PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CC-2021/53

Security Enclave TESIC-04001R20 in SEQUANS communication SOC Monarch 2/N-SQN3401 (Référence TESIC-04001R20-BL2.0-AL28-CL3.0.F)

Paris, le 11 novembre 2021

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-2021/53

Nom du produit

Security Enclave TESIC-04001R20 in SEQUANS communication SOC Monarch 2/N-SQN3401

Référence/version du produit

Référence TESIC-04001R20-BL2.0-AL28-CL3.0.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.

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

TIEMPO SAS

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

Commanditaire

TIEMPO SAS

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

Centre d'évaluation

CEA - LETI

17 avenue des martyrs,
38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2.

SOG-IS

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est le « *Security Enclave TESIC-04001R20 in SEQUANS communication SOC Monarch 2/N-SQN3401*, Référence TESIC-04001R20-BL2.0-AL28-CL3.0.F » développé par TIEMPO SAS.

La TOE (*Target of Evaluation*) est l'enclave sécurisée TESIC-04001R20 intégrée dans le SoC Sequans Monarch 2/N - SQN3401.

Le SoC Monarch 2/N est un composant pour les applications IoT incluant des capteurs, des accessoires connectés et d'autres *devices*. Le SoC peut être utilisé comme une plateforme IC pour une certification en composition d'un produit GSMA (norme de téléphonie mobile de 3ème génération proche de la 4G).

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* » ;
- le *package* « *loader dedicated for usage by authorized users only* ».

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits dans la cible de sécurité [ST], section « *TOE Definition* » :
- le contrôle d'accès aux mémoires ;
- la gestion de la mémoire externe ;
- le mécanisme de sécurité pour passer en mode test, en mode pré-perso, en *admin mode* et en *firmware mode* ;
- des mécanismes de lecture/écriture des mémoires intégrant des algorithmes de chiffrement/déchiffrement, un mécanisme d'intégrité, des techniques de brouillage, et l'utilisation de CRC (code de détection d'erreurs) ;
- le support au chiffrement cryptographique à clés symétriques (DES, TDES, AES) ;
- l'accélérateur de Montgomery pour RSA et ECC résistant ;
- le support à la génération de nombres non prédictibles (TRNG[1] et PRNG[2]) ;
- les services de la librairie cryptographique.

1.2.3 *Architecture*

Le produit est décrit au chapitre 1.2 « *TOE Overview and TOE Description* ».

La figure 1 synthétise un aperçu des composants présents dans le Monarch SoC. La TOE est décrite dans la figure par « TESIC TOE ».

[1] *True Random Number Generator.*

[2] *Pseudo Random Number Generator*.

