



*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-2010/02-M04**

**SA23YR48B / SB23YR48B / SA23YR80B /**  
**SB23YR80B**

**Certificat de référence : ANSSI-CC-2010/02**

*Paris, le 13 décembre 2016*

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

Guillaume POUPARD  
[ORIGINAL SIGNE]



## 1. Références

[CER]	Rapport de certification ANSSI-CC-2010/02, Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 10 février 2010, ANSSI.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Lettre, Surveillance d'un produit certifié, 1674/ANSSI/SR/CCN, 30 juin 2011, ANSSI.
[R-S02]	Lettre, Surveillance d'un produit certifié, 2783/ANSSI/SDE/PSS/CCN, 27 septembre 2012, ANSSI.
[R-S03]	Rapport de surveillance ANSSI-CC-2010/02-S03, SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B, 4 décembre 2013, ANSSI.
[R-S04]	Rapport de surveillance ANSSI-CC-2010/02-S04, SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B, 20 novembre 2014, ANSSI.
[R-S05]	Rapport de surveillance ANSSI-CC-2010/02-S05, SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B, 25 août 2016, ANSSI.
[MAI]	Procédure ANSSI MAI/P/01 – Maintien de la confiance : Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2010/02-M01, Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 19 mars 2010, ANSSI.
[R-M02]	Rapport de maintenance ANSSI-CC-2010/02-M02, Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 8 juillet 2010, ANSSI.
[R-M03]	Rapport de maintenance ANSSI-CC-2010/02-M03, Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 26 février 2013, ANSSI.
[IAR]	Impact Analysis Report – Development Environment Evolution on ST23 Platform, SMD_ST23YR80&R160_SIA_16_001, v01.03, 23 novembre 2016, STMicroelectronics.
[RM-Lab]	Evaluation Technical Report Addendum Lafite Project, Lafite_ETR_ADD_v1.0, 25 novembre 2016, Serma Safety & Security.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 8th, 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.

## 2. Identification du produit maintenu

Le produit maintenu est la famille de microcontrôleurs sécurisés « SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B » développée par la société *STMICROELECTRONICS*, initialement certifiée sous la référence [CER], et ayant déjà fait l'objet de trois maintenances sous les références [R-M01], [R-M02] et [R-M03].

## 3. Description des évolutions

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

- Suppression d'un site de production *Front End* :
  - Global Foundries, 60 Woodlands industrial park, D street 2, 738406, Singapore.
- Suppression d'un site de production *Back End* :
  - Disco HI-TEC Europe GmbH, Liebigstrasse 8, D-85551 Kirchheim beu Munchen, Germany.
- Ajout du site de production *Back end* :
  - STM Calamba, 9 Mountain Drive, LISP II, Brgy La Mesa, Calamba,4027, Philippines.
- Ajout du site de production *Back-end* :
  - AMKOR Technologies Philippines ATP1 : Km 22 East Service roas south superhighway, 1771 Muntipula City, Philippines.
  - AMKOR Technologies Philippines ATP3/4 : 119N Science avenue, Laguna technopark, 4024 Binan Laguna Philippines.

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, du produit évalué et sont applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M04] référence la présente maintenance.

[GUIDES]	ST23YR48 Data Sheet, DS_23YR48 Rev 2.	[R-S03]
	ST23YR80 Data Sheet, DS_23YR80 Rev 4.	[R-S04]
	ST23YR80/48 Recommendations for contactless operation, AN_23YR80_RCMD Rev 5.	[R-S04]
	ST23 platform security guidance Application note, AN_SECU_23 Rev 12.	[R-S05]
	ST23 secure MCUs with AES NesLib security guidance, AN_23_AES_NesLib Rev 3.	[R-S04]
	How to identify certified hardware devices using additional ST traceability information (composite certification), AN_TRACE Rev 2.	[R-S03]
	NesLib 2.0 cryptographic library User Manual, UM_23_NesLib_2.0 Rev 7.	[R-S03]
	NesLib 3.0 cryptographic library User Manual, UM_23_NesLib_3.0 Rev 5.	[R-S03]
	ST23 AIS31 compliant random numbers User Manual, UM_23_AIS31 Rev2.	[R-M02]
	ST23 AIS31 Reference implementation Start-up, Online and Total FailureTests, AN_23_AIS31 Rev2.	[R-M02]
	ST21/23 programming manual, PM_21_23 Rev3.	[R-M03]
[ST]	SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B Security target – public version, SMD_Sx23YRxx_ST_09_002, Rev 03.02, novembre 2016.	[R-M04]
[CONF]	Addendum à la liste de configuration : Impact Analysis Report – Development Environment Evolution on ST23 Platform, SMD_ST23YR80&R160_SIA_16_001, Rev 01.03, 23 novembre 2016, STMicroelectronics.	[R-M04]

## 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, à la date de certification.

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 la 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<sup>1</sup>, 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 CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires<sup>2</sup>, 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 :



---

<sup>1</sup> Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

<sup>2</sup> Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.