Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0695-2011-MA-02

Infineon smart card IC (Security Controller) M7820 M11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software

from

Infineon Technologies AG

Common Criteria Recognition Arrangement
for components up to EAL4

Common Criteria

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 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-0695-2011 updated by a re-assessment on 27 March 2013.

The change to the certified product is at the level of none security relevant mask changes for yield improvements and including additional sites. The changes have no effect on assurance. The identification of the maintained product is indicated by the lot number. The changes are related to an infonote [5] belonging to the user guidance [8] and including additional delivery and production sites already evaluated into the scope of the certificate BSI-DSZ-CC-0827-2013.

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-0695-2011 dated 11 May 2011 updated by a re-assessment on 27 March 2013 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-0695-2011.

Bonn, 24 June 2013

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

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 smart card IC (Security Controller) M7820 M11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software, 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 smart card IC (Security Controller) M7820 M11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software was changed due to none security relevant mask changes for yield improvements and including additional sites. The improvements have no effect on any transistor dimensions. Further no electrical parameters were changed. The changes are related to an infonote [5] belonging to the user guidance [8] and including additional delivery and production sites already evaluated into the scope of the certificate BSI-DSZ-CC-0827-2013.

Configuration Management procedures required a change in the product identifier.To identify these changes, the lot number is used. The identification is described in [5], which provides a table, that maps the changes to the lot numbers affected by these changes. The lot number of a TOE can be determined via the Chip Identification Mode.

The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2) are fulfilled for the additional delivery and production sites of the TOE listed below:

Site	Adress	Function
Burlington - ASK	ASK-intTag, LLC Building 966 1000 River St., Essex Junction, Vermont 05452 USA	Inlay Mounting
Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA	Inlay Testing, Distribution Center
Galway - HID covered by [AIS47] Site certification from 2012-09-19 (cert ID	HID Global Ireland Teoranta Pairc Tionscail na Tulaigh Baile na hAbhann Co. Galway	Inlay Mounting

Site	Adress	Function
BSI-DSZ-CC-S-0015-2012)	Ireland	
Agrate - DNP	DNP Photomask Europe S.p.A. Via C. Olivetti 2/A 20041 Agrate Brianza Italy	Mask Production
Round Rock - Toppan	Toppan Printing Company America, Inc. Round Rock Site 2175 Greenhill Drive Round Rock, Texas 78664 USA	Inlay Mounting

Conclusion

The change to the certified product is at the level of none security relevant mask changes for yield improvements and including additional sites. The change has no effect on assurance. The identification of the maintained product is indicated by the lot name described in the infonote [5]. The changes are related to an infonote [5] belonging to the user guidance [8] and including additional delivery and production sites already evaluated into the scope of the certificate BSI-DSZ-CC-0827-2013.

The Security Target [4] is still valid for the TOE.

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 state ment as outlined in the Certification Report BSI-DSZ-CC-0695-2011 dated 11 May 2011 updated by a re-assessment on 27 March 2013 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [6] and [7] 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 [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 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).

The strength of the cryptographic algorithms was not rated in the course of the product certification (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for these functions it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

The Cryptographic Functionalities 2-key Triple DES (3DES), RSA 1024 provided by the TOE achieves a security level of maximum 80 Bits (in general context).

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 CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Impact Analysis M7820 M11 including optional Software Libraries RSA - EC – SHA-2 - Toolbox BSI-DSZ-CC-0695-2011, Version 1.1, 2013-06-19 (confidential document)

[3] Certification Report BSI-DSZ-CC-0695-2011 for Infineon smart card IC (Security Controller) M7820 M11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software, Bundesamt für Sicherheit in der Informationstechnik, 11 May 2011

[4] Security Target M7820 M11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox version 1.4, 2011-04-18, Infineon Technologies AG [5] Referenz Update Configuration List

[5] Information Note N° 047/13, PL=81, 2013-06-14, Infineon Technologies AG

[6] ETR for composite evaluation according to AIS 36 for the Product M7820 M11, Version 3, 2013-03-25, TÜV Informationstechnik GmbH, Evaluation Body for IT Security (confidential document)

[7] Evaluation Technical Report, M7820 M11, Version 3, 2013-03-25, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)

[8] SLx 70 Family SLE78 & SLB78 Product (C11FL/C120FL technology) Errata Sheet, version 2011-04-15, 2011-04-15, Infineon Technologies AG