Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1147-2020-MA-01

MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121)

from

MaskTech 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-1147-2020.

The certified product itself did not change. The changes are related to the Initialization and Pre-personalization Phase of the card product and related documentation.

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-1147-2020 dated 18 December 2020 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-1147-2020.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 9 April 2021

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 of the MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121), MaskTech 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. To support a wider range of card readers, the configuration script for initializing the MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121) was amended to activate the Card Identifier (CID) function as part of the implemented ISO/IEC 14443 protocol.

The changes involve an additional script to activate the Card Identifier function during the Initialization Phase when the COS is loaded on the secure platform controller. Accordingly, the guidance for Initialization and Pre-personalization [4] was updated. Both document updates lead to a new configuration list [5].

A user may check the state of CID with software and card reader from the IC developer performing the ‘Request to Answer to Select’ (RATS). In return, the TC1-byte of ‘Answer to Select’ (ATS) will result in ‘00h’ if CID is off and ‘02h’ if CID was activated.

Conclusion

The maintained change is at the level of configuration of protocols for external communication and according guidance documentation. The change has no effect on product assurance, but the updated guidance documentation has to be followed.

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 <u>not</u> been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1147-2020 dated 18 December 2020 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[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 – Changes and Impact Analysis, MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121), Version 1.0, 27 January 2021, MaskTech International GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-1147-2020 for MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121) from MaskTech International GmbH, 18 December 2020, Bundesamt für Sicherheit in der Informationstechnik

[4] Guidance for Initialization and Pre-personalization – MTCOS Pro 2.5 ePassport / P71D352 (N7121), Version 1.2, 27 January 2021, MaskTech International GmbH

[5] Configuration List for MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121) (EAC)/(BAC), Version 0.7, 04 February 2021, MaskTech International GmbH