Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1119-2023-MA-01

cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0

from

cv cryptovision GmbH

SOGIS
Recognition Agreement
for components up to
EAL 4

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-1119-2023.

The certified product itself did not change. The changes are 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-1119-2023 dated 24.01.2023 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-1119-2023.

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

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

The vendor for the cryptovision CSP – Java Card applet providing Cryptographic Service Provider 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], as well as an addendum to the prior ETR for Composition [4]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target of the previous certification.

The development sites now are as follows:

Name of site / Company name	**Address**	**Type of site**
cv cryptovision GmbH	Munscheidstr. 14, 45886 Gelsenkirchen, Germany	SW Development
cv cryptovision GmbH	Oberforstbacher Str. 271a, 52076 Aachen, Germany	
Eviden Germany GmbH	Otto-Hahn-Ring 6, 81739 München, Germany	
Eviden Germany GmbH	Würzburger Str. 121, 90766 Fürth, Germany	
Atos IT Solutions and Services d.o.o.	Matice Hrvatske 15, 21000 Split Kroatien	

Table 1: Relevant development sites

The STAR report for ALC-Reuse has been updated [6].

Conclusion

The maintained change is at the level of life cycle aspects. The change has no effect on product assurance but the updated documentation (e.g. STAR) has to be followed.

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-1119-2023 dated 24.01.2023 is of relevance and has to be considered when using the product.

The validity period for the ETR for Composition of the previous certification procedure has not been enhanced, the new addendum does not change the prior validity period.

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 hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation of the previous certification procedure.

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months[1] and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[2] Section 9, Para. 4, Clause 2).

1 In this case the eighteen month time frame is related to the date of the initial version of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.

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

In cases, where this current certification procedure is used in the context of further composite certification procedure, the foundation for usage of the certificate updated by this maintenance procedure is:

- Use of the the document ETR for composite evaluation of base certification procedure BSI-DSZ-CC-1119-2023, including the new addendum [4].

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 CSP version 2.0, Impact Analysis Report”, Version 1.0, 2024-01-26, cv cryptovision GmbH (confidential document),

[3] Certification Report of procedure BSI-DSZ-CC-1119-2023, Bundesamt für Sicherheit in der Informationstechnik,

[4] Evaluation Technical Report for Composite ADDENDUM, Version 2, 2024-11-06, ”EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION ADDENDUM”, TÜV Informationstechnik GmbH, (confidential document) ,

[5] Evaluation Technical Report, Version 1, 2024-11-06, ”EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)”, TÜV Informationstechnik GmbH, (confidential document),

[6] STAR, “Site Technical Audit Report (STAR) – Cryptovision”, Version 2, 2024-11-06.