Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0910-2016-MA-01

S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) 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 developer's 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-0910-2016.

The certified product itself did not change. The changes are related to changes in the sites used to build the TOE. The life cycle security has continuously been assured by newer audits and site certificates for each site used.

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-0910-2016 dated 30 November 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-0910-2016.

Common Criteria
Recognition Arrangement
recognition for components

up to EAL 2

Bonn, 20 December 2018

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) 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 life cycle security aspects. The ALC re-evaluation was performed by the TÜV Informationstechnik GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [5] as well as an editorial update to the ETR for Composition [6]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

The sites and related certificates listed in Annex B of Certification Report BSI-DSZ-CC-0910-2016 are replaced by the following development and production sites:

Name of site / Company name	Address	Type of site
Samsung Giheung	Samsung Electronics. Co., Ltd. San24, Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggido, 449- 711, Korea	Wafer fab, Warehouse / Delivery
Samsung Hwasung	Samsung Electronics. Co., Ltd. San #16, Banwol-Ri, Hwasung-Eup, Gyeonggi-Do, 445-701, Korea DSR Building, B-Tower, 17-floor, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, 445-330, Korea	Development, IT (Server room), Mask data preparation
Samsung Onyang	Samsung Electronics. Co., Ltd. San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Chungcheongnam-Do, 449-711, Korea	Warehouse / Delivery, Grinding, Sawing, Assembly, Module testing

Name of site / Company name	Address	Type of site
Toppan Icheon	Toppan Photomasks Korea Ltd. 345-1, Sooha-Ri ShinDoon-Myon, 467-840 Icheon, Korea	Mask house
PKL Cheonan	PKL Co., Ltd. Plant, 493-3 Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, 330-300, Korea	Mask house
Hanamicron Asan	HANAMICRON Co., Ltd. #95-1, Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, 449-711, Korea	Grinding, Sawing, Assembly and Module testing
Inesa Shanghai	Inesa Co., Ltd. No. 818 Jin Yu Road, Jin Qiao Export Processing Zone Pudong, Shanghai, China	Grinding, Sawing, COB Assembly, Warehouse/Delivery
Eternal Shanghai	ETERNAL Co., Ltd. No.1755, Hong Mei South Road, Shanghai, China	Sawing, Assembly, Warehouse/Delivery
Tesna Pyeungtaek	TESNA Co., Ltd. No. 450-2 Mogok-Dong, Pyeungtaek-City, Gyeonggi, Korea	Wafer testing, Initialization and Pre-personalization
Paju Plant (ASE)	ASE Korea Co., Ltd., Sanupdanjigil 76, Paju, Korea	Grinding, Sawing, Assembly
SFA Semicon	SFA Semicon Co. Ltd. Bumping Factory, 30, 2gongdan 7-gil, Seobuk-gu, Cheonan-si, Chungcheongnam-do, Korea 31075	IC Bumping

Table 1: Relevant development/production sites

Conclusion

The maintained change is at the level of an update of life cycle security aspects covered by newer audits and site certificates for each site of the life cycle considered herein. The change has no effect on product 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.

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-0910-2016 dated 30 November 2016 is of relevance and has to be considered when using the product.

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[1] 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[2] Section 9, Para. 4, Clause 2).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

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

[1] In this case the eighteen month time frame is related to the date of the initial version [5] of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.

[2] 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] Kiowa IAR (Impact Analysis Report), Version 2.1, 30 March 2018, Samsung Electronics (confidential document)

[3] Certification Report BSI-DSZ-CC-0910-2016 for S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including specific IC Dedicated Software, 30 November 2016 Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target BSI-DSZ-CC-0910-2016 Lite, Project Kiowa Security Target of Samsung S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH 32-bit RISC Microcontroller for Smart Card with optional Secure ECC Library including specific IC Dedicated Software, Version 1.8, 07 October 2016, Samsung Electronics (sanitised public document)

[5] Evaluation Technical Report, Version 8, 05 December 2018, Evaluation Ttechnical Report Summary (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[6] Evaluation Technical for Composite Evaluation (ETR COMP) for the S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH Revision 0, version 8, 05 December 2018, TÜV Informationstechnik GmbH