Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1170-2023-MA-01

cryptovision SMAERS, Version 2.0

from

cv cryptovision 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-1170-2023.

The certified product itself did not change. The changes are related to some accompanying life-cycle documentation. This documentation is not in the scope of the Common Criteria evaluation and was approved by the BSI in a separate process. The purpose of this maintenance was solely to update and include the updated documents.

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-1170-2023 dated 27 April 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-1170-2023.

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

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

Bonn, 31 October 2024

The Federal Office for Information Security

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

The vendor for the cryptovision SMAERS, Version 2.0, cv cryptovision 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 Evaluation Technical Report (ETR) [5]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

Conclusion

The maintained change is an update of the references of the life-cycle documentations. This required a update of the ETR. 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-1170-2023 dated 27 April 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.

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).

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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].

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.2, 30 September 2021

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.0, November 2019

[2] cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems, Impact Analysis Report, Version 1.0, 2023-06-06 (confidential document)

[3] Certification Report BSI-DSZ-CC-1170-2023 for cryptovision SMAERS, Version 2.0, 2023-04-27, Bundesamt für Sicherheit in der Informationstechnik,

[4] Security Target BSI-DSZ-CC-1170-2023, Version 2.6, 2023-03-21, “cryptovision SMAERS - Java Card applet providing Security Module Application for Electronic Record-keeping Systems Security Target”, cv cryptovision GmbH (confidential document)

[5] Evaluation Technical Report, Version 1, 2024-10-10, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)