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-2017/56

Microcontrôleur TESIC-SC-02.1 avec librairie cryptographique v 1.0.D optionnelle

Paris, le 27 septembre 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2017/56

Nom du produit

Microcontrôleur TESIC-SC-02.1 avec librairie cryptographique v 1.0.D optionnelle

Référence/version du produit

TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC25 (TC25)
TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC40 (TC40)
TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC55 (TC55)
TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC70 (TC70)

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0,

certifié BSI-CC-PP-0084-2014 le 19 février 2014

avec conformité aux packages :

“Loader dedicated for usage in Secured Environment only”
“Loader dedicated for usage by authorized users only”

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)

Tiempo S.A.S.

110 rue Blaise Pascal, Bâtiment Viseo – Inovallée
38330 Montbonnot St-Martin - France

Commanditaire

Tiempo S.A.S.

110 rue Blaise Pascal, Bâtiment Viseo – Inovallée
38330 Montbonnot St-Martin - France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

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 TESIC-SC-02.1 avec librairie cryptographique v 1.0.D optionnelle » développé par *TIEMPO S.A.S.*

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

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 [PP0084], avec les *packages* « *Loader dedicated for usage in secured environment only* » et « *Loader dedicated for usage by authorized users only* ».

1.2.2. 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 température ;
  - de détection de signaux transitoires (*glitch*) ;
  - de détection de sondage (*probing*, présence d'un bouclier actif) ;
  - de contrôle des modes *Admin*, *Kernel* et *User* ;
  - de contrôles d'accès aux mémoires intégrant du chiffrement, du *scrambling* et du calcul de CRC ;
  - de protection contre les attaques *side-channel* tels que le *jitter* et le masquage des données ;
  - de sécurité contre les attaques par perturbation telle que l'injection de fautes par laser ;
- la gestion sécurisée de la mémoire (MPU[2]) ainsi qu'une protection des accès à cette mémoire ;
- la cryptographie symétrique, grâce aux processeurs DES[3] et AES ;
- la cryptographie asymétrique grâce à l'accélérateur matériel ;

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

- la génération de nombres aléatoires ;
- le démarrage du composant (*Bootloader*) ;
- l'accès sécurisé au logiciel de chargement de la mémoire FLASH (*Admin loader*).

1.2.3. Architecture

Le produit est constitué des éléments suivants :

- une partie matérielle composée en particulier :
  - d'un processeur sécurisé TAM16EXV2S ;
  - d'un accélérateur cryptographique sécurisé pour les opérations à clé publique pour des tailles d'opérandes jusqu'à 4224 bits ;
  - d'un moteur CRC 16 conforme à l'ISO/IEC 13239 ;
  - de processeurs DES et AES matériels ;
  - d'un contrôleur d'interruption à 2 niveaux ;
  - d'un générateur d'alea physique ;
  - de trois *timers* ;
  - de contrôleurs d'interfaces ISO 7816 et ISO 14443 ;
  - de mémoires :
    - ROM : 16Ko ;
    - FLASH : 504 Ko ;
    - RAM : 6Ko + 2Ko dédiés à l'accélérateur cryptographique ;
- une partie logicielle comprenant :
  - un logiciel de démarrage du composant (*Secure boot loader*) ;
  - un logiciel d'accès sécurisé au chargement de la mémoire (*Admin loader*) ;
  - une librairie cryptographique supportant les courbes elliptiques et le chiffrement à clé publique de type RSA ;
  - un logiciel de test (en dehors du périmètre de la TOE).

