Assurance Continuity Maintenance Report

BSI-DSZ-CC-0593-2009-MA-01

Infineon Smart Card IC (Security Controller)
SLE66CLX206PEM / m2084-a12,
SLE66CLX206PE / m2085-a12,
SLE66CLX206PES / m2086-a12,
SLE66CDX206PEM / m2099-a12,
SLE66CLX203PEM / m2098-a12,
SLE66CLX207PEM / m2980-a12,
SLE66CLX207PE / m2981-a12,
SLE66CLX207PES / m2982-a12,
SLE66CLX126PEM / m2087-a12,
SLE66CLX126PE / m2088-a12,
SLE66CLX126PES / m2089-a12,
SLE66CLX127PEM / m2997-a12,
SLE66CLX127PE / m2998-a12,
SLE66CLX127PES / m2999-a12,
all with optional libraries RSA V1.6, EC V1.1,
SHA-2 V1.0 and all with specific IC dedicated
software

from

Common Criteria Recognition
Arrangement
for components up to EAL4

Infineon Technologies AG

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-0593-2009.

The change to the certified product is at the level of the improvement in the TOE firmware (Mifare component), a change that 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.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0593-2009 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 BSI-DSZ-CC-0593-2009.

Bonn, 8 June 2009

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 Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a12, SLE66CLX206PE / m2085-a12, SLE66CLX206PES / m2086-a12, SLE66CDX206PEM / m2099-a12, SLE66CLX203PEM / m2098-a12, SLE66CLX207PEM / m2980-a12, SLE66CLX207PE / m2981-a12, SLE66CLX207PES / m2982-a12, SLE66CLX126PEM / m2087-a12, SLE66CLX126PE / m2088-a12, SLE66CLX126PES / m2089-a12, SLE66CLX127PEM / m2997-a12, SLE66CLX127PE / m2998-a12, SLE66CLX127PES / m2999-a12, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all 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) SLE66CLX206PEM / m2084-a12, SLE66CLX206PE / m2085-a12, SLE66CLX206PES / m2086-a12, SLE66CDX206PEM / m2099-a12, SLE66CLX203PEM / m2098-a12, SLE66CLX207PEM / m2980-a12, SLE66CLX207PE / m2981-a12, SLE66CLX207PES / m2982-a12, SLE66CLX126PEM / m2087-a12, SLE66CLX126PE / m2088-a12, SLE66CLX126PES / m2089-a12, SLE66CLX127PEM / m2997-a12, SLE66CLX127PE / m2998-a12, SLE66CLX127PES / m2999-a12, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software was changed due to improvement of the TOE firmware (Mifare component). All changes are minor firmware (Mifare) changes only. The change is considered by new versions of the Configuration Management Scope Documentation [6]. The change is not significant from the standpoint of security, however Configuration Management procedures required a change in the version number from a11 to a12 and the RMS library version from RMS_E V07 to RMS_E V07_09.

Conclusion

The change to the certified product is at the level of the improvement in the minor Mifare software, a change that has no effect on assurance. Examination of the evidence indicates that the changes performed are limited to the Mifare part of the RMS library. The Security Target [4] is still valid for the changed 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. 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 4, Para. 3, Clause 2). In addition to the baseline certificate BSI notes, that cryptographic functions 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). This report is an addendum to the Certification Report [3].

References

[1]   Common Criteria document CCIMB-2004-02-009 "Assuarance Continuity: CCRA Requirements", Version 1.0, February 2004

[2]   Impact Analysis, Chipcard and Security ICs, SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6 and ECC V1.1 and SHA-2 V1.0, Version 1.0 from 2009-05-25, Infineon AG (confidential document)

[3]   Certification Report BSI-DSZ-CC-0593-2009 for Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11,all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik, 8 May 2009

[4]   Security Target SLE66CLX206PEM / m2084-a11SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11SLE66CLX127PE / m2998-a11SLE66CLX127PES / m2999-a11 all with optional libraries RSA V1.6, EC V1.1 and SHA-2, V1.0, Version 1.4 from 2009-03-05, Infineon AG

[5]   Evaluation Technical Report – Summary (ETR SUMMARY), SLE66CLX206PEM / m2084-a11SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11 all with optional libraries RSA V1.6, EC V1.1 and SHA-2 V1.0, Version 2 from 2009-04-09, Evaluation Body for IT Security of TÜV Informationstechnik GmbH (confidential document)

[6]   Configuration Management Scope, Security and Chipcard ICs,
       SLE66CLX206PEM / m2084-a12, SLE66CLX206PE / m2085-a12,
       SLE66CLX206PES / m2086-a12, SLE66CDX206PEM / m2099-a12,
       SLE66CLX203PEM / m2098-a12,   SLE66CLX207PEM / m2980-a12,
       SLE66CLX207PE / m2981-a12, SLE66CLX207PES / m2982-a12,
       SLE66CLX126PEM / m2087-a12, SLE66CLX126PE / m2088-a12,
       SLE66CLX126PES / m2089-a12, SLE66CLX127PEM / m2997-a12,
       SLE66CLX127PE / m2998-a12, SLE66CLX127PES / m2999-a12, All with optional
       libraries RSA V1.6 and ECC V1.1 and SHA-2 V1.0, Version 1.1 from
       2009-05-26, Infineon Technologies AG (confidential document)