



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0955-2016-MA-01

**NXP Smart Card Controller P6021y VB with IC
Dedicated Software**

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 developers 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-0955-2016.

The change to the certified product is at the level of document clarifications and functional aspects. The change has no effect on assurance. The identification of the maintained product is indicated by new respective version numbers for documents and configuration file versions.

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-0955-2016 dated 17.03.2016 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-0955-2016.

Bonn, 13 June 2016

The Federal Office for Information Security



Common Criteria
Recognition Arrangement
for components up to
EAL 4



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 P6021y VB with IC Dedicated Software, 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 P6021y VB with IC Dedicated Software was changed due to document clarifications and functional aspects. Configuration Management procedures required a change in the product identifier. Therefore respective document- and configuration file version numbers changed.

Conclusion

The change to the TOE is at the level of document clarifications and functional aspects. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The Security Target [4] is still valid for the TOE.

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.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

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-0955-2016 dated 17.03.2016 is of relevance and has to be considered when using the product.

Additional 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 [7].

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 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 BSIG¹ Section 9, Para. 4, Clause 2).

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

¹ 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] Referenz IARs (confidential documents):
NXP Secure Smart Card Controller P602xy VB, Impact Analysis Report Configuration Update RNG, Rev. 1.1 — 31 May 2016, NXP Semiconductors
NXP Secure Smart Card Controller P6021y VB, Impact Analysis Report Update Supported Package Types, Rev. 1.1 — 31 May 2016, NXP Semiconductors
- [3] Certification Report BSI-DSZ-CC-0955-2016 for NXP Secure Smart Card Controller P6021y VB including IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 17.03.2016
- [4] Security Target Lite BSI-DSZ-CC-0955-2016, Version 0.93, 2016-01-25, NXP Secure Smart Card Controller P6021y VB Security Target Lite, NXP Semiconductors (sanitised public document)
- [5] Configuration lists for the TOE:
NXP Secure Smart Card Controller P6021y VB, Configuration List - Hardware IC, Rev. 1.4 — 21 March 2016, NXP Semiconductors
NXP Secure Smart Card Controller P6021y VB, Customer specific Appendix of the Configuration List, Rev. 1.0 — 21 March 2016, NXP Semiconductors
NXP Secure Smart Card Controller P6021y VB, Appendix of the Configuration List for composite evaluation, Rev. 1.0 — 21 March 2016, NXP Semiconductors
- [6] NXP Secure Smart Card Controller P6021y VB, Evaluation Reference List, Rev. 1.60 — 06 June 2016, , NXP Semiconductors
- [7] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0955-2016, Version 3, 2016-02-12, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)