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-2020/20-R01

MS6003 embarquant la bibliothèque cryptographique Toolbox version 06.04.01.05 et la bibliothèque Wear Levelling version 06.03.02.02 (révision C)

Paris, le 30 Mars 2025

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

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 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 Résumé

Référence du rapport de certification **ANSSI-CC-2020/20-R01**
Nom du produit **MS6003 embarquant la bibliothèque cryptographique Toolbox version 06.04.01.05 et la bibliothèque Wear Levelling version 06.03.02.02**
Référence/version du produit **révision C**
Type de produit **Cartes à puce et dispositifs similaires**
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"*
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report (full ETR) - SIROCCO-C_2024* référence LETI.CESTI.SIR.FULL.001 – V2.1 version 2.1 26 février 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Exigences de configuration du produit, hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage
Développeur **SEALSQ France** Arteparc Bachasson, Bât. A, rue de la carrière de Bachasson 13590 Meyreuil, France

Commanditaire **SEALSQ France** Arteparc Bachasson, Bât. A, rue de la carrière de Bachasson 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.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « MS6003 embarquant la bibliothèque cryptographique Toolbox version 06.04.01.05 et la bibliothèque Wear Levelling version 06.03.02.02, révision C » développé par SEALSQ France.

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.

2.2 Description du produit

2.2.1 *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 »*.

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits au chapitre 1.2.1 « *TOE Overview* » de la cible de sécurité [ST].

2.2.3 *Architecture*

La TOE[1], comme décrit au chapitre 1.2.4 « *TOE Description* » de la cible de sécurité [ST], est constituée des éléments suivants :

- une partie matérielle composée en particulier :
  - d'un processeur *ARM SecureCore SC300 32bit RISC* ;
  - d'un accélérateur cryptographique 32-bit Ad-X3 pour les opérations de cryptographie asymétrique ;
  - d'un moteur CRC 16 et 32 conforme à l'ISO/IEC 3309 ;
  - de composants matériels DES[2] ;
  - d'un composant matériel AES (128, 192 et 256 bits) ;
  - d'un contrôleur d'interruption à 2 niveaux ;

[1] *Target of Evaluation*

[2] Seul l'usage du chiffrement TDES est inclus dans le périmètre de l'évaluation.

- d'un générateur aléatoire physique ;
- de deux *timers* l'un 16 bits, l'autre 32 bits ;
- de contrôleurs d'interfaces ISO 7816, SPI (*Single protocol Interface*), I2C (*Inter Integrated Circuit*), USB et GPIO (*General Purpose Input/Output Interface)* ;
- de mémoires :
  - ROM : 64Ko contenant la bibliothèque cryptographique Toolbox et la bibliothèque optionnelle *Wear Levelling* ;
  - FLASH : 1 Mo ;
  - RAM : 24Ko dont 4Ko partagés entre l'accélérateur matériel Ad-X3 et le CPU.

- une partie logicielle comprenant :
  - la bibliothèque cryptographique *Toolbox* ;
  - la bibliothèque optionnelle *Wear Levelling* ;
  - le logiciel optionnel *Secure Bootloader*.

2.2.4 *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 fournis en table 1 (pour les éléments matériels et logiciels) et table 2 (pour les éléments documentaires) de la cible de sécurité [ST].

Ces éléments peuvent être vérifiés par lecture des registres (voir [GUIDES]).

2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 1.3 « *TOE Life Cycle* » de la cible de sécurité [ST] ; il est conforme à celui décrit dans [PP0084].

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Le produit comporte deux modes possibles :

- le mode *Test*, qui permet de tester la TOE, de charger le code utilisateur et de commuter en mode *User*. Ce mode est également utilisé pour analyser les produits défaillants lors de retours terrains par exemple. Le basculement du mode *User* en mode *Test* donne systématiquement lieu à un effacement total de la mémoire FLASH, rendant inexploitables les données de l'utilisateur final ;
- le mode *User,* qui correspond au mode final d'utilisation de la TOE.

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur d'une application à embarquer dans le microcontrôleur.

