrement 3DES est inclus dans le périmètre de l'évaluation.

- o de contrôleurs ISO 7816 (contact) et ISO/IEC 14443 (sans-contact) ;
- o de mémoires :
  - ROM : 256Ko à disposition de l'utilisateur, 32Ko réservés à la bibliothèque *Toolbox* ;
  - EEPROM : 80Ko ;
  - RAM : 8Ko pour le CPU dont 2Ko partagés avec l'accélérateur matériel Ad-X2.

- une partie logicielle comprenant :
  - o 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 ;
  - o en ROM, la librairie cryptographique « *Toolbox* » appartenant à la famille 00.03.2x.xx décrite en 1.2.2. La librairie fait partie intégrante de la TOE ;

1.2.5. 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 Rousset
ZI Rousset Peynier
13106 Rousset Cedex
France

Inside East Kilbride
Scottish Enterprise Technology Park
East Kilbride
G75 OQR
Ecosse

Inside Aix
Parc du Golf
350 rue Guilibert Gauthier de la Lauzière
ZI Les Milles
13856 Aix en Provence
France

Inside Nice
Space Antipolis 9
2323 chemin Saint-Bernard
06225 Vallauris
France

Inside Singapour
77 science park drive
#02-18/19 CINTECH III
Singapore 118256

Inside Pologne
Sp. Z o.o.
Ul. Ostrobramska 101/336
04-041 Warszawa
Pologne

- la fabrication des masques est assurée sur les sites :

Toppan Europe
Toppan Photomaks Europe
01109 Dresden
Allemagne

Compugraphics International Limited
Newark Road North
Eastfield Industrial Estate
KY7 4NT
Ecosse

Toppan Europe
Toppan Photomaks Europe
91105 Corbeil Essonne Cedex
France

TCE
1127-3 Hopin Road
Padeh City
Taoyuan
Taïwan 30080 (République de Chine

- la fabrication des « wafers » est assurée sur les sites :

Lfoundry
Lfoundry Rousset
Zone Industrielle
13106 Rousset Cedex
France

UMC
Fab 8C & 8D
No. 3, Li-Hsin 2nd Road
Hsinchu Science Park
Hsin-Chu
Taiwan (République de Chine)

- les tests sont effectués sur les sites :

ASE GROUP Kaohsiung (ASE)
26 Chin 3rd road
Nantze Export Processing Zone
Kaohsiung
Taiwan (République de Chine)

UTAC
73 Moo 5
Bangsamak
Bangpakong
Chachoengsao 24180
Thaïlande

Chipbond Technology Corporation
Kaohsiung branch n°5
South 6th road
K.E.P.Z. Kaohsiung
Taiwan (République de Chine)

- le découpage des wafers est effectué sur le site :

  DISCO
  Kircheim bei Munich
  Allemagne

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.

1.2.6. 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 AT90SC28880RCFV2 en révision C incluant la bibliothèque cryptographique « *Toolbox »* en version complète 00.03.22.04. Enfin, pour les besoins de l'évaluation, une application de test 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 4** [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 [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG 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 9 décembre 2013, 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] 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.5 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 – High ».
Par ailleurs, les 4 variantes de la « *Toolbox* » comprennent des routines d'autotest pour le TRNG.
Comme énoncé dans le document [REF] 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 AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants AVA_VAN.5 et ALC_DVS.2.

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 AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04 » 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 microcircuit 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 les recommandations se trouvant dans les guides fournis [GUIDES], notamment celles indiquées comme obligatoires (« *mandatory* »).

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 [CCv3.1R4]

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_SPM						**1**	1		
	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_FLR									
	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**	1	**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 AT90SC28880RCFV2 (Krypton)*, réf. : Krypton_ST_V1.6, version 1.6, 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 AT90SC28880RCFV2*, réf. : TPG0224C, version C, Inside Secure.
[RTE]	Rapport technique d'évaluation : - *KRYPTON Evaluation Technical Report : RTE*, réf. : LETI.CESTI.KRY.RTE.001 – v1.3, CEA Leti, 9 décembre 2013. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *KRYPTON Evaluation Technical Report Lite: ETR-lite*, réf. : LETI.CESTI.KRY.RTE.002 - v1.3, CEA Leti, 9 décembre 2013.
[CONF]	Liste de configuration du produit : - *KRYPTON Configuration List*, réf. : KRY_EDL_revC_v1.0, version 1.0, Inside Secure.

[GUIDES]	Guides du produit : - *Wafer Saw Recommendations*, réf. : TPG0079BX, version B, Inside Secure ; - *SmartACT User's Manual*, réf. : TPR0134DX, version D, Inside Secure ; - *Secured Hardware DES/TDES on AT90SC 0.13µm products*, réf. : TPR0400JX, version J, Inside Secure ; - *The Code Signature Module for 0.13µm Products*, TPR0409CX, version C, Inside Secure ; - *Secured Hardware AES on AT90SC products (0.13µm)*, réf. : TPR0428EX, version E, Inside Secure ; - *AT90SC 0.13µm products Technical Datasheet*, réf. : TPR0447EX, version E, Inside Secure ; - *Ad-X2 Datasheet*, réf. : TPR0452DX, version D, Inside Secure ; - *Security Recommendations for 0.13µm Products -2*, réf. : TPR0456EX, version E, Inside Secure ; - *Efficient use of Ad-X2*, réf. : TPR0463CX, version C, Inside Secure ; - *Generating Random numbers to known standards for 0.13µm Products*, réf. : TPR0468EX, version E, Inside Secure ; - *Toolbox 00.03.2x.xx Datasheet*, réf. : TPR0504EX, version E, Inside Secure ; - *Secure use of TBX 00.3.2x.xx*, réf. : TPR0505FX, version F, Inside Secure ; - *AT90SC28880RCFV2 Technical Datasheet*, réf. : TPR0548DX, version D, Inside Secure ; - *Customer Option Form*, réf. : COF v4.91b.pdf, version 4.9b, Inside Secure.
[PP]	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

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[JIWG IC]	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[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]	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 (RGS_B_2), voir www.ssi.gouv.fr.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).

Nota bene : Dans le cadre de l'accord de reconnaissance du CCRA, les documents supports du CCRA correspondant à ceux du SOG-IS s'appliquent.