Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1086-2018-MA-01

OPTIGA™ Trusted Platform Module SLB9670_2.0 v7.85.4555.00, v7.85.4567.00,

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-1086-2018.

The certified product itself did not change. Since the changes of the TOE are related to the ALC aspect only, all other evaluation results from the predecessor are still valid and were taken over for the current evaluation.

Consideration of the nature of the change leads to the conclusion that it is classified as an ALC re-evaluation 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-1086-2018 dated October 29th 2018 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-1086-2018.

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

Bonn, 21 May 2021

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 OPTIGA™ Trusted Platform Module SLB9670_2.0 v7.85.4555.00, v7.85.4567.00, 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.

For the OPTIGA™ Trusted Platform Module SLB9670_2.0 v7.85.4555.00, v7.85.4567.00, the production and personalization system was changed due to the introduction of a new TPM 2.0 production system. The Hardware and the Firmware/Software of the current TOE are identical to that used in the predecessor. For the *production and personalization process* of the TOE a new TPM 2.0 production system (TPM-CA3) is used. The TPM-CA2 which was already used for the predecessor remains with no changes.

In more detail, the new TPM 2.0 production and personalization system is based on Utimaco “Security Server Se” and Ncipher “nShield Connect XC” HSMs (TPM-CA3). The used Utimaco “Security Server Se” HSMs have a Common Criteria certificate EAL4+ with AVA_VAN.4 including a Random Number Generator according BSI AIS31, and the used Ncipher “nShield Connect XC” HSMs have a FIPS 140-2 certificate.

The main new features of the CA (Certification Authority) software are the following:

1. A new transport encryption scheme using AES256 algorithm in addition to the already used TDES algorithm. Nevertheless, for the current TOE the TDES based encryption scheme is used.
2. The generation of RSA keys is done by the PDG-HSM according FIPS186-4 Mode B.3.6. Now also 3k and 4k bits key can be generated and the key components can be chosen out of a parameter set (e.g. only p and q parameter). For the current TOE only 2048 bit RSA keys are generated and all CRT parameter are chosen.
3. Generation of ECC keys additionally up to 521 bitlength possible and three different generating methods are available which can be chosen during production:
    1. HSM native key generation according FIPS 186-4 B.4.1 “Key Pair Generation Using Extra Random Bits”
    2. CTR-DRBG used for key generation according to NIST 800-90A, which is implemented in the firmware extension source code of the HSM module.

3. KDFa used for key generation according NIST 800-108 section 5.1 KDF in Counter Mode using HMAC (based on SHA256 as PRF), which is implemented in the firmware extension source code of the HSM module.

   For the current TOE the method 2. above is used.

Moreover, a new site ASE Kaohsiung has been added for the assembly process.

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) [4].

Conclusion

The maintained change is at the level of production and personalization. The change has no effect on product assurance.

Consideration of the nature of the change leads to the conclusion that it is classified as an ALC re-evaluation 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-1086-2018 dated October 29th 2018 is of relevance and has to be considered when using the product. As a result of this re-assessment, the document [4] is the current version of the ETR.

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.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] 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 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 Report, “SLB9670_2.0 v7.85 Impact Analysis”, Version 3.7, March 19th, 2021, Infineon Technologies AG

[3] Certification Report BSI-DSZ-CC-1086-2018 for “Infineon Technologies AG OPTIGA™ TrustedPlatform Module SLB9670_2.0 v7.85.4555.00,v7.85.4567.00”, Bundesamt für Sicherheit in der Informationstechnik, October 29th 2018

[4] Evaluation Technical Report, Version 2, March 22nd, 2021, ”Evaluation Technical Report Summary”, TÜV Informationstechnik GmbH, (confidential document)