Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0824-2014-MA-01

NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 including 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-0824-2014.

The change to the certified product is at the level of configuration of the product. The change has no effect on assurance. The identification of the maintained product is indicated by an extension of the product name.

The certified product itself did not change.

The nature of the changes was considered by the ITSEF T-Systems GEI GmbH, approved by BSI. The conclusion was that they are classified as minor changes with no impact on security 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-0824-2014 dated 18 June 2014 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-0824-2014.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 16 October 2014

The Federal Office for Information Security

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

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 Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 including 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 Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 including IC Dedicated Software was changed due to improvement of yield and operational stability. Configuration Management procedures required a change in the product identifier. Therefore other product names were introduced, P61N1M3VD-1 and P61N1M3VE-1. The product will now be referenced as “NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1”.

The changes also include an update of the user guidance manual [6].

The certified product hardware itself did not change.

For formal reasons it was neccessary to provide an updated version of the ETR for comopsition [9]. No new tests were done, therefore the validity of the previous ETR for composition [8] is not extended.

Conclusion

The change to the TOE is at the level of configuration of the product. 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 was editorially updated [7].

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-0824-2014 dated 18 June 2014 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.

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.

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

References

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

[2] Impact Analysis Report, NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1, Rev. 0.3, 09. September 2014, NXP Semiconductors, Business Unit Identification (confidential document)

[3] Certification Report BSI-DSZ-CC-0824-2014 for NXP Secure Smart Card ControllerP61N1M3PVD/VE including IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 18 June 2014

[4] NXP Secure Smart Card Controller P61N1M3PVD/VE Security Target Lite, NXP Semiconductors, Business Unit Identification, Rev. 2.3, 17 October 2013 (sanitised public document)

[5] NXP Secure Smart Card Controller P61N1M3PVD/VE Appendix of the Configuration List for composite evaluation, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0824, Rev. 1.3, 2 September 2014 (confidential document) and
NXP Secure Smart Card Controller P61N1M3PVD/VE Customer specific Appendix of the Configuration List, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0824, Rev. 1.1, 29 July 2014 (confidential document) and
NXP Secure Smart Card Controller P61N1M3PVD/VE Configuration List, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0824, Rev. 1.13, 9 September 2014 (confidential document)

[6] NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 Information on Guidance and Operation, NXP Semiconductors, Business Unit Identification, Revision 1.5, Document Number 257015, 2 September 2014 (confidential document)

[7] NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE Security Target Lite, NXP Semiconductors, Business Unit Identification, Revision 2.5, 27 August 2014 (sanitised public document)

[8] ETR for composition according to AIS36, NXP P61N1M3PVD/VE, T-Systems GEI GmbH, Version 1.1, 15 May 2014 (confidential document)

[9] ETR for composition according to AIS36, NXP P61N1M3PVD/VD-1/VE-1, T-Systems GEI GmbH, Version 1.2, 30 September 2014 (confidential document)

[10] Evaluation Technical Report, NXP P61N1M3PVD/VD-1/VE-1, T-Systems GEI GmbH, Version 1.7, 30 September 2014 (confidential document)