



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0582-2009-MA-01
STARCOS 3.4 Health QES C2
from
Giesecke & Devrient GmbH



Common Criteria Recognition
Arrangement
for components up to EAL4

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-0582-2009.

The change to the certified product is at the level of the developer documentation and the corresponding software implementation, a change that has 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 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, the assurance as outlined in the Certification Report BSI-DSZ-CC-0582-2009 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0582-2009.

Bonn, 14 September 2010



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], the Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the STARCOS 3.4 Health QES C2, 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 QES C2 was changed due to some security irrelevant modifications of the underlying STARCOS 3.4 operating system and the related developer documentation. The change is not significant from the standpoint of security, however Configuration Management procedures required a change in the version number from STARCOS 3.4 Health QES C1 to STARCOS 3.4 Health QES C2.

Conclusion

The change to the TOE is at the level of a security irrelevant change of the developer documentation and the corresponding software implementation, a change that has no effect on assurance. Examination of the evidence indicates that the changes performed are limited to the specification of the underlying STARCOS 3.4 operating system and its implementation. The Security Target was editorially updated [6]. 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.

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.

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 [8].

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

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 C3 / STARCOS 3.4 Health QES C2, Version 0.9, 29th April 2010, Giesecke & Devrient GmbH (confidential document)
- [3] Certification Report BSI-DSZ-CC-0582-2009 for STARCOS 3.4 Health QES C1, Bundesamt für Sicherheit in der Informationstechnik, 30th April 2009
- [4] Security Target Lite STARCOS 3.4 Health QES C1, Version 0.8, 19th March 2009, Giesecke & Devrient GmbH (sanitised public document)
- [5] Configuration List STARCOS 3.4 Health QES C2, Version 1.3, 30th April 2010, Giesecke & Devrient GmbH (confidential document)
- [6] Security Target Lite STARCOS 3.4 Health QES C2, Version 0.9, 30th April 2010, Giesecke & Devrient GmbH (sanitised public document)