Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0719-2011-MA-01

Samsung S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 1 with optional Secure RSA/ECC Library Version 1.0 including specific IC Dedicated Software

from

Samsung Electronics

Common Criteria Recognition Arrangement
for components up to EAL4

Common Criteria

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 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-0719-2011 updated by a re-assessment on 26 February 2013.

The change to the certified product is at the level of power selection improvement in the Dual Interface Priority Mode (DIPM). The change has 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.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0719-2011 dated 19 May 2011 and updated by a re-assessment on 26 February 2013 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0719-2011.

Bonn, 10 September 2013

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the Samsung S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 1 with optional Secure RSA/ECC Library Version 1.0 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 S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 1 with optional Secure RSA/ECC Library Version 1.0 including specific IC Dedicated Software was changed due to improvement of power selection in the Dual Interface Priority Mode (DIPM). There are no changes in the timing and internal voltages. It is just function improvement by adjustment of capacitance and resistance in contactless module. The change is not significant from the standpoint of security, however Configuration Management procedures required a change in the product identifier. Therefore, the TOE version number changed from revision 0 to revision 1.

Conclusion

The change to the TOE is at the level of power selection improvement in the Dual Interface Priority Mode (DIPM).The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The Security Target was editorially updated [4].

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.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0719-2011 dated dated 19 May 2011 and updated by a re-assessment on 26 February 2013 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [7] and [8] are the current versions of the ETR for composite evaluation and the ETR itself.

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 [7].

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months 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[1] Section 9, Para. 4, Clause 2).

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

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report, S3CT9KA and S3CT9K7 and S3CT9K3 Revision Comparison (Revision 0 vs Revision 1), Version 1.3, Issued on 13 August 2013 (confidential document)

[3] Certification Report BSI-DSZ-CC-0719-2011 for Samsung S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 0 with optional Secure RSA/ECC Library Version 1.0 including specific IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 19 May 2011

[4] Security Target Lite of S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Cards – Project Crow II, Version 2.0, 29 July 2013, Samsung Electronics (sanitized public document)

[5] Life Cycle Definition (Class ALC_CMC.4/CMS.5) – Project Crow II, Version 1.1, 2013-07-25, Samsung Electronics (confidential document)

[6] Security Target of S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Cards with optional Secure RSA and ECC Library – Project Crow II, Version 2.0, 2031-07-29, Samsung Electronics (confidential document)

[7] ETR for Composite Evaluation (ETR-COMP), BSI-DSZ-CC-0719, S3CT9KA / S3CT9K7 / S3CT9K3, Version 2, 22 January 2013, TÜViT (confidential document)

[8] Evaluation Technical Report Summary (ETR SUMMARY), BSI-DSZ-CC-0719, S3CT9KA / S3CT9K7 / S3CT9K3, Version 2, 22 January 2013, TÜViT (confidential document)