Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0945-2017-MA-01

IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated 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-0945-2017.

The change to the certified product is at the level of production test changes and documentation updates. The change has no effect on assurance. The identification of the maintained product is indicated by an additional firmware 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-0945-2017 dated 10th July 2017 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-0945-2017.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 24 August 2017

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 IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated 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 IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated firmware was changed due to changes in production tests and editorial updates of the Security Target. Configuration Management procedures thus lead to a change in the product identifier. Due to the nature of said tests, an additional firmware identifier was introduced, adding the identifier 80.100.17.1 to the already available 80.100.17.0. The firmware code itself was not changed. The Security Target was updated accordingly (from the old version [4] to the new version [5]) to incorporate the additional identifier and editorial changes. Likewise, the documents [6] – [8] now reflect said change.

Conclusion

The change to the TOE is at the level of The change to the certified product is at the level of production test changes and documentation updates. The change has no effect on assurance.

The Security Target was editorially updated as well, see [5], as well as other documents (see [6] – [8]).

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-0945-2017 dated 10th July 2017 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 [9].

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).

In addition to the baseline certificate BSI notes that cryptographic functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionality it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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, “Impact Analysis Report Common Criteria with Evaluation Assurance Level EAL6 augmented (EAL6+), IFX_CCI_3h - 5h - 8h - Ch - 13h - 14h - 15h - 1Ch and 1Dh - H13”, Version 0.2 ACM, 2017-08-22 (confidential document)

[3] Certification Report BSI-DSZ-CC-0945-2017 for IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated firmware, Bundesamt für Sicherheit in der Informationstechnik, 2017-07-10

[4] Previous Security Targets (public and confidential):

Public Security Target BSI-DSZ-CC-0945-2017, Version 0.5, 22.05.2017, “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, design step H13”, Infineon Technologies AG (sanitised public document)

Confidential Security Target BSI-DSZ-CC-0945-2017, Version 1.2, 22.05.2017, “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, design step H13”, Infineon Technologies AG (confidential document)

[5] Updated Security Targets (public and confidential):

Public Security Target BSI-DSZ-CC-0945-2017-MA-01, Version 0.6 ACM, 2017-08-22, “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, design step H13”, Infineon Technologies AG (sanitised public document)

Confidential Security Target BSI-DSZ-CC-0945-2017-MA-01, Version 1.3 ACM, 2017-08-22, "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, design step H13”, Infineon Technologies AG (confidential document)

[6] "16-bit Security Controller 65-nm Technology, Programmer's Reference Manual", Rev. 9.6, 2017-07-04, Infineon Technologies AG (confidential document)

[7] "16-bit Security Controller – V01 Errata sheet", Rev. 5.0, 2017-08-17, Infineon Technologies AG (confidential document)

[8] “16-bit Security Controller Family -V01, Hardware Reference Manual (HRM), Rev.5.1, 2017-04-13”, Infineon Technologies AG (confidential document)

[9] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0945-2017, Version 1.24, 27.06.2017, ETR for composite evaluation (EFC), T-Systems International GmbH (confidential document)