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-2017/41

Microcontrôleur ORION_CB_03 révision matériel C

Paris, le 26 juillet 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-2017/41**
Nom du produit **Microcontrôleur ORION_CB_03**
Référence/version du produit **Révision matériel C**
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) **INVIA Secure Semiconductor Meyreuil** **Arteparc – Bât D, route de la côte d'Azur, 13590 Meyreuil, France**
Commanditaire **INVIA Secure Semiconductor Meyreuil** **Arteparc – Bât D, route de la côte d'Azur, 13590 Meyreuil, France**
Centre d'évaluation **CEA - LETI** **17 rue des martyrs, 38054 Grenoble Cedex 9, France**
Accords de reconnaissance applicables **Ce certificat ne fait pas l'objet d'une reconnaissance internationale.**

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 ORION_CB_03, révision matériel C » développé et fabriqué par la société *INVIA SECURE SEMICONDUCTOR MEYREUIL*.

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, applications mobiles, carte SIM 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* 1 : « *loader dedicated for usage in secured environment only* ».
Du fait des exigences additionnelles de sécurité du produit, le logiciel peut être chargé en mémoire FLASH après le point de livraison en environnement non-audité car le microcontrôleur est auto-protégé et a la capacité de s'authentifier vis-à-vis de l'utilisateur.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE[1] ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ou asymétriques ;
- le support à la génération de nombres non prédictibles.

1.2.3. Architecture

Le produit est constitué des éléments suivants (voir figure 1) :
- une partie matérielle comprenant :
  - un CPU[2] 32-bit ;
  - des mémoires :
    - 48Ko de ROM ;
    - 1376Ko de Flash ;
    - 40Ko de RAM, dont 32Ko SRAM pour un usage général, 4Ko pour la PKI RAM et 4Ko pour la *stack* RAM ;

[1] *Target Of Evaluation* – périmètre de l'évaluation.
[2] *Central Processing Unit* – processeur.

- des modules de sécurité : mécanisme de chiffrement de la mémoire et des bus, mécanisme d'intégrité de données, génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- des modules fonctionnels : gestion des entrées / sorties en mode contact (ISO7816), interface sans contact (protocole de communication SWP), générateur de nombres aléatoires – PTRNG[1], coprocesseurs cryptographiques implémentant des instructions dédiées pour les algorithmes symétriques et de hashages, crypto-coprocesseur PKI fournissant des instructions pour l'implémentation d'algorithmes cryptographiques asymétriques,

- une partie logicielle composée :
  - d'un *loader* permettant le chargement du logiciel par le client ;
  - d'un *secure boot loader* permettant le chargement sécurisé du code utilisateur.

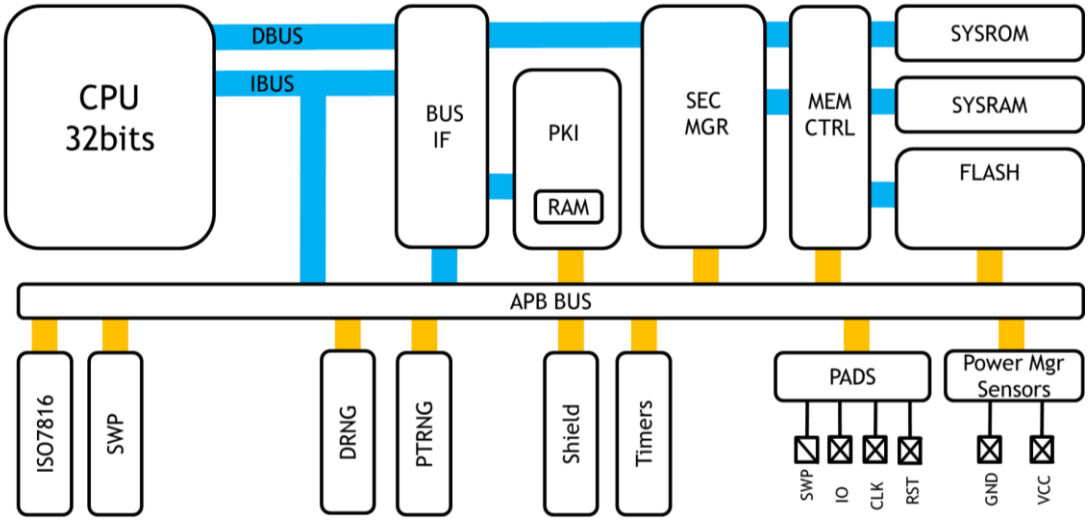

Figure 1 : Architecture du produit

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du microcontrôleur est identifiable par les éléments donnés dans la table ci-après. Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide « Orion User Manual », voir [GUIDES].

