Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0421-2008-MA-02

Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00

from

Atmel Corporation

Common Criteria Recognition
Arrangement
for components up to EAL4

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0421-2008.

The changes to the certified product are at the level of the hardware implementation, the improvement of the temperature behaviour and editorial changes in the guidance documentation, changes that have no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0421-2008 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0421-2008.

Bonn, 6 April 2009

Common Criteria

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], the Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00, Atmel Corporation, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The hardware implementation and the temperature behaviour of the Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 was improved to attain an ESD Yield Enhancement and the guidance documentation was improved. The change is not significant from the standpoint of security, however Configuration Management procedures required a change in the revision number from D to G.

Conclusion

The changes to the TOE are at the level the hardware implementation, the improvement of the temperature behaviour and editorial changes in the guidance documentation, changes that have no effect on assurance. Examination of the evidence indicates that the changes performed are limited to an analogue circuitry in a security irrelevant part of the TOE, the trim values of the temperature sensors and editorial changes in the guidance document “Securing Toolbox Operations using version 00.03.10.xx on ASL5 products”, Literature Number: TPR0260IX, 25 January 09 [7]. The Security Target [5] and the Security Target lite [6] were editorially updated. Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG Section 4, Para. 3, Clause 2). In addition to the baseline certificate BSI notes, that cryptographic functions with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore, for these functions it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

This report is an addendum to the Certification Report [3].

References

[1] Common Criteria document CCIMB-2004-02-009 “Assuarance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Roper (AT90SC28872RCU / AT90SC28848RCU) Impact Analysis Report, Version 1.4, 06 March 2009 (confidential document)

[3] Certification Report BSI-DSZ-CC-0421-2008 for Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00, Bundesamt für Sicherheit in der Informationstechnik, 04 December 2008

[4] Security Target BSI-DSZ-0421-2008, Version 2.2, 14.04.2008, Roper Security Target, Atmel Corporation (confidential document)

[5] Security Target BSI-DSZ-0421-2008, Version 2.3, 05.12.2008, Roper Security Target, Atmel Corporation (confidential document)

[6] Security Target BSI-DSZ-0421-2008, Version TPG0139E, 06.03.2009, AT90SC28872RCU / AT90SC28848RCU Security Target Lite, Atmel Corporation (sanitised public document)

[7] Securing Toolbox Operations using version 00.03.10.xx on ASL5 products, Literature Number: TPR0260IX, 25 January 09