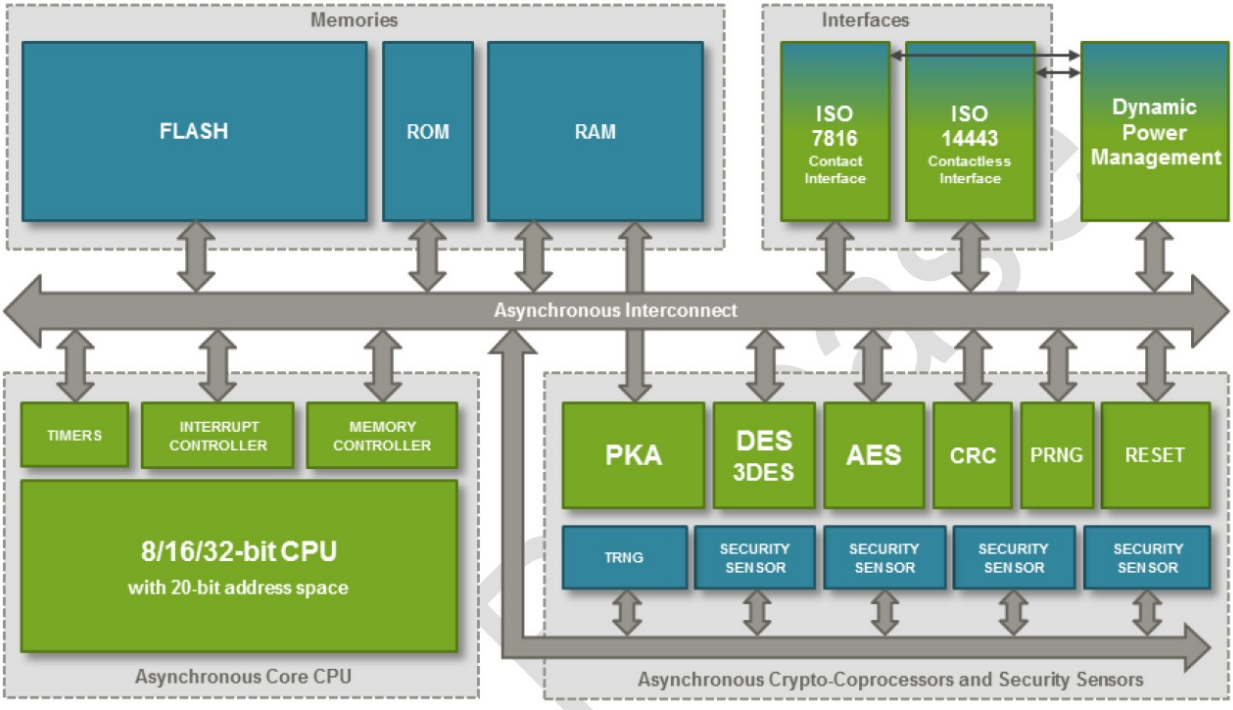

Figure 1. Architecture de la TOE

1.2.4. 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 (voir [GUIDES]) :

- l'identification du microcontrôleur TESIC-SC-02.1 (*Product number identification*) : 0x0005 par lecture de la valeur IC TYPE ;
- la version du micro-circuit (*Hardware revision, capacitor value*) et l'identification du site de fabrication : par lecture de la valeur CHIP ID ;
- la version du logiciel dédié (*IC Dedicated Software*) : 0x0001 par lecture de la valeur ROM ID ou par lecture de la valeur LDR_VERSION ;
- la version de la librairie cryptographique (*Crypto library*) : 1.0.D par l'appel de la fonction *tpoCryptoGetVersion* de la librairie cryptographique.

Quatre configurations du produit sont identifiées ci-dessous et diffèrent uiquemement par la valeur de la capacitance de l'entrée radio-fréquence :

- TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC25 (TC25) ;
- TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC40 (TC40) ;
- TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC55 (TC55) ;
- TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC70 (TC70).

Les éléments d'identification de ces quatre configurations sont les suivants :

Product	Manufacturer	IC type	ROM boot firmware	Admin loader	Mask revision	Capacitor value
TC25	0xFFFF	0x0005	0x0001	0x0001	0x2	0x11 (25 pF)
TC40	0xFFFF	0x0005	0x0001	0x0001	0x2	0x00 (40 pF)
TC55	0xFFFF	0x0005	0x0001	0x0001	0x2	0x01 (55 pF)
TC70	0xFFFF	0x0005	0x0001	0x0001	0x2	0x10 (70 pF)

1.2.5. Cycle de vie

Le produit a été développé sur les sites suivants :

- la conception est assurée sur le site suivant :

  TIEMPO SAS
  110 rue Blaise Pascal
  Bâtiment Viseo – Inovallée
  38330 Montbonnot Saint Martin
  France

- la fabrication des masques est assurée sur les sites suivants :

  LFOUNDRY
  Herrngasse 379-381
  84028 Landshut
  Germany

  COMPUGRAPHICS INT. LTD.
  Newark Road North
  Eastfield industrial Estate
  Glenrothes
  Fife, KY7 4NT
  Scotland

- la fabrication des *wafers* est assurée sur le site suivant :

  LFOUNDRY
  Via A. Pacinotti 7
  67051 Avezzano (AQ)
  Italy

- les tests et la pré-personnalisation sont effectués sur le site suivant :

  PRESTO-ENGINEERING
  Arteparc de Bachasson – Bât A
  Rue de la carrière de Bachasson
  13590 Meyreuil
  France

- le *packaging* est effectué sur les sites suivants :

  SPS
  Avenue de la Plaine
  ZI de Rousset
  13106 Rousset
  France

  MICRO-PACKS
  Centre de Microélectronique de Provence
  880 avenue de Mimet
  13451 Gardanne
  France

  HCM
  Z.I. Périgny
  34 Avenue Joliot-Curie
  17185 Perigny
  France

  NEDCARD B.V.
  Bijsterhuizen 2529
  6604 LM Wijchen
  Hollande

  PRESTO UTAC-TH
  UTAC Thai Limited (UTL3)
  C1 (Building C, 1st floor)
  73 Moo 5
  Wellgrow Industrial Estate
  Bangsamak, Bangpakong
  Chachoengsao, 24180
  Thailande

