Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1206-V5-2025-MA-02

IFX_CCI_000068h/80h/97h/99h G12 and IFX_CCI_000093h R11/R12 with firmware v80.505.04.1 or v80.511.00.0, opt.HSL v04.05.0040, opt.UMSLC v02.01.0040, opt.Crypto Suite v.05.02.002, opt. NRG™ v06.10.0002 or v06.10.0005, opt.Ascon-128 MISE v1.1.2, opt.SHA256 MISE v1.1.1 and user guidance documents

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-1206-V5-2025 and the report addendum of BSI-DSZ-CC-1206-V5-2025-MA-01.

The change to the certified product is at the level of maintenance. The certified product changed with respect to a minor configuration.

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-1206-V5-2025 dated 22nd July 2025 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 of BSI-DSZ-CC-1206-V5-2025 and the addendum of BSI-DSZ-CC-1206-V5-2025-MA-01.

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

Bonn, 2 September 2025

The Federal Office for Information Security

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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] the SOG-IS procedure on “Interpretation of EUCC Implementing Regulation article 49” [9] (paragraph 7) and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product [3], its Security Target [4] and the Evaluation Technical Report as referenced in the certification report [3] and the ETR Summary addendum of BSI-DSZ-CC:1206-V5-2025-MA-01 [7].

The vendor for the IFX_CCI_000068h/80h/97h/99h G12 and IFX_CCI_000093h R11/R12 with firmware v80.505.04.1 or v80.511.00.0, opt.HSL v04.05.0040, opt.UMSLC v02.01.0040, opt.Crypto Suite v.05.02.002, opt. NRG™ v06.10.0002 or v06.10.0005, opt.Ascon-128 MISE v1.1.2, opt.SHA256 MISE v1.1.1 and user guidance documents, Infineon Technologies AG (see Security target [4] for specific availability of library versions) 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 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_000068h/80h/97h/99h G12 and IFX_CCI_000093h R11/R12 with firmware v80.505.04.1 or v80.511.00.0, opt.HSL v04.05.0040, opt.UMSLC v02.01.0040, opt.Crypto Suite v.05.02.002, opt. NRG™ v06.10.0002 or v06.10.0005, opt.Ascon-128 MISE v1.1.2, opt.SHA256 MISE v1.1.1 and user guidance documents (see Security target [4] for specific availability of library versions) was changed due to a sensor reconfiguration for the following design step G12 derivatives

- IFX_CCI_000068h,
- IFX_CCI_000080h and
- IFX_CCI_000097h.

However, the derivative

- IFX_CCI_000099h,

as well as the R11 and R12 design step derivative

- IFX_CCI_000093h

remain unchanged.

Conclusion

The maintained change is at the level of minor configuration change. The change has no effect on product assurance, but the updated documentation [8] has to be taken into account.

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. This is also supported by a dedicated ITSEF assessment, see [10].

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-1206-V5-2025 dated 22nd July 2025 and the certification report addendum of BSI-DSZ-CC-1206-V5-2025-MA-01 dated 29th July 2025 are of relevance and have 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] and [6].

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 [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 3.1, 29 February 2024

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

[2] “BSI-DSZ-CC-1206 - Impact Analysis”, version 1.10, 2025-08-20, Infineon Technologies AG (confidential document)

[3] Current/unchanged Certification Report of BSI-DSZ-CC-1206-V5: Certification Report for BSI-DSZ-CC-1206-V5-2025 version 1.0, dated 22nd July 2025, Bundesamt für Sicherheit in der Informationstechnik (public document)

[4] Current/unchanged Security Target Lite of BSI-DSZ-CC-1206-V5: Security Target Lite BSI-DSZ-CC-1206-V5-2025, Version 2.8, 2025-07-02, “IFX_CCI_000068h/80h/97h/99h G12 and IFX_CCI_000093h R11/R12 Security Target Lite”, Infineon Technologies AG (public document)

[5] Current/unchanged ETR-COMP of BSI-DSZ-CC-1206-V5: ETR for composite evaluation according to AIS 36 for the Product, Version 2, 2025-07-11, “Evaluation Technical for Composite Evaluation (ETR COMP) for the IFX_CCI_000068h, IFX_CCI_000080h, IFX_CCI_000097h, IFX_CCI_000099h G12 and IFX_CCI_000093h R11/R12”, TÜV Informationstechnik GmbH (confidential document)

[6] ETR-COMP addendum of BSI-DSZ-CC-1206-V5-2025-MA-01: Addendum for ETR-COMP, “EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION ADDENDUM (ETR COMP_ADD)”, version 1, 2025-07-17, TÜV Informationstechnik GmbH (confidential document)

[7] Current ETR Summary report (of BSI-DSZ-CC:1206-V5-2025-MA-01): Evaluation Technical Report Summary, Version 2, 2025-07-23, “EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)”, TÜV Informationstechnik, (confidential document)

[8] New/updated document: “ATE_Mappings.xlsx”, Version 0.2, 2025-08-25, Infineon Technologies AG (confidential document)

[9] “Interpretation of EUCC Implementing Regulation article 49 for phasing out SOG-IS schemes”, version 1.0, August 2024 (public document)

[10] “Statement regarding the maintenance certification of BSI-DSZ-CC-1206-V5-MA-02”, 2025-08-21, TÜV Informationstechnik GmbH (confidential document)