Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0904-2015-MA-02

TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P

from

T-Systems International 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-0904-2015 and amended by BSI-DSZ-CC-0904-2015-MA-01.

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-0904-2015 dated 3 July 2015 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-0904-2015.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 13 May 2020

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 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 TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, T-Systems International 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 and covers only the replacement of a specific production site.

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) [7]. The document ETR Addendum for gSMC-K Composite Evaluation [8] covered by BSI-DSZ-CC-0904-2015-MA-01 [4] has expired and was not updated in the course of this evaluation. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [5].

The production site exceet Card Group AG, Senefelderstraße 10, D-33100 Paderborn (Card Embedding) listed in Annex B of Certification Report BSI-DSZ-CC-0904-2015 [3] is replaced by the following production site:

exceet Card Group AG, Edisonstraße 3, D-85716 Unterschleißheim (Card Embedding)

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-0904-2015 dated 3 July 2015 is of relevance and has to be considered when using the product. As a result of this maintenance process with ALC re-evaluation an updated ETR [7] is provided. The document ETR Addendum for gSMC-K Composite Evaluation [8] covered by BSI-DSZ-CC-0904-2015-MA-01 [4] has expired and was not updated.

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.

Some security measures are partly implemented in the TOE and require additional configuration or control or measures to be implemented by the applications running on the TOE.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the applications running on the TOE on how to securely use the TOE and which measures have to be implemented in the applications in order to fulfil the security requirements of the Security Target of the TOE.

The document ETR Addendum for gSMC-K Composite Evaluation [8] is intended to be used for a composite evaluation of a Konnektor in the German health care system that integrates a gSMC-K card product from T-Systems International GmbH running on the TOE according to the certification procedure BSI-K-TR-0226-2015 [9]. Please refer to BSI-DSZ-CC-0904-2015-MA-01 [4] for usage of the document ETR Addendum for gSMC-K Composite Evaluation [8].

According to the scheme rules, evaluation results outlined in the document ETR Addendum for gSMC-K Composite Evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR Addendum for gSMC-K Composite Evaluation is not older than eighteen months and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully. Please note that the eighteen month time frame of the document ETR Addendum for gSMC-K Composite Evaluation [8] has expired and was not updated in the course of the present maintenance process with ALC re-evaluation.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] 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] IAR for TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, Version 0.1, 16 March 2020, T-Systems International GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-0904-2015 for TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, 3 July 2015, Bundesamt für Sicherheit in der Informationstechnik

[4] Assurance Continuity Maintenance Report BSI-DSZ-CC-0904-2015-MA-01 for TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, 4 November 2015, Bundesamt für Sicherheit in der Informationstechnik

[5] Security Target BSI-DSZ-CC-0904-2015, Specification of the Security Target TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, Version 2.0.1, 5 June 2015, T-Systems International GmbH

[6] Configuration List BSI-DSZ-CC-0904-2015-MA-02 for TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, Version 1.1, 29 April 2020, T-Systems International GmbH (confidential document)

[7] Evaluation Technical Report (ETR) BSI-DSZ-CC-0904-2015-MA-02 for TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P, Version 1.4, 7 May 2020, SRC Security Research & Consulting GmbH (confidential document)

[8] ETR Addendum for gSMC-K Composite Evaluation, Version 1.1, 30 October 2015, BSI-DSZ-CC-0904-2015-MA-01, SRC Security Research & Consulting GmbH (confidential document)

[9] Certification Report BSI-K-TR-0226-2015 for TCOS Security Module Card – K Version 2.0 Release 1, 15 September 2015, Bundesamt für Sicherheit in der Informationstechnik