Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0348-2006-MA-03

NXP Smart Card Controller
P5CT072V0S, P5CN072V0S, P5CC072V0S
P5CD072V0S, P5CD036V0S and P5CN036V0S
each with specific IC Dedicated Software

from

NXP Semiconductors Germany GmbH

Common Criteria Recognition
Arrangement
for components up to EAL4

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 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-0348-2006.

The change to the certified product is at the level of documentation and performance optimization, a change that has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

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, the assurance as outlined in the Certification Report BSI-DSZ-CC-0348-2006 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Reports BSI-DSZ-CC-0348-2006, BSI-DSZ-CC-0348-2006-MA-01 and BSI-DSZ-CC-0348-2006-MA-02.

Bonn, 29 June 2009

Common Criteria

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], the Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the NXP Smart Card Controller P5CT072V0S, P5CN072V0S, P5CC072V0S, P5CD072V0S, P5CD036V0S and P5CN036V0S each with specific 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 P5CT072V0S, P5CN072V0S, P5CC072V0S, P5CD072V0S, P5CD036V0S and P5CN036V0S each with specific IC Dedicated Software was changed due to:

- For identification and traceability the type identification name plate is changed from T023P to T023S.
- For performance reasons, the HF-sensor connected to the external clock pad is disabled while operating with internal clock.

The changes are not significant from the standpoint of security, however Configuration Management procedures required a change in the version number from P5CT072V0P, P5CN072V0P, P5CC072V0P, P5CD072V0P, P5CD036V0P and P5CN036V0P to P5CT072V0S, P5CN072V0S, P5CC072V0S, P5CD072V0S, P5CD036V0S and P5CN036V0S. Included are configurations introduced in the previous Maintainance process BSI-DSZ-CC-0348-2006-MA-01 P5CN072V0P and P5CN036V0P changed their version number to P5CN072V0S and P5CN036V0S.

Conclusion

The change to the TOE is at the level of documentation and performance optimization, a change that has no effect on assurance. Examination of the evidence indicates that the changes performed are limited to adapted mask layers and an update of documentation.

The Security Target [4], the Security Target Lite [5], the User Guidance Manual [23], the Configuration List [6] and additional evaluation documentation of the vendor NXP Semiconductors Germany GmbH [7] - [22] and [24]-[28] were editorially updated.

The ETR [31] and ETR for Composition [32] were updated within the previous Maintenance processes [29], [30] and remain unchanged and valid.

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

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG Section 4, Para. 3, Clause 2). BSI notes, that cryptographic functions with a security level of 80 bits or

lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore, for these functions it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

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

References

[1] Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004

[2] Impact Analysis Report BSI-DSZ-CC-0348-2009-MA-03, P5CT072/ P5CN072/ P5CC072/ P5CD072/ P5CD036/ P5CN036 V0S, Rev. 1.0, NXP Semiconductors Germany GmbH, 05. March 2009 (confidential document)

[3] Certification Report BSI-DSZ-CC-0348-2006 for Phillips Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 26 March 2006

[4] Security Target BSI-DSZ-0348, Version 1.0, 5 March 2009, Evaluation of the P5CT072/P5CC072/P5CD072/P5CD036 V0S Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (confidential document)

[5] Security Target Lite BSI-DSZ-0348, Version 1.0, 5 March 2009, Evaluation of the P5CT072/P5CC072/P5CD072/P5CD036 V0S Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (sanitised public document)

[6] Configuration List, Version 1.6, 03 March 2009, Evaluation of the Phillips P5CT072V0S/Q, Smart Card Controller, NXP Semiconductors, Business Line Identification

[7] Customer specific Appendix of the Configuration List, Philips P5CT072V0S Secure Smart Card Controller, Version 1.0, 03 March 2009, NXP Semiconductors, Business Line Identification

[8] Functional Specification for the P5CT072V0S, BSI-DSZ-CC-0348, Version 1.2, 03 March 2009, Phillips Semiconductors

[9] Product Data Sheet Addendum SmartMX, Rev. 3.2, 03 March 2009, Wafer Specification P5CT072V0S, NXP Semiconductors GmbH

