Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1162-V2-2023-MA-01

CardOS V6.0 ID R1.1

from

Eviden Germany 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-1162-V2-2023.

The certified product itself did not change. The changes are related to an update of life cycle security aspects, concerning an updated version of the Site Technical Audit Reports (STAR) for the sites Munich, Fuerth and Split of Eviden Germany GmbH.

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-1162-V2-2023 (V2.0) dated 17 October 2023 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-1162-V2-2023 (V2.0).

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

Bonn, 29 July 2024

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 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 [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the CardOS V6.0 ID R1.1, Eviden Germany 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 changes are related to an update of life cycle security aspects. The ALC re-evaluation was performed by the ITSEF TÜV Informationstechnik GmbH. The procedure led to an updated version of the Site Technical Audit Reports (STAR) for the sites Munich, Fuerth and Split of Eviden Germany GmbH [6] and a corresponding update of the Evaluation Technical Report (ETR) [5]. These sites may now not only be used for development of smartcard embedded software of Eviden Germany GmbH itself, but may also be used by affiliated companies of Eviden Germany GmbH for such development tasks. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

Conclusion

The maintained change is at the level of life cycle security aspects. The change has no effect on product assurance.

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-1162-V2-2023 (V2.0) dated 17 October 2023 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.

Additional security requirements supplement the security requirements and recommendations for secure use of the TOE which are already provided by the TOE guidance documentation and in chapter 10 of the Certification Report, part B [3].

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 3.1, February 2024

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, Version 1.2, March 2024

[2] IAR: Minutes Kick Off for BSI-DSZ-CC-1162-V2-2023-MA-01 (confidential document)

[3] Certification Report BSI-DSZ-CC-1162-V2-2023 for CardOS V6.0 ID R1.1, Version 2.0, 17 October 2023, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target for BSI-DSZ-CC-1162-V2-2023, Security Target ’CardOS V6.0 ID R1.1’, Revision 2.10R, Edition 09/2023, Eviden Germany GmbH

[5] Evaluation Technical Report Summary (ETR Summary) for BSI-DSZ-CC-1162-V2-2023-MA-01 for CardOS V6.0 ID R1.1, Version 6, 15 July 2024, TÜV Informationstechnik GmbH (confidential document)

[6] STAR Reports (confidential documents):

Site Technical Audit Report (STAR) – Munich, Version 1, 15 July 2024, TÜV Informationstechnik GmbH

Site Technical Audit Report (STAR) – Fuerth, Version 1, 15 July 2024, TÜV Informationstechnik GmbH

Site Technical Audit Report (STAR) – Split, Version 1, 15 July 2024, TÜV Informationstechnik GmbH

Note: End of report