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-2016/16

Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 0x06040102

Paris, le 10 juin 2016

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-2016/16

Nom du produit

Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 0x06040102

Référence/version du produit

Part number 0x44, Hardware revision E, Toolbox Library version 0x06040102, Wear Levelling Library version0x06020201

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 à

“Package 1: Loader dedicated for usage in Secured Environment 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)

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 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 MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 0x06040102 » 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, 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 le package « *Loader dedicated for usage in secured environment only* ». Les logiciels applicatifs sont entièrement chargés en mémoire en mémoire FLASH avant le point de livraison.

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 : MS6001, *Revision hardware E* ; la référence interne *INSIDE SECURE* est 90T02; celle-ci, ainsi que la lettre E de la révision sont marquées sur le composant ;
- bibliothèque cryptographique logicielle : *Toolbox version 0x06040102* ;
- bibliothèque optionnelle *Wear Levelling*[1] *version 0x06020201*.

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

- identification du microcontrôleur MS6001 : 0x44 par lecture du registre PID ;
- révision : 0x04 pour la révision E par lecture du registre SNB1 ;
- version de la bibliothèque cryptographique *Toolbox* disponible via la commande *SelfTest*. Les valeurs retournées sont : 0x06040102 ;
- version de la bibliothèque *Wear Levelling* disponible dans le champ *wl_rom* de la structure de données *lib_wl_Config_struct* apès initialisation de la bibliothèque. Les valeurs retournées sont : 0x06020201.

[1] Uniformisation d'usure.

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, à l'accélérateur matériel Ad-X3 pour la cryptographie asymétrique ainsi qu'à la librairie cryptographique *Toolbox* ;
- 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 ARM SecureCore SC300 32bit *RISC* ;
  - d'un accélérateur cryptographique 32-bit Ad-X3 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 ;
  - d'un contrôleur d'interruption à 2 niveaux ;
  - d'un générateur d'alea physique ;
  - de deux *timers* 16 bits et d'un oscillateur interne programmable ;
  - de contrôleurs d'interfaces ISO 7816, SPI (*Single Wire Protocol Interface*), I2C (*Inter integrated Circuit*) et GPIO (*General Purpose Input/Output Interface*) ;
  - de mémoires :
    - ROM : 64Ko contenant la bibliothèque cryptographique *Toolbox* et la bibliothèque optionnelle *Wear Levelling ;*
    - FLASH : 1 Mo ;
    - RAM : 24Ko pour le CPU dont 4Ko partagés avec l'accélérateur matériel Ad-X3,
- une partie logicielle comprenant :
  - la librairie cryptographique *Toolbox* ;
  - la bibliothèque optionnelle *Wear Levelling.*