[10] Product Data Sheet Addendum SmartMX, Rev. 3.2, 03 March 2009, Wafer Specification P5CN072V0S, NXP Semiconductors GmbH

[11] Product Data Sheet Addendum SmartMX, Rev. 3.2, 03 March 2009, Wafer Specification P5CC072V0S, NXP Semiconductors GmbH

[12] Product Data Sheet Addendum SmartMX, Rev. 3.2, 03 March 2009, Wafer Specification P5CD072V0S/V0Q, NXP Semiconductors GmbH

[13] Product Data Sheet Addendum SmartMX, Rev. 3.2, 03 March 2009, Wafer Specification P5CD036V0S/V0Q, NXP Semiconductors GmbH

[14] Product Data Sheet Addendum SmartMX, Rev. 3.2, 03 March 2009, Wafer Specification P5CN036V0S, NXP Semiconductors GmbH

[15] Data Sheet SmartMX P5CT072 V0S/V0Q, Rev. 3.1, 03 March 2009, Secure Triple Interface Smart Card Controller, NXP

[16] Data Sheet SmartMX P5CN072V0S, Rev. 3.2, 03 March 2009, Secure Secure Dual Interface PKI Smart Card Controller, NXP Semiconductors GmbH

[17] Data Sheet SmartMX P5CD072 V0S/V0Q, Rev. 3.1, 03 March 2009, Secure Dual Interface PKI Smart Card Controller, NXP Semiconductors GmbH

[18] Data Sheet SmartMX P5CC072 V0S, Rev. 3.1, 03 March 2009, Secure PKI Smart Card Controller, NXP Semiconductors GmbH

[19] Data Sheet SmartMX P5CD036 V0S/V0Q, Rev. 3.1, 03 March 2009, Secure Dual Interface Smart Card Controller, NXP Semiconductors GmbH

[20] Data Sheet SmartMX P5CN036 V0S, Rev. 3.2, 03 March 2009, Secure Dual Interface PKI Smart Card Controller, NXP Semiconductors GmbH

[21] Vulnerability Assessment, V1.0, 16 March 2005, BSI-DSZ-0348/349, Evaluation of the Philips P5CT072V0P/Q Secure Smart Card Controller, Philips Semiconductors, Business Line Identification

[22] Production Flows P5CT072V0S/Q (T023S) Smart Card Controller, Version 1.0, 03 March 2009, NXP Semiconductors, Business Line Identification

[23] Guidance, Delivery and Operation Manual for the NXP P5CT072V0S/V0Q, Secure Triple Interface Smart Card Controller, Version 1.3, 03 March 2009, NXP Semiconductors GmbH, Business Line Identification

[24] Order Entry Form, P5CT072, Release 4.0, 08 January 2009, NXP Semiconductors, Business Line Identification

[25] Order Entry Form, P5CN072, Release 3.1, 19 July 2009, NXP Semiconductors, Business Line Identification

[26] Order Entry Form, P5CC072, Release 4.0, 08 January 2009, NXP Semiconductors, Business Line Identification

[27] Order Entry Form, P5CD036, Release 4.0, 08 January 2009, NXP Semiconductors, Business Line Identification

[28] Order Entry Form, P5CD072, Release 4.0, 08 January 2009, NXP Semiconductors, Business Line Identification

[29] Maintenance Report BSI-DSZ-CC-0348-2006-MA-01 for Philips Secure Smart Card Controller P5CD072V0P, P5CD036V0P, P5CN072V0P and P5CN036V0P each with specific IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 20 June 2006

[30] Maintenance Report BSI-DSZ-CC-0348-2006-MA-02 for NXP Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with IC specific Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 26 June 2009

[31] Evaluation Technical Report, BSI-DSZ-CC-0348, Version 1.4, 13 June 2009, NXP P5CT072V0P Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (confidential document)

[32] Evaluation Technical Report for composition, BSI-DSZ-CC-0348, Version 1.3, 20 April 2009, NXP P5CT072V0P Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (confidential document)