



Bundesamt  
für Sicherheit in der  
Informationstechnik

## Assurance Continuity Maintenance Report

**BSI-DSZ-CC-0548-2008-MA-01**

**S3CC924/S3CC928 16-bit RISC Microcontroller  
for Smart Card, Revision 3**

from

**Samsung Electronics Co., Ltd.**



Common Criteria 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-0548-2008.

The change to the certified product is at the level of the improvement of the high voltage generation and the pad layout, a change that has no effect on assurance.

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-0548-2008 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-0548-2008.

Bonn, 19 May 2009



## 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 Lite [4] and the Evaluation Technical Report as outlined in [6].

The vendor for the S3CC924/S3CC928 16-bit RISC Microcontroller for Smart Card, Revision 3, Samsung Electronics Co., Ltd., 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 S3CC924/S3CC928 16-bit RISC Microcontroller for Smart Card, Revision 3 was changed due to the improvement of the high voltage generation and the pad layout. The changes are not significant from the standpoint of security, however Configuration Management procedures required a change in the version number from S3CC924/28, Revision 1 to S3CC924/28, Revision 3. The device type for S3CC924/28, Revision 3 is identified by IC version 03<sub>H</sub>. This information is stored in the EEPROM and can be read out by the user of the card via the normal EEPROM read command.

## Conclusion

The changes to the TOE are at the level of the improvement of the high voltage generation and the pad layout, a change that has no effect on assurance. Examination of the evidence indicates that the changes performed are limited to the documentations [2] and [4] of the TOE. The Security Target Lite [4] was 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](http://www.bsi.bund.de)). This report is an addendum to the Certification Report [3]. This report is an addendum to the Certification Report [3].

## References

- [1] Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004
- [2] Impact Analysis Report, S3CC928/24 Revision Comparison, Version 1.3 issued on 16th April 2009, Samsung Electronics (confidential document)
- [3] BSI-DSZ-CC-0548-2008 for S3CC924/S3CC928 16-bit RISC Microcontroller for Smart Card, Revision 1 from Samsung Electronics Co., Ltd. Bundesamt für Sicherheit in der Informationstechnik, 11. December 2008.
- [4] Security Target Lite of S3CC924/S3CC928 16-bit RISC Microcontroller For Smart Cards Revision 3, Version 1.2, 30th March 2009, Samsung Electronics
- [5] Project <CHOCTAW> Configuration Management Documentation (Class ACM\_AUT/CAP/SCP), Version 1.3 issued on 26th March 2009, Samsung Electronics (confidential document)
- [6] EVALUATION TECHNICAL REPORT-SUMMARY (ETR SUMMARY), 8104491414 / BSI-DSZ-CC-0548, S3CC924/928, Version 2, 2008-11-28, TÜViT (confidential document)