PREMIÈRE
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2023/01

AQUARIUS_BA_09
AQUARIUS_v1

Paris, le 11 Janvier 2023

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

Vincent STRUBEL

[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-2023/01

Nom du produit

AQUARIUS_BA_09

Référence/version du produit

AQUARIUS_v1

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"

"Loader dedicated for usage in Secured Environment only"

"Loader dedicated for usage by authorized users only"

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL6 augmenté

ASE_TSS.2, ALC_FLR.2

Développeur

THALES DIS DESIGN SERVICES

Arteparc, Bât D, Route de la côte d'Azur
13590 Meyreuil, France

Commanditaire

THALES DIS DESIGN SERVICES

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

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.2.

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 « AQUARIUS_BA_09, AQUARIUS_v1 » développé par THALES DIS DESIGN SERVICES.

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* » ;
- 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 :
- la protection physique du produit et des données qu'il contient notamment grâce à son *active shield* et différents détecteurs de sécurité ;
- des mécanismes de chiffrement de mémoires et bus ;
- des mécanismes d'intégrité des données ;
- un générateur physique d'aléa (PTRNG) ;
- un accélérateur cryptographique matériel fournissant des instructions de support pour l'implémentation des algorithmes Triple DES et AES ;
- un crypto-processeur appelé MEXPA fournissant des instructions de support pour l'implémentation d'algorithmes asymétriques (par exemple : RSA, ECDSA et ECDH).

1.2.3 *Architecture*

Le produit est constitué d'une partie matérielle et d'une partie logicielle toutes deux décrites dans le chapitre 1.2.3 de la cible de sécurité [ST].

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 qui sont détaillés dans la cible de sécurité [ST] au chapitre 1.2.1.

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur	Nom de la TOE (AQUARIUS_BA_09)	0x09
	Révision matérielle (B)	0x42
Identification des logiciels embarqués	Révision logicielle de la plateforme ROM (A)	0x41
	Révision logicielle FLASH (09)	0x09
	Version du *loader* (2.2)	0x0202

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 « Aquarius User Manual » (voir [GUIDES]).

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit dans la cible de sécurité [ST], chapitre 1.2.4, il est conforme au cycle de vie de sept phases décrit dans le profil de protection [PP0084].

Les sites impliqués dans le cycle de vie du produit (phases 2, 3 et 4) sont indiqués dans la table 3 de la cible de sécurité [ST]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

1.2.6 *Configuration évaluée*

Le certificat porte sur le microcontrôleur tel que décrit au chapitre 1.2.3 et identifié au chapitre 1.2.4. Toute autre application, y compris les routines éventuellement embarquées pour les besoins de l'évaluation, ne font 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 27 octobre 2022, 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

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].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence des vulnérabilités exploitables pour le niveau d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur matériel d'aléa 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.

Ce générateur matériel d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31] et suivant les dispositions décrites dans la note d'application [CC-NOTE-24], il répond aux exigences de la classe PTG.2.

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 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], 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 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.eu.

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[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 :

[2] 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 : - *Security Target for Aquarius (Microcontroller AQUARIUS_BA_09)*, référence AQUARIUS_ST, version 0.9, 19 octobre 2022. 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 AQUARIUS (Microcontroller AQUARIUS_BA_09)*, référence *AQUARIUS_B_ST_Lite*, version 002, 19 octobre 2022.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) – ERIDAN*, référence LETI.CESTI.ERI.FULL.001, version 1.0, 27 octobre 2022. 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) – ERIDAN*, référence LETI.CESTI.ERI.COMPO.001, version 1.0, 27 octobre 2022.
[CONF]	Liste de configuration du produit : - *ERIDAN – Documentation List*, référence ERIDAN – Documentation List_v2.5, version 2.5, 25 octobre 2022 ; - *Aquarius Identification*, référence AQUARIUS_BA_09_Identification_v005, version 005, 12 septembre 2022 ; - *Hardware Configuration list*, référence *AQUARIUS_ALC_Hardware* Configuration List-v1.2, version 1.2, 1 septembre 2022 ; - *Aquarius Firmware Tracking File*, référence Aquarius_Firmware_Tracking_File_v1.3, version 1.3, 3 octobre 2022 ; - *Aquarius Flash loader Tracking File*, référence AQUARIUS_FlashLoader_Tracking_File_v004, version 004, 14 septembre 2022.
[GUIDES]	Guide d'installation du produit : - *Aquarius User Manual*, référence AquariusUM_1.5, version 1.5, 12 octobre 2022 ; - *User Manual for Aquarius (Microcontroller AQUARIUS S8)*, référence AQUARIUS_Loader_User_Manual_v010, version 10, 14 septembre 2022 ; - *Aquarius Security Guidance*, référence *INVIA_Aquarius_Security_Guidance_v0.7*, version 0.7, 12 octobre 2022 ; - *S8 Embedded Application Binary Interface (EABI)*, référence s8-abi, version 0.6, mars 2013 ; - *Secure 23 bits CPU Instruction Set Architecture*, référence s8-isa-v1.3_rc, version 1.3_rc, octobre 2020 ; - *Aquarius Assembly instructions*, référence Aquarius_assy, version 0.4, 12 janvier 2020 ; - *Guidance – Secure delivery*, référence AGD – Secure Delivery – v1.2, version 1.2, 30 novembre 2021.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN22_ALC_GEN_v1.1 ;

	- [MEY] DISGEN21-MEY_STAR_v1.1 ; - [MuE] DISGEN21-MuE_STAR_v1.1 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN22_SGP_STAR_v1.0 ; - [PDMC] PDMC_2020_STAR_v1.0.
[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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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 and similar devices*, version 3.1, juin 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.
[AIS20/31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[CC-NOTE-24]	Evaluations de générateurs d'aléa selon AIS20/31 dans le schéma français, référence ANSSI-CC-NOTE-24_1.0, 2 mars 2021.

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