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-2009/33-M01

Microcontrôleur sécurisé ATMEL AT90SC320288RCT/AT90SC144144CT - Rév. D

Certificat de référence : ANSSI-CC-2009/33

Paris, le 15 mai 2013

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

[ORIGINAL SIGNE]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

1. Références

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

[CER] Microcontrôleur sécurisé ATMEL AT90SC320288RCT / AT90SC144144CT - Rév. D, Rapport de certification ANSSI-CC-2009/33, 15 oct 2009, ANSSI ;

[SUR2] Lettre de surveillance, N°427/ANSSI/SR/CCN, 17 fév 2012, ANSSI ;

[IAR] Longbow Security Impact Analysis, Longbow_SIA_V1.2, 30 Jun 2012, Inside Secure ;
Longbow Security Impact Analysis, Longbow_SIA_V1.3, 10 Déc 2012, Inside Secure ;

[SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, Jan 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

Le produit maintenu est le micro-circuit « AT90SC320288RCT / AT90SC144144CT » (référence AT58888, révision D) développé par la société Inside Secure.

Ce produit a été initialement certifié sous la référence ANSSI-CC-2009/33 (référence [CER]).

3. Description des évolutions liées à la présente maintenance

Les rapports d'analyse d'impact de sécurité (référence [IAR]) mentionnent que les modifications suivantes ont été opérées :

- utilisation d'un nouveau modèle de documents pour les guides ;
- addition du nouveau centre de test audité ASE GROUP Kaohsiung.

4. Fournitures prises en compte

Suite à la surveillance de ce produit en 2012 (référence [SUR2]) un guide a été mis à jour avec de nouvelles recommandations sécuritaires, donnant lieu à la version suivante :

[GUIDES_SRV]	– Securing cryptographic operations on AT90SC products with the Toolbox 3.x, référence TPR0141LX, 27 janvier 2012.

5. Fournitures impactées

Les évolutions du produit, objets de la présente maintenance, donnent lieu aux versions suivantes :

[GUIDES_2011]	– AT90SC Addressing Modes & Instruction Set, 1323DX_28Jan11 ; – Generating Unpredictable Random Numbers on the AT90SC Family Devices, 1573DX_07Mar11 ;

	– Wafer Saw Recommendations, TPG0079B_10Feb11 ; – Secured Hardware DES/TDES on the AT90SC ASL4 Products ,TPR0063KX_22Feb11 ; – Using the Checksum Accelerator on AT90SC ASL4 Products, TPR0065BX_22Feb11 ; – Security recommendations for the AT90SC ASL4 products, TPR0066IX_22Feb11 ; – Using the Supervisor and User Modes on the AT90SC ASL4 products, TPR0095CX_22Feb11 ; – AT90SC320288RCT Technical Datasheet TPR0115B_18Mar11 ; – Ad-X for AT90SC Family TPR0116FX_14Feb11 ; – Toolbox 3.x on AT90SCxxxxC Family with Ad-X TPR0133FX_18Mar11 ; – Efficient use of Ad-X for Implementing Cryptographic Operations TPR0142EX_21Feb11 ; – AT90SC320288RCT 58807 Errata Sheet, TPR0151EX_11Mar11 ; – Generating Random Numbers with a controlled entropy on AT90SC Family Devices, TPR0166EX_04Mar11 ; – Full NVM Erase Errata, TPR0254BX_08Mar11 ; – Flash-EEPROM Configuration of AT90SC ROM Products, TPR0323DX_11Mar11.
[ST_2012]	– Longbow Security Target, Longbow_ST_V1.6, 10 Déc 12, Inside Secure ; – AT90SC320288RCT / AT90SC144144CT Security Target Lite, TPG0132G_10Dec12, Inside Secure.

6. Conclusions

Les évolutions listées au chapitre 3 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 [SUR2]) moyennant la prise en compte des recommandations sécuritaires mises à jour dans le guide [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 la dernière surveillance [SUR2] 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.

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.