



**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 maintenance ANSSI-CC-2019/20-M01

ST54J / ST54K A03

Certificat de référence : ANSSI-CC-2019/20

Paris, le 15 octobre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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.

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

La reproduction de ce document sans altération ni coupure est autorisée.

1 Références

[CER]	Rapport de certification ANSSI-CC-2019/20, ST54J A01, 18 avril 2019.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2019/20-S01, ST54J A02, 10 mars 2020.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01
[IAR]	Security Impact Analysis Report-ST54J A03, référence SMD_ST54J_A03_SIA_20_001, version 1.4, 20 juillet 2020.
[RM-Lab]	Evaluation Technical Report Addendum, PEACOCK1 Project, reference PEACOCK1_ETR_ADD_v1.0/1.0, Serma Safety & Security.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</i>
[CCRA]	<i>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.</i>

2 Identification du produit maintenu

Les produits objets de la présente maintenance sont les microcontrôleurs « ST54J / ST54K A03 » développés par la société STMICROELECTRONICS. Le microcontrôleur ST54J A03 existe dans les révisions C & D, tandis que le microcontrôleur ST54K A03 existe uniquement dans la révision D.

Le produit « ST54J A01 » (révision C) a été initialement certifié sous la référence ANSSI-CC-2019/20 (référence [CER]).

Les versions maintenues du produit sont identifiables par les éléments suivants :

Eléments de configuration		Données d'identification lues
Identification des microcontrôleurs ST54J / ST54K A03	<i>IC maskset name</i>	K520B
	<i>IC version C (ST54J)</i>	43
	<i>IC version D (ST54J/ST54K)</i>	44
	<i>Master identification number</i>	01 CA
Identification des logiciels embarqués	<i>Firmware version 3.1.2</i>	03 01 02
	<i>OST version 09.01</i>	09 01
Identification des bibliothèques	<i>N/A</i>	N/A

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) décrit les modifications opérées. Ces dernières sont présentées dans cette section.

Dans sa révision C, le ST54J correspond au produit certifié sous la référence [CER] et surveillé sous la référence [R-S01]. La présente maintenance introduit la révision D. Le ST54J en révision D sera proposé pour les nouveaux projets ne demandant pas le nouveau bus SPI, afin de bénéficier des améliorations de rendement et de qualité de la révision D.

La présente maintenance introduit également le microcontrôleur « ST54K », aussi appelé « ST54K_SE ». Ainsi la plateforme ST54K est composée du microcontrôleur « ST54K_SE », d'un module NFC, nommé « ST54K_NFC » et d'un module IORING nommé « ST54K IOs ». La configuration du firmware du module NFC active un bus SPI additionnel pour contrôler, par exemple, une puce RF UWB (*Ultra Wide Band*). Les modules NFC et IORING sont en dehors du périmètre d'évaluation. Le ST54K n'existe que dans la révision D.

Le nom commercial ST54K a été introduit en plus du ST54J pour des raisons de clarté et d'héritage.

De plus, le rapport d'analyse d'impact de sécurité (référence [IAR]) précise l'ajout de 5 sites impliqués dans le cycle de vie des produits :

- Samsung Hwaseung (*Mask Data Preparation*) ;
- Toppan Icheon (*Mask Manufacturing*) ;
- Samsung Giheung (*Wafer Manufacturing*) ;
- Samsung Onyang (*Wafer Storage*) ;
- ST Ljubljana (site de développement).

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.

Les guides contenant de nouvelles recommandations sécuritaires obligatoires par rapport au certificat initial apparaissent en gras. Bien que certains guides en gras réfèrent [R-M01], les nouvelles recommandations sécuritaires ont été prises en compte à travers [R-S01].

[GUIDES]	NFC controller and secure element system in package - ST54J ST54K datasheet, référence DS_ST54J, version 7, juin 2020.	[R-M01]
	ST54J SE OS developer's guide - User Manual - ST54J platform SE subsystem OS developer's guide, référence UM_ST54J_SE, version 8, février 2020.	[R-M01]
	ST54J platform SE subsystem Security guidance, référence AN_SECU_ST54J_SE, version 3, décembre 2019.	[R-S01]
	ST54J_SE firmware V3 - User manual, référence UM_ST54J_SE_FWv3, version 8, mai 2020.	[R-M01]
	ARM® SC300 r0p1 Technical Reference Manual, référence ARM_DDI_0447, version A, 24 juin 2009.	[CER]
	ARM® Cortex M3 r2p0 Technical Reference Manual, référence ARM_DDI_0337, version F3c, 31 janvier 2008.	[CER]
	ARM® Core SC300 Product Errata, référence ARM-EPM-041935 (précédemment PR326-PRDC-009983), version 11, 24 février 2015.	[CER]
	ST54J_SE platform - AIS31 compliant random number - User manual, référence UM_ST54J_SE_AIS31, version 1, mars 2018.	[CER]
	ST54J_SE platform - AIS Reference implementation: Startup, on-line and total failure tests – AN, référence AN_ST54J_SE_AIS1, version 1, avril 2017.	[CER]
	ST54J_SE Device Limitations – Errata Sheet, référence ES_ST54J_SE, version 1, juin 2020.	[R-M01]
[ST]	ST54J A03 Security Target, référence SMD_ST54J_ST_17_001, version A03.2, juillet 2020. Version publique : ST54J A03 Security Target for composition, référence SMD_ST54J_ST_17_002, version A03.2, juillet 2020.	[R-M01]
[CONF]	ST54J A03 HW rev C- configuration list, référence SMD_ST54J_A03_CFGL_20_001, version 1.0, 2 juin 2020. ST54J A03 HW rev D- configuration list, référence SMD_ST54J_A03_CFGL_20_002, version 1.0, 2 juin 2020.	[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 surveillée. Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

6 Reconnaissance du certificat

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'accord¹, 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 :



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 signataires², 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.