Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1079-2018-MA-01

Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and 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 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-1079-2018

The change to the certified product is at the level of an editorial correction of the Security Target. The identification of the maintained product's Security Target is indicated by a new 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-1079-2018 dated 26th September 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-1079-2018.

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

Bonn, 3 December 2018

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 Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and 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 Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware was changed due to erroneous Hash-values for specific cryptographic libraries.

The certified product itself did not change.

In more detail:

Both the public and the confidential Security Target of the underlying base certification contained two tables of erroneous hash values for the components MifareOS.LIB and MifareManagement.LIB of the Mifare Compatible Software (MCS) library v02.03.3446. - These Hash-values have been corrected in the new Security Target versions. - *Note that the MCS library is not part of the TOE security functionality (TSF).*

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 v1.0 (confidential) to v1.1 (confidential) and
- from v1.0 (public) to v1.1 (public).

No other changes have been made to the Security Targets. The certified hardware, firmware, libraries or further guidance documentation (as listed in Certification Report of BSI-DSZ-CC-1079-2018 dated 26th September 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. The corrected Hash-values have been inserted in

reliance upon the manufacturer's assurance and not been subject to a dedicated verification by the certification body.

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-1079-2018 dated 26th September 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 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[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).

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

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

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

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_00000Fh with options G12”, version 0.5, 2018-11-08, Infineon Technologies AG (confidential document)

[3] Certification Report “BSI-DSZ-CC-1079-2018 for IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG”, Bundesamt für Sicherheit in der Informationstechnik, 2018-09-26

[4] Previous (confidential) ST:

“Confidential Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+; IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch; G12”, Revision 1.0, 2018-09-20, Infineon Technologies AG

[5] **New** (confidential) ST:

“Confidential Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+; IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch; G12”, Revision 1.1, 2018-11-20, Infineon Technologies AG

[6] Previous (public) ST:

“Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+, IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch, G12”, Revision 1.0, 2018-09-20, Infineon Technologies AG (sanitised public document)

[7] **New** (public) ST:

“Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+; IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch; G12”, Revision 1.1, 2018-11-20, Infineon Technologies AG (sanitised public document)