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-2018/51

Microcontroller CENTAURUS_FB_04 (Révision du matériel F)

Paris, le 29 novembre 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2018/51

Nom du produit

Microcontroller CENTAURUS_FB_04

Référence/version du produit

Révision du matériel F

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

"Authentication of the security IC" et "Loader dedicated for usage in Secured Environment 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

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 avenue 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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 6
1.2.4. Identification du produit 7
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. TRAVAUX D'EVALUATION 10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 10
2.4. ANALYSE DU GENERATEUR D'ALEAS 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RESTRICTIONS D'USAGE 11
3.3. RECONNAISSANCE DU CERTIFICAT 11
3.3.1. Reconnaissance européenne (SOG-IS) 11
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 14

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 15

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Microcontroller CENTAURUS_FB_04, Révision du matériel F » développé par *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, 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 « *authentication of the security IC* » ;
- le package « *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 :
- une partie matérielle comprenant :
  - un CPU[2] 32-bit ;
  - des mémoires (RAM, ROM, Flash) ;

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

  - o 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. ;
  - o des modules fonctionnels : gestion des entrées / sorties en mode contact (ISO7816), générateur de nombres aléatoires – PTRNG1, et DRNG2, 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 :
  - o d'un *loader* permettant le chargement du logiciel par le client ;
  - o d'un *boot loader* permettant l'initialisation, la configuration et le démarrage du produit ;
  - o de PEOS[3] (logiciel inclus dans le *boot loader*) fournissant un ensemble de commandes très réduit pour le test final et non disponible pour le client. PEOS est hors TOE.

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 « *Centaurus User Manual* », voir [GUIDES].

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur	Nom de la TOE, CENTAURUS	0x05
	Révision du matériel, version F	0x46
Identification des logiciels embarqués	*Platform ROM Firmware*, version B	0x42
	Platform Flash Firmware, version 04	0x04
	Loader, version 2.1 *Loader MKS checkpoint*, version 1.8	0x3231
Identification des bibliothèques	N/A	N/A

[1] *Physical True Random Number Generator* - Générateur physique de nombres aléatoires.
[2] *Digital Random Number Generator* - Générateur digital de nombres aléatoires.
[3] *Product Engineering Operating System* - Système d'exploitation d'ingénierie du produit.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité [ST], il est conforme au cycle de vie de 7 phases décrit dans [PP0084] :

