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-2018/02

Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02

Paris, le 29 janvier 2018

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-2018/02

Nom du produit

Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02

Référence/version du produit

Part number 0x44, hardware revision E, Toolbox Library version 0x06040107, Wear Levelling Library version 0x06030202

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 au

“ Package 1 : Loader dedicated for usage by authorized users only”

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

Wisekey Semiconductors

Arteparc Bachasson, Bât. A, rue de la carrière de Bachasson, 13590 Meyreuil, France.

Commanditaire

Wisekey Semiconductors

Arteparc Bachasson, Bât. A, rue de la carrière de Bachasson, 13590 Meyreuil, 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 MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02 » développé par la société *WISEKEY SEMICONDUCTORS*.

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 par exemple. 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 seront donc entièrement chargés en mémoire FLASH avant le point de livraison.

1.2.2. Services de sécurité

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

- ceux correspondant à l'*ARM Secure Core SC300* ;
- les protections contre les attaques liées à l'environnement d'utilisation telles que :
  - le détecteur de tension ;
  - le détecteur de fréquence ;
  - le détecteur de température ;
  - le détecteur de signaux transitoires sur la tension d'alimentation (*glitch*).
- les protections contre les attaques physiques incluant :
  - la détection de sondage (*probing)* assurée par la présence d'un bouclier actif (*active shield*) ;
  - la génération de l'horloge interne ;
  - les détecteurs de lumière ;
  - la détection de perturbation (présence de registres redondés) ;
  - la détection de violation d'EPO (*Enhanced Protection Object*) ;
  - la vérification de la pile (*CStack*).
- les protections des mémoires par :

[1] *Target Of Evaluation.*

- la détection d'erreurs de parité des mémoires RAM, ROM et des registres ;
- le chiffrement des mémoires RAM, ROM et FLASH ;
- le chiffrement des données et des adresses ;
- la détection des erreurs liées à la répartition de l'usure de la RAM.

- la cryptographie, grâce aux processeurs DES et AES et à l'accélérateur matériel Ad-X3 ;
- l'accélérateur de calculs de CRC16 et 32 ;
- le générateur hardware de nombres aléatoires ;
- la bibliothèque cryptographique (*Toolbox*) incluant le RSA (STD et CRT) et les courbes elliptiques.

1.2.3. 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 de cryptographie asymétrique ;
  - d'un moteur CRC 16 et 32 conforme à l'ISO/IEC 3309 ;
  - de composants matériels DES[1] ;
  - d'un composant matériel AES (128, 192 et 256 bits) ;
  - d'un contrôleur d'interruption à 2 niveaux ;
  - d'un générateur aléatoire physique ;
  - de deux *timers* l'un 16 bits, l'autre 32 bits ;
  - de contrôleurs d'interfaces ISO 7816, SWP (*Single Wire Protocol Interface*), SPI (*Single 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 dont 4Ko partagés entre l'accélérateur matériel Ad-X3 et le CPU.
- une partie logicielle comprenant :
  - la bibliothèque cryptographique Toolbox ;
  - la bibliothèque optionnelle *Wear Levelling.*

[1] Seul l'usage du chiffrement TDES est inclus dans le périmètre de l'évaluation.

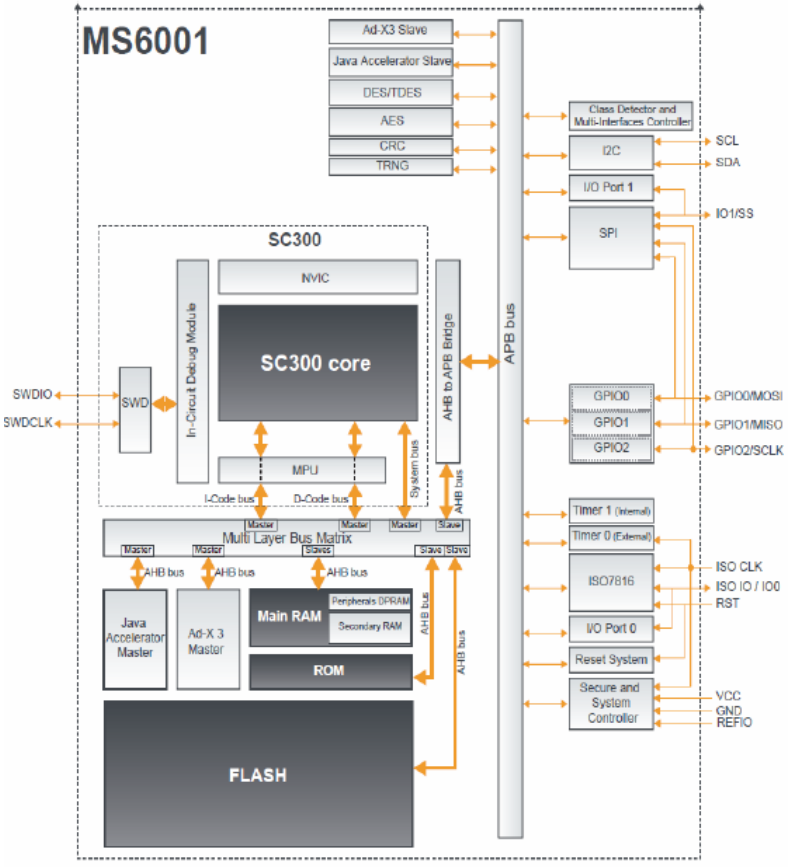

Figure 1 : Architecture de la TOE

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 :

- identification du microcontrôleur : MS6001, *Revision hardware E* : la référence interne du produit 90T02 ainsi que la révision E sont masquées sur le composant ;
- bibliothèque cryptographique logicielle : *Toolbox* version 0x06040107 ;
- bibliothèque optionnelle *Wear Levelling* version 0x06030202.