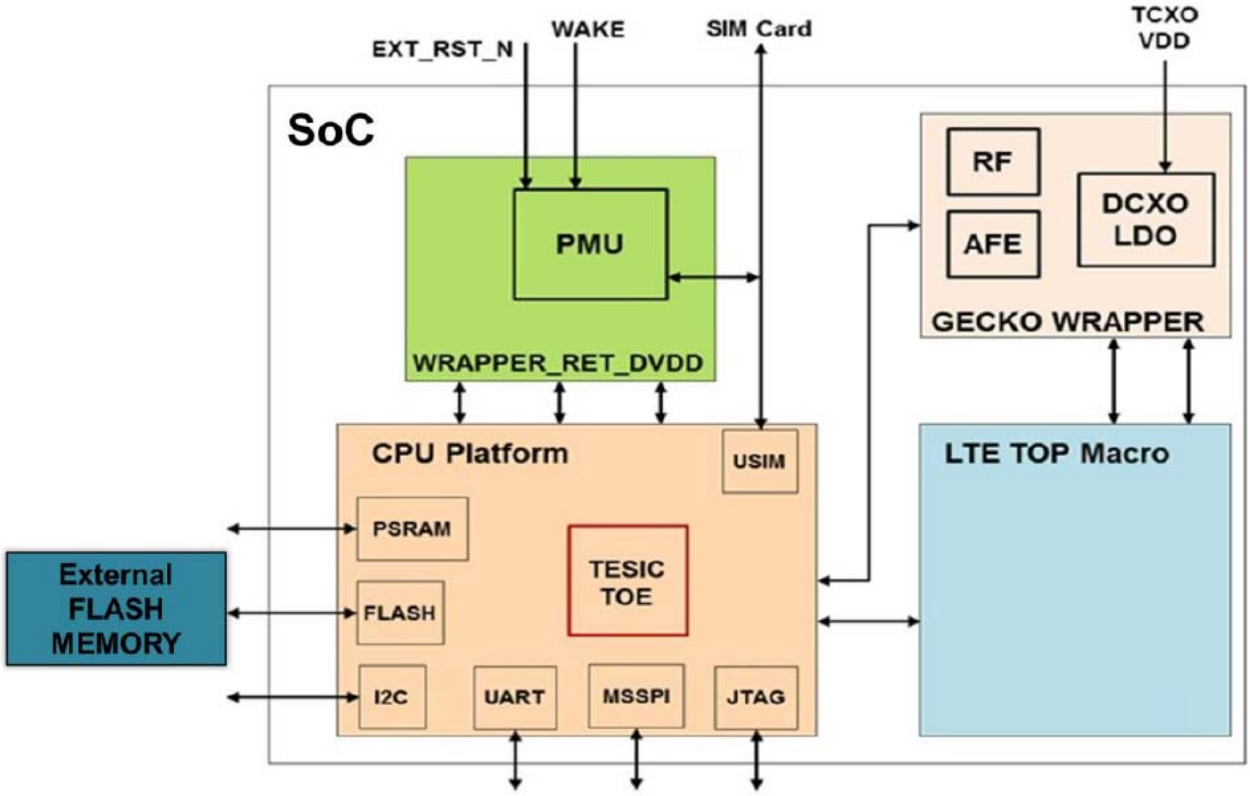

Figure 1 Architecture simplifiée du SoC

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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Overview and TOE Description* ».

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur TESIC-04001R20-BL2.0-AL28-CL3.0.F	*Hardware version of the security enclave, PRODUCTID version*	0x0400
	Mask layer revision MASKID0	0x1110
	Mask layer revision MASKID1	0x0001
	Mask layer revision MASKID2	0x5000
	Mask layer revision MASKID3	0x0005
	TESIC Test Access Port - JTAGID	0x00400AAB
Identification des logiciels embarqués	*Secure Bootloader v2.0 (ROM_version)*	0x0002
	Admin Loader and services v28 (optional) *Write interface installer v1.0 (optional)*	0x1C
Identification des bibliothèques	*Cryptographic library v3.0.F (optional)*	0x0000030F

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

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit dans [ST], au chapitre 1.2.6 *«TOE Life Cycle »*. Dans ce chapitre y est également décrit les sites de développement du produit :

- TIEMPO SAS Montbonnot, site certifié sous la référence ANSSI-CC-SITE-2021/13 ;
- Taïwan Semiconductor Manufacturing Company (TSMC), site certifié sous la référence BSI-DSZ-CC-S-0157-2020 ;
- UTAC Singapore (USG1), site certifié sous la référence ANSSI-CC-SITE-2018/05 et réaudité en 2020 ;
- SPIL Taiwan, site certifié sous la référence BSI-DSZ-CC-S-0157-2020.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le développeur de l'application à embarquer dans le microcontrôleur.

1.2.6 *Configuration évaluée*

Le certificat porte sur l'enclave sécurisée et la bibliothèque logicielle qu'elle embarque tels que définis 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.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Cette analyse n'a pas permis de mettre en évidence des biais statistiques bloquants. 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.

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY/P/01] et les résultats ont été consignés dans le rapport [RTE].

