PREMIER 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-2024/06

ST33J2M0 including optional cryptographic library NESLIB (F01)

Paris, le 11 Mars 2024

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

Vincent STRUBEL

[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-2024/06

Nom du produit

ST33J2M0 including optional cryptographic library NESLIB

Référence/version du produit

F01

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

EAL5 augmenté

ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2, AVA_VAN.5.

Développeur

STMICROELECTRONICS

190 avenue Celestin Coq, ZI de Rousset,
13106 Rousset, France

Commanditaire

STMICROELECTRONICS

190 avenue Celestin Coq, ZI de Rousset,
13106 Rousset, France

Centre d'évaluation

SERMA SAFETY & SECURITY

14 rue Galilée, CS 10071,
33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.1.

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.cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « ST33J2M0 including optional cryptographic library NESLIB, F01 » développé par STMICROELECTRONICS.

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 :

- l'initialisation de la plateforme matérielle et des attributs ;
- l'intégrité logique du produit ;
- la gestion sécurisée du cycle de vie ;
- la protection physique ;
- la protection logicielle ;
- la génération d'aléa ;
- la gestion d'accès aux mémoires ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support au chiffrement cryptographique à clés asymétriques ;
- la librairie cryptographique optionnelle *NesLib*.

Ces principaux services de sécurité fournis par le produit sont décrits au chapitre 1.5 « *TOE overview* » de la cible de sécurité [ST].

1.2.3 *Architecture*

Ce produit peut être décomposé en deux parties distinctes : une partie logicielle et une partie matérielle.

La partie matérielle du produit est principalement constituée de :
- un processeur ;
- mémoires (ROM, RAM, Flash) ;
- des accélérateurs optionnels pour les algorithmes cryptographiques (RSA/ECC, SHA-1/SHA-256, SHA-384, AES) ;
- un générateur physique d'aléa ;
- le processeur cryptographique NESCRYPT optionnel ;
- un module d'horloge ;
- une interface de communication série entièrement compatible avec la norme ISO/IEC 7816-3 ;
- une interface SWP pour les communications NFC dans les applications *Secure Element* ;
- un module de communication pour les interfaces SPI et I2C.

La partie logicielle se décline en deux versions (3.2.5 et 3.3.0) et est composée de :
- un logiciel dédié, nommé OST, participant au démarrage du composant *(boot sequence)* ;
- un logiciel dédié, nommé *firmware*, assurant la gestion du cycle de vie, le chargement de la mémoire *Flash (Secure Flash loader)*, et l'interfaçage avec l'application *(drivers)*.

La version logicielle 3.2.5 est embarquée sur la révision matérielle H uniquement. La version logicielle 3.3.0 est embarquée sur les révisions matérielles H et I.

L'architecture détaillée du produit est décrite dans la cible de sécurité au chapitre 1.6 « *TOE Description* ».

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur ST33J2M0 F01	*IC Maskset name*	K500A
	Master identification number	0137h
	IC Version	H et I
Identification des logiciels embarqués	*OST*	330504
	Firmware	3.2.5
		3.3.0
Identification des bibliothèques	*Optional NesLib crypto library*	6.3.4

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Le produit est identifiable par lecture de registres comme indiqué dans les [GUIDES]. La version certifiée correspond aux valeurs indiquées dans la table 1 de la cible de sécurité [ST].

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit dans la cible de sécurité [ST] au chapitre 1.7 « *TOE life cycle* ». Il est conforme au cycle de vie de sept phases décrit dans [PP0084].

Le produit a été développé sur les sites mentionnés dans la table 16 de la cible [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 identifié dans la cible de sécurité [ST] au chapitre 1.4 *« TOE identification »*, dans ses configurations permises par les [GUIDES]. Les différentes variantes présentées en table 2 de la cible de sécurité sont toutes couvertes par le certificat. Au regard du cycle de vie, le certificat porte sur le produit livré à l'issue de la phase 3 comme de la phase 4.

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, 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]et [SOG-IS 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 de vulnérabilité exploitable 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 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] et [SOG-IS 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 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].

