Assurance Continuity Maintenance Report

BSI-DSZ-CC-0829-V2-2015-MA-02

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 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 <u>minor change</u> and that certificate maintenance is the correct path to continuity of assurance.

Common Criteria

The resistance to attacks has <u>not</u> 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 (including addendum of BSI-DSZ-CC-0829-V2-2015-MA-01 of 20th March 2016) 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
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 24 October 2017

The Federal Office for Information Security

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

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] and [5], its Security Target and the Evaluation Technical Report as outlined in [3] and [5].

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 changes are related to an update of the user guidances. The updates concern User's Manuals, Security Guidelines and an Errata Sheet, see [9]-[12].

Conclusion

The change to the TOE is at the level of guidance documentation. The change has no effect on assurance.

The former Security Target [4] was updated [6].

Consideration of the nature of the change leads to the conclusion that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] (and [5]) is maintained for this version of the product.

The resistance to attacks has <u>not</u> 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] remain 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 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] and [5].

---

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]   "Chipcard   and Security Evaluation Documentation - Impact Analysis, M7820 A11 including optional Software Libraries RSA - EC – SHA-2 - Toolbox", Version 0.1, 2017-09-28, Infineon Technologies AG, (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]   Assurance Continuity Maintenance Report BSI-DSZ-CC-0829-V2-2015-MA-01 for Infineon smart card IC (Security Controller) M7820A11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013libraries and with specific IC dedicated software, Bundesamt für Sicherheit in der Informationstechnik, 2016-03-30

[6]   Public Security Target Assurance Continuity Maintenance "M7820 A11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox" for certification BSI-DSZ-CC-0829-V2-2015-MA-02, Version 2.2, 2017-10-19, 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)

[9]   SLx 70 Family Production and Personalization User's Manual, 2015-04-01, Infineon Technologies AG

[10]   SLE 70 Family Programmer's Reference User's Manual, 2017-07-04, Infineon Technologies AG

[11]   SLE70 Asymmetric Crypto Library Crypto@2304T, RSA / ECC / Toolbox, Users Interface (optional) – additional Errata Sheet Section, 2017-06-20, Infineon Technologies AG

[12]   M7820 Controller Family for Security Application, Security Guidelines, 2017-09-18, Infineon Technologies AG