Ces éléments peuvent être vérifiés par lecture des registres (voir [GUIDES]) :

- identification du microcontrôleur MS6001 : 0x44 par lecture du registre PID ;
- révision : 0x04 pour la révision E par lecture du registre SNB0 ;
- version de la bibliothèque cryptographique *Toolbox* : 0x06040107 obtenue à partir de la commande *SelfTest* ;
- version de la bibliothèque *Wear Levelling* : 0x06030202 disponible dans le champ *wl_rom* de la structure de données *lib_wl_Config_struct* après initialisation de la bibliothèque.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

Etape de développement	Nom de la société	Adresse de la société
Conception du produit	**WISEKEY**	Arteparc Bachasson, Bât A Rue de la carrière de Bachasson, CS70025 13590 Meyreuil France
Fabrication des masques et des wafers	**TSMC**	Fab14, 8D N° 3 1-1 Nan Ke Road Tainan Science Park Tainan 471_44 Taiwan
Tests	***ASE GROUP KAOHSIUNG*** **(ASE)**	26 Chin 3rd road Nantze Export Processing Zone Kaohsiung Taiwan
Stockage	**PRESTO Engineering**	Arteparc Bachasson, Bât A Rue de la carrière de Bachasson, CS70025 13590 Meyreuil France

Le produit comporte deux modes possibles :

- le mode *Test*, qui permet de tester la TOE, de charger le code utilisateur et de commuter en mode *User*. Ce mode est également utilisé pour analyser les produits défaillants lors de retours terrains par exemple. Le basculement du mode *User* en mode *Test* donne systématiquement lieu à un effacement total de la mémoire FLASH, rendant inexploitables les données de l'utilisateur final ;
- le mode *User*, qui correspond au mode final d'utilisation de la TOE.

1.2.6. Configuration évaluée

Le certificat porte sur le « Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02 ».
Toute autre application, 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 issu de la phase 3 du cycle de vie.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

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 22 décembre 2017, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

Cette évaluation s'appuie également sur les résultats obtenus dans le cadre de d'évaluation [ANSSI-CC-2016/16].

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 vulnérabilité 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 [AIS 31] lors de l'évaluation initiale (voir [ANSSI-CC- 2016/16]).
Pour mémoire, ce générateur répond aux exigences de la classe PTG.2.

Comme énoncé dans le document [REF], il convient de rappeler 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 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02 » 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 strictement 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 puce 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 : - MS6001 Security Target, référence Mistral_ST_V1.5, version 1.5 du 12/09/2017, *WISEKEY*. 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, référence TPR0234, version D du 13/09/2017, *WISEKEY*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) - MISTRAL-E, référence LETI.CESTI.MISE.FULL.001 - V1.1, version 1.1 du 20/12/2017, *LETI*. 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-E, référence LETI.CESTI.MISE.COMPO.001 - V1.1, version 1.1 du 20/12/2017, *LETI*.
[CONF]	Liste de configuration du produit : - MISTRAL-E delivery list, référence Mistral_EDL_V3.5.xls, version 3.5 du 13/9/2017, *WISEKEY*.

[GUIDES]	Guides du produit : - MS6xxx Technical Datasheet, référence TPR0702DX, version D du 9/3/2017, *WISEKEY* ; - MS6001 Technical Datasheet, référence TPR0705EX, version E du 9/3/2017, *WISEKEY* ; - Security Recommendations for MS6XXX 90nm Products – Application note, référence TPR706CX, version C du 8/9/2017, *WISEKEY* ; - Security Hardware DES/TDES on MSXXX 90nm Products – Application note, référence TPR0707DX, version D du 13/3/2017, *WISEKEY* ; - Security Hardware AES on MSXXX Products (90nm) – Application note, référence TPR0708DX, version D du 29/8/2017, *WISEKEY* ; - Ad-X3 Datasheet, référence TPR0701CX, version C du 13/3/2017, *WISEKEY* ; - Generating Random Numbers on MS6XXX Products (90nm) – Application note, référence TPR0709DX, version D du 13/3/2017, *WISEKEY* ; - Toolbox 06.04.01.XX on MS6XXX – Application note, référence TPR0711HX, version H du 16/3/2017, *WISEKEY* ; - TBX 06.04.01.XX Erratasheet – Application note, référence TPR0727DX, version D du 14/3/2017, *WISEKEY* ; - Securing TBX 06.04.01.XX on MSXXXX 90nm Products – Application note, référence TPR0712JX, version J du 11/9/2017, *WISEKEY* ; - Wear Levelling library and low level FLASH drivers – Application note, référence TPR0710BX, version B du 5/1/2017, *WISEKEY* ; - Efficient Use of Ad-X3 – Application note, référence TPR0726DX, version D du 14/3/2017, *WISEKEY* ; - MS6XXX Secure Acceptance Guidance, référence TPR0754BX, version B du 27/3/2017, *WISEKEY* ; - SmartACT's User Manual – Application note, référence TPR0134FX, version F du 18/8/2017, *WISEKEY* ; - MS600X Customer Options Form, version 1.1_1 d'avril 2017, *WISEKEY*.
[PP0084]	Protection Profile, 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-PP-0084-2014.*
[ANSSI-CC-2016/16]	Rapport de certification ANSSI-CC-2016/16, Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 0x06040102. Certifié par l'ANSSI le 10 juin 2016 sous la référence ANSSI-CC-2016/16.

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 Septembre 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.