Assurance Continuity Maintenance Report

BSI-DSZ-CC-0533-2009-MA-03

STARCOS 3.4 Health eGK C4

from

Giesecke & Devrient GmbH

Common Criteria Recognition
Arrangement
for components up to EAL4

Common Criteria

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 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-0533-2009.

The changes to the certified product are at the level of the developer documentation and the corresponding software implementation whereby only the application part of the TOE is affected. The changes to the product result from changes in the eHC specifications by the Gematik GmbH and the corresponding changes in the eHC Protection Profile [7]. The changes have no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

Consideration of the nature of the changes leads to the conclusion that they are 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-0533-2009 dated 30 April 2009 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-0533-2009.

Bonn, 19 July 2011

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 STARCOS 3.4 Health eGK C1 (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3]. In the past, the TOE has undergone two further preceding assurance continuity processes. The first one is related to the product STARCOS 3.4 Health eGK C2 and is registered under BSI-DSZ-CC-0533-2009-MA-01, the second one corresponds to the product STARCOS 3.4 Health eGK C3 and is registered under BSI-DSZ-CC-0533-2009-MA-02.

The vendor for the product STARCOS 3.4 Health eGK C4, Giesecke & Devrient 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 STARCOS 3.4 Health eGK C4 was changed due to changes in the eHC specifications by the Gematik GmbH and the corresponding changes in the eHC Protection Profile [7]. Configuration Management procedures required a change in the product identifier. Therefore the version number changed from STARCOS 3.4 Health eGK C3 (registered under BSI-DSZ-CC-0533-2009-MA-02) to STARCOS 3.4 Health eGK C4.

The changes are related to an update of the user guidance [8]. The changes of the document reflect the changes in the eHC specifications by the Gematik GmbH and the corresponding changes in the eHC Protection Profile [7].

Conclusion

The changes to the TOE are at the level of security irrelevant changes of the developer documentation and the corresponding software implementation whereby only the application part of the TOE is affected. The changes have no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The Security Target was editorially updated [6].

Consideration of the nature of the changes 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 <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-0533-2009 dated 30 April 2009 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.

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

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

References

[1]   Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004

[2]   Impact Analysis Report STARCOS 3.4 Health eGK C4, Version 1.2, 15 July 2011, Giesecke & Devrient GmbH (confidential document)

[3]   Certification Report BSI-DSZ-CC-0533-2009 for STARCOS 3.4 Health eGK C1, Bundesamt für Sicherheit in der Informationstechnik, 30 April 2009

[4]   Security Target Lite STARCOS 3.4 Health eGK C1, Version 1.0, 16 April 2009, Giesecke & Devrient GmbH (sanitised public document)

[5]   Configuration List STARCOS 3.4 Health eGK C4, Version 1.93, 15 July 2011, Giesecke & Devrient GmbH (confidential document)

[6]   Security Target Lite STARCOS 3.4 Health eGK C4, Version 1.5, 15 July 2011, Giesecke & Devrient GmbH (sanitised public document)

[7]   Common Criteria Protection Profile electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), Version 2.61, 19 April 2011, registered by Bundesamt für Sicherheit in der Informationstechnik under the certification ID BSI-CC-PP-0020-V2-2007-MA-03

[8]   Benutzerhandbuch STARCOS 3.4 Health eGK C4, Version 3.8, 15 July 2011, Giesecke & Devrient GmbH