

## Assurance Continuity Maintenance Report

### MF3D(H)x3

Sponsor and developer: **NXP Semiconductors Germany GmbH**  
Tropowitzstrasse 20  
22529 Hamburg  
Germany

Evaluation facility: **Brightsight**  
Brassersplein 2  
2612 CT Delft  
The Netherlands

Report number: **NSCIB-CC-0011955-MA**

Report version: **1**

Project number: **0011955**

Author(s): **Denise Cater**

Date: **10 June 2020**

Number of pages: **5**

Number of appendices: **0**



*Reproduction of this report is authorized provided the report is reproduced in its entirety.*

## **CONTENTS:**

<b>1 Summary</b>	<b>3</b>
<b>2 Assessment</b>	<b>4</b>
2.1 Introduction	4
2.2 Description of Changes	4
<b>3 Conclusion</b>	<b>5</b>
<b>4 Bibliography</b>	<b>5</b>

## 1 Summary

The IT product identified in this report was assessed according to the Assurance Continuity: CCRA Requirements [AC], the developer's Impact Analysis Report [IAR] and evaluator's IAR Analysis [IA]. The baseline for this assessment was the Certification Report [CR], the Security Target and the Evaluation Technical Report of the product certified by the NSCIB under NSCIB-CC-20-0011955.

The changes to the certified product are related to minor changes in the firmware and MIFARE DESFire Software components not impacting the security functionality of the certified product. The identification of the maintained product is modified to MF3D(H)x3 in combination with the Production week and year, as detailed in guidance document [WAFER-DF] section 4.1.

Consideration of the nature of the changes leads to the conclusion that they can be classified as minor changes and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance as outlined in the Certification Report [CR] is maintained for the new version of the product.

This report is an addendum to the Certification Report NSCIB-CC-0011955-CR [CR] and reproduction is authorised provided the report is reproduced in its entirety.

## 2 Assessment

### 2.1 Introduction

The IT product identified in this report was assessed according to the Assurance Continuity: CCRA Requirements [AC], the developer's Impact Analysis Report [IAR] and evaluator's IAR Analysis [IA]. The baseline for this assessment was the Certification Report [CR], the Security Target and the Evaluation Technical Report of the product certified by the NSCIB under NSCIB-CC-20-0011955.

On 20 May 2020 NXP Semiconductors Germany GmbH submitted a request for assurance maintenance for the MF3D(H)x3.

NSCIB has assessed the [IAR] according to the requirements outlined in the document Assurance Continuity: CCRA Requirements [AC].

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.

This is supported by the evaluator's IAR Analysis [IA].

### 2.2 Description of Changes

The TOE is Secure Smart Card Controller to be used with Proximity Coupling Devices (also called "terminal") according to ISO 14443 Type A. It is primarily designed for secure contactless transport applications and related loyalty programs as well as access control management systems as well as closed loop payment systems. The TOE is a smart card comprising a hardware platform and a fixed software package.

The changes to the certified product as described in the [IAR] are updates to the firmware and MIFARE DESFire Software components classified by developer [IAR] and original evaluator [IA] as minor changes with no impact on security.

The TOE identifier, MF3D(H)x3, is unchanged as the updated firmware and MIFARE DESFire Software components are injected in the NVM during production. Hence the modified portion of the TOE identifier is reflected by the Production week and year obtained through the GetVersion command issued as detailed in the (updated) guidance document [WAFER-DF] section 4.1.

The configuration list for the TOE has been updated as a result of the changes to include the updated Security Target [ST] and guidance documentation.

### 3 Conclusion

Consideration of the nature of the changes leads to the conclusion that they can be classified as minor changes and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance as outlined in the Certification Report [CR] is maintained for this version of the product.

### 4 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

- [AC] Assurance Continuity: CCRA Requirements, 2012-06-01, Version 2.1, June 2012.
- [CR] Certification Report MF3D(H)x3, NSCIB-CC-0011955-CR, version 1 16 April 2020.
- [DS-DF] MF3D(H)x3 MIFARE DESFire EV3 contactless smartcard IC, Preliminary data sheet, Rev. 3.0, 4 May 2020.
- [DS-DF-MFC] MF3D(H)x3C MIFARE DESFire EV3C contactless smartcard IC, Product data sheet, Rev. 3.0, 4 May 2020.
- [IA] Analysis Report of ROM 4 Patches for the NXP "MF3D(H)x3", 20-RPT-555, version 1.0, 5 June 2020.
- [IAR] MF3D(H)x3 ROM 4 Patches, Rev. 0.2, 2 June 2020 (confidential document)
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
- [ST] MF3D(H)x3 Security Target, Version 2.1, 2 June 2020.
- [ST-Lite] Security Target Lite, MF3D(H)x3, Rev. 2.0, 5 June 2020.
- [WAFER-DF] MF3D(H)x3 Wafer and Delivery Specification, 580830, Rev 3.0, 15 May 2020.

(This is the end of this report).