Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0870-2014

for

NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1

from

NXP Semiconductors Germany GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0870-2014

Smartcard Controller

NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 19 February 2014

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition Agreement

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

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

This evaluation contains the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ASE_TSS.2, ATE_DPT.3 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 has undergone the certification procedure at BSI.

The evaluation of the product NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 was conducted by T-Systems GEI GmbH. The evaluation was completed on 19 December 2013. T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: NXP Semiconductors Germany GmbH.

The product was developed by: NXP Semiconductors Germany GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

[6] Information Technology Security Evaluation Facility

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1, has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] NXP Semiconductors Germany GmbH
Stresemannallee 101
22529 Hamburg

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1. The TOE provides a hardware platform for the implementation of smart card operating systems including multiple applications. The IC Dedicated Software can comprise either the MIFARE Plus MF1PLUSx0 Software or the MIFARE DESFire EV1 Software or a combination of the MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 Software. These different configurations are denoted as MIFARE Software in the following. The MIFARE Software offers a set of functions to manage data stored in the non-volatile EEPROM partition assigned to the MIFARE application. If the IC Dedicated Software includes the MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 Software, both applications can be used in parallel and both parts of the MIFARE Software are fully separated in time and space. The hardware platform provides coprocessors for Triple-DES with up to three keys, AES with different key lengths, large integer arithmetic operations and cyclic redundancy check calculation. Further the hardware platform includes a True Random Number Generator suitable to generate cryptographic keys. The TOE supports the ISO/IEC 7816 contact interface with UART and the ISO/IEC 14443 A contactless interface. The implementation of multiple applications is supported by the CPU offering different CPU modes with gradual permissions and memory management control supporting the separation of different memory segments. The IC Dedicated Software supports the smart card operating systems providing EEPROM write operation. Additionally the smart card operating systems can call the MIFARE Software (i.e. MIFARE PLUS MF1PLUSx0 and/or MIFARE DESFire EV1) primarily designed for secure contact-less transport applications and related loyalty programs as well as access management systems.

As already outlined in the Security Target ([6] and [8]), the configurations MC1 and MC4 are limited to MIFARE classic functionality in Security Level 1. These configurations are fixed to Security Level1. The functionality provided by the IC Dedicated Software when configured to MC1 and MC4 was not part of the evaluation. The configuration MP2 and MP4 provide the Security Funtionalities claimed for MIFARE Plus MF1PLUSx0 in the Security Target only in Security Level 0 and Security Level 3. In Security Level 1 and Security Level 2 the configurations MP2 and MP4 support MIFARE classic functionality that does not support evaluated Security Functionalities. The configuration MP2 and MP4 allow to change from Security Level 1 and the Security Level 2 to the Security Level 3 (MIFARE Plus) in the field (phase 7). However this presumes that the related level switch keys are configured in Security Level 0 and the constraints described in the guidance manual [20], section 3.1 are considered. The MIFARE DESFire EV1 supports different authentication procedures depending on the personalisation. The authentication using 3-key Triple-DES and AES are covered by the evaluation. The evaluation of the protected communication channel is limited to the cryptographic operation using AES. All options of the backward compatible mode as well as DES and 2-key Triple-DES do not provide evaluated Security Functionalities or Services.

The TOE "NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1" is referenced as P60x144/080yVA in the following.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SS.RNG	Random Number Generator
SS.HW_DES	Triple-DES coprocessor
SS.HW_AES	AES coprocessor
SS.CRC	Cyclic Redundancy Check
SS.RECONFIG	Post Delivery Configuration
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control
SF.FFW	Firmware Firewall
SF.FIRMWARE	Firmware Support
SS.MFP_AUTH	MIFARE Plus Authentication
SS.MFP_ACC_CTRL	Access Control to MIFARE Plus data
SS.MFP_ENC	MIFARE Plus Encryption
SS.MFP_MAC	MIFARE Plus Message Authentication Code
SS.DF_AUTH[8]	DESFire Authentication
SS.DF_ACC_CTRL[8]	Access Control to DESFire Data
SS.DF_ENC[8]	DESFire Communication Encryption
SS.DF_MAC[8]	DESFire Message Authentication Code
SS.DF_TRANS[8]	DESFire Transaction Protection

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [8], chapter 7.

[8] Note that these Security Functionalities are not available for the TOE configuration only providing MIFARE Plus MF1PLUSx0.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.2 to 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating of cryptographic algorithms (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery	P60D144/ 080MVA	P60D144/ 080DVA	P60D144/ 080JVA	P60N144 JVA
1	HW	NXP Secure Smart Card Controller P60x144/080yVA	nameplate 9050B	wafer, module, inlay or package	x	x	x	x
2a	SW	Test ROM Software (IC Dedicated Test Software), Test-ROM on the chip acc. to 9050B_CL015_TESTROM_v1_btos_07 v0B_fos_6v10.hex	Release 07.0B, 29 March 2012	stored in ROM on the chip	x			
2b	SW	Test ROM Software (IC Dedicated Test Software), Test-ROM on the chip acc. to 9050B_CM095_TESTROM_v1_btos_07 v10_fos_8v00.hex	Release 07.10, 17 Decembe r 2012	stored in ROM on the chip		x	x	x
3a	SW	Boot ROM Software (part of the IC Dedicated Support Software), Boot-ROM on the chip acc. to 9050B_CL015_TESTROM_v1_btos_07 v0B_fos_6v10.hex	Release 07.0B, 29 March 2012	stored in ROM on the chip	x			
3b	SW	Boot ROM Software (part of the IC Dedicated Support Software), Boot-ROM on the chip acc. to 9050B_CM095_TESTROM_v1_btos_07 v10_fos_8v00.hex	Release 07.10, 17 Decembe r 2012	stored in ROM on the chip		x	x	x