2.2.6 *Configuration évaluée*

Le certificat porte sur le « Microcontrôleur MS6003 révision C embarquant la bibliothèque cryptographique *Toolbox* version 06.04.01.05 et la bibliothèque *Wear Levelling* version 06.03.02.02 ».

Toute autre application, notamment les logiciels de test du microcontrôleur embarqués pour les besoins de l'évaluation, ne fait donc pas partie du périmètre d'évaluation.

Au regard du cycle de vie, le produit évalué est le produit issu de la phase 3 du cycle de vie.

3 L'évaluation

3.1 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).

3.2 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** ».

3.3 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 [ANA_CRY].

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 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.

3.4 Analyse du générateur d'aléa

Le produit comporte un générateur physique d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

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 de vulnérabilité exploitable pour le niveau d'attaquant visé. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies.

Dans le cas où le générateur d'aléa serait utilisé à des fins cryptographiques, il est obligatoire de le combiner à un mécanisme algorithmique de génération de pseudo-aléa, de nature cryptographique, afin de fournir des données aléatoires cryptographiquement satisfaisantes, comme énoncé dans le document [ANSSI Crypto].

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 [NOTE-24].

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-2020/20-R01, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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].

4.4 Reconnaissance du certificat

4.4.1 *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 :

4.4.2 *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 : - *SIROCCO-C_2024 Security Target*, référence SIROCCO-C_2024_ST v2.4, version 2.4, 25 février 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MS6003 Security Target Lite*, référence TPG0235C, version C, 25 février 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) - SIROCCO-C_2024*, référence LETI.CESTI.SIR.FULL.001 – V2.1, version 2.1, 26 février 2025.
[ANA_CRY]	Cotation des mécanismes cryptographiques SIROCCO-C, référence LETI.CESTI.RT.001- V1.0, version 1.0, 3 décembre 2024.
[CONF]	Liste de configuration du produit : - *SIROCCO delivery list*, référence Sirocco_EDL_V1.3.xls, version 1.3, 25 février 2025.
[GUIDES]	Guides du produit : - *MS6xxx Technical Datasheet*, référence TPR0702EX, version E, 7 novembre 2024 ; - *MS6003 Technical Datasheet*, référence TPR0704DX, version D, 11 octobre 2024 ; - *Security Recommendations for MS6XXX 90nm Products – Application note*, référence TPR706EX, version E, 16 octobre 2024 ; - *Security Hardware DES/TDES on MSXXX 90nm Products – Application note, référence TPR0707FX, version F, 15 octobre 2024 ;* - *Security Hardware AES on MSXXX Products (90nm) – Application note*, référence TPR0708EX, version E, 15 octobre 2024 ; - *Ad-X3 Datasheet*, référence TPR0701DX, version D, 10 octobre 2024 ; - *Generating Random Numbers on MS6XXX Products (90nm) – Application note*, référence TPR0709FX, version F, 15 octobre 2024 ; - *Toolbox 06.04.01.XX on MS6XXX – Application note*, référence TPR0711JX, version J, 10 octobre 2024 ; - *TBX 06.04.01.XX Erratasheet – Application note*, référence TPR0727EX, version E, 7 novembre 2024 ; - *Securing TBX 06.04.01.XX on MSXXXX 90nm Products – Application note*, référence TPR0712OX, version O, 25 février 2025 ; - *Wear Levelling library and low level FLASH drivers – Application note*, référence TPR0710CX, version C, 7 novembre 2024 ;

	- *Efficient Use of Ad-X3 – Application note*, référence TPR0726EX, version E, 7 novembre 2024 ; - *MS6XXX Secure Acceptance Guidance*, référence TPR0754CX, version C, 28 janvier 2020 ; - *SC300 Technical Reference Manual*, référence DDI0447A, version A, 24 juin 2009 ; - *SmartACT's User Manual – Application note*, référence TPR0134FX, version F, 18 août 2017 ; - *MS600X Customer Options Form*, référence MS600X_COF_V1.1_RV, version 1.1_1, avril 2017.
[SITES]	Rapports d'audit de site pour la réutilisation : - WISEKEY-2024_ 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, 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 3.2.1, février 2024.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[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*).
[NOTE-24]	Note d'application – Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, référence ANSSI-CC-NOTE-24, version en vigueur.

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