Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0757-2011-MA-01

Infineon Technologies SmartCard IC (Security Controller) M7793 A12 with optional RSA v1.02.010, EC v1.02.010 and Toolbox v1.02.010 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-0757-2011 updated by a re-assessment on 06 February 2012.

The changes to the certified product are at the level of a non security relevant firmware improvement, editorial update of user documentation and included production and delivery sites, the changes that have no effect on assurance. No changes of hardware are applied.

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-0757-2011 dated 28 September 2011 updated by a re-assessment on 06 February 2012 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-0757-2011.

Bonn, 21 February 2012

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 and the Evaluation Technical Report as outlined in [3].

The vendor for the Infineon Technologies SmartCard IC (Security Controller) M7793 A12 with optional RSA v1.02.010, EC v1.02.010 and Toolbox v1.02.010 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 SmartCard IC (Security Controller) M7793 A12 with optional RSA v1.02.010, EC v1.02.010 and Toolbox v1.02.010 libraries and with specific IC-dedicated software, was changed due to a minor non-security relevant firmware improvement, editorial update of user documentation [7] and included production and delivery sites. No changes of hardware are applied. The firmware improvement leads to a change in RMS and flashloader version. The flashloader version is changed due to infrastructure related constraints. The content of the flashloader remains unchanged. The RMS version changes from V7790b0118 and Overall patch v7032 to V7790b0118 and Overall Patch v7048. The flashloader patch version changed from 3.93.003 to 3.93.004. Due to the change of the certified product the configuration management changed from version 1.5 to 1.7. The ST Lite changed from version 2.0 to 2.1.

The changes are related to including an additional production and delivery sites already evaluated into the scope of the certification procedure BSI-DSZ-CC-0786-2012. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)
are fulfilled for the following included sites:

Sites	Address	Function
Bangkok – SmarTrac covered by BSI-DSZ-CC-S-0007-2011	Smartrac Technology Ltd., 142/121/115 Moo, Hi-Tech industrial Estate, Tambon Ban Laean, Amphor Bang-Pa-In, 13160 Ayutthaya, Thailand	Inlay antenna mounting
Chanhassen	Smartrac Technology US Inc. 1546 Lake Drive West Chanhassen, MN 55317 USA	Inlay antenna mounting
Ranzan - Toppan	Toppan Printing Co., Ltd. 6-2, Hanami-Dai, Ranzan-Machi, Hiki-Gun Saitama 355-0204 Japan	Inlay antenna mounting
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	Inlay antenna mounting
Hsinchu - ARDT	Ardentec Corporation No. 3, Gungye 3rd Rd., Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien, Taiwan 30351, R.O.C. Taiwan 30351, R.O.C.	Wafer Testing

Conclusion

The change to the certified product is at the level of a non security relevant firmware improvement, editorial update of user documentation and included production and delivery sites, the changes that have no effect on assurance. No changes of hardware are applied. Due to the change of the certified product the ST [4] and ST Lite [6] changed from version 2.0 to 2.1. As a result of the changes the configuration list for the TOE has been updated [5].

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-0757-2011 dated 28 September 2011 updated by a re-assessment on 06 February 2012 is of relevance and has to be considered when using the product. As a result of this re-assessment, 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 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[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 CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Impact Analysis M7793 A12, BSI-DSZ-CC-0757-2011 including optional Software Libraries, RSA - EC – Toolbox, version 1.2, 2012-01-16 (confidential document)

[3] Certification Report BSI-DSZ-CC-0757-2011 for Infineon Technologies SmartCard IC (Security Controller) M7793 A12 with optional RSA v1.02.010, EC v1.02.010 and Toolbox v1.02.010 libraries and with specific IC-dedicated software, Bundesamt für Sicherheit in der Informationstechnik, 28 September 2011

[4] Security Target, BSI-DSZ-CC-0757, M7793 A12 including optional Software Libraries RSA – EC – Toolbox, version 2.1, 2011-12-15, Infineon Technologies AG (confidential document)

[5] Configuration Management Scope M7793 A12 including optional Software Libraries RSA – EC – Toolbox, version 1.7, 2012-01-09, Infineon Technologies AG (confidential document)

[6] Security Target Lite, BSI-DSZ-CC-0757, M7793 A12 including optional Software Libraries RSA – EC – Toolbox, version 2.1, 2011-12-15, Infineon Technologies AG (sanitized public document)

[7] Slx 77FXxxxP (M7793) Security Guidelines User's Manual, dated 2011-12-12

[8] ETR for composite evaluation according to AIS 36 for the Product M7793 A12, version 3, 2012-01-27, TÜV Informationstechnik GmbH, Evaluation Body for IT Security (confidential document)

[9] Evaluation Technical Report, M7793 A12, version 3, 2012-01-27, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)