TÜVRheinland®
Precisely Right.

Assurance Continuity Maintenance Report

JCOP 4 P71

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-180212-MA**
Report version:	**1**
Project number:	**180212**
Author(s):	**Denise Cater**
Date:	**23 December 2019**
Number of pages:	5
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

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-19-180212.

The changes to the certified product are related to minor changes in the guidance not impacting the security functionality of the certified product. The identification (JCOP 4 P71) of the maintained product is unchanged.

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-180212-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-19-180212.

On 30 November 2019 NXP Semiconductors Germany GmbH submitted a request for assurance maintenance for the JCOP 4 P71.

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, referred to as JCOP 4 P71, consists of the Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The JCOP 4 Operating System (JCOP 4 OS) consists of the software stack without the Crypto Library (Crypto Lib) and without the Micro Controller Firmware (MC FW). The TOE uses one or more communication interfaces to communicate with its environment. The original evaluation of the TOE was conducted as a composite evaluation and used the results of the CC evaluation of the underlying hardware certified as described in *[HW CERT]*.

The changes to the certified product as described in the *[IAR]* are only related to minor updates to guidance documentation. This update to the guidance was classified by developer *[IAR]* and original evaluator *[IA]* as minor changes with no impact on security.

There are no changes in the software component of the TOE.

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

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 JCOP 4 P71, NSCIB-CC-180212-CR, 23 July 2019
[ETRfc]	Evaluation Technical Report for Composition NXP “JCOP 4 P71” – EAL6+, 19-RPT-177, v3.0, 23 December 2019
[IA]	Analysis Report of IAR on “JCOP 4 P71”, 19-RPT-1085, version 2.0, 20 December 2019
[IAR]	JCOP 4 P71 Impact Analysis Report for JCOP 4 P71 Maintenance, Rev. 1.0, 02 December 2019 (confidential document)
[HW-CERT]	Certification Report, BSI-DSZ-CC-1040-2019, NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors Germany GmbH, v1.0
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[ST]	JCOP 4 P71, Security Target for JCOP 4 P71 / SE050, Rev. 3.4.1, 27 November 2019.
[ST-Lite]	JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050, Rev. 3.4.1, 27 November 2019

(This is the end of this report).