Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance ANSSI-CC-2014/60-M01

Microcontrôleurs sécurisés SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 et SB23ZD04 incluant optionnellement la librairie cryptographique NesLib révision 3.1

Certificat de référence : ANSSI-CC-2014/60

Paris, le 21 juillet 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Microcontrôleurs sécurisés SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 et SB23ZD04 incluant optionnellement la librairie cryptographique NesLib révision 3.1, 21 octobre 2014, ANSSI-CC-2014/60.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	POMEROL2 Project : Surveillance Technical Report, 28 avril 2015, référence POMEROL-2_STR_v1.0, version 1.0.
[R-S02]	POMEROL2 Project : Surveillance Technical Report, 14 avril 2016, référence POMEROL-2_STR_v2.0, version 2.0.
[R-S03]	POMEROL2 Project : Surveillance Technical Report, 12 mai 2017, référence POMEROL-2_STR_v3.0, version 3.0.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Security Impact Analysis Report, Development environment evolution on SC23Z018 Platform, référence SMD_SC23Z018_SIA_17_001, rev. 1.01, 21 March 2017, STMicroelectronics.
[RM-Lab]	Site Visit Report - STM CROLLES site audit, ST-Crolles 2016_SVR_v1.0, 23 septembre 2016, Serma Safety & Security.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CCRA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

2. Identification du produit maintenu

Le produit « Microcontrôleurs sécurisés SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 et SB23ZD04 incluant optionnellement la librairie cryptographique NesLib révision 3.1 » a été initialement certifié sous la référence ANSSI-CC-2014/60 (référence [CER]) et fait l'objet de la présente maintenance.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- les sites ci-dessous sont retirés du cycle de vie du produit :

  - ***NEDCARD***
    Bijsterhuizen 25-29
    6604 LM Wijchen
    Pays-Bas

- ***DISCO HI-TEC EUROPE GMBH***
  Liebigstrasse 8,
  D-85551 Kirchheim bei München,
  Allemagne

- ***GLOBAL FOUNDRIES***
  60 Woodlands industrial park,
  D street 2
  Singapore 738406
  Singapour

- le site ci-dessous est ajouté au cycle de vie du produit:

  - ***STMICROELECTRONICS***
    850 rue Jean Monnet
    38926 Crolles
    France

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	*SC23Zxxx/SB23ZDxx Secure MCU with enhanced security, crypto-processor, 18-Kbyte EEPROM and I2C-bus Fast-mode slave interface – Datasheet*, référence DS_SC23Z018, version 2, mars 2014, STMicroelectronics .	[CER]
	Application note SB23Z012/SC23Z018 and derivative devices security guidance, référence AN_SECU_Sx23Z0xx, version 4, 5 septembre 2014, STMicroelectronics.	[CER]
	User Manual – ST23 Secure MCUs NesLib 3.1 cryptographic library, référence 3 UM_23_NesLib_3.1, version 5, 30 août 2013, STMicroelectronics.	[CER]
	Application Note, ST23Z secure microcontrollers power supply gitch detector characteristics, 3 référence *AN_23Z_GLITCH*, version 1, février 2013.	[CER]
	ST23 – AIS31 Compliant Random Number user manual, référence UM_23_AIS31, version 2, février 2013.	[CER]
	ST23 – AIS31 Reference Implementation – Start-up, online and total failure tests – Application Note,	[CER]

	référence *AN_23AIS31*, 4 version 2, septembre 2009.	
[ST]	Cibles de sécurité de référence: - *SC23Z018 and 7 derivative products with optional cryptographic library NESLIB 3.1 SECURITY TARGET*, référence: SMD_SC23Z018_ST_12_001_V02.09, version 2.09 du 21 mars 2017, STMicroelectronics. Version publique : - *SC23Z018 and 7 derivative products with optional NesLib3.1 Security Target - Public Version*, référence: SMD_SC23Z018_ST_13_001 Rev 01.09, March 2017, STMicroelectronics.	[R-M01]

5. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur.
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.
Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

6. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été 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 EAL4 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] Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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