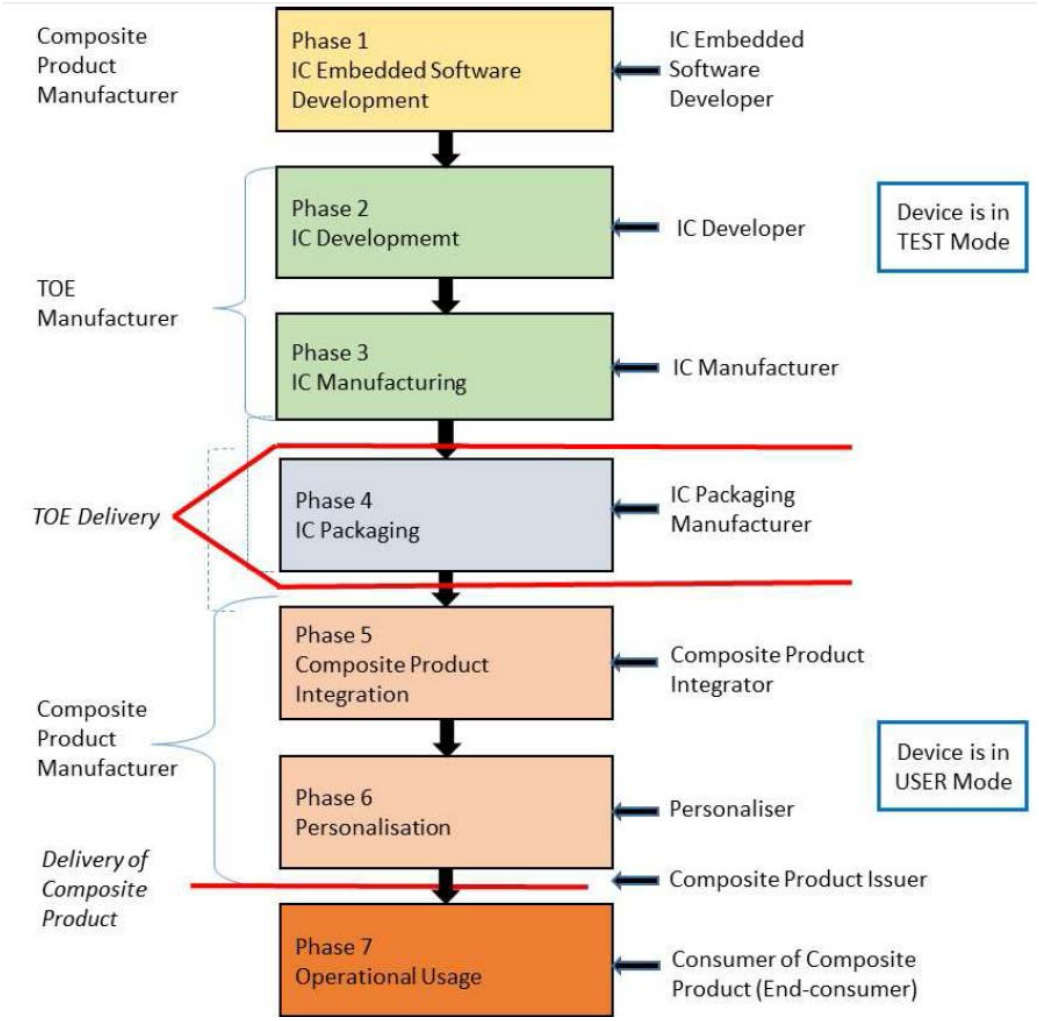

Figure 1 : Cycle de vie du produit

Seules les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de *wafers* ou de *wafers* sciés (*dices*). En option, la TOE peut également être livrée à la fin de la phase 4, dans sa forme finale, par exemple en format carte.
La phase 2 correspond à la phase de développement du microcontrôleur. Elle comprend notamment la conception du circuit et le développement du logiciel dédié.
La phase 3 couvre la fabrication du microcontrôleur. Elle comprend l'intégration et la fabrication du masque, la fabrication du circuit, le test du circuit, la préparation et la pré-personnalisation si nécessaire.
La phase 4, pouvant être gérée optionnellement par *INVIA SECURE SEMICONDUCTOR MEYREUIL*, comprend le conditionnement, le test et la pré-personnalisation si nécessaire.

Les sites impliqués dans le cycle de vie pour les phases 2, 3 et 4 sont indiqués dans la table ci-après :

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 USG1 5 Serangoon North Avenue 5, Singapore 554916 Singapour	
UTAC Thai Limited 1 (UTL1) 237 Lasalle road, Bangna, Bangkok, 10260 Thaïlande	**UTAC Thai Limited 3 (UTL3)** 73 Moo5, Bangsamak, Chachoengsao, 24180 Thaïlande

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. La TOE est délivrée dans ce mode.

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 (voir [GUIDES] : « *Centaurus Security Guidance* »).

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application à embarquer dans 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 *wafers* ou de *dices*.

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 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 Centaurus_DB_04, révision du matériel D » certifié le 16 novembre 2017 sous la référence ANSSI-CC-2017/67, voir [CER].

Le rapport technique d’évaluation [RTE], remis à l’ANSSI le 7 novembre 2018, 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 produit « Microcontroller CENTAURUS_FB_04, Révision du matériel F » 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 « Microcontroller CENTAURUS_FB_04, Révision du matériel F » 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]. Il devra suivre scrupuleusement 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 « *Centaurus Security Guidance* ». En particulier, l'implémentation des algorithmes cryptographiques devra être entièrement évaluée durant l'évaluation en composition.

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 :

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

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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 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 : - Security Target for CENTAURUS (Microcontroller CENTAURUS_FB_04), version 3.3, 16 avril 2018, *INVIA*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite for CENTAURUS (Microcontroller CENTAURUS_FB_04), version 1.0, 16 avril 2018, *INVIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – CENTAURUS-R, référence : LETI.CESTI.CENR.FULL.001, version 1.1, 5 novembre 2018, *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) – CENTAURUS-R, référence : LETI.CESTI.CENR.COMPO.001, version 1.0, 20 avril 2018, *LETI*.
[CONF]	Liste de configuration du produit : - CENTAURUS_FB_04, documentation list, version 3, 16 avril 2018, *INVIA*.
[GUIDES]	- Centaurus User Manual, référence CentaurusUM_1.5RC4, version 1.5, 28 mars 2018, *INVIA* ; - Centaurus Loader User Manual, référence UserManual_CC_Loader_v1.4, version 1.4, 18 août 2017 ; - Centaurus Security Guidance, référence INVIA_Centaurus_Security_guidance_v1.8, version 1.8, 11 avril 2018 ; - Secure 32 bits CPU Instruction Set Architecture (ISA), référence s8-isa, mai 2017 ; - Secure 32 bits CPU Embedded Application Binary Interface (EABI), référence s8-abi, version 0.6, mars 2013 ; - Guidance - Secure Delivery, référence AGD-Secure delivery-v1.0, version 1.0, 12 décembre 2016 ; - Centaurus Assembly Instructions, référence Centaurus Assembly – rev 0.5, version 0.5, 13 décembre 2016.
[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.*
[CER]	« Microcontrôleur Centaurus_DB_04, revision du materiel D ». *Certifié par l'ANSSI sous la référence ANSSI-CC-2017/67*.

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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), 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.