Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0976-2015-RA-01

STARCOS 3.6 COSGKV C1

from

Giesecke+Devrient Mobile Security GmbH

SOGIS
Recognition Agreement

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-0976-2015 [5] has undergone a reassessment 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-0976-2015.

Common Criteria

Common Criteria Recognition Arrangement recognition for components up to EAL 2 only

Bonn, 19 September 2017

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 IT Security Evaluation Facility (ITSEF) SRC Security Research & Consulting GmbH, approved by BSI.

The following guidance specific for the technology have been applied as a refinement of CC and CEM (see [4]):

- Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents and the document ETR for composite evaluation of the underlying platform have been applied in the TOE reassessment.
- Guidance for Smartcard Evaluation.
- Application of Attack Potential to Smartcards (see AIS 26).
- Functionality classes and evaluation methodology of physical and deterministic random number generators.

For smart card specific evaluation methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used.

For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

The results of the reassessment are documented in an updated version of the ETR [8].

Within the scope of this reassessment the guidance documentation related to the product has been updated (see [9], [10], [11], [12], [13], [14] and [15]) replacing the guidance documentation (references [11], [12], [13], [14], [15], [16] and [17] respectively as listed in [5]).

In order to address the developer’s reorganisation including a change of the developer’s business name and to cover the updated guidance documentation the Security Target [6] and [7] was adapted accordingly.

In addition, the production site ‘Giesecke & Devrient GmbH Dienstleistungscenter (DLC)’ (see [5], Annex B) is no longer relevant for the TOE life-cycle model.

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Security Target [6] and [7].

The obligations and recommendations as outlined in the certification report [5] are still valid and have to be considered (by using the updated guidance documentation [9], [10], [11], [12], [13], [14] and [15]).

The obligations and recommendations as outlined in the guidance documentation [9], [10], [11], [12], [13], [14] and [15] have to be considered by the user of the product. In particular, the following aspects need to be taken into account when using the TOE:

- [10], chapters 5.1.1 and 5.1.2 including subchapters.

- [11], chapters 4.1, 4.2.1 and 4.2.2.
- [12], chapters 5.8.1 and 5.8.2.

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, Revision 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-0976-2015 for STARCOS 3.6 COSGKV C1, Bundesamt für Sicherheit in der Informationstechnik, 29 December 2015

[6] Security Target BSI-DSZ-CC-0976-2015-RA-01, Security Target STARCOS 3.6 COSGKV C1, Version 1.1.3, 11 September 2017, Giesecke+Devrient Mobile Security GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-0976-2015-RA-01, Security Target Lite STARCOS 3.6 COSGKV C1, Version 1.1.3, 11 September 2017, Giesecke+Devrient Mobile Security GmbH (sanitised public document)

[1] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- 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 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[8] ETR BSI-DSZ-CC-0976-2015-RA-01, Evaluation Technical Report (ETR) – Summary for STARCOS 3.6 COSGKV C1, Version 1.8, 14 September 2017, SRC Security Research & Consulting GmbH (confidential document)

[9] Guidance Documentation STARCOS 3.6 – Main Document, Version 1.8, 17 August 2017, Giesecke+Devrient Mobile Security GmbH

[10] Guidance Documentation for the Usage Phase STARCOS 3.6 COS, Version 2.10, 11 September 2017, Giesecke+Devrient Mobile Security GmbH

[11] Guidance Documentation for the Initialization Phase STARCOS 3.6 COS, Version 2.18, 11 September 2017, Giesecke+Devrient Mobile Security GmbH

[12] Guidance Documentation for the Personalisation Phase STARCOS 3.6 COS, Version 2.3, 11 September 2017, Giesecke+Devrient Mobile Security GmbH

[13] STARCOS 3.6 Functional Specification - Part 1: Interface Specification,Version 1.20, 17 August 2017, Giesecke+Devrient Mobile Security GmbH

[14] STARCOS 3.6 Internal Design Specification, Version 1.4, 17 August 2017, Giesecke+Devrient Mobile Security GmbH

[15] STARCOS 3.6 COS C1/2 Guidance Documentation for the Wrapper, Version 1.5, 17 August 2017, Giesecke+Devrient Mobile Security GmbH

[16] STARCOS 3.6 COSGKV C1 Configuration List, Version 1.5, 11 September 2017, Giesecke+Devrient Mobile Security GmbH (confidential)