Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0967-2016-MA-01

CardOS DI V5.3 EAC/PACE Version 1.0

from

ATOS Information Technology 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 developers 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-0967-2016.

The certified product itself did not change. The changes are related to the usage of the product.

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-0967-2016 dated 23 June 2016 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-0967-2016.

Common Criteria
Recognition Arrangement
for components up to
EAL 2

Bonn, 21 December 2017

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 *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 for the CardOS DI V5.3 EAC/PACE Version 1.0, ATOS Information Technologies 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 changes on how to use the product and outlines the security impact of the changes.

The certified product itself did not change.

The changes are related to the usage of the product.

When using the product in RSA configuration the guidance documentation as listed in the certification report [3] has to be used, whereby the following constraints have to be followed:

- If the TOE is used in the RSA configuration both keys pairs CA_RSA_KeyPair and AA_RSA_KeyPair (if used) shall be imported to the card, as in the default configuration of the personalization script ‘ConfigApp_Person.csf’ and not generated on the TOE.
- For the externally generated RSA key pairs confidentiality of the private key and quality must be ensured.

Conclusion

The change to the TOE is at the level of limiting the method on how to use the product in addition to the user guidance documentation. The Security Target [4] is still valid for the TOE, but the extended notes on how to use the product need to be considered.

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.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

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-0967-2016 dated 23 June 2016 is of relevance and has to be considered when using the product.

Additional 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.

This report is an addendum to the Certification Report [3].

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report, V1.00, 06 September 2017, CardOS DI V5.3 EAC/PACE Version 1.0 (confidential document)

[3] Certification Report BSI-DSZ-CC-0967-2016 for CardOS DI V5.3 EAC/PACE Version 1.0 from Atos IT Solutions and Services GmbH, Bundesamt für Sicherheit in der Informationstechnik, 23 June 2016

[4] Security Target BSI-DSZ-CC-0967-2016, Version 2.01, 19.04.2016, Security Target 'CardOS DI V5.3 EAC/PACE Version 1.0', Atos IT Solutions and Services GmbH

[5] Evaluation Technical Report BSI-DSZ-CC-0967-2016, Version 6, 20 June 2016, TÜV Informationstechnik GmbH