Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0487-2009-MA-01

NXP Mifare DESFire8 MF3ICD81 V0C/004 Secure SmartCard Controller with Embedded Software

from

NXP Semiconductors Germany GmbH

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-0487-2009.

The change to the certified product is the inclusion of an additional site for wafertest and -treatment, a change that has no effect on assurance. 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-0487-2009 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-0487-2009.

Bonn, 4 December 2009

Common Criteria

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], the Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the NXP Mifare DESFire8 MF3ICD81 V0C/004 Secure SmartCard Controller with Embedded Software, NXP Semiconductors Germany GmbH, 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 Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for all audited sites of the TOE including the additional site for wafertest and -treatment NXP Semiconductors Thailand (APB):

NXP Semiconductors (Thailand)

Assembly Plant Bangkok

303 Chaengwattana Rd.

Laksi, Bangkok 10210

Thailand

The NXP Mifare DESFire8 MF3ICD81 V0C/004 Secure SmartCard Controller with Embedded Software was changed due to an additional site for wafertest and -treatment. The TOE did not change. The change is not significant from the standpoint of security.

Conclusion

The change to the TOE is at the level of an additional site for wafertest and -treatment, a change that has no effect on assurance. The TOE did not change.

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 9, Para. 4, Clause 2). 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] Mifare DESFire8 MF3ICD81, Impact Analysis Report, Rev. 1.2 — June 16, 2009 (confidential document)

[3] Certification Report BSI-DSZ-CC-0487-2009 for NXP Mifare DESFire8 MF3ICD81 V0C/004 Secure SmartCard Controller with Embedded Software, 1 April 2009, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target Lite, MF3ICD81 Contactless Multi-Application IC with DES/3DES and AES Security, NXP Semiconductors, Rev. 1.1, 10 October 2008 (sanitised public document)