Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0879-2014-MA-01

Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware)

from

Infineon Technologies AG

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 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-0879-2014.

The change to the certified product is at the level of a none security relevant USB software driver improvement. The software update has no effect on assurance and the design step did not change as well as other items of the TOE.

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-0879-2014 dated 18 March 2014 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-0879-2014.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 4 December 2014

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 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 M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware) was changed by a none security relevant USB software driver update to improve the communication capabilities of the USB interface. The changes are on the level of an introduced delay of the USB pipe selection handling, waiting loops and signal timing improvement. The software changes have been implemented in a new Flash Loader patch changing the version of the firmware identifier from 78.019.03.1 to the new version 78.019.03.4. The change improves the communication capabilities of the USB interface and is accompanied with an Errata Sheet update [7].

Conclusion

The change to the certified product is at the level of a none security relevant USB software driver improvement. The software update has no effect on assurance and the design step did not change as well as other items of the TOE. The entire security concept, Security Functional Requirements with security policy as well as the targeted assurance level EAL6 augmented, are kept unchanged and are not affected.

As a result of the changes the configuration list [5] and Errata Sheet [7] for the TOE have been editorially updated. The Security Target was editorially updated [4].

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 continue the 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-0879-2014 dated 18 March 2014 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 “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report IAR for M7893 B11 Including optional Software Libraries RSA - EC - SHA-2 – Toolbox, Version 0.2, 2014-10-21, Infineon Technologies AG (confidential document)

[3] Certification Report BSI-DSZ-CC-0879-2014 for M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware), 2014-03-18, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target BSI-DSZ-CC-0879-2014-MA-01, M7893 B11 including optional Software Libraries RSA – EC –Toolbox, Version 1.5, 2014-12-01, Infineon Technologies AG (confidential document)

[5] Configuration Management Scope M7893 B11 including optional Software Libraries RSA – EC –Toolbox, Version 0.4, 2014-10-20, Infineon Technologies AG (confidential document)

[6] Security Target Lite BSI-DSZ-CC-0879-2014-MA-01, M7893 B11 including optional Software Libraries RSA – EC – Toolbox, Version 1.5, 2014-12-01, Infineon Technologies AG (sanitised public document)

[7] M7893 Errata Sheet, Revision 1.4, 2014-11-25, Infineon Technologies AG (confidential document)

[8] ETR for composite evaluation according to AIS 36 for the Product M7893 B11, Version 1, 2013-12-20, TÜV Informationstechnik GmbH (confidential document)