Au regard du cycle de vie, le produit évalué est le produit qui sort de la phase 3 (tests et pré-personnalisation) ou de la phase 4 (*packaging*) du cycle de vie (au titre d'ALC). Le loader peut être utilisé de la phase 3 à la phase 5 et doit être verrouillé en phase 6 avant la personnalisation.
Le produit comporte lui-même une gestion de son cycle de vie, prenant la forme de trois modes :

- mode *Admin*, qui permet à l'administrateur de changer les paramètres par défaut de la TOE et de charger le système d'exploitation (*firmware*). La TOE est livrée dans ce mode à la fin de la phase 3 ou de la phase 4 ;
- mode *Kernel*, mode privilégié dans lequel le logiciel chargé est démarré. Ce mode permet au logiciel chargé de configurer la MPU et ainsi autoriser l'accès aux ressources du composant par l'application ;
- mode *User*, c'est le mode final non-privilégié d'utilisation du microcontrôleur par le porteur du produit (exécution du logiciel applicatif chargé). Le composant a été évalué dans ce mode.

1.2.6. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur. Toute application éventuellement embarquée, notamment les logiciels de test du microcontrôleur embarqués pour les besoins de l'évaluation, ne fait pas partie du périmètre d'évaluation.
Le produit évalué par le centre d'évaluation est le « Microcontrôleur TESIC-SC-02.1 avec librairie cryptographique v 1.0.D optionnelle » en mode *User*.

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

L'évaluation s'appuie sur les résultats d'évaluation du produit « Microcontrôleur TESIC-SC-500-02 révision 2.0.1 » certifié le 14 novembre 2016 sous la référence [CER-2016/12].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 juillet 2017, 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

Le produit embarque un générateur matériel d'aléa (PTRNG[1]), qui a fait l'objet d'une analyse par le CESTI et par l'ANSSI.
Les règles RègleArchiGVA-1 et RègleArchiGVA-2 ainsi que la recommandation RecomArchiGVA-1 de [REF] s'avèrent respectées lorsque ce générateur d'aléa est utilisé comme indiqué dans les guides « *TESIC-SC-02.1 Hardware User Manual* » et « *TESIC-SC-02.1 Developer role description* » (voir [GUIDES]). Le document [REF] impose, pour un usage cryptographique, que la sortie d'un générateur matériel de nombres aléatoires subisse un retraitement algorithmique de nature cryptographique ; ce retraitement n'est pas implémenté dans le produit et devra être développé par l'utilisateur le cas échéant.

[1] *Physical True Random Number Generator*.

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 TESIC-SC-02.1 avec librairie cryptographique v 1.0.D optionnelle » 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 ALC_DVS.2 et AVA_VAN.5.

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 TESIC-SC-02.1 avec librairie cryptographique v 1.0.D optionnelle » 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 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 lorsque les dépendances CC sont satisfaites. 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 EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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_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 : - TESIC-SC-02.1 Security Target, réf. : D-SPD-402-510-2.0, version 2.0, 27/07/2017, Tiempo S.A.S. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - TESIC-SC-02.1 Security Target Lite, réf. : D-SPD-402-511-2.0, version 2.0, 27/07/2017, Tiempo S.A.S.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) DEVOLUY, réf. : LETI.CESTI.DEV.FULL.001 – v1.0, CEA-LETI, 28/07/2017. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Report (ETR for composition) DEVOLUY, réf. : LETI.CESTI.DEV.COMPO.001 – v1.0, CEA-LETI, 28/07/2017.
[GUIDES]	Guides du produit : - TESIC-SC-02.1 Hardware User Manual, réf. : D-SPD-301-310-2.0, version 2.0, 21/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Operational User Guidance, réf. : D-SPD-402-340-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Developer role description, réf. : D-SPD-402-320-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Loader role, réf. : D-SPD-402-342-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 PRE-loader role, réf. : S-SPD-402-345-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 ADMIN Loader User Manual, réf. : D-SPD-302-330-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Crypto Library User Manual, réf. : S-SPD-302-310-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Crypto Library Security Guidelines, réf. : S-SPD-402-320-2.0, version 2.0, 12/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Packaging Specifications for Assembly, réf. : D-SPD-402-402-2.0, version 2.0, 21/07/2017, Tiempo S.A.S. ; - TESIC-SC-02.1 Software Development Kit User Manual, réf. : D-SPD-302-340-5.0, version 5.0, 03/11/2016, Tiempo S.A.S. .
[CONF]	Liste de configuration du produit : - TESIC-SC-02.1 Release Configuration, réf. : D-SPD-401-220, 27/07/2017, Tiempo S.A.S.
[CER-2016/12]	Rapport de certification ANSSI-CC-2016/12 « Microcontrôleur TESIC-SC-500-02 révision 2.0.1 » émis le 14/11/2016, ANSSI.

[PP0084]	Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la* référence BSI-CC-PP-0084-2014 le 19 février 2014.

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, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.