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-2014/18-M01

Microcontrôleur AT90SO72 révision C embarquant la bibliothèque cryptographique optionnelle Toolbox version 00.03.12.00

Certificat de référence : ANSSI-CC-2014/18

Paris, le 13 novembre 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Microcontrôleur AT90SO72 révision C embarquant la bibliothèque cryptographique optionnelle Toolbox version 00.03.12.00, référence ANSSI-CC-2014/18, 9 avril 2014, ANSSI.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2014/18-S01, 17 février 2016.
[R-S02]	Rapport de surveillance ANSSI-CC-2014/18-S02, 17 février 2017.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Beetle AT90SO72 Security Impact Analysis, référence Beetle-SIA_RecC_V1.2, version 1.2 du 26 juin 2018, *WISEKEY*.
[RM-Lab]	ETR Addendum – BEETLE project, référence BEETLE_ETR_ADD_V1.1, version 1.1, 6/11/2018, *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 « Microcontrôleur AT90SO72 révision C embarquant la bibliothèque cryptographique optionnelle Toolbox version 00.03.12.00 » a été initialement certifié sous la référence ANSSI-CC-2014/18 (référence [CER]).

Le produit objet de la présente maintenance est « Microcontrôleur AT90SO72 révision C embarquant la bibliothèque cryptographique optionnelle Toolbox version 00.03.12.00 » initialement développé par la société *INSIDE SECURE* devenue aujourd'hui *WISEKEY*.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) indique que le cycle de vie du produit a été modifié d'où cette maintenance. Les sites entrant maintenant dans le cycle de vie sont ceux mentionnés dans la cible de sécurité (voir §1.4.2.1).

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.
Il est à noter qu'aucun guide n'a été modifié ou ajouté depuis la dernière surveillance.

[GUIDES]	- Secured Hardware DES/TDES on AT90SC 0.13µm products, reference TPR0400LX, version L, *INSIDE SECURE* ; - The Code Signature Module for 0.13µm Products, reference TPR0409CX, version C, *INSIDE SECURE* ; - Secured Hardware AES on AT90SC products (0.13µm), reference TPR0428EX, version E, *INSIDE SECURE* ; - AT90SC 0.13µm products Technical Datasheet, reference TPR0447EX, version E, *INSIDE SECURE* ; - Ad-X2 Datasheet, reference TPR0452DX, version D, Inside Secure ; - Security Recommendations for 0.13µm Products - 2, reference TPR0456HX, version H, *WISEKEY* ; - Efficient use of Ad-X2, reference TPR0463CX, version C, *INSIDE SECURE* ; - Generating Random numbers to known standards for 0.13µm Products, reference TPR0468FX, version F, *INSIDE SECURE* ; - Toolbox 00.03.1x.xx Datasheet, reference TPR0454DX, version D, *INSIDE SECURE* ; - Secure use of TBX 00.3.1x.xx, reference TPR0455HX, version H, *INSIDE SECURE* ; - AT90SO72 Technical Datasheet, reference TPR0438EX, version E, *INSIDE SECURE*. -	[R-S01] [CER] [CER] [CER] [CER] [R-S02] [CER] [R-S01] [CER] [R-S01] [CER]
[ST]	Cibles de sécurité de référence: - Security Target AT90SO72, version 1.9, 27/6/2018, *WISEKEY*. Version publique : - Security Target Lite AT90SO72, reference TPG0227F, version F, 31/5/2018, *WISEKEY*.	[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].

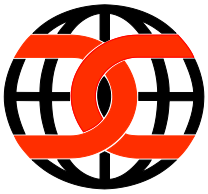
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

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[1], 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 :



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] Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.