Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Maintenance Report DCSSI-2008/18-M01

ATMEL Secure Microcontroller AT90SC256144RCFT / AT90SC25672RCFT rev. F

Reference Certificate : DCSSI-2008/10

Courtesy Translation

Paris, le 5 janvier 2009

[FRENCH ORIGINAL SIGNED with a mistake about the revision in title – corrected so as to insert the right revision F in the title of the current report - Rev. E being the certified product.]

SÉCURITÉ CERTIFICATION

References

- [MAI] Procédure MAI/P/01 Continuité de l'assurance
- [ST] : cible de sécurité du produit certifié, Torro Security Target, référence: Torro_ST_V1.5_29Jan08, version 1.5, Atmel.
- [ST-lite] : cible de sécurité publique du produit certifié, AT90SC256144RCFT Security Target Lite, référence : TPG0167A_06Mar08, Atmel.
- [CER] : Rapport de certification DCSSI-2008/10 - Microcontrôleur sécurisé Atmel AT90SC256144RCFT / AT90SC25672RCFT rev. E, 25 mars 2008, SGDN/DCSSI.
- [SIA] : Security Impact Analysis, Torro_SIA_V1.5, version 1.5, Atmel.
- [IAR] : Impact analysis report, TORRO5_REP_01_V1.0, version 1.0, ITSEF Serma Technologies.

Identification of the maintained product

The maintained product is the secure microcontroller AT90SC256144RCFT / AT90SC25672RCFT rev. F, following modifications on the certified product AT90SC256144RCFT / AT90SC25672RCFT rev. E, developped by Atmel, as identified within the certification report [CER].

Description of changes

Evolution concerns a design modification to improve ESD (Electro-Static Discharge) protection.

ESD protection circuit is built on all silicon devices (such as Transistors, Integrated circuits, …) to protect against high voltage transients brought either by human (HBM) or by equipment (MM). The security impact analysis [SIA] claims that this protection circuit is therefore not related to device functionality nor to security. Its aim is to avoid the device destruction or damage during handling.

Extra 40µA of powerdown Idd current was detected after 2kV & 4kV HBM ESD and extra leakage was observed in a Low Voltage (LV) inverter.

To resolve this weakness, the revision E is updated by revision F so as the sensitive LV circuitry is completely disconnected from the active current paths and its electrical function is now implemented with spare High Voltage (HV) transistors.

Revision F devices have now been tested and successfully pass 1KV, 2KV, 3kV & 4kV HBM ESD.

Impacted deliverables

Updated deliverables impacted are the following :

[CONF]	Mask list, 58879RF_DESIGN_MASK_ORDER, Rev F, Atmel.
[ST]	Torro_ST Security Target V1.6_09Dec08, v1.6, Atmel.

Conclusions

The examination reported in [IAR] by the ITSEF of the modified modules design allows assessing that no modification was done on the Glitch detection part. Only the size of some PMOS transistors has been changed (increasing the W/L size) on the Vcc circuitry and with addition of some grounded capacitors. The initial design architecture is kept identical.

In conclusion, the manufacturing change defined in [SIA] by Atmel on ESD protection (i.e. replacement of LV transistors by HV transistors) from revision E to F is confirmed by ITSEF in its [IAR] as being minor and does not affect the security functions.

The above listed changes are considered as having a **minor** impact.
The assurance level of this new product revision is thus identical to the certified revision, at the date of the certification [CER].

Warning

The resistance level of a certified product is declining as time goes by. The vulnerability analysis of this product revision versus the new attacks that would have appeared since the certificate release has not been conducted in the frame of this current maintenance. Only a re-evaluation or a “surveillance” of the new product revision would allow maintaining the assurance level in a timely and efficient manner.

Recognition of the certificate

European recognition (SOG-IS)

The reference certificate was issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

International common criteria recognition (CCRA)

The reference certificate was released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

This maintenance report is released in accordance with the document: « Assurance Continuity: CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.