Assurance Continuity Maintenance Report

BSI-DSZ-CC-0348-2006-MA-02

NXP Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with IC specific 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 delivery, test configuration, additional site and documentation, a change that has no effect on assurance. The TOE description of BSI-DSZ-CC-348-2006 remains unchanged.

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 Report BSI-DSZ-CC-0348-2006.

Bonn, 26 June 2009

Common Criteria

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 Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with IC specific 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 P5CT072V0P, P5CC072V0P, P5CD072V0P, and P5CD036V0P each with IC specific Dedicated Software was changed due to the following issues:

- A new wafer delivery form EWD for the evaluated product P5CT072V0P and its configurations is introduced.

- New delivery forms EVD and EVE for the evaluated product P5CT072V0P and its configurations P5CC072V0P, P5CD072V0P and P5CD036V0P are introduced. The difference between the evaluated package and the new package is a differnt color (the golden contacts are covered by an additional thin palladium layer).

- For the evaluated and certified delivery form SSOP20 package (Commercial product name P5CT072ETS/T0Prrffz, with USB functions used), a change in the handling during production will be introduced. A part of the second wafertest will be transferred into the final test.

- For performance reasons, the User Guidance Manual and the Guidance, Delivery and Operation Manual for the P5CT072V0P and its configurations had been updated.

- An additional production site NXP Semiconductors Thailand (APB) is used for wafertest and -treatment:

Site	Process
NXP Semiconductors Germany GmbH, Business Line Identification (BL ID), Georg-Heyken-Strasse 1, 21147 Hamburg, Germany	development center
NXP Semiconductors Germany GmbH, IC Manufacturing Operations - Test Center Hamburg (IMO TeCH), Stresemannallee 101, 22529 Hamburg, Germany	assembly, test, delivery

NXP Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (test, assembly, delivery)	assembly, delivery
NXP Semiconductors GmbH, Business Line Identification, Document Control Office, Mikron-Weg 1, 8101 Gratkorn, Austria	delivery
Systems on Silicon Manufacturing Co. Pte. Ltd. 8 (SSMC), 70 Pasir Ris Drive 1, Singapore 519527, Singapore	semiconductor factory
Photronics Singapore Pte. Ltd., 6 Loyang Way 2, Loyang Industrial Park, Singapore 507099, Singapore	mask shop
Photronics Semiconductors Mask Corp. (PSMC), 1F, No.2, Li-Hsin Rd., Science-Based Industrial Park, Hsin-Chu City Taiwan R.O.C.	mask shop

- A change referring to the test pad configuration had been introduced. This change has already been evaluated for the NXP Products P5CD144V0B, P5CD080V0B, P5CD040V0B in maintenance processes BSI-DSZ-CC-0411-MA-03, BSI-DSZ-CC-0410-MA-04 and BSI-DSZ-CC-0404-MA-04.

- A reassessment has been applied. The Guidance Manual [11], the ETR for composition [22] and the ETR [21] were updated in this context.

The version of the product remains unchanged. The change is not significant from the standpoint of security.

Conclusion

The change to the TOE is at the level of delivery, test configuration, additional site and documentation, a change that has no effect on assurance. Examination of the evidence indicates that the changes performed are limited to those issues.

The Security Target [4], the Security Target Lite [5], the Guidance, Delivery and Operation Manual [14], the Configuration List [6] and additional evaluation documentation of the vendor NXP Semiconductors Germany GmbH [7] - [13] and [15] - [19] were editorially updated.

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-0348-2006-MA-02, P5CT072/ P5CC072/ P5CD072/ P5CD036 V0P, Revision 1.1, NXP Semiconductors Germany GmbH, 10. December 2008 (confidential document)

[3]   Certification Report BSI-DSZ-CC-0348-2006, 28 March 2006, Phillips Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with specific IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik

[4]   Security Target BSI-DSZ-CC-0348, Version 1.6, 16 September 2008, Evaluation of the P5CT072/P5CC072/P5CD072/P5CD036 V0P Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (confidential document)

[5]   Security Target BSI-DSZ-CC-0348, Version 1.6, 16 September 2008, Evaluation of the P5CT072/P5CC072/P5CD072/P5CD036 V0P Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (sanitised public document)

[6]   Configuration List, Version 1.5, 08 December 2008, Evaluation of the Phillips P5CT072V0P/V0Q Secure Smart Card Controller, NXP Semiconductors, Business Line Identification

[7]   Data Sheet, SmartMX P5CT072V0P/V0Q, Rev. 3.1, 03 March 2009, Secure Triple Interface Smart Card Controller, NXP Semiconductor GmbH

[8]   Data Sheet, SmartMX P5CD072V0P/V0Q, Rev. 3.1, 03 March 2009, Secure Dual Interface Smart Card Controller, NXP Semiconductor GmbH

[9]   Data Sheet, SmartMX P5CC072V0P, Rev. 3.1, 03 March 2009, Secure PKI Smart Card Controller, NXP Semiconductor GmbH

[10]   Data Sheet, SmartMX P5CD036V0P/V0Q, Rev. 3.1, 03 March 2009, Secure Dual Interface Smart Card Controller, NXP Semiconductor GmbH

[11]   Guidance, Delivery and Operation Manual for the NXP P5CT072V0P/V0Q, Secure Triple Interface Smart Card Controller, Version 1.2, 15 May 2008, NXP Semiconductors, Business Line Identification

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

[13]   Production Flows P5CT072V0P/Q Smart Card Controller, Version 1.40, 29 October 2008, Philips Semiconductors Hamburg, Business Line Identification

[14]   Order Entry Form, P5CT072, 29 October 2008, Release 3.3, NXP Semiconductors, Business Line Identification

[15]   Order Entry Form, P5CC072, 29 October 2008, Release 3.3, NXP Semiconductors, Business Line Identification

[16] Order Entry Form, P5CD036, 29 October 2008, Release 3.3, NXP Semiconductors, Business Line Identification

[17] Order Entry Form, P5CD072, 29 October 2008, Release 3.3, NXP Semiconductors, Business Line Identification

[18] Design Report, P5CT072 Secure 8-bit Smart Card Controller, 28 October 2005, Revision 0.96, Philips Semiconductors

[19] Electrical Test Specification ETS 2, P5CT072 V0, Revision 12.0, 10 December 2008, Philips Semiconductors

[20] Maintenance Report BSI-DSZ-CC-0348-2006-MA-01, 20 June 2006, Phillips Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with specific IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik

[21] 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)

[22] 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)