



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0801-2012-MA-01

**Samsung S3CT9P3 16-Bit RISC Microcontroller for
Smart Cards, Revision 0 with optional Secure RSA
and ECC Library (Version 2.0) including specific IC
Dedicated Software**

from

Samsung Electronics



SOGIS
Recognition Agreement

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-0801-2012 updated by a re-assessment on 29 August 2016.

The certified product itself did not change. The changes are related to / an update of the user guidance.

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-0801-2012 dated 13 August 2012 updated by a re-assessment on 29 August 2016 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-0801-2012.



Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 19 January 2017

The Federal Office for Information Security



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 S3CT9P3 16-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure RSA and ECC Library (Version 2.0) 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 certified product itself did not change. The changes are related to an update of the user guidance [5].

Conclusion

The change to the TOE is at the level of guidance documentation. The change has no effect on assurance. The Security Target [4] is still valid for the TOE.

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-0801-2012 dated 13 August 2012 updated by a re-assessment on 29 August 2016 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [6] and [7] 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 [6].

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.

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

References

- [1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012
- [2] Impact Analysis Report S3CT9P3, Version 2.0, 2016-09-02, Samsung Electronics (confidential document)
- [3] Certification Report BSI-DSZ-CC-0801-2012 for Samsung S3CT9P3 16-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure RSA and ECC Library (Version 2.0) including specific IC Dedicated Software, 2012-08-13 Bundesamt für Sicherheit in der Informationstechnik
- [4] Security Target Lite of S3CT9P3 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software – Project Crow V, Version 1.0, 2012-03-23, Samsung Electronics
- [5] Security Application Note, S3CT9KA_K7_K3_PC_PA_P7_P3_A C_AA_A7, Version 1.6, 2016-05-03, Samsung Electronics (confidential document)
- [6] ETR for composite evaluation according to AIS 36 for the Product S3CT9P3 Revision 0, Version 6, 2016-06-03, TÜV Informationstechnik GmbH (confidential document)
- [7] Evaluation Technical Report Summary (ETR Summary), BSI-DSZ-CC-0801-2012, S3CT9P3 Revision 0, Version 6, 2016-06-03, TÜV Informationstechnik GmbH (confidential document)