Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0758-2012-MA-01

Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

from

Infineon Technologies AG

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-0758-2012 updated by a re-assessment on 24 July 2012.

The change to the certified product is at the level of a non security relevant hardware quality improvement, compliance to the new AIS31, improvement of the flashloader firmware and editorial update of user documentation (errata sheet). The optional software remains unchanged. 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 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-0758-2012 dated 6 February 2012 updated by a re-assessment on 24 July 2012 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-0758-2012.

Bonn, 27 July 2012

SOGIS IT SECURITY CERTIFIED

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 Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), 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 Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) was changed due to minor non security relevant hardware improvements, improvement of the flashloader firmware, introduction of a new derivative of equal hardware and a consecutive update of the user documentation. The compliance to the new AIS31 and the new guidance have been evaluated by the evaluation body in the procedure BSI-DSZ-CC-0814-2012. The updated user guidance (errata sheet) has the version 27 February 2012 [6]. Also a minor non security relevant improvement for the flashloader part of the firmware was introduced. The new version of the flashloader is 3.92.024 with patch version 3.93.006. The firmware identifier changes to 78.015.14.1. The old flashloader version, which was certified for design step A21, may also be used by this TOE. Furthermore, the design step A21 will be kept certified due to non security changes in the design step B11. The new Security Target [7] and Security Target Lite [4] reflect this by listing two firmware identifiers [4, chapter 1.1]. The optional software remains unchanged. The hardware changes lead to small layout improvements, improved ESD robustness, due to customer request even beyond the original specification, and serve for improved communication stability during contactless communication and start-up in weak fields. In addition, a new derivative has been introduced, where the radio frequency interface is permanently disabled to have a contact based only communication derivative. All changes have no effect on assurance. Configuration Management [5] procedures required a change in the product identifier. Therefore, the Configuration Management version number changed from 1.0 to 1.01.

Conclusion

The change to the certified product is at the level of a non security relevant hardware quality improvement, compliance to the new AIS31, improvement of the flashloader firmware and editorial update of user documentation (errata sheet) [6]. The optional software remains unchanged. 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 [7] was editorially updated, too.

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-0758-2012 dated 6 February 2012 updated by a re-assessment on 24 July 2012 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [8] and [9] are the current versions of the ETR for composite evaluation and the ETR itself.

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 one year 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 M7892 A21 versus B11 including optional Software Libraries, RSA - EC – Toolbox, version 1.5, 2012-07-25 (confidential document)

[3] Certification Report BSI-DSZ-CC-0758-2012 for Infineon Security Controller M7892 A21 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), Bundesamt für Sicherheit in der Informationstechnik, 6 February 2012

[4] Security Target Lite Maintenance M7892 B11, Version 1.2, 2012-07-24, Infineon Technologies AG (sanitized public document)

[5] Configuration Management Scope M7892 B11 including optional Software Libraries RSA – EC – Toolbox, version 1.01, 2012-07-24, Infineon Technologies AG (confidential document)

[6] M7892 Controller Family for Security Applications, Errata Sheet, 2012-02-27

[7] Security Target Maintenance M7892 B11 including optional Software Libraries RSA – EC –SHA-2 – Toolbox, Version 1.2, 2012-07-24, Infineon Technologies AG

[8] ETR for composite evaluation according to AIS 36 for the Product M7892 A21, version 3, 2012-07-16, TÜV Informationstechnik GmbH, Evaluation Body for IT Security (confidential document)

[9] Evaluation Technical Report, M7892 A21, version 3, 2012-07-16, TÜV Informationstechnik GmbH, Evaluation Body for IT Security (confidential document)