



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0904-V2-2021-MA-01

TCOS FlexCert Version 2.0 Release 2/SLC52

from

Deutsche Telekom Security GmbH



SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] 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-0904-V2-2021.

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

Considering 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-0904-V2-2021 dated 24 June 2021 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-0904-V2-2021.



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

Bonn, 29 July 2025

The Federal Office for Information Security



Assessment

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [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 product TCOS FlexCert Version 2.0 Release 2/SLC52, Deutsche Telekom Security GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [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 change is related to an update of life cycle security aspects, more precisely concerning the relocation of the development and production site of the developer to a new site. The partial 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 development and production site of the developer moved from

- Deutsche Telekom Security GmbH, Untere Industriestraße 20, 57250 Netphen
- to the new site
- Deutsche Telekom Security GmbH, Koblenzer Straße 87-93, 57072 Siegen.

Conclusion

The maintained change is at the level of life cycle security aspects addressing the relocation of the development and production site of the developer to a new site. The change has no effect on product assurance.

Considering the nature of the change performed in the present partial ALC re-evaluation 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 site audit performed in the framework of this partial ALC re-evaluation is valid till 4 December 2027.

The resistance to attacks has not been re-assessed in the course of this maintenance process. The update of the vulnerability assessment of the underlying hardware as provided in BSI-DSZ-CC-1079-V5-2024 was not considered in this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0904-V2-2021 dated 24 June 2021 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 BSIG¹ 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 3.1, 29 February 2024
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, Version 1.2, March 2024
- [2] Impact Analysis Report, TCOS FlexCert Version 2.0 Release 2/SLC52, Version 0.1, 25 September 2024, Deutsche Telekom Security GmbH (confidential document)
- [3] Certification Report BSI-DSZ-CC-0904-V2-2021 for TCOS FlexCert Version 2.0 Release 2/SLC52 from Deutsche Telekom Security GmbH, Version 1.0, 24 June 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [4] Security Target BSI-DSZ-CC-0904-V2-2021, Specification of the Security Target TCOS FlexCert Version 2.0 Release 2/SLC52, Version 2.0.2, 25 May 2021, Deutsche Telekom Security GmbH
- [5] Configuration List BSI-DSZ-CC-0904-V2-2021-MA-01, Konfigurationsliste von TCOS FlexCert Version 2.0 Release 2/SLC52, Version 0.93, 25 June 2025, Deutsche Telekom Security GmbH (confidential document)
- [6] ETR BSI-DSZ-CC-0904-V2-2021-MA-01, Evaluation Technical Report (ETR) – Summary for TCOS FlexCert Version 2.0 Release 2/SLC52, Version 1.6, 23 July 2025, SRC Security Research & Consulting GmbH (confidential document)

Note: End of report