Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1156-V4-2024-MA-01

IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 and 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, 3.35.001, v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 and user guidance

from

Infineon Technologies AG

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] 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-1156-V4-2024.

The certified product itself did not change. The changes are related to an update of the user guidance.

Considering 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-1156-V4-2024 dated 2024-09-04 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-1156-V4-2024.

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

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

Bonn, 25 March 2025
The Federal Office for Information Security

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 procedures on Assurance Continuity [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 [4] and the Evaluation Technical Report [6] as outlined in [3].

The vendor for the IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 and 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, 3.35.001, v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 and user guidance, Infineon Technologies AG, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [1]. In accordance with those requirements, the IAR in general describes (if applicable) (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.

In this maintenance procedure, the user guidance [5] version number was updated to the correct version number. This resulted in an editorial change in the Security Target [4] and Security Target lite [8]. Additionally a note from the Security Target was added to the Security Target lite adding additional information to the publicly available document.

Conclusion

The maintained change is at the level of guidance documentation. The change has no effect on product assurance, but the updated guidance documentation has to be followed.

Considering 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-1156-V4-2024 dated 2024-09-04 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 [7].

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).

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 [7] 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 3.1, 29 February 2024

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.2, March 2024

[2] Impact Analysis Report, Version 1.0, 2025-01-14, Evaluation Documentation: Impact Analysis, Infineon Technologies AG (confidential document)

[3] Certification Report for BSI-DSZ-CC-1156-V4-2024, Bundesamt für Sicherheit in der Informationstechnik, 2024-09-09

[4] Security Target BSI-DSZ-CC-1156-V4-2024-MA-01, Version 6.9, 2025-01-24, IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch, S11 Security Target, Infineon Technologies AG (confidential document)

[5] ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox,v3.35.001, 2024-11-15

[6] Evaluation Technical Report for BSI-DSZ-CC-1156-V4-2024, Version 1, 2024-08-22, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[7] ETR for composite evaluation according to AIS 36 for BSI-DSZ-CC-1156-V4-2024, Version 1, 2024-08-22, “EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR for COMP)”, TÜV Informationstechnik GmbH (confidential document

[8] Security Target lite BSI-DSZ-CC-1156-V4-2024-MA-01, Version 6.9, 2025-01-24, IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch, S11 Security Target Lite, Infineon Technologies AG (sanitised public document)