



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0829-V2-2015-MA-01

**Infineon smart card IC (Security Controller) M7820
A11 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**

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-0829-V2-2015.

The change to the certified product is at the level of re-introduction of an already certified firmware package. The change has no effect on assurance. The identification of the maintained product is indicated by an additional 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-0829-V2-2015 dated 3rd August 2015 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-0829-V2-2015.



Common Criteria
Recognition Arrangement
for components up to
EAL4

Bonn, 30 March 2016

The Federal Office for Information Security



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 smart card IC (Security Controller) M7820 A11 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, 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 smart card IC (Security Controller) M7820 A11 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, was changed due to re-introduction of an already certified firmware package version. Configuration Management procedures required a change in the product identifier. Therefore the firmware overall package version number v8014 was introduced.

Conclusion

The change to the TOE is at the level of TOE configuration enhancement. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The former Security Target [4] was editorially updated to [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.

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-0829-V2-2015 dated 3rd August 2015 is of relevance and has to be considered when using the product. The documents [7] and [8] 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 [7].

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 BSIG¹ 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, M7820 A11 including optional Software Libraries RSA - EC – SHA-2 - Toolbox, Version 0.1, 2016-02-16, Infineon Technologies AG, Chipcard and Security Evaluation Documentation (confidential document)
- [3] Certification Report BSI-DSZ-CC-0829-V2-2015 for Infineon smart card IC (Security Controller) M7820 A11 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, Bundesamt für Sicherheit in der Informationstechnik, 2015-08-03
- [4] Security Target BSI-DSZ-CC-0829-V2-2015, M7820 A11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox, Version 1.9, 2015-07-14, Infineon Technologies AG
- [5] Configuration Management Scope, M7820 A11 including optional Software Libraries RSA - EC - SHA-2 – Toolbox, Version 0.1, 2016-02-19 (Confidential document)
- [6] Security Target BSI-DSZ-CC-0829-V2-2015-MA-01, M7820 A11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox, Version 2.0, 2016-03-11, Infineon Technologies AG
- [7] ETR for composite evaluation according to AIS 36 for the Product M7820 A11, Version 5, 2015-07-16, TÜV Informationstechnik GmbH - Evaluation Body for IT Security (confidential document)
- [8] Evaluation Technical Report, M7820 A11, Version 5, 2015-07-16, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)