Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0910-2016-RA-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 certified under the certification procedure BSI-DSZ-CC-0910-2016 amended by Assurance Maintenance Procedures [5] has undergone a re-assessment of the vulnerability analysis according to the current state of the art attack methods and based on the Security Target [6].

This reassessment confirms resistance of the product against attacks on the level of AVA_VAN.5 as stated in the product certificate.

More details are outlined on the following pages of this report.

This report is an addendum to the Certification Report BSI-DSZ-CC-0910-2016.

Common Criteria
Recognition
Arrangement
for components up to
EAL 2

Bonn, 20 December 2018

The Federal Office for Information Security

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

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 reassessment was performed based on CC [1], CEM [2] and relevant AIS [4] and according to the BSI Certification Procedures [3] by the ITSecurity Evaluation Facility (ITSEF) TÜV Informationstechnik GmbH, approved by BSI.

The following guidance specific for the technology have been applied as a refinement of CC and CEM:

- The Application of CC to Integrated Circuits [4, AIS 25]
- Evaluation Methodology for HW Integrated Circuits [4, AIS 26] including
  Application of Attack Potential to Smartcards and
  Attack Methods for Smartcards and Similar Devices.
- Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren [4, AIS31],
- Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (Ccv3.1) [4, AIS34] and
- Reuse of evaluation results [4, AIS38].

The results are documented in an updated version of the ETR [7].

To support composite evaluations according to AIS 36 the document ETR for composite evaluation was updated and has been approved [8]. It replaces the previous versions of this document. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Securtiy Target [6].

The obligations and recommendations as outlined in the certification and maintenance reports [5] are still valid and have to be considered.

The obligations and recommendations as outlined in the guidance documentation [9] have to be considered by the user of the product.

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation [8] as listed above are intended to be used for composite evaluations building on top of this evaluation procedure, as long as the ETR for composition document is not older than eighteen months and an attacks assumed to be feasible within the scope of these evaluations have not been performed successfully.

In case the composite evaluation process or the risk assessment process related to the usage of the product confirms that critical attack scenarios are of minor relevance in a specific application context, critical ratings might be overruled. The lifetime of the product and e.g. the risks on a long term product usage have to be considered.

Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[1] https://www.bsi.bund.de/AIS

[5] 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
amended by the following Assurance Maintenance Report:
Assurance Continuity Maintenance Report BSI-DSZ-CC-0910-2016-MA-01

[6] 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)

1 Specifically

- AIS 14, Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 19, Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document Application of Attack Potential to Smartcards, Joint Interpretation Library, Version 2.9, January 2013 and Attack Methods for Smartcards and Similar Devices, Joint Interpretation Library, Version 2.2, January 2013.
- AIS31, Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ and EAL 6
- AIS 38, Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28, Bundesamt für Sicherheit in der Informationstechnik.

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

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