



## Assurance Continuity Maintenance Report

**BSI-DSZ-CC-0952-V2-2016-MA-01**

**STARCOS 3.5 ID GCC C3**

from

**Giesecke+Devrient Mobile Security GmbH**



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-0952-V2-2016.

The certified product itself did not change. The changes are related to an update of life cycle security aspects.

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-0952-V2-2016 dated 16 December 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-0952-V2-2016.



Common Criteria  
Recognition Arrangement  
recognition for components  
up to EAL 4

Bonn, 23 February 2018

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 STARCOS 3.5 ID GCC C3, Giesecke+Devrient Mobile Security GmbH, 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 ITSEF SRC Security Research & Consulting GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [6]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

The changes of the live cycle following sites are related to:

- Relocation of Development Site  
Giesecke+Devrient Mobile Security Development Center Germany  
Prinzregentenstrasse 159  
81677 München  
Germany  
Site Security Certificate: BSI-DSZ-CC-S-0083-2017 [8]
- Additional Storage Facility  
Giesecke & Devrient Secure Data Management GmbH  
Austraße 101b  
96465 Neustadt bei Coburg  
Germany  
Site Security Certificate: BSI-DSZ-CC-S-0058-2016 [7]

## Conclusion

The maintained change is at the level of life cycle security aspects. 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-0952-V2-2016 dated 16 December 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.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG<sup>1</sup> 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 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] Impact Analysis Report STARCOS 3.5 ID GCC C3, Version 1.4, 14.02.2018, Giesecke+Devrient Mobile Security GmbH (confidential document)
- [3] Certification Report BSI-DSZ-CC-0952-V2-2016 for STARCOS 3.5 ID GCC C3 from Giesecke & Devrient GmbH, Bundesamt für Sicherheit in der Informationstechnik, 16 December 2016
- [4] Security Target Lite BSI-DSZ-CC-0952-V2-2016, Version 1.10, 06.12.2016, STARCOS 3.5 ID GCC C3 Security Target lite, Giesecke & Devrient GmbH (sanitised public document)
- [5] Configuration List STARCOS 3.5 ID GCC C3, Version 1.7 / 14.02.2018, file name: ConfigList\_C3, Giesecke+Devrient Mobile Security GmbH (confidential document)
- [6] Evaluation Technical Report (ETR) BSI-DSZ-CC-0952-V2-2016-MA-01 for STARCOS 3.5 ID GCC C3, Version 1.5, 14.02.2018, SRC Security Research & Consulting GmbH (confidential document)
- [7] Site certificate BSI-DSZ-CC-S-0058-2016 for Giesecke & Devrient Secure Data Management GmbH, Austraße 101b, 96465 Neustadt bei Coburg of Giesecke & Devrient GmbH, 3 March 2016, Bundesamt für Sicherheit in der Informationstechnik
- [8] Site certificate BSI-DSZ-CC-S-0083-2017 for Giesecke+Devrient Mobile Security Development Center Germany of Giesecke+Devrient Mobile Security GmbH, 4 October 2017, Bundesamt für Sicherheit in der Informationstechnik