Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0945-V2-2018-MA-01

Infineon smart card IC (Security Controller) IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 00022Dh, design step H13 with optional libraries CCL V2.0.0002, RSA2048/4096 V2.07.003 / V2.06.003, EC V2.07.003 / V2.06.003, Toolbox V2.07.003 / V2.06.003, HSL V02.01.6634 / V01.22.4346, MCS V02.02.3389 / V02.03.3446, SCL V2.02.010 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 developer's 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-0945-V2-2018.

The change to the certified product is at the level of an editorial correction of the Security Target. The identification of the maintained product part (Security Target) is indicated by a new version number compared to the previously 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-0945-V2-2018 dated 20th April 2018 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-0945-V2-2018.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 20 August 2018

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

The vendor for the Infineon smart card IC (Security Controller) IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 00022Dh, design step H13 with optional libraries CCL V2.0.0002, RSA2048/4096 V2.07.003 / V2.06.003, EC V2.07.003 / V2.06.003, Toolbox V2.07.003 / V2.06.003, HSL V02.01.6634 / V01.22.4346, MCS V02.02.3389 / V02.03.3446, SCL V2.02.010 and with specific IC dedicated software by 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) IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 00022Dh, design step H13 with optional libraries CCL V2.0.0002, RSA2048/4096 V2.07.003 / V2.06.003, EC V2.07.003 / V2.06.003, Toolbox V2.07.003 / V2.06.003, HSL V02.01.6634 / V01.22.4346, MCS V02.02.3389 / V02.03.3446, SCL V2.02.010 and with specific IC dedicated software was changed due to

- an erroneous note (“note 23”) in the Security Target as well as
- more prominently underlining of the proprietary nature of FCS_CKM.1/RSA-1 and FCS_CKM.1/RSA-1 by addition of the sentence “RSA key generation according to Infineon key generation methods”.

In detail:

All changes only serve the purpose to provide editorial corrections and clarifications.

- The previous informal note 23 lead to a confusion with statements in the certification report. Thus, an editorial change of said Security Target note was initiated. No functionality was changed, nor new or different functionality introduced or removed.
- The additional editorial change in the description of FCS_CKM.1/RSA-1 and FCS_CKM.1/RSA-2 serves the purpose to eliminate possible misinterpretations. The goal is to unambiguously clarify the nature of implemented cryptography. No functionality was changed, nor new or different functionality introduced or removed.

Please note that both items were already correctly addressed in the Certification Report of BSI-DSZ-CC-0945-V2-2018 (dated 20th April 2018).

Due to the above mentioned changes, Configuration Management procedures required a change in the Security Target identifiers.

Therefore the Security Target version numbers changed

- from v1.6 (confidential) to v1.61 (confidential) and
- from v0.7 (public) to v0.71 (public).

The certified hardware, firmware, libraries or further guidance documentation (as listed in Certification Report of BSI-DSZ-CC-0945-V2-2018 dated 20th April 2018) themselves did not change.

Conclusion

The maintained change is at the level of an editorial Security Target change. The change has no effect on product assurance.

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-0945-V2-2018 dated 20th April 2018 is of relevance and has to be considered when using the product.

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 a 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[1] 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[2] Section 9, Para. 4, Clause 2), unless stated otherwise.

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

This report is an addendum to the Certification Report [3].

[1] In this case the eighteen month time frame is related to the date of the initial version [9] of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.

[2] 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] IAR, “Impact Analysis for Common Criteria with Evaluation Assurance Level EAL6 augmented (EAL6+), IFX_CCI_3h - 5h - 8h - Ch - 13h - 14h - 15h - 1Ch - 1Dh - 21h - 22h, design step H13”, version 1.2, 2018-07-30, Infineon Technologies AG (confidential document)

[3] Certification Report BSI-DSZ-CC-0945-V2-2018 for “Infineon smart card IC (Security Controller) IFX_CCI_000003h, 000005h, 000008h, 00000Ch,000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 00022Dh, design step H13 with optional libraries CCL V2.0.0002, RSA2048/4096 V2.07.003 / V2.06.003, EC V2.07.003 / V2.06.003, ToolboxV2.07.003 / V2.06.003, HSL V02.01.6634 / V01.22.4346, MCS V02.02.3389 / V02.03.3446, SCL V2.02.010 and with specific IC dedicated software from Infineon Technologies AG”, Bundesamt für Sicherheit in der Informationstechnik, 2018-04-20

[4] Previous (confidential) ST:
Confidential Security Target for BSI-DSZ-CC-0945-V2-2018, Version 1.6, 2017-11-06, “Confidential Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (confidential document)

[5] **New** (confidential) ST:
Confidential Security Target for BSI-DSZ-CC-0945-V2-2018, **Version 1.61, 2018-07-30**, “Confidential Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (confidential document)

[6] Previous (public) ST:
Public Security Target BSI-DSZ-CC-0945-V2-2018, Version 0.7, 06.11.2017, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (sanitised public document)

[7] **New** (public) ST:
Public Security Target BSI-DSZ-CC-0945-V2-2018, **Version 0.71, 2018-07-30**, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (sanitised public document)