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-2012/21-M01

# Microcontrôleur RISC AT90SC28880RCV / AT90SC28848RCV, Rev B

**Certificat de référence : ANSSI-CC-2012/21**

*Paris, le 16 mai 2013*

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

[Original signé]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

## 1. Références

[MAI] Procédure MAI/P/01 Continuité de l'assurance.

[ST] *KIBERIA Security Target*, référence: Kiberia_ST_V1.4, version 1.4, Inside Secure.

[ST Lite] *Security Target Lite AT90SC28880RCV / AT90SC28848RCV*, référence: TPG0219B, version B, Inside Secure.

[CER] Microcontrôleur RISC AT90SC28880RCV / AT90SC28848RCV, Rev A, 12 juin 2012, ANSSI-CC-2012/21.

[IAR] Kiberia AT90SC28880RCV / AT90SC28848RCV Security Impact Analysis, 12 février 2013, référence: Kiberia_SIA_RevB.doc, Inside Secure.

[2012-35] Microcontrôleur AT90SC20818RCFV, Rev. E, 12 juillet 2012, ANSSI-CC-2012/35.

[SUR] *Surveillance Technical Report KIBERIA projects March 2013*, référence : KIBERIA_STR_v1.0, version 1.0, SERMA TECHNOLOGIES.

[SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 Janvier 2010, Management Committee.

[CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.

## 2. Identification du produit maintenu

Les produits maintenus sont les microcontrôleurs sécurisés AT90SC28880RCV et AT90SC28848RCV en révision B développés par Inside Secure.

Les produits AT90SC28880RCV et AT90SC28848RCV en révision A ont été initialement certifiés sous la référence [CER].

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

- microcontrôleurs : AT90SC28880RCV et AT90SC28848RCV, révision B ; la référence interne d'Inside Secure est AT59U12 ; celle-ci, ainsi que la lettre B de la révision sont marquées sur les composants ;
- librairie cryptographique logicielle : « Toolbox 00.03.12.00 ou 00.03.11.08 ou 00.03.10.02 ou 00.03.14.03 » (de la version la plus complète à la moins complète, voir ci-dessous).

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire EEPROM (non effaçable) :

- identification du microcontrôleur AT90SC28880RCV : 0x56 par lecture du registre SN_0 ;
- révision : 0x01 pour la révision B par lecture du registre SN_1 ;
- version de la bibliothèque cryptographique disponible via la commande *SelfTest*. Les valeurs retournées devront être :
    - 0x00031403 pour la version 00.03.14.03 incluant les fonctionnalités suivantes : *SelfTest, AIS31OnlineTest, PrimeGen (Miller Rabin), RSA without CRT* et *RSA with CRT* ;
    - 0x00031002 pour la version 00.03.10.02 incluant les fonctionnalités précédentes ainsi que SHA-1, SHA-224 et SHA 256 ;

- 0x00031108 pour la version 00.03.11.08 incluant les fonctionnalités précédentes ainsi que *ECDSA over Zp* et *EC-DH over Zp* ;
- 0x00031200 pour la version 00.03.12.00 incluant toutes les fonctionnalités précédentes ainsi que *ECDSA over GF ($2^n$), EC-DH over GF ($2^n$)*, SHA-384 et SHA-512.

## 3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence e) mentionne que les modifications suivantes ont été opérées.

Sur le microcontrôleur, une porte logique *MUX* non utilisée du bloc d'alimentation a été déconnectée afin de résoudre les coupures potentielles de tension lors de la mise en marche du composant.
Les changements apportés à la TOE n'affectent pas les performances du produit ; en effet le mécanisme à l'origine de ce comportement servait uniquement en phase de test et sa suppression n'a aucun impact sur la TOE à l'issue de la phase 3.

Les guides suivants ont également été modifiés :

- le document « *Ad-X2 Datasheet* » passe en version D afin de corriger les noms des bits de registre cache dans le schéma 5.1. Cette modification n'a pas d'impact sécuritaire et corrige une incohérence entre le schéma et le reste du chapitre ;
- le document « *Security Recommendations for 0.13µm products – 2* » passe en version E afin de prendre en compte les versions de la bibliothèque cryptographique appartenant à la famille 00.03.2x.xx. Cette modification ne concerne pas les microcontrôleurs qui font l'objet de cette maintenance ;
- le document « *Toolbox 00.03.1x.xx on AT90SCxxxxC* » passe en version D ; au paragraphe 9.1.1 sont ajoutées les références aux deux variantes des guides d'utilisation du RNG ;
- le document « *Efficient use of Ad-X 2* » passe en version C et corrige la référence R1.

Enfin, concernant le cycle de vie des produits, le site de tests suivant est ajouté à la phase de développement de la TOE :

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

Ce site de tests a été audité dans le cadre du projet certifié sous la référence [2012-35].

## 4. Fournitures prises en compte

Suite à la surveillance du produit (référence [SUR]) en mars 2013 les guides ont été mis à jour. Les guides d'utilisation du produit sont désormais constitués, en plus de ceux référencés dans le certificat initial, des documents suivants :

| | |
|---|---|
| [GUIDES SRV] | Addendum aux guides identifiés dans le rapport de certification [CER-2012/21] :<br>- *Secure Hardware DES/TDES on AT90SC 0.13µm products*, référence: TPR0400IX, version I, Inside Secure. |

## 5. Fournitures impactées

Suite à cette maintenance, les fournitures suivantes ont été mises à jour depuis le certificat initial :

| | |
|---|---|
| [CONF] | Liste de configuration :<br>- *Kiberia Configuration List*, référence: Kiberia_EDL_B_V1.0, version 1.0, Inside Secure. |
| [GUIDES] | Guides du produit :<br>- *Ad-X2 Datasheet*, référence: TPR0452DX, version D, Inside Secure.<br>- *Security Recommendations for 0.13µm products – 2*, référence: TPR0456EX, version E, Inside Secure.<br>- *Toolbox 00.03.1x.xx on AT90SCxxxxC*, référence: TPR0454DX, version D, Inside Secure.<br>- *Efficient use of Ad-X2*, référence: TPR0463CX, version C, Inside Secure. |
| [ST] | Cible de Sécurité :<br>- *Security Target AT90SC28880RCV / AT90SC28848RCV (Kiberia)*, référence: Kiberia_ST_V1.5, version 1.5, Inside Secure. |
| [ST Lite] | Cible de Sécurité *Lite* :<br>- Security Target Lite AT90SC28880RCV / AT90SC28848RCV, référence: TPG0219C, version C, Inside Secure. |

## 6. 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, confirmé par la dernière surveillance (référence [SUR]), moyennant la prise en compte des recommandations sécuritaires mises à jour dans les guides [GUIDES_SRV].

## 7. 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.

## 8. 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'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 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.