Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1206-V5-2025-MA-01

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.

The change to the certified product is at the level of lifecycle maintenance. The certified product itself did not change. The changes are related to an optional update of production sites.

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.

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

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

Bonn, 29 July 2025

The Federal Office for Information Security

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” [10] (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 (old) Evaluation Technical Report as referenced in the certification report [3].

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, i.e. 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 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, from a functional or otherwise technical perspective.

The overall changes thus are only related to an optional addition of a production site certified by the Spanish CC scheme CCN under CCN-CC-8/2025 [9]. 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) [7] as well as an Addendum to the ETR for Composition [6]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

In detail, the production flow changed as follows:

- For **IFX_CCI_000093h R11 and R12**:

  The site “Giesecke+Devrient (Jiangxi) Technology Co., Ltd.” located at 399 Huoju Avenue, High-New Tech Development Zone, Nanchang City, Jiangxi Province, 330096 P.R. China (including aspects of internal delivery), certified by the Spanish CC scheme CCN under CCN-CC-8/2025 [9], is added as an additional option for intermediary production flow steps.

- For **IFX_CCI_000068h/80h/97h/99h G12**:

  No change regarding lifecycle aspects took place, i.e. no change at all for these TOE configurations, compared to the previous certification BSI-DSZ-CC-1206-V5-2025.

No individual audit of the newly added site was conducted by BSI or the ITSEF, as it was already certified by the Spanish scheme CCN under the certification identifier CCN-CC-8/2025 [9].

Conclusion

The maintained change is at the level of production sites by inclusion of an CC certified site (CCN-CC-8/2025) for the given TOE type.

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.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target (or included Site Security Targets) 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 inclusion of a new production site 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).

1 In this case the eighteen month time frame is related to the date of the initial version [5] of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.

The foundation for usage of the certificate updated by this maintenance procedure is:

- Use of the „ETR for composite evaluation“ [5] of the base certificate,
- its new ETR-COMP Addendum [6],
- the updated ETR Summary [7] and
- the updated configuration list [8].

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

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 R5, 29 February 2024

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

[2] “BSI-DSZ-CC-1206 - Impact Analysis”, version 1.9, 2025-07-14, 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] New ETR-COMP addendum:
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] New/updated ETR Summary report:
Evaluation Technical Report Summary, Version 2, 2025-07-23, “EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)”, TÜV Informationstechnik, (confidential document)

[8] New/updated configuration list:
“Configuration list” for the TOE, Version 1.1, 2025-07-14 (confidential document)

[9] “CERTIFICATE CCN-CC-8/2025, Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN)”, 2025-04-22 (public document)

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