Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1040-2019-MA-01

NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2)

from

NXP Semiconductors Germany GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developer's Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-1040-2019.

The change to the certified product is at the level of minor implementation aspects and guidance documentation. The identification of the maintained product is indicated by a new version number compared to the certified product.

The developer performed changes to the IC Dedicated Support Software (Firmware) component of the TOE. Changes focus on improvement of reliability and interoperability of the product in the field and addressing of bug-fixes without impacting the overall security of the product.

The nature of the changes was considered by the ITSEF Brightsight BV. The conclusion was that they are classified as minor changes with no impact on assurance 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 statement as outlined in the Certification Report BSI-DSZ-CC-1040-2019 dated 14 June 2019 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-1040-2019.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 4 March 2020

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2), NXP Semiconductors Germany GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. 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.

The NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) was changed at the level of minor implementation aspects and guidance documentation with no impact on the overall security of the product.

The developer performed changes to the IC Dedicated Support Software (Firmware) component of the TOE. Changes focus on improvement of reliability and interoperability of the product in the field and addressing of bug-fixes without impacting the overall security of the product.

The ITSEF Brightsight BV has performed an impact analysis [11] of the changes to the Certified TOE based on the IAR provided by the developer as well as taking into account evidence of the evaluation of the Certified TOE.

Based on the impact analysis, the ITSEF concluded that all changes are considered a minor change without affecting assurance evidence of the Certified TOE.

The identification of the maintained product is indicated by a new version number compared to the certified product. Therefore the version number changed from “NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library” to “NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2)”.

The Security Target was editorially updated [4]. The differentiation between the Certified TOE and the Maintained TOE is described in the Security Target [4] respectively in Table 5 and Table 6.

The Guidance documentation (data sheets) was also updated to reflect the added/patched configurations. For more details refer to [6]-[8].

Conclusion

The maintained change is at the level of minor implementation aspects and guidance documentation. The change has no effect on product assurance. As a result of the changes the configuration list for the TOE has been updated [5].

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change 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 statement as outlined in the Certification Report BSI-DSZ-CC-1040-2019 dated 14 June 2019 is of relevance and has to be considered when using the product.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [9].

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months[1] and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[2] Section 9, Para. 4, Clause 2).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] Annex C.

This report is an addendum to the Certification Report [3].

[1] In this case the eighteen month time frame is related to the date of the initial version [9] of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report, Product Update R2, NXP Secure Smart Card Controller N7121, v1.0, 15 January 2020, NXP Semiconductors (confidential document)

[3] Certification Report BSI-DSZ-CC-1040-2019 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors GmbH, 14 June 2019, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target Lite, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library, Rev. 1.3, 8 January 2020, NXP Semiconductors (sanitised public document)

[5] NXP Secure Smart Card Controller N7121, Common Criteria CIL, Evaluation documentation, Revision 1.0, 6 January 2020, NXP Semiconductors (Confidential document)

[6] MMU Configuration and NXP Firmware Interface Specification, NXP Secure Smart Card Controller N7121, 30 October 2019 Rev. 3.4, NXP Semiconductors (Confidential document)

[7] Shared OS Libraries, NXP Secure Smart Card Controller N7121, Rev. 3.2, 30 October 2019, NXP Semiconductors (Confidential document)

[8] NXP System Mode OS, NXP Secure Smart Card Controller N7121, Rev. 3.4, 30 October 2019, NXP Semiconductors (Confidential document)

[9] ETR for Composition NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (N7121), BSI-DSZ-CC-1040-2019, Version 8.0, 31 May2019, Brightsight BV (confidential document)

[10] NXP Secure Smart Card Controller N7121, Evaluation Reference List, Evaluation documentation, Revision 1.6, 8 January 2020, NXP Semiconductors (Confidential document)

[11] Analysis Report of Product Update R2 for the NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library, Version 6.0, 18 February 2020, Brightsight BV (confidential document)