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur	Nom de la TOE, ORION	0x04
	Révision matériel, version C	0x43
Identification des logiciels embarqués	*Platform ROM Firmware*, version B	0x42
	Platform Flash Firmware, version 03	0x03
	Loader, version 2.0	0x3230
Identification des bibliothèques	N/A	N/A

[1] *Physical True Random Number Generator* - Générateur physique de nombres aléatoires.

1.2.5. Cycle de vie

Le cycle de vie du produit est représenté par le schéma suivant :

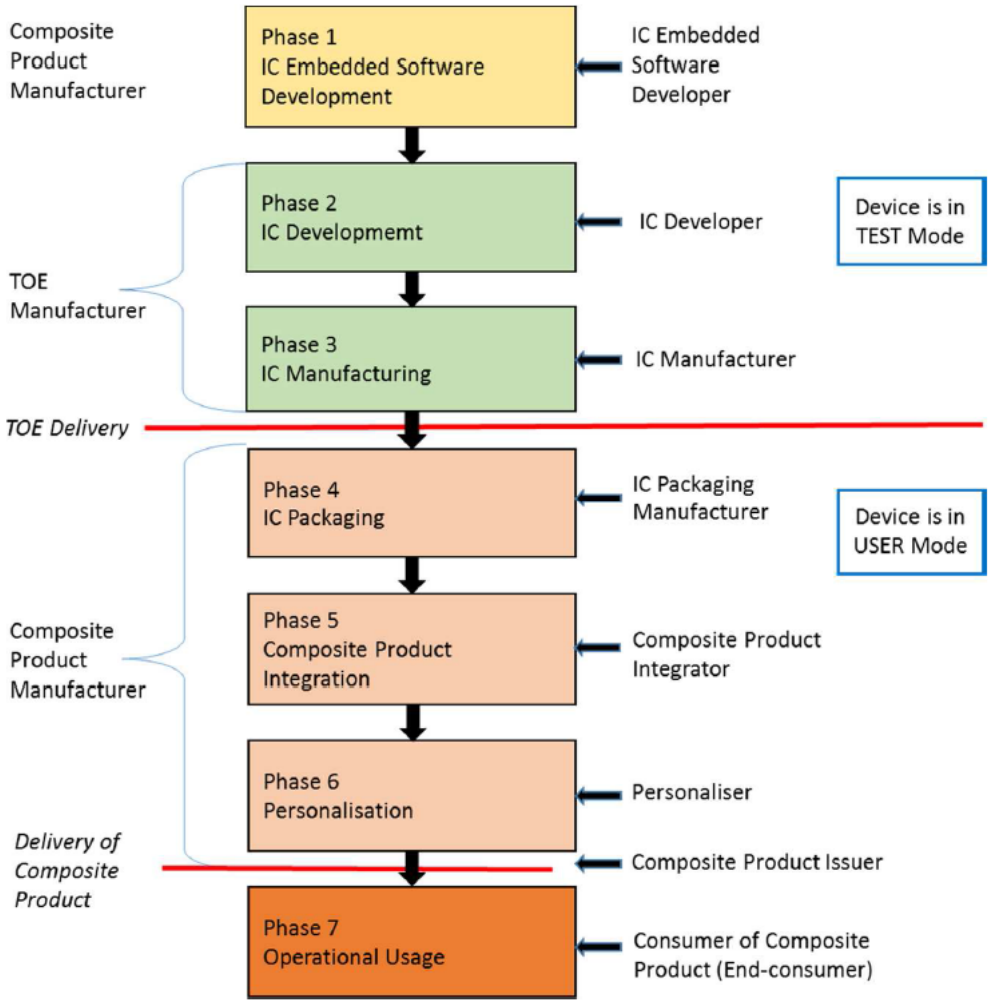

Figure 2 : Cycle de vie du produit

La phase 1 correspond au développement du logiciel embarqué sur le microcontrôleur, cette phase est en dehors du périmètre de la TOE.
Seules les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de *wafer* ou de *wafer* scié, appelé *dice*.
La phase 2 correspond à la phase de développement du microcontrôleur et comprend notamment les étapes suivantes :

- conception du circuit ;
- développement du logiciel dédié.

