Bundesamt
für Sicherheit in der
Informationstechnik

# Assurance Continuity Maintenance Report

## BSI-DSZ-CC-0946-V2-2015-MA-01

## Infineon Technologies AG Smartcard IC (Security Controller) M5072 G11 including optional Software Libraries RSA-EC-Toolbox

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 developers 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-0946-V2-2015.

The change to the certified product is at the level of configuration and minor firmware changes. The change has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

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-0946-V2-2015 dated 23rd November 2015 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-0946-V2-2015.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 15 March 2016

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 Infineon Technologies AG Smartcard IC (Security Controller) M5072 G11 including optional Software Libraries RSA-EC-Toolbox, 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 Infineon Technologies AG Smartcard IC (Security Controller) M5072 G11 including optional Software Libraries RSA-EC-Toolbox, was changed due to required adjustment of configuration values. Configuration Management procedures required a change in the product identifier. Therefore an additional BOS version with respective identifier 80001145 was introduced.

# Conclusion

The change to the TOE is at the level of configuration and minor firmware changes. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The Security Target [4] consequently was editorially updated to [6].

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.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

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-0946-V2-2015 dated 23rd November 2015 is of relevance and has to be considered when using the product. The documents [8] and [9] are the current versions of the ETR for composite evaluation and the ETR itself.

### Additional 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 [8].

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 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[1] Section 9, Para. 4, Clause 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] Inputs for Impact Analysis for M5072_BOS_V1 Firmware Update (confidential document)

[3] Certification Report BSI-DSZ-CC-0946-V2-2015 for “Infineon Technologies Smart Card IC (Security Controller) M5072 G11 with optional RSA v1.03.006, EC v1.03.006 and Toolbox v1.03.006 with specific IC dedicated software”, Bundesamt für Sicherheit in der Informationstechnik, 23rd November 2015

[4] Security Target Lite M5072 including optional Software Libraries RSA - EC – Toolbox, v0.3, 2015-09-28

[5] configuration Management Scope, v0.4, 2015-12-17 (Confidential document)

[6] Security Target Lite M5072 including optional Software Libraries RSA - EC – Toolbox, v0.4, 2015-12-17

[8] ETR for composite evaluation according to AIS 36 for the M5072 G11, Version 6, 2015-11-02, TÜV Informationstechnik GmbH (confidential document)

[9] Evaluation Technical Report Summary (ETR Summary) for the M5072 G11 with Crypto Libraries, Version 6, 2015-11-02, TÜV Informationstechnik GmbH, (confidential document)