Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0917-2014-MA-01

M7794 A12/G12 with optional RSA v1.02.13 or v2.00.002 and EC v1.02.13 or v2.00.002 and Toolbox v1.02.13 or v2.00.002 libraries and with specific IC-dedicated software

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 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-0917-2014.

The change to the certified product is at the level of none security relevant data settings. The change has no effect on assurance. The design step did not change as well as all other items of the TOE.

The certified product itself did not change. 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-0917-2014 dated 3 February 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-0917-2014.

Bonn, 12 June 2014

SOGIS Recognition
Agreement

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 M7794 A12/G12 with optional RSA v1.02.13 or v2.00.002 and EC v1.02.13 or v2.00.002 and Toolbox v1.02.13 or v2.00.002 libraries and 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 M7794 A12/G12 with optional RSA v1.02.13 or v2.00.002 and EC v1.02.13 or v2.00.002 and Toolbox v1.02.13 or v2.00.002 libraries and with specific IC-dedicated software was changed due to none security relevant data settings. This data is read and output by the GCIM. None of this changed data is used to identify the TOE. The new data settings change the output of the GCIM but not the GCIM functionality. These none security relevant data changes do not change the TOE, as these data fields are variable anyhow. Now they are set to the fixed value “0”. Whether the new or previous data settings are used, can be determined by the user ([7], chapter 4.24). In case this byte is 0x0 the new data settings are used. In case this byte is different from 0x0, the previous data settings are used.

Conclusion

The change to the TOE is at the level of none security relevant data settings. A detailed description can be found in [7], chapter 4.24. These none security relevant data changes do not change the TOE, as these data fields are variable anyhow. Now they are set to the fixed value “0”. The change has no effect on assurance. As a result of the changes the Errata Sheet for the TOE has been updated [7]. The Security Target [4] is still valid for 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.

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-0917-2014 dated 3 February 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 M7794 A12 and G12 Including optional Software Libraries RSA - EC - SHA-2 – Toolbox, Version 1.1, 2014-06-02, Infineon Technologies AG (confidential document)

[3] Certification Report BSI-DSZ-CC-0917-2014 for M7794 A12/G12 with optional RSA v1.02.13 or v2.00.002 and EC v1.02.13 or v2.00.002 and Toolbox v1.02.13 or v2.00.002 libraries and with specific IC-dedicated software, 2014-02-03, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target BSI-DSZ-CC-0917-2014-MA-01, M7794 A12 and G12 including optional Software Libraries RSA – EC – Toolbox, Version 3.3, 2013-11-27, Infineon Technologies AG (confidential document)

[5] Configuration Management Scope M7794 A12 and G12 including optional Software Libraries RSA – EC – Toolbox, Version 2.1, 2013-10-24, Infineon Technologies AG (confidential document)

[6] Security Target Lite BSI-DSZ-CC-0917-2014-MA-01, M7794 A12 and G12, Version 2.3, 2013-11-27 (sanitised public document)

[7] M7790, M7791, M7793, M7794 Controller Family for Security Applications, Errata Sheet, Revision 2.1, 2014-05-06, Infineon Technologies AG (confidential document)

[8] ETR for composite evaluation according to AIS 36 for the Product M7794 A12 and G12, Version 2, 2013-11-27, TÜV Informationstechnik GmbH (confidential document)