



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-2011/65-M01

Microcontrôleur RISC AT90SC20818RCV/AT90SC20812RCV (référence 59U13/révision C1)

Certificat de référence : ANSSI-CC-2011/65

Paris, le 11 juillet 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]



Références

- a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
- b) [ST] « Security Target AT90SC20818RCV/AT90SC20812RCV (Dakala) », référence Dakala_ST_V1.6, version 1.6, 25 novembre 2011, Inside Secure.
- c) [CER] : Rapport de certification ANSSI-CC-2011/65 du 19 décembre 2011 pour les microcontrôleurs RISC AT90SC20818RCV / AT90SC20812RCV, rev. C, ANSSI.
- d) [SIA_C1] Dakala AT90SC20818RCV / AT90SC20812RCV rev C1 Impact Analysis Report, 15 June 2012, V1.0, Inside Secure.
- e) [VAULT_IC_rev] VaultIC Product revision Change, 15 June 2012, V1.1, Inside Secure.
- f) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
- g) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.

Identification du produit maintenu

Les produits maintenus sont les microcontrôleurs sécurisés AT90SC20818RCV / AT90SC20812RCV, référence 59U13 révision C1, développés par INSIDE SECURE.

Les évolutions des produits Inside Secure sont désormais identifiées ainsi ([VAULT_IC_rev]):

- dans le cas d'évolutions estimées majeures par le développeur: la lettre (« *revision* ») est mise à jour (par exemple : de la révision A à la révision B) ;
- dans le cas d'évolutions estimées mineures par le développeur: le chiffre de révision (« *subset revision* ») est mis à jour (par exemple : de la révision A à la révision A1).

La révision dans sa globalité (lettre + chiffre) est identifiée par les marqueurs identifiants les versions de masques qui sont visibles sur le dessus de la puce. Ces marqueurs doivent être conformes à ceux notifiés dans la liste de configuration des réticules.

Le registre SN_1 ne notifie que la lettre de révision. Si le chiffre de révision seul est mis à jour, le registre d'identification de la révision SN_1 du produit n'est pas modifié.

Pour la révision C1 des produits AT90SC20818RCV / AT90SC20812RC, le masque « *metal2* » est identifié par le marqueur « 60 D » comme indiqué dans la liste de configuration des réticules [MO_C1] (alors qu'il était identifié par « 60 C » pour la révision C du produit).

La révision C1 de la TOE est donc parfaitement identifiable et distinguable de la révision C.

Description des évolutions

Une modification mineure a été apportée au « *layout* » du composant pour améliorer le rendement de production de celui-ci : une porte logique MUX non utilisée du bloc d'alimentation électrique a été déconnectée afin de résoudre les coupures potentielles de tension lors de la mise en marche du composant.

Fournitures impactées

Seuls deux documents relatifs à l'identification du produit ont changé.

[CONF]	- Liste des fournitures Dakala <i>Deliverable List, reference Dakala_EDL_VI.6</i> , Inside Secure.
[MO_C1]	- Liste de configuration des réticules <i>Manufacturing Configuration Liste, reference 59U13_DESIGN_C1_MASK_ORDER.htm</i> , Inside Secure.

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.

Le niveau de confiance dans cette nouvelle version C1 du produit est identique à celui de la version certifiée, à la date de certification.

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 ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

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'accord¹, 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 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.

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 signataires¹, 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 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, Singapour, la Suède et la Turquie.