Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0640-2010-MA-02

Infineon Technologies Smart Card IC (SecurityController) M7820 A11 with optional RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1 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-0640-2010 and BSI-DSZ-CC-0640-2010-MA-01.

The change to the certified product is at the level of the included production and delivery sites, a change that has no effect on assurance. No changes of hardware or IC dedicated software are applied, the TOE version did not change. The changes are related to include additional production and delivery sites already evaluated in the scope of the certification procedure BSI-DSZ-CC-0757.

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-0640-2010 dated 28 July 2010 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-0640-2010.

Bonn, 8 August 2011

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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 [4] and the Evaluation Technical Report as outlined in [7].

The vendor for the Infineon Technologies Smart Card IC (SecurityController) M7820 A11 with optional RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1 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 Technologies Smart Card IC (SecurityController) M7820 A11 with optional RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1 libraries and with specific IC dedicated software was changed due to included production and delivery sites. The configuration management [5] has not been changed. The certified product itself did not change. The changes are related to included production and delivery sites.

The changes are related to including an additional production and delivery sites already evaluated into the scope of the certification procedure BSI-DSZ-CC-0757. 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 following included sites:

Site	Address	Function
Munich	Giesecke & Devrient GmbH Distribution Center DLC Prinzregentenstraße 159 81677 Munich Germany	Distribution Center
Reichshof-Wehnrath	Smartrac Technology Germany Building RW2 Gewerbeparkstr. 10 51580 Reichshof-Wehnrath Germany	Inlay antenna mounting Delivery

Conclusion

The change to the TOE is at the level of the included production and delivery sites. The change has no effect on assurance. Examination of the evidence indicates that changes required are limited to inclusion of the additional production and delivery sites. 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 statement as outlined in the Certification Report BSI-DSZ-CC-0640-2010 dated 28 July 2010 is of relevance and has to be considered when using the product.

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 one year 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 Section 9, Para. 4, Clause 2).

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

References

[1] Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Impact Analysis M7820 A11 BSI-DSZ-CC-0640-2010 including optional Software Libraries RSA - EC - SHA-2 – Toolbox Version 0.2, 2011-07-04 (confidential document)

[3] Certification Report BSI-DSZ-CC-0640-2010 for Infineon Technologies Smart Card IC (SecurityController) M7820 A11 with optional RSA2048/4096v1.1.18, EC v1.1.18 and SHA-2 v1.1 libraries andwith specific IC dedicated softwarefromInfineon, Bundesamt für Sicherheit in der Informationstechnik, 28 July 2010

[4] Security Target Security M7820 A11 Maintenance including optional Software Libraries RSA–EC–SHA-2, Version 0.7 from 2010-08-11, Infineon Technologies AG

[5] a) Document Reference M7820 A11 including optional Software Libraries RSA–EC – SHA-2, version 0.4, 2010-07-26
b) Configuration Management Scope M7820 A11 including optional SoftwareLibraries RSA v1.0 – EC v1.0 –- SHA-2 v1.0, version 1.3 from 2010-06-10, Infineon Technologies AG (confidential document)

[6] ETR for composite evaluation according to AIS 36 for the Product SLE78CLXxxxP/M/PS / M7820 A11, Version 4 from 2010-07-26, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)

[7] Evaluation Technical Report, SLE78CLXxxxP/M/PS / M7820 A11, Version 4 from 2010-07-26, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)