



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de maintenance DCSSI-2009/10-M01

Microcontrôleur sécurisé ATMEL AT90SC256144RCFT / AT90SC25672RCFT rev. F

Certificat de référence : DCSSI-2009/10

Paris, le 20 Mai 2009

*Le Directeur central de la sécurité des
systèmes d'information*

Patrick Pailloux
[ORIGINAL SIGNE]



Références

- [MAI] Procédure MAI/P/01 Continuité de l'assurance
- [ST] : cible de sécurité du produit certifié, référence : Torro-5_ST_V2.3, Atmel.
- [ST-lite] : cible de sécurité publique du produit certifié AT90SC256144RCFT/AT90SC256144RCFT, EAL5+ Security Target Lite, référence: TPG0182B, 29 Jan 09, Atmel.
- [CER] : Rapport de certification DCSSI-2009/10 - Microcontrôleur sécurisé Atmel AT90SC256144RCFT / AT90SC25672RCFT rev. E, mai 2009, SGDN/DCSSI.
- [SIA] : Analyse d'impact sur la sécurité, Torro_SIA_V1.5, version 1.5, Atmel.
- [IAR] : Rapport d'analyse d'impact, TORRO5_REP_01_V1.0, version 1.0, ITSEF Serma Technologies.

Identification du produit maintenu

Le produit maintenu est le microcontrôleur sécurisé AT90SC256144RCFT / AT90SC25672RCFT rev. F, suite à la réalisation de modifications du produit AT90SC256144RCFT / AT90SC25672RCFT rev. E, certifié EAL5+ et développé par Atmel, tel qu'identifié au sein du rapport de certification [CER].

Description des évolutions

L'évolution porte sur une modification pour l'amélioration de la tenue à l'ESD (décharge électro-statique).

La protection à l'ESD des circuits est construite sur tous les composants silicium (tels que les transistors, circuits intégrés, etc.) pour faire face à des charges élevées produites lors d'une interaction avec l'homme (HBM) ou un équipement (MM). L'analyse d'impact sur la sécurité [SIA] déclare que cette protection de circuit n'est pas liée aux fonctionnalités du composant, ni à sa sécurité. L'objectif est d'éviter une destruction ou un dommage durant sa manipulation.

Une augmentation de 40 μ A du courant de fuite a été constatée lors de tests HBM ESD à 2kV et 4kV. Des fuites ont été observées dans un inverseur basse tension (transistors LV).

Pour résoudre cette faiblesse, la révision E est remplacée par la révision F pour laquelle le circuit sensible LV est à présent complètement déconnecté et dont la fonction électrique est implémentée avec des transistors haute tension HV.

Les composants en révision F ont été testés en HBM ESD en supportant avec succès des tensions de 1kV, 2kV, 3kV et 4kV.

Fournitures impactées

La mise à jour des fournitures ci-dessous a été réalisée.

[CONF]	Mask list, 58879RF_DESIGN_MASK_ORDER, Rev F, Atmel.
[ST]	Torro-5_ST_V2.3, v2.3, Atmel.

Conclusions

Le rapport [IAR] déclare que l'analyse du CESTI des modules de conception modifiés par Atmel permet d'évaluer qu'aucune modification n'a été faite sur la partie dédiée à la détection de *glitches*. Néanmoins, la taille de quelques transistors PMOS a été changée sur le circuit Vcc et des condensateurs ont été ajoutés. L'architecture initiale est restée identique.

En conclusion, la modification définie dans l'analyse [SIA] d'Atmel sur la protection ESD (i.e. le remplacement des transistors LV sensibles par des transistors HV) de la révision E à F est confirmée par le CESTI [IAR] comme étant mineure et n'affecte pas les fonctions de sécurité de la TOE.

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 [CER].

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

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 1999 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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 CCRA [CCRA].

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 :



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 ».

¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, 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.