Assurance Continuity Maintenance Report

BSI-DSZ-CC-1233-2025-MA-01

Y7, 4.3.1:1.3.2 with eHealth Application 1.1.24

from

JDM Payment Solutions SAS

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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-1233-2025.

The change to the certified product focuses on the payment application which is security non-interfering. The identification of the maintained product is indicated by a new version number compared to the certified product.

Considering the nature of the change leads to the conclusion that it is classified as a <u>minor change</u> 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-1233-2025 dated 8 July 2025 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-1233-2025.

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

Bonn, 10 February 2026

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 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 Y7, 4.3.1:1.3.2 with eHealth Application 1.1.24, JDM Payment Solutions SAS, 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 Y7, 4.3.1:1.3.2 with eHealth Application 1.1.24 was changed due to changes mainly regarding the payment application which is security non-interfering. The changes in the eHealth Application do not affect the TSF. Configuration Management procedures required a change in the product identifier. Therefore, the version number changed from 4.3.1:1.2.9 with eHealth Application 1.1.20 to 4.3.1:1.3.2 with eHealth Application 1.1.24.

The Security Target [4] was editorially updated.

The Configuration List [5] was updated.

Conclusion

The maintained change focuses on the payment application which is security non-interfering. 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 <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-1233-2025 dated 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 [4] 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 52, 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 2 December 2025, BGBl. 2025, no. 301, p. 2

References

[1]   Common Criteria document "Assurance Continuity: CCRA Requirements",
        version 3.1, 29 February 2024

        Common Criteria document "Assurance Continuity: SOG-IS Requirements",
        version 1.2, March 2024

[2]   Common Criteria Impact Analysis Report, Version 0.4, 13 February 2026, JDM
        Payment Solutions SAS, (confidential document)

[3]   Certification Report BSI-DSZ-CC-1233-2025 for BSI-DSZ-CC-1233-2025 for Y7
        4.3.1:1.2.9 with eHealth Application 1.1.20 from JDM Payment Solutions SAS, 8
        July 2025, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[4]   Security Target BSI-DSZ-CC-1233-2025, ASE_ST Y7 Security Target for the
        Evaluation of the Product JDM Y7 of JDM Payment Solutions SAS according to the
        Common Criteria 3.1 Level EAL3+ Certification Id: BSI-DSZ-CC-1233, Version
        0.0.18, 30.01.2026, JDM Payment Solutions SAS

[5]   Configuration List for the TOE, CC Configuration Items List, Version 0.0.9, JDM
        Payment Solutions SAS, (confidential document)