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-2013/59-M01

Microcontrôleur AT90SC28880RCFV2 révision D embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04

Certificat de référence : ANSSI-CC-2013/59

Paris, le 26 février 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Microcontrôleur AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04, certifié le 24 décembre 2013 sous la référence ANSSI-CC-2013/59.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2013/59-S01 du 13 janvier 2015.
[R-S02]	Rapport de surveillance ANSSI-CC-2013/59-S02 du 18 décembre 2015.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	*Krypton AT90SC28880RCFV2 Rev D Impact Analysis Report*, référence : Krypton SIA Rev D v1.6, 11 septembre 2015.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 08 janvier 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, juillet 2014.

2. Identification du produit maintenu

Le produit maintenu est le « Microcontrôleur AT90SC28880RCFV2 révision D embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04 » développé par la société *INSIDE SECURE*.

Le produit « Microcontrôleur AT90SC28880RCFV2 révision C embarquant la bibliothèque cryptographique optionnelle TBX version 00.03.22.04 » a été initialement certifié sous la référence ANSSI-CC-2013/59 (référence [CER]).

La version maintenue du produit est identifiable par l'élément suivant :

- révision : 0x83 pour la révision D par lecture du registre SN_1 (voir paragraphe **1.2.2** de [CER]).

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne qu'une modification a été apportée sur la couche métallique n°2 afin d'améliorer le temps de démarrage du mode ISO7816-3.
Cette modification est jugée mineure et ne remet pas en cause la sécurité du produit ainsi que les résultats des tests menés lors de l'évaluation initiale ou des différentes surveillances.

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-M01] référence la présente maintenance.

[GUIDES]	*Secure use of Tbx 00.03.2x.xx on AT90SC*, référence : TPR0505IX, version I, *INSIDE SECURE*.	[R-S02]
	Security Recommendations for 0.13µm Products -2, référence : TPR0456, version F, *INSIDE SECURE*.	[R-S02]
	Secured Hardware DES/TDES for 0.13 µm Products, référence : TPR0400, version L, *INSIDE SECURE*.	[R-S02]
	AT90SC28880RCFV2Technical Datasheet, référence : TPR0548, version E, *INSIDE SECURE*.	[R-S02]
	Generating Random numbers to known standards for 0.13µm Products, réf. : TPR0468FX, version F, *INSIDE SECURE*.	[R-S01]
	Wafer Saw Recommendations, réf. : TPG0079BX, version B, *INSIDE SECURE*.	[CER]
	SmartACT User's Manual, réf. : TPR0134DX, version D, *INSIDE SECURE*.	[CER]
	The Code Signature Module for 0.13µm Products, TPR0409CX, version C, INSIDE SECURE.	[CER]
	Secured Hardware AES on AT90SC products (0.13µm), réf. : TPR0428EX, version E, *INSIDE SECURE*.	[CER]
	AT90SC 0.13µm products Technical Datasheet, réf. : TPR0447EX, version E, *INSIDE SECURE*.	[CER]
	Ad-X2 Datasheet, réf. : TPR0452DX, version D, *INSIDE SECURE*.	[CER]
	Efficient use of Ad-X2, réf. : TPR0463CX, version C, *INSIDE SECURE*.	[CER]
	Toolbox 00.03.2x.xx Datasheet, réf. : TPR0504EX, version E, *INSIDE SECURE*.	[CER]
	Customer Option Form, réf. : COF v4.91b.pdf, version 4.9b, *INSIDE SECURE*.	[CER]
[ST]	Cibles de sécurité de référence: - *Krypton Security Target v1.9*, référence : Krypton_ST_V1.9, version 1.9, *INSIDE SECURE* ; Version publique : - *Security Target-Lite AT90SC28880RCFV2*, référence : TPG0224F, version F, *INSIDE SECURE*.	[R-M01] [R-M01]
[CONF]	*KRYPTON Manufacturing Configuration List for Rev D*, référence : Krypton_MCL_V1.3, version 1.3, *INSIDE SECURE*.	[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, 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[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 CC RA [CC RA]

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] 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.

[2] 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, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.