2.4 Analyse du générateur d'aléa

Le produit embarque un générateur physique de nombres aléatoires, TRNG, qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. 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 [ANSSI Crypto], 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'aléa n'a pas révélé de faiblesse.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 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 la TOE 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[3], 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 [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[4] , 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 :

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

[4] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *ASE – Security Target, Security Target of the Security Enclave in SEQUANS communication SoC, Monarch 2/N-SQN3401*, révision 1.12, 30 juillet 2021. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ASE – Security Target Lite, Security Target Lite of the Security Enclave in SEQUANS communication SoC, Monarch 2/N-SQN3401*, révision 1.0, 30 juillet 2021
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) MOUCHEROTTE* référence LETI.CESTI.MOU.FULL.001-V1.0, 30 juillet 2021. 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) MOUCHEROTTE*, référence LETI.CESTI.MOU.COMPO.001-V1.0 30 juillet 2021.
[CONF]	Liste de configuration du produit : - *Software Configuration lists for TESIC_04001R20*, *reference configuration_lists,* 30 juillet 2021 ; - *TESIC_04001R20 Release Configuration, reference HW_SW_Release_Configuration*, 30 juillet 2021.
[GUIDES]	*TESIC_04001R20 AGD – Preparative*, référence TESIC_04001R20_AGD-Pre, Version 1.1, 22 juillet 2021 ; *TESIC-0400R10 AGD_OPE – Operational user guidance*, référence *TESIC-04000R10-AGD_OPE-Operational_User_Guidance*, Version 1.2, 16 juillet 2021 ; *TESIC-04001R20 Hardware User Manual*, référence *TESIC_04001R20-Hardware_User_Manual,* version 1.11, 8 juillet 2021 ; *TESIC-04001R20 Crypto Library User Manual*, référence *tpoCryptoUserManua*l, version 3.0.F, revision 1, 30 juillet 2021 ; *TESIC SDK User Manual,* référence *TESIC-SDK_User_Manual,* version 1.1, 30 juillet 2021 ; *TESIC-04001R20 Host Loader User Manual*, référence *TPOLDR_User_Manual-1.5*, version 1.5, 6 avril 2021 ;

	TESIC-04001R20 ADMIN loader user specification, référence *TESIC_04001R20 – ADMIN loader user guide*, version 1.0, 22 janvier 2021 ; *TESIC-04001R20 AGD_OPE- Developer role description*, référence *TESIC_04001R20-AGD_OPEDeveloper_role*, version 2.4, 16 juillet 2021 ; *TESIC-04001R20 AGD_OPE- eNVM Loader role,* référence *TESIC_04001R20 - AGD_OPE -eNVM loader role*, version 1.4, 1 juillet 2021 ; *TESIC-04001R20 AGD_OPE- Package generator role*, référence *TESIC_04001R20 - AGD_OPE -Package generator role,* version 1.3, 11 juin 2021 ; *TESIC-04001R20 AGD_OPE - Flash write interface specification*, référence *AGD_OPE - Flash Write interface specification*, version 1.6, 28 novembre 2019 ; *TESIC-04001R20 Crypto Library - AGD_OPE – Security Guidelines*, référence *TESIC-04001R20-CLAGD_OPESecurity_guidelines*, version 1.2, 11 juin 2021 ; *TESIC-04001R20 AGD_OPE ADMIN Package generator role*, référence *TESIC_04001R20 ADM -AGD_OPE - Package generator role*, version 1.3, 6 juillet 2021 ; *TESIC-04001R20 ADMIN AGD_OPE - Developer role*, référence *TESIC_04001R20 ADM -AGD_OPE - Developer role*, version 1.1, 2 juillet 2021 ; *TESIC-04001R20 ADMIN AGD_OPE - loader user role*, référence *TESIC_04001R20 ADM - AGD_OPE - Loader role*, version 1.3, 01 juillet 2021 ; *TESIC-04001R20 ADMIN services - User guide*, référence *TESIC_04001R20 – ADMIN service user guide*, version 1.1, 16 avril 2021 ; *Monarch N platform - SQN3410 Chipset – Datasheet, référence Sequans Monarch_2_N-3410_SoC_Specification*, version 2, 23 janvier 2020.
[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 B. 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.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, 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 hardware devices with security boxes*, version 3.0, juillet 2020.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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