No	Type	Identifier	Release	Form of Delivery	P60D144/080MVA	P60D144/080DVA	P60D144/080JVA	P60N144JVA
4a	SW	Firmware Operating System (FOS) including MIFARE Plus MF1PLUSx0 (part of the IC Dedicated Support Software), Firmware Operating System on the chip acc. to 9050B_CL015_TESTROM_v1_btos_07v0B_fos_6v10.hex	Version 6.11[9], 29 March 2012	stored in ROM on the chip	x			
4b	SW	Firmware Operating System (FOS) including MIFARE DESFire EV1 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 (part of the IC Dedicated Support Software), Firmware Operating System on the chip acc. to 9050B_CM095_TESTROM_v1_btos_07v10_fos_8v00.hex	Release 08.01[10], 17 December 2012	stored in ROM on the chip		x	x	x
5	DOC	Product Data Sheet, SmartMX2 family P60D080/144 and P60C080/144 VA, Secure high-performance smart card controller, NXP Semiconductors, Business Unit Identification	Rev. 4.0, 30 August 2013	electronic form [11]	x	x	x	x
6	DOC	Product Data Sheet Addendum SmartMX2 family Firmware Interface Specification, (FIS), NXP Semiconductors	Rev. 3.8, 05 July 2013	electronic form [12]	x	x	x	x
7	DOC	Instruction Set for the SmartMX2 family, Secure smart card controller, NXP Semiconductors, Business Unit Identification	Rev. 3.1, 2 February 2012	electronic form [13]	x	x	x	x
8	DOC	Product Data Sheet Addendum, SmartMX2 family Chip Health Mode (CHM), NXP Semiconductors	Rev. 3.0, 11 May 2012	electronic form [14]	x	x	x	x
9	DOC	Product Data Sheet Addendum, SmartMX2 family Post Delivery Configuration (PDC), NXP Semiconductors	Rev. 3.2, 4 February 2013	electronic form [15]	x	x	x	x
10	DOC	Guidance and Operation Manual, NXP Secure Smart Card Controller P60x080VA/P60x144VA, NXP Semiconductors	Rev. 2.2, 15 July 2013	electronic form [16]	x	x	x	x
11	DOC	Product Data Sheet addendum: SmartMX2 family P60D080/144 VA and P60C080/144 VA Wafer and delivery specification, NXP Semiconductors	Rev. 3.6, 5 July 2013	electronic form [17]	x	x	x	

[9] Note that the ROM mask is released according to version 6.10, but the evaluated version includes a Firmware patch to version 6.11.

[10] Note that the ROM mask is released according to version 8.00, but the evaluated version includes a Firmware patch to version 8.01.

No	Type	Identifier	Release	Form of Delivery	P60D144/ 080MVA	P60D144/ 080DVA	P60D144/ 080JVA	P60N144 JVA
12	DOC	Product Data Sheet Addendum: MIFARE Plus Functionality of implementation on smart card controllers, NXP Semiconductors, Business Unit Identification	Rev. 3.2, 27 February 2013	electronic form [18]	x		x	x
13	DOC	Product Data Sheet Addendum: MIFARE DESFire EV1 Functionality of implementations on smart card controllers, NXP Semiconductors, Business Unit Identification,	Rev. 3.2, 22 July 2013	electronic form [19]		x	x	x
14	DOC	Guidance, Delivery and Operation Manual, MIFARE Plus MF1PLUSx0, NXP Secure Smart Card Controller P60xeeey, NXP Semiconductors, Business Unit Identification	Rev. 1.5, 21 June 2013	electronic form [20]	x		x	x
15	DOC	Guidance, Delivery and Operation Manual, MIFARE DESFire EV1, NXP Secure Smart Card Controller P60xeeey, NXP Semiconductors, Business Unit Identification,	Rev. 1.3, 10 June 2013	electronic form [21]		x	x	x
16	DOC	Product Data Sheet SmartMX2 family P60N144VA, Secure high-performance smart card controller, NXP Semiconductors, Business Unit Identification	Rev. 3.1, 3 July 2013	electronic form [22]				x
17	DOC	Product Data Sheet Addendum: SmartMX2 family P60N144 VA Wafer and delivery specification, NXP Semiconductors, Business Unit Identification	Rev. 3.1., 18 June 2013	electronic form [23]				x

Table 2: Deliverables of the TOE

Note that only the hardware platform and the documents but not the IC Dedicated Software are delivered as separated items since the IC Dedicated Software is delivered on chip as part of the hardware platform stored in ROM and EEPROM. All documentation belonging to the TOE is delivered as electronic document. Depending on the configuration the set of applicable documents is different. Therefore the table above includes an assignment between the documentation and the configuration. The applicable documentation also depends on the configuration set by the post delivery configuration. If the MIFARE PLUS MF1PLUSx0 and/or the MIFARE DESFire EV1 is disabled by post delivery configuration the interfaces of the disabled components of the IC Dedicated Software are not accessible and the related Data Sheet and User Guidance are not applicable.

The hardware platform as part of the TOE is available in different packages as listed in the following table. The table lists in the last column the package types that are supported in this evaluation:

P60D144/ 080MVA	P60D144/ 080DVA	P60D144/ 080JVA	P60N144 JVA	
Ux	Ux	Ux	Ux	Wafer not thinner than 50 µm (The letter “x” in “Ux” stands for a capital letter or a number, which identifies the wafer type)
Xