Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0640-2010-MA-01

Infineon Technologies Smart Card IC (Security Controller) 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

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 BS BSI-DSZ-CC-0640-2010.

The change to the certified product is at the level of additional ways how user data are programmed into the TOE within the secure environment, those changes have no effect on assurance. The TOE itself did not change.

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, the assurance as outlined in the Certification Report BS BSI-DSZ-CC-0640-2010 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BS BSI-DSZ-CC-0640-2010.

Bonn, 30 August 2010

Common Criteria

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], the Security Target [4] and the Evaluation Technical Report as outlined in [5].

The vendor for the Infineon Technologies Smart Card IC (Security Controller) 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 (Security Controller) 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 additional ways how user data are programmed into the TOE within the secure environment of Infineon Technologies. The TOE itself did not change. This is just about new combinations of already certified ways user data will take. It turned out that there are further cases which have to be included.

Therefore, the complete combination ways for user data are listed below:

1	The user or/and a subcontractor downloads the software into the EEPROM flash memory on his own. Infineon Technologies has not received user software and there are no user data in the ROM.	The Flash Loader (FL) can be activated or reactivated by the user or subcontractor to download his software in the EEPROM flash memory.
2	The user provides software for the download into the EEPROM flash memory to Infineon Technologies AG. The software is downloaded to the EEPROM flash memory during chip production. I.e. there are no user data in the ROM.	There is no FL present.

3	The user provides software for the download into the EEPROM flash memory to Infineon Technologies AG. The software is downloaded to the EEPROM flash memory during chip production. I.e. there are no user data in the ROM.	The FL is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the EEPROM flash memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.
4	The user provides the software for implementation into the ROM mask.	There is no FL present.
5	The user provides the software for implementation into the ROM mask.	The FL is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the EEPROM flash memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.
6	The user provides the software for implementation into the ROM mask and provides software for the download into the EEPROM flash memory to Infineon Technologies.	There is no FL present.
7	The user provides the software for implementation into the ROM mask and provides software for the download into the EEPROM flash memory to Infineon Technologies.	The FL is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the EEPROM flash memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.

Table 1: Combination of user data

Conclusion

The change to the TOE is at the level of additional ways how user data are programmed into the TOE within the secure environment, those changes that have no effect on assurance. The TOE itself did not change. Examination of the evidence indicates that the changes performed are limited to the The Security Target [4]. The Security Target was editorially updated [4]. 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.

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 composition as listed above can usually be used for composite evaluations building on top, as long as the ETR for composition document 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 including optional Software Libraries RSA-EC-SHA-2 Version 0.1, 2010-08-11 (confidential document)

[3] Certification BSI-DSZ-CC-0640-2010 for Infineon Technologies Smart Card IC (Security Controller) 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, Bundesamt für Sicherheit in der Informationstechnik, 28 July 2010

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

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