Assurance Continuity Maintenance Report

BSI-DSZ-CC-0519-V2-2018-MA-01

Stationäres eHealth-Kartenterminal Ingenico ORGA 6141 online V3.7.2:1.2.0

from

Ingenico Healthcare GmbH

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 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-0519-V2-2018.

The certified product itself did not change. The changes are related to an update of life cycle security aspects (additional delivery chains).

Consideration of 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-0519-V2-2018 dated 02 March 2018 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-0519-V2-2018.

Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 13 September 2018

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 *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 Stationäres eHealth-Kartenterminal Ingenico ORGA 6141 online V3.7.2:1.2.0, Ingenico Healthcare 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 (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 (i.e. additional delivery chains). 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) [4]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target.

Conclusion

The maintained change is at the level of life cycle security aspects. The change has no effect on product assurance, but the updated delivery documentation [6] + [7] has to be followed.

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 <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-0519-V2-2018 dated 02 March 2018 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).

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 2.1, June 2012

[2]   "BSI-DSZ-CC-0519-V2 Auswirkungsanalyse", V1.0.0, 23 March 2018, Ingenico

[3]   Certification Report BSI-DSZ-CC-0519-V2-2018, Bundesamt für Sicherheit in der Informationstechnik, 02 March 2018

[4]   ETR Summary ORGA 6141 online 3.7.2:1.2.0, Version 4, 18 July 2018, TÜV Informationstechnik GmbH

[5]   Configuration List, V1.70, 25 June 2018, Ingenico

[6]   Sichere Lieferkette für den Palettenversand von Großmengen, Version 21, 05 April 2018, Ingenico

[7]   Sichere Lieferkette – Lieferung an Endnutzer/LEI", Version 6, 15 May 2018, Ingenico