



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-2012/08-M01**

**Microcontrôleur RISC
AT90SC24036RCV, Rev. C**

Certificat de référence : ANSSI-CC-2012/08

Paris, le 10 août 2012

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

Capitaine de vaisseau Dominique RIBAN
[ORIGINAL SIGNE]



Références

- a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
- b) [ST] Cible de Sécurité – Vulcan Security Target, référence : Vulcan_ST_v1.5, version 1.5, Inside Secure.
- c) [ST-Lite] Cible de Sécurité publique – Security Target Lite AT90SC24036RCV, référence TPG0215B, version B, Inside Secure.
- d) [CER] Rapport de certification ANSSI-CC-2012/08 – Microcontrôleur RISC AT90SC24036RCV, Rev A, 2 Mars 2012, ANSSI.
- e) [IAR] Rapport d'analyse d'impact – Vulcan AT90SC24036RCV Security Impact Analysis, référence Vulcan_SIA_RevC, version 1.1, Inside Secure.
- f) [VISITE] Rapport d'évaluation 2011 de l'environnement de développement d'Inside Secure – INSIDE SECURE Development Environment Site visits 2011, référence INSIDE_VISIT_01_v1.0/v1.0, 28 décembre 2011, Serma Technologies.
- g) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
- h) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.

Identification du produit maintenu

Le produit maintenu est le microcontrôleur AT90SC24036RCV, numéro d'identifiant 59U04, révision C, développé par la société Inside Secure.

La version maintenue du produit est identifiable par les éléments suivants situés en EEPROM :

- identification du microcontrôleur AT90SC24036RCV : **0x55** par lecture du registre SN_0 ;
- révision : **0x02** pour la **révision C** par lecture du registre SN_1.

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.

Une modification mineure a été apportée permettant une plus grande fiabilité de l'EEPROM : l'« *active area* » du silicium a été allongé dans le cas de l'EEPROM, ce qui permet de mieux isoler les bits 7 et 0.

Une modification mineure a été apportée au cycle de vie du produit. Un nouveau centre de test remplace celui identifié et audité aux Philippines :

ASE GROUP Kaohsiung
No. 26, Chin 3rd Road, Nantze Export Processing Zone
Kaohsiung, Taïwan
République de Chine

Ce centre de test est inclus dans le rapport d'audit de sites [VISITE] du CESTI Serma Technologies et fait l'objet d'une visite annuelle par ce CESTI pour des besoins identiques.

Inside Secure a souhaité par ailleurs mettre à jour les guides utilisateurs, d'une part pour apporter des clarifications permettant aux utilisateurs d'avoir une meilleure compréhension des produits, d'autre part pour introduire des recommandations sur l'implémentation de nouvelles contre-mesures suite à une nouvelle attaque sur un autre produit de la famille AT90SC 0.13µm.

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[ST]	<p>Cible de Sécurité :</p> <ul style="list-style-type: none"> - Security Target AT90SC24036RCV (Vulcan) Référence : Vulcan_ST_V1.7 Version 1.7 du 1^{er} août 2012 Inside Secure. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite AT90SC24036RCV Référence : TPG0215D Version D du 1^{er} août 2012 Inside Secure.
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none"> - Vulcan Configuration List Référence : Vulcan_EDL_RevC_V1.1, version 1.1 Inside Secure.
[GUIDES]	<p>Guides du produit :</p> <ul style="list-style-type: none"> - Secure Hardware DES/TDES on AT90SC 0.13µm products Référence : TPR0400, version H Inside Secure. - Ad-X2 Technical Datasheet Référence : TPR0452, version D Inside Secure. - Security Recommendations for 0.13µm products -2 Référence : TPR0456, version E Inside Secure.

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.

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 :



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 signataires², 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 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.