

Assurance Continuity Maintenance Report

NXP JCOP 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1, R5.02.1

Sponsor and developer: **NXP Semiconductors GmbH**
Business Unit Security & Connectivity
Beiersdorfstraße 12
22529 Hamburg
Germany

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

Report number: **NSCIB-CC-2300174-01-MA1**

Report version: **1**

Project number: **NSCIB-2300174-01-MA1**

Author(s): **Kjartan Jæger Kvassnes**

Date: **30 June 2024**

Number of pages: **5**

Number of appendices: **0**



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



CONTENTS:

1 Summary	3
2 Assessment	4
2.1 Introduction	4
2.2 Description of Changes	4
3 Conclusion	5
4 Bibliography	5

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 under NSCIB, reference NSCIB-CC-2300174-01.

The changes to the certified product are related to a minor change in the software not impacting the security functionality of the certified product.

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-2300174-01-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]. delete if no evaluator activity has been performed. 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-2300174-01.

On 11 December 2023 NXP Semiconductors 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] include the addition of a new TOE configuration, namely the JCOP 6.2 R5.02.1. The changes that are introduced are provided in an IAR [IAR] and comprise the following:

- New ST version which includes the new JCOP 6.2 R5.02.1 variant;
- New guidance documentation is released for JCOP 6.2 R5.02.1;
- Platform Identifier Information is changed for JCOP 6.2 R5.02.1, the eUICC plugin is no longer separately identified, as it is fully integrated into the TOE (Same as R5.01.1)

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, Version 2.2, 30 September 2021
[AGD_UGM]	NXP JCOP 6.2 R5.02.1, User Guidance Manual, Rev 1.0, dated 05 March 2024
[AGD_UGMSEMS]	NXP JCOP 6.2 R5.02.1, AMD I SEMS Application User Manual Addendum, Rev 1.0, dated 06 February 2024
[AGD_CSP]	NXP. JCOP 6.2 R5.02.1, CSP User Manual Addendum, Rev 1.0, Dated 06 February 2024
[CR]	Certification Report for NXP JCOP 6.2 on SN220 Secure Element, NSCIB-CC-2300174-01-CR, issue 1, dated 17 June 2024
[EA]	Evaluator Assessment of Changes Report (EAR) NXP JCOP 6.2 on SN220 Secure Element – Partial ETR, 24-RPT-445, version 4.0, dated 21 June 2024
[IAR]	JCOP 6.2 R5 on SN220 JCOP6.2 on SN220 Secure Element, Rev.1.1, dated 18 January 2024
[HW-CERT]	Certification Report SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, version 1, dated 10 May 2024, registered under the reference NSCIB-CC-2300181-01-CR
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	NXP JCOP 6.2 on SN220 Secure Element Security Target, Rev.2.1.3, 14 June 2024
[ST-Lite]	NXP JCOP 6.2 on SN220 Secure Element Security Target Lite, Rev.2.1.3, 14 June 2024

(This is the end of this report).