Assurance Continuity Maintenance Report

BSI-DSZ-CC-0482-2008-MA-05

Infineon Smart Card IC (Security Controller)
SLE66CLX800PE / m1581-e13/a14,
SLE66CLX800PEM / m1580-e13/a14,
SLE66CLX800PES / m1582-e13/a14,
SLE66CX800PE / m1599-e13/a14,
SLE66CLX360PE / m1587-e13/a14,
SLE66CLX360PEM / m1588-e13/a14,
SLE66CLX360PES / m1589-e13/a14,
SLE66CLX180PE /m2080-a14,
SLE66CLX180PEM / m2081-a14,
SLE66CLX120PE / m2082-a14,
SLE66CLX120PEM / m2083-a14 all with optional
libraries RSA V1.5 and ECC V1.1 and all 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 BSI-DSZ-CC-0482-2008.

The change to the certified product is at the level of minor editorial changes of the Security Target. The TOE 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 BSI-DSZ-CC-0482-2008 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-0482-2008.

Common Criteria

Bonn, 15 April 2009

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) SLE66CLX800PE / m1581-e13/a14, SLE66CLX800PEM / m1580-e13/a14, SLE66CLX800PES / m1582-e13/a14, SLE66CX800PE / m1599-e13/a14, SLE66CLX360PE / m1587-e13/a14, SLE66CLX360PEM / m1588-e13/a14, SLE66CLX360PES / m1589-e13/a14, SLE66CLX180PE /m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX120PEM / m2083-a14 all with optional libraries RSA V1.5 and ECC V1.1 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) SLE66CLX800PE / m1581-e13/a14, SLE66CLX800PEM / m1580-e13/a14, SLE66CLX800PES / m1582-e13/a14, SLE66CX800PE / m1599-e13/a14, SLE66CLX360PE / m1587-e13/a14, SLE66CLX360PEM / m1588-e13/a14, SLE66CLX360PES / m1589-e13/a14, SLE66CLX180PE /m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX120PEM / m2083-a14 all with optional libraries RSA V1.5 and ECC V1.1 and all with specific IC dedicated software did not change. The Security Target is updated to version 1.3.

Conclusion

The change to the certified product is at the level of minor editorial changes of the Security Target. 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, SLE66CLX800PE m1581 e13 a14, SLE66CLX800PEM m1580 e13/a14, SLE66CLX800PES m1582 e13/a14, SLE66CX800PE* m1599 e13/a14, SLE66CLX360PE m1587 e13/a14, SLE66CLX360PEM m1588 e13/a14, SLE66CLX360PES m1589 e13/a14, SLE66CLX180PE m2080 a14, SLE66CLX180PE M m2081 a14, SLE66CLX120PE m2082 a14, SLE66CLX120PE M m2083 a14, Version 1.0, 2009-03-18, Infineon Technologies AG, (confidential document)

[3]   Certification Report BSI-DSZ-CC-0482-2008 for SLE66CLX800PE / m1581-e13/a14, SLE66CLX800PEM / m1580-e13/a14, SLE66CLX800PES / m1582-e13/a14, SLE66CX800PE / m1599-e13/a14, SLE66CLX360PE / m1587-e13/a14, SLE66CLX360PEM / m1588-e13/a14, SLE66CLX360PES / m1589-e13/a14, SLE66CLX180PE / m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX120PEM / m2083-a14, all optional with RSA2048 V1.5 and ECC V1.1 and all with specific IC dedicated software from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik, 27 Mai 2008

[4]   Security Target BSI-DSZ-CC-0482, SLE66CLX800PE m1581 e13 a14, SLE66CLX800PEM m1580 e13/a14, SLE66CLX800PES m1582 e13/a14, SLE66CX800PE* m1599 e13/a14, SLE66CLX360PE m1587 e13/a14, SLE66CLX360PEM m1588 e13/a14, SLE66CLX360PES m1589 e13/a14, SLE66CLX180PE m2080 a14, SLE66CLX180PE M m2081 a14, SLE66CLX120PE m2082 a14, SLE66CLX120PE M m2083 a14, all optional with RSA2048 V1.5 and ECC V1.1, Version 1.3, 2008-03-18, Infineon Technologies AG

[5]   Evaluation Technical Report, Version 1, 2008-03-11, 8103819623 / BSI-DSZ-CC-0482, Product: SLE66CLX800PE / m1581-e13/a14, SLE66CLX800PEM / m1580-e13/a14, SLE66CLX800PES / m1582-e13/a14, SLE66CX800PE / m1599-e13/a14, SLE66CLX360PE / m1587-e13/a14, SLE66CLX360PEM / m1588-e13/a14, SLE66CLX360PES / m1589-e13/a14, SLE66CLX180PE / m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX120PEM / m2083-a14, all optional with RSA2048 V1.5 and ECC, TÜViT (confidential document)