Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1102-2019-MA-01

Infineon Technologies Security Controller IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h design step S11 and M11 with optional HSL v2.62.7626, optional SCL version v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.304.01.0 and user guidance,

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-1102-2019.

The certified product itself did not change. The changes are related to an update of life cycle security aspects.

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-1102-2019 dated 15 February 2019 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-1102-2019.

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

Bonn, 19 June 2020

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 Technologies Security Controller IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h design step S11 and M11 with optional HSL v2.62.7626, optional SCL version v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.304.01.0 and user guidance, 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 certified product itself did not change. The changes are related to an update of life cycle security aspects. The ALC re-evaluation was performed by the ITSEF TÜV Informationstechnik GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [6] as well as an editorial update to the ETR for Composition [5]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

The relevant sites and related certificates listed in Annex B of Certification Report BSI-DSZ-CC-1102-2019 are replaced by the following delivery sites:

Name of site / Company name	**Address**
DHL Singapore	DHL Supply Chain Singapore Ptd Tampinese LogisPark 1 Greenwich Drive Singapore 533865
G&D Neustadt	Giesecke & Devrient Secure Data Management GmbH Austraße 101b 96465 Neustadt bei Coburg Germany
IFX Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA
KWE Shanghai	KWE Kintetsu World Express (China) Co., Ltd. Shanghai Pudong Airport Pilot Free Trade Zone No. 530 Zheng Ding Road Shanghai, P.R. China

Name of site / Company name	Address
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany

Table 1: Relevant delivery sites

Conclusion

The maintained change is at the level of life cycle security aspects. 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-1102-2019 dated 15 February 2019 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 [5].

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.

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 of the Evaluation Technical Report for Composite Evaluation [6] 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] Impact Analysis M5273 S11 and M11 based on BSI-DSZ-CC-1102-2019, Version 1.0, Date 01 July 2019, Infineon Technologies AG (confidential document)

[3] Certification Report BSI-DSZ-CC-1102-2019 for Infineon Technologies Security Controller IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h design step S11 and M11 with optional HSL v2.62.7626, optional SCL version v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.304.01.0 and user guidance, Bundesamt für Sicherheit in der Informationstechnik, 15 February 2019

[4] Security Target for BSI-DSZ-CC-1102-2019, Version 1.7, 2018-12-12, “IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h S11 and M11 Security Target Lite”, Infineon Technologies AG (sanitised public document)

[5] Evaluation Technical Report for Composite Evaluation, BSI-DSZ-CC-1102-2019-MA-01, Version 3, 04 April 2020, TÜV Informationstechnik GmbH

[6] Evaluation Technical Report, BSI-DSZ-CC-1102-2019-MA-01, Version 6, 04 April 2020, TÜV Informationstechnik GmbH