Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0801-2012-RA-03

Samsung S3CT9P3 16-bit SecuCalm RISC Microcontroller for Smart Card with optional Secure RSA and ECC library 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-0801-2012 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 [9].

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-0801-2012.

Common Criteria
Recognition
Arrangement
for components up to
EAL2

Bonn, 9 May 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 [8] was updated and has been approved. 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.

Within the scope of this reassessment, the following guidance documentation related to the product has been updated and replaced the former one:

Guidance Documentation	**Previous version**	**New version**
Security Application Note, S3CT9KA_K7_K3_PC_PA_P7_P3_A C_AA_A7	1.6, 2016-05-03	2.1, 2017-12-08

Tabelle 1: List of changed documents

As a consequence, the Security Target [6] was updated editorially as well, leading to version [9], thereby reflecting the above stated guidance documentation version number changes.

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Securtiy Target [9].

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 [10] 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-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, amended by the following Assurance Maintenance Report:

1 specifically
- AIS 14, Version 7, Anforderungen an den Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anwendungshinweise und Interpretationen zum Schema (AIS)
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluationen
- AIS 38, Version 2, Reuse of evaluation results

- Assurance Continuity Maintenance Report BSI-DSZ-CC-0801-2012-MA-01, 2017-01-19, Bundesamt für Sicherheit in der Informationstechnik

[6] 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

[7] Evaluation Technical Report Summary (ETR Summary), BSI-DSZ-CC-0801-2012, S3CT9P3 Revision 0, Version 9, 2016-06-03, TÜV Informationstechnik GmbH (confidential document)

[8] Evaluation Technical Report for Composite Evaluation (ETR COMP) for the S3CT9P3 Revision 0, version 9, 2018-02-23, TÜV Informationstechnik GmbH. (confidential document)

[9] Security Target Lite of Samsung S3CT9P3 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software – Project Crow V, Version 1.2, 2018-02-23, Samsung Electronics

[10] TORNADO-2Mx2 RSA/ECC Library API Manual, Version 2.08, 2014-02-04, Samsung Electronics

[11] Security Application Note, S3CT9KA_K7_K3_PC_PA_P7_P3_A C_AA_A7, Version 2.1, 2017-12-08, Samsung Electronics