Assurance Continuity Maintenance Report

NXP JCOP 6.2 on SN220 Secure Element

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Business Unit Security & Connectivity
Troplowitzstrasse 20
22529 Hamburg
Germany

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

Report number: **NSCIB-CC-0428888-MA**

Report version: **1**

Project number: **0428888-1m1**

Author(s): **Wim Ton & Jordi Mujal**

Date: **12 April 2022**

Number of pages: **5**

Number of appendices: **0**

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 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-21-0428888.

The changes to the certified product are related to minor changes in the software not impacting the security functionality of the certified product. The identification of the maintained product remains as NXP JCOP 6.2 on SN220 Secure Element, and the configuration "JCOP 6.2 R1.02.1" has been added.

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-0428888-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-21-0428888.

On 21 February 2022 NXP Semiconductors *Germany GmbH* submitted a request for assurance maintenance for the NXP JCOP 6.2 on SN220 Secure Element.

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 GP functionality, extended with eUICC and CSP functionality. It can be used to load, install, instantiate and execute off-card verified Java Card applets. The eUICC part is a UICC embedded in a consumer device and may be in a removable form factor or otherwise. It connects to a given mobile network, by means of its currently enabled MNO profile. The CSP part offers Cryptographic Service Provider functionality

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]* and [EA] consist of:

- The addition of a new TOE configuration "JCOP 6.2 R1.02.1" with the associated changes:
  - Update of the guidance documents (*[AGD_AS]*, *[AGD_CSP]*, *[AGD_eUICC]* and *[AGD_UGM]*)
  - Changes of the JCOP, eUICC and the eUICC plugin

The updates to the software 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].*

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
[AGD_AS]	NXP JCOP 6.2 R1.02.1, AMD I SEMS Application User Manual Addendum, Rev. 1.1, 03 March 2022
[AGD_CSP]	NXP JCOP 6.2 R1.02.1, CSP User Manual Addendum, Rev.1.1, 03 March 2022
[AGD_eUICC]	NXP JCOP 6.2 R1 eUICC Profile Package Interpreter Guide, Rev.1.2, 03 February 2022
[AGD_UGM]	NXP JCOP 6.2 R1.02.1, User Guidance Manual, Rev. 1.1, 03 February 2022
[CR]	Certification Report NXP JCOP 6.2 on SN220 Secure Element, NSCIB-CC-0428888-CR, version 2, 02 November 2021
[EA]	Evaluator Assessment of Changes Report (EAR) JCOP 6.2 on SN220 –Partial ETR, 22-RPT-105, version 4.0, dated 30 March 2022
[IAR]	JCOP 6.2 R1.02.01 on SN220 CC Impact Analysis Report, Rev. 1.0, 4 February 2022
[HW-CERT]	CC-21-0258298 SN220 Series – Secure Element with Crypto Library SN220 SE B0.1 C13
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	NXP JCOP 6.2 on SN220 Secure Element, Security Target, Rev. 1.2, 03 March 2022
[ST-Lite]	NXP JCOP 6.2 on SN220 Secure Element, Security Target Lite, Rev. 1.1, 03 March 2022

(This is the end of this report).