Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0827-2013-MA-01

Infineon Technologies Smart Card IC (Security Controller) M9900 A22 with optional RSA v1.03.006, EC v1.03.006, Toolbox v1.03.006 and Flash Translation Layer V1.01.0008 libraries with specific IC dedicated software

from

Infineon Technologies AG

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-0827-2013.

The change to the certified product is at the level of a non security relevant hardware layout modification due to a new derivative of equal design sources. The change has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product. The changes are related to an update of the user guidance.

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-0827-2013 dated 22 February 2013 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-0827-2013.

Bonn, 19 June 2013

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 Infineon Technologies Smart Card IC (Security Controller) M9900 A22 with optional RSA v1.03.006, EC v1.03.006, Toolbox v1.03.006 and Flash Translation Layer V1.01.0008 libraries with specific IC dedicated software, Infineon Technologies AG, 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 Infineon Technologies Smart Card IC (Security Controller) M9900 A22 with optional RSA v1.03.006, EC v1.03.006, Toolbox v1.03.006 and Flash Translation Layer V1.01.0008 libraries with specific IC dedicated software was changed due to a non security relevant hardware layout modification. Configuration Management procedures required a change in the product identifier. Therefore, the design step A21 will be kept certified due to non-security changes in the design step A22.

The changes are related to the user guidance [6]. The changes in view of the design step A22 are updated in the user guidance.

Conclusion

The change to the certified product is at the level of a non security relevant hardware layout modification due to a new derivative of equal design sources. Furthermore, the design step A21 will be kept certified due to non-security changes in the design step A22. The change has 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 [7].

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-0827-2013 dated 22 February 2013 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.

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 composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

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).

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 CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Impact Analysis for Assurance Continuity Maintenance M9900 A21 versus A22 including optional Software Libraries RSA - EC – Toolbox – FTL, Version 1.2, 2013-06-18 (confidential document)

[3] Certification Report BSI-DSZ-CC-0827-2013 forInfineon Technologies Smart Card IC (Security Controller) M9900 A21 with optional RSA v1.03.006, EC v1.03.006, Toolbox v1.03.006 and Flash Translation Layer V1.01.0008 libraries with specific IC dedicated software, Bundesamt für Sicherheit in der Informationstechnik, 22 February 2013

[4] Security Target Lite M9900 A21 including optional Software Libraries RSA - ECToolbox – FTL, Version 1.2, 2013-01-22, Infineon Technologies AG (sanitised public document)

[5] Configuration Management Scope M9900 A22 including optional Software Libraries RSA - EC – Toolbox – FTL, Version 0.5, 2013-05-03, Document Title (confidential document)

[6] M9900 Errata Sheet, Infineon Technologies AG, Rev. 1.4, 2013-06-04

[7] Security Target Lite M9900 A22 including optional Software Libraries RSA - ECToolbox – FTL, Version 1.3, 2013-06-07, Infineon Technologies AG (sanitised public document)

[8] ETR for composite evaluation according to AIS 36 for the M9900 A21, Version 3 2013-02-08, TÜV Informationstechnik GmbH (confidential document)