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

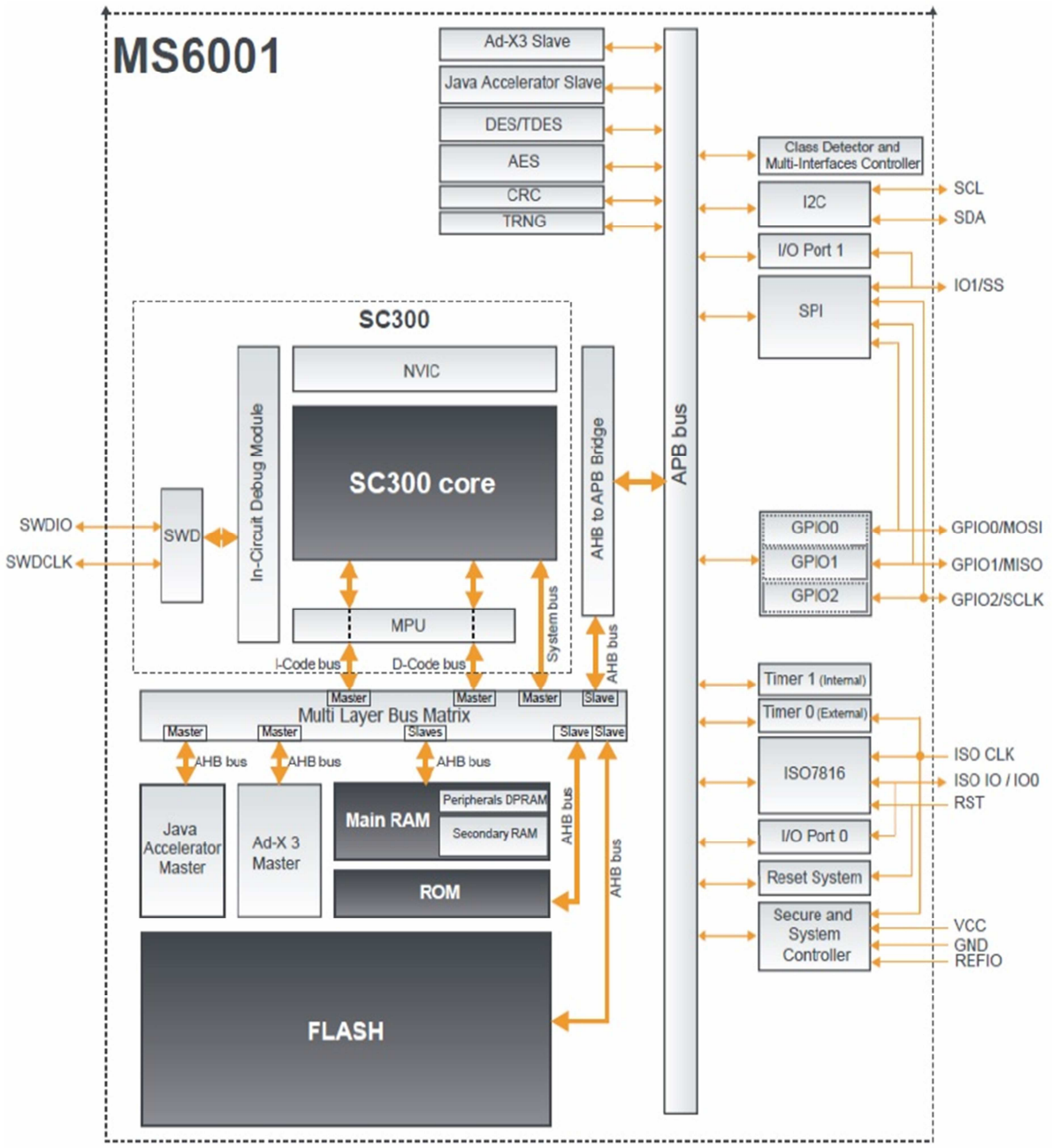

Figure 1. Architecture de la TOE

1.2.5. Cycle de vie

Le produit a été développé sur les sites suivants :

- la conception est assurée sur les sites suivants :

  ***INSIDE* Meyreuil**
  Arteparc de Bachasson – Bat A
  Rue de la Carrière de Bachasson
  CS 70025
  Meyreuil
  France

  ***INSIDE* East Kilbride**
  Scottish Enterprise Technology Park
  East Kilbride
  G75 OQR
  Ecosse

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

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

  TSMC
  Fab14, 8D N° 3
  1-1 Nan Ke Road
  Tainan Science Park
  Tainan 471_44
  Taiwan (République de Chine)

  ***TOPPAN PHOTOMASKS* (TCE)**
  1127-3 Hopin Road
  Padeh City
  Taoyuan
  Taiwan 30080 (République de Chine)

- les tests sont effectués sur le site suivant :

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

- le stockage est effectué sur le site suivant :

  ***FEDEX* Hong Kong RDC**
  9/F, Phase One
  Warehouse Building
  Hong Kong
  Chine

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

- mode *Test*, qui permet à l'administrateur de tester la TOE, de charger le code embarqué de l'utilisateur et de commuter en mode *User*. Ce mode est aussi utilisé pour diagnostiquer le produit s'il se trouve défaillant, dans ce cas, l'application de l'utilisateur chargée en FLASH est automatiquement effacée ;

- mode *User*, c'est le mode final d'utilisation du microcontrôleur par le porteur du produit ; celui-ci a été évalué dans ce mode.

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. Le produit fourni au centre d'évaluation est le microcontrôleur MS6001 en révision E incluant la bibliothèque cryptographique *Toolbox* en version 0x06040102 et la bibliothèque optionnelle *Wear Levelling* en version 0x06020201.

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 11 mars 2016, 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 générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS31] et il répond aux exigences de la classe PTG.2.
Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. 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 MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 0x06040102 » 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 MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 0x06040102 » 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 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. 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] 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, 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 : - Mistral MS6001 Security Target, réf. : Mistral_ST_V1.0, version 1.0, Inside Secure. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MS6001 Security Target-Lite, réf. : TPG0234B, version B, Inside Secure.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) MISTRAL-INS, réf. : LETI.CESTI.MIS.FULL.001 – v1.0, CEA-LETI, 11 mars 2016. 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) MISTRAL-INS, réf. : LETI.CESTI.MIS.COMPO.001 – v1.0, CEA-LETI, 11 mars 2016.
[GUIDES]	Guides du produit : - MS6xxx Technical Datasheet, réf. : TPR0702CX, version C, Inside Secure ; - MS6001 Technical Datasheet, réf. : TPR0705DX, version D, Inside Secure ; - SmartACT User's Manual, réf. : TPR0134EX, version E, Inside Secure ; - Secured Hardware DES/TDES on MSXXXX 90 nm products, réf. : TPR0707CX, version C, Inside Secure ; - Secured Hardware AES on MSXXXX products (90 nμm), réf. : TPR0708BX, version B, Inside Secure ; - Ad-X3 Datasheet, réf. : TPR0701BX, version B, Inside Secure ; - Efficient use of Ad-X3, réf. : TPR0726CX, version C, Inside Secure ; - Security Recommendations for MS6xxx products, réf. : TPR0706BX, version B, Inside Secure ; - Generating Random numbers on MS6XXX Products (90 nm), réf. : TPR0709CX, version C, Inside Secure ; - Toolbox 06.04.01.xx on MS6001XXX, réf. : TPR0711GX, version G, Inside Secure ; - Toolbox 06.04.01.xx Errata sheet, réf. : TPR0727AX, version A, Inside Secure ; - Securing Toolbox 06.04.01.xx on MSXXX 90 nm products, réf. : TPR0712EX, version E, Inside Secure ; - Wear Levelling Library and Low Level Flash Drivers, réf. : TPR0701AX, version A, Inside Secure ; - MS6xxx Secure Acceptance Guidance, réf. TPR0754AX, version A, Inside Secure.

[CONF]	Liste de configuration du produit : - MISTRAL Configuration List, réf. : Mistral_EDL_V3.0.xls, version 3.0, Inside Secure.
[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.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).

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