Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0891-V6-2021-MA-01

Infineon Security Controller M7892 Design Steps D11 and G12, with the optional libraries RSA2048/4096 v2.03.008 or v2.07.003, EC v2.03.008 or v2.07.003, SHA-2 v1.01, Toolbox v2.03.008 or v2.07.003 and symmetric crypto library v2.02.010, as well as with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE),

from

Infineon Technologies AG

SOGIS
Recognition Agreement

Common Criteria

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

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-0891-V6-2021.

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-0891-V6-2021 dated 23.11.2021 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-0891-V6-2021.

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

Bonn, 28 January 2022

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 *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 M7892 Design Steps D11 and G12, with the optional libraries RSA2048/4096 v2.03.008 or v2.07.003, EC v2.03.008 or v2.07.003, SHA-2 v1.01, Toolbox v2.03.008 or v2.07.003 and symmetric crypto library v2.02.010, as well as with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE), 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 Security Target did not change.

The STAR report for ALC-Reuse of the following sites has been updated: [7],[8], [9],[10], [11].

The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1 and ALC_TAT.2, depending on the site) are fulfilled for the sites listed below

Name of site / Company name	Address
IFX Regensburg	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany
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
Toppan Round Rock	Toppan Printing Company America, Inc. Round Rock Site 2175 Greenhill Drive Round Rock, Texas 78664 USA
K&N Großostheim	Kühne & Nagel

	Stockstädter Strasse 10 63762 Großostheim Germany

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-0891-V6-2021 dated 23.11.2021 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.

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.

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].

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] Chipcard and Security Documentation Impact Analysis M7892 D11 and G12, V1.1, 2021-12-23, Infineon Technologies AG (Confidential document)

[3] Certification Report BSI-DSZ-CC-0891-V6-2021 for Infineon Security Controller M7892 Design Steps D11 and G12, with the optional libraries RSA2048/4096 v2.03.008 or v2.07.003, EC v2.03.008 or v2.07.003, SHA-2 v1.01, Toolbox v2.03.008 or v2.07.003 and symmetric crypto library v2.02.010, as well as with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension(MAE) , Bundesamt für Sicherheit in der Informationstechnik, (2021-11-23)

[4] Security Target lite BSI-DSZ-CC-0891-V6-2021, Version 3.6, 2021-10-06, Security Target Lite Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12, Infineon Technologies AG (sanitised public document)

[5] Evaluation Technical Report for Composite Evaluation Addendum, BSI-DSZ-CC-0891-V6-2021-MA-01, Version 2, 2021-01-13, TÜV Informationstechnik GmbH

[6] Evaluation Technical Report, BSI-DSZ-CC-891-V6-2021-MA-01, Version 2, 2022-01-13, TÜV Informationstechnik GmbH

[7] Site Technical Audit Report (STAR) KWE Kintetsu World Express (China) Co., Version 3, 2020-01-13, TÜV Informationstechnik GmbH

[8] SITE TECHNICAL AUDIT REPORT (STAR), Toppan Printing Company America, Inc., Round Rock, USA – Network Administration , Version 1, 2021-12-14, TÜV Informationstechnik GmbH

[9] SITE TECHNICAL AUDIT REPORT (STAR), Toppan Printing Company America, Inc., Round Rock, USA – Production Environment, Version 2, 2021-12-14, TÜV Informationstechnik GmbH

[10] Site Technical Audit Report (STAR) Kuehne & Nagel, Großostheim, Version 2, 2021.11.02,TÜV Informationstechnik GmbH

[11] Site Technical Audit Report (STAR) Infineon Technologies AG, Regensburg, Version 2, 2021-12-14, TÜV Informationstechnik GmbH