La phase 3, qui couvre la fabrication du microcontrôleur, comprend les étapes suivantes :

- intégration et fabrication du masque ;
- fabrication du circuit ;
- test du circuit ;
- préparation ;
- pré-personnalisation si nécessaire.

Le produit a été développé sur les sites suivants :

INVIA Secure Semiconductor Meyreuil Arteparc – Bâtiment D, Route de la côte d'Azur, 13590 Meyreuil, France	**MU-Electronics** 49 rue Jabal Tazekka, 1er étage, Agdal, 10000 Rabat, Maroc
Gemalto La Vigie, Avenue du Jujubier, Z.I. Athelia IV 13705 La Ciotat Cedex, France	**PDMC** **Masks Manufacturing (1A)** 1stFloor, N°2, Li-Hsin Rd, Science Park, Hsinchu, 30078 Taïwan **Masks Manufacturing (1B)** N°13, Tongshan Rd, Daya District, Taichung 42879 Taïwan **Masks Manufacturing (1D)** N°6, Li-Hsin 7th Rd, Science Park, Hsinchu 30078 Taïwan
UMC Fab 12i No.3, Pasir Ris Drive 12, Singapore 519528, Singapour	
UTAC 5 Serangoon North Avenue 5, Singapore 554916 Singapour	

Le produit comporte une gestion de son cycle de vie, prenant la forme de trois modes :

- « *boot mode* » : ce mode est le premier utilisé à chaque démarrage ;
- « *test mode* » : à la fin de la fabrication, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM. Cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration « *user mode* » ;
- « *user mode* » : il s'agit du mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible.

Le *boot loader* et le *loader* sont présents dans le produit en phase 3. Le *loader* permet le chargement du système d'exploitation en phase 5. Le *loader* est utilisé en mode opérationnel et est ensuite bloqué (ou supprimé) en phase 5 par le développeur du logiciel embarqué sur le microcontrôleur.

1.2.6. Configuration évaluée

Le certificat porte sur le microcontrôleur tel que défini au chapitre 1.2.4. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.
Au regard du cycle de vie détaillé au chapitre 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de *wafer* ou de *dice.*

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].
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 17/05/2017, 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 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 [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 « microcontrôleur ORION_CB_03, révision matériel C » 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 ORION_CB_03, révision matériel C » 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 microcontrôleur 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]. Il devra suivre les recommandations, en particulier les contremesures à implémenter dans le code embarqué sur le microcontrôleur se trouvant dans les guides fournis [GUIDES], notamment dans le document « Orion Security Guidance ».

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 : - Security Target for ORION, microcontroller ORION_CB_03, référence INVIA_ORION_ST_Security_Target_v2.6, version 2.6, 19/04/2017. Pour les besoins de composition, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite for ORION, microcontroller ORION_CB_03, référence INVIA_ORION_ST_Security_Target_Lite_v1.1, version 1.1, 19/04/2017.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – ORION, référence LETI.CESTI.ORI.FULL.001, version 1.1, 17/05/2017. 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) – ORION, référence LETI.CESTI.ORI.COMPO.001, version 1.1, 17/05/2017.
[CONF]	Liste de configuration du produit : ORION List of documentation, référence List_of_documentation _CC_v0.25, version 0.25, 20/04/2017.
[GUIDES]	- Orion User Manual, référence Orion_user_Manual_rev.1.2, version 1.2, 11/04/2017 ; - Orion Security Guidance, référence INVIA_ORION_Security_guidance_v024, version 0.24, 11/04/2017 ; - Guidance –Secure Delivery, référence AGD-Secure delivery-v1.0, version 1.0, 12/12/2016 ; - Orion Assembly Instructions, référence Orion Assembly – rev 0.2, version 0.2, 13/11/2015 ; - Orion Loader User Manual, référence UserManual_CC_Loader_v1.7, version 1.7, 16/01/2017 ; - S8 Embedded Application Binary Interface (EABI), référence s8-abi, version 0.6, 03/2013 ; - S8 instruction Set Architecture, référence s8-isa, 07/2015.
[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.*

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 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.
[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.