Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0624-2010-MA-03

Samsung S3CC9LA 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA 3.7S and ECC 2.4S Libraries including specific IC Dedicated Software

from

Samsung Electronics Co., Ltd.

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-0624-2010.

The change to the certified product is at the level of a different configuration setting by blocking of the EEPROM size from 72 kByte to 36 kByte, a change that has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0624-2010 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-0624-2010.

Bonn, 30 June 2010

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

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 [5].

The vendor for the Samsung S3CC9LA 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA 3.7S and ECC 2.4S Libraries including specific IC Dedicated Software, Samsung Electronics, 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 Samsung S3CC9LA 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA 3.7S and ECC 2.4S Libraries including specific IC Dedicated Software was changed due to a reduction of the EEPROM size from 72 kByte to 36 kByte. The change is not significant from the standpoint of security, however Configuration Management procedures required a change in the version number from S3CC9LC, Revision 9 to S3CC9LA, Revision 2. The device type for S3CC9LA, Revision 2 is identified by 150AH. 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 change to the TOE is at the level of different configuration setting by blocking of the EEPROM size from 72 kByte to 36 kByte, a change that has no effect on assurance. Examination of the evidence indicates that the changes performed are limited to the Configuration Management Documentation [7] of the TOE. Security Target Lite [6] 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 obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [8].

According to the scheme rules, evaluation results outlined in the document ETR for composition as listed below can usually be used for composite evaluations building on top, as long as the ETR for composition document is not older than one year and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.
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 9, Para. 4, Clause 2).
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] Security Impact Analysis Report, S3CC9LC and S3CC9LA Comparison, version 1.0, issued on 28th May 2010, Samsung Electronics (confidential document)

[3] Certification Report BSI-DSZ-CC-0624-2010 for Samsung S3CC9LC 16-bit RISC Microcontroller for Smart Card, Revision 9 with optional secure RSA 3.7S and ECC 2.4S Libraries including specific IC Dedicated Software, Samsung Electronics Co., Ltd. Bundesamt für Sicherheit in der Informationstechnik, 29. January 2010.

[4] Security Target of Samsung S3CC9LA 16-bit Secure RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, Version 2.2, 31st May 2010 (confidential document).

[5] Evaluation Technical Report Summary (ETR SUMMARY), 8105621102 / BSI-DSZ- CC-0624, S3CC9LC, Version 2, 2010-01-28, TÜViT (confidential document)

[6] Security Target Lite of Samsung S3CC9LA 16-bit Secure RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, Version 1.5, 31st May 2010

[7] Configuration Management Documentation (Class ACM_AUT/CAP/SCP), <CHEYENNEII ECC S3CC9LA>, version 2.0, issued on 31th May 2010, Samsung Electronics (confidential document)

[8] ETR for Composite Evaluation (ETR-COMP), 8104953923 / BSI-DSZ-CC-0624, S3CC9LC, Version 2, 2010-01-28, TÜViT (confidential document)