



Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0620-2010-MA-01

NXP MIFARE Plus MF1SPLUSx0y1

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-0620-2010.

The change to the certified product is at the level of a modification of the VSS pad layout in connection with the nameplate update, type identifier renaming and incrementation, and document update. The changes have 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-0620-2010 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 BSI-DSZ-CC-0620-2010.

Bonn, 30 August 2010



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 the Certification Report [3].

The vendor for the NXP MIFARE Plus MF1SPLUSx0y1, 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 NXP MIFARE Plus MF1SPLUSx0y1 was changed due to an NXP internal design rule that required the connection of the IC internal GND level to be moved to a different location to solve production problems for specific customers. In order to make the new hardware version unique and traceable, the layout nameplate was updated. Furthermore, the type identifier has been renamed from “SW-version” to “product version” and has been incremented. All documents using the expression “type identifier” have been updated. The changes affect a number of documents, namely the Security Target [4], the Security Target Lite [7], the User Guidance Manual [6], the Product Datasheet [8], and the Configuration List [5]. The changes are not significant from the standpoint of security, however Configuration Management procedures require a change in the version number, therefore the name plate was updated and the type identifier was updated from MF1SPLUSx0y1Dpp/I2 to MF1SPLUSx0y1Dpp/I3.

Conclusion

The change to the TOE is at the level of a modification of the VSS pad layout in connection with the nameplate update, type identifier renaming and incrementation, and document update. These are changes that have no effect on assurance. Examination of the evidence indicates that the changes performed are limited to the modification of the VSS pad layout in connection with the nameplate update, type identifier renaming and incrementation, and document update of the TOE. The Security Target [4] and [7] was editorially updated. 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 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 or her system risk management process. In order for the evolution of attack methods and techniques to be covered, he or she should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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 Report, MIFARE Plus MF1SPLUSx0y1, NXP Semiconductors, Business Line Identification, Rev. 1.1, 20 August 2010 (confidential document)
- [3] Certification Report BSI-DSZ-CC-0620-2010, NXP MIFARE Plus MF1SPLUSx0y1, Bundesamt für Sicherheit in der Informationstechnik, 17 February 2010
- [4] Security Target, MF1SPLUSx0y1, NXP Semiconductors, Revision 1.2, 14 May 2010 (confidential document)
- [5] Configuration List, MF1PLUSx0y1 and MF1SPLUSx0y1, NXP Semiconductors, Revision 1.8, 17 August 2010 (confidential document)
- [6] Guidance, Delivery and Operation Manual, MF1SPLUSx0y1, NXP Semiconductors, Revision 1.4, 17 August 2010
- [7] ST-lite, BSI-DSZ-CC-0620, MIFARE Plus MF1SPLUSx0y1, NXP Semiconductors, Revision 1.2, 14 May 2010
- [8] MF1SPLUSx0y1 Product Data Sheet, Mainstream contactless smart card IC for fast and easy solution development, NXP Semiconductors, Revision 3.2, 17 August 2010