

## Assurance Continuity Maintenance Report

### JCOP 4.5 P71

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

Evaluation facility: **SGS Brightsight B.V.**  
Brassersplein 2  
2612 CT Delft  
The Netherlands

Report number: **NSCIB-CC-0313985-MA**

Report version: **1**

Project number: **0313985\_1m1**

Author(s): **Denise Cater**

Date: **04 January 2023**

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 assessment [EA]. 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 CC-22-0313985.

The changes to the certified product are related to update of the TOE guidance in [UG] and maintenance of the underlying hardware without change of the software. The identification of the maintained product is unchanged, and remains as JCOP 4.5 P71.

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-0313985-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 assessment [EA]. 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 CC-22-0313985.

On 04 November 2022 NXP Semiconductors Germany GmbH submitted a request for assurance maintenance for the JCOP 4.5 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 assessment [EA].

### 2.2 Description of Changes

The TOE is a Java Card with a GP Framework, It is a composite product consisting of a certified Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. 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 additional usage in combination with the updated hardware that has been certified in a maintenance procedure of the hardware [HW-MA]. The update to the hardware was classified as minor changes with no impact on security.

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

The updates to the TOE guidance in [UG] were classified by developer [IAR] and original evaluator [EA] as minor changes with no impact on security.

The configuration list for the TOE has been updated as a result of the changes to include the updated Security Target [ST] and [ST-Lite] to reflect the update to the underlying hardware.

### 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
[UG]	User manual for JCOP 4.5 P71, Rev. 1.7, 13 October 2022
[CR]	Certification Report JCOP 4.5 P71, NSCIB-CC-0313985-CR, v1, 02 August 2022
[EA]	Partial ETR JCOP4.5 P71– Partial ETR, 22-RPT-1374, v3.0, 22 December 2022
[IAR]	Impact Analysis Report for JCOP 4.5 P71 Maintenance, Rev. 1.1, 02 December 2022
[HW-CERT]	Certification Report, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1149-2022
[HW-MA]	Assurance Continuity Maintenance Report BSI-DSZ-CC-1149-2022-MA-01 NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2), 30 November 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	JCOP 4.5 P71 Security Target, Rev. 1.7, 15 December 2022
[ST-Lite]	JCOP 4.5 P71 Security Target Lite, Rev. 1.5, 27 October 2022

(This is the end of this report).