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 :

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 :

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

[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 : - *ST33J2M0 F01 including optional cryptographic library NESLIB Security Target*, SMD_ST33J2M0_ST_19_003, version F01.2, 1er septembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ST33J2M0 F01 including optional cryptographic library NESLIB Security Target for composition*, SMD_ST33J2M0_ST_19_004, version F01.2, septembre 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report PERCEVAL C03 and F01 Projects*, PERCEVAL-C03-F01_ETR_v1.1, version 1.1, 2 février 2024. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report Lite for composition PERCEVAL F01 Project*, PERCEVAL-F01_ETR_v1.1_Lite, version 1.1, 2 février 2024.
[CONF]	Liste de configuration du produit : - *ST33J2M0 F01 – HW Rev H – CONFIGURATION LIST*, SMD_ST33J2M0_F01_CFGL_23_001, version 1.0, 30 août 2023. - *ST33J2M0 F01 – HW Rev I – CONFIGURATION LIST*, SMD_ST33J2M0_F01_CFGL_23_002, version 1.0, 30 août 2023.
[GUIDES]	- *ST33J2M0 datasheet : Secure MCU with 32-bit SecurCore SC300 CPU with SWP, ISO, SPI, I2C & Flash*, DS_ST33J2M0, version 9, avril 2020. - *ST33J Secure MCU platforms Security Guidance*, AN_SECU_ST33J, version 10, 11 décembre 2019. - *ARM® SC300 r0p1 Technical Reference Manual*, ARM_DDI_0447 version A, 24 juin 2009. - *ARM® Cortex M3 r2p0 Technical Reference Manual*, ARM DDI 0337F3c, version F3c, 31 janvier 2018. - *ARM® SecurCore SC300 Errata*, PR326-PRDC-009983, version 11, 24 février 2015. - *ST33J2M0 firmware V3 User manual*, UM_ST33J2M0_FWv3, version 21, 22 juin 2023. - *ST33J platform – AIS31 compliant random number – User manual*, UM_ST33J_AIS31, version 1, 17 mai 2016. - *ST33J platform – AIS Reference implementation : Startup, on-line and total failure tests – AN*, AN_ST33J_AIS1, version 1, 17 mai 2016. - *NesLib cryptographic library Neslib 6.3 – User Manual,* UM_NesLib_6.3, version 4, juillet 2019. - *ST33J secure MCU platforms NesLib 6.3 security recommendations – Application Note*, AN_SECU_ST33J_NESLIB_6.3, version 7.

	- *NesLib 6.3.4 for ST33 Lockstep platforms – Release note*, RN_ST33J_NESLIB_6.3.4, version 6.
[SITES]	Références des rapports d'analyse documentaire et d'audit de site pour la réutilisation : - STM_2023_ALC_GEN_v1.1 ; - STM_2022_ATP1_ATP3-4_STAR_v1.0 ; - STM_2021_ATT3_STAR_v1.1 ; - STM-2021_DNP_STAR_v1.0 ; - STM_2022_DPE_STAR_v1.1 ; - STM2022_FEI_STAR_v1.0 ; - STM_2022_AMK1_STAR_v1.0 ; - STM-2021_TPY-AMK6_STAR_v1.0 ; - STM_2023_BSK_STAR_v1.0 ; - STM_2022_CAL_STAR_v1.0 ; - STM_2022_CAT-PAL_STAR_v1.1 ; - STM_2022_CRL_STAR_v1.1 ; - STM_2021_RST_STAR_v1.1 ; - STM_2022_GNB_STAR_v1.1 ; - STM_2022_LJU_STAR_v1.1 ; - STM_2023_LYG_STAR_v1.0 ; - STM_2022_RNS_STAR_v1.1 ; - STM_2021_SOP_STAR_v1.1 ; - STM_2022_TNS_STAR_v1.0 ; - STM_2022_JSCC_STAR_v1.0 ; - STM-2021_STS_STAR_v1.0 ; - STM_2022_ZVT_STAR_v1.1 ; - STM_2021_WIN_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 3.2, novembre 2022.
[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.
[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.2, 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]	Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, ANSSI-CC-NOTE-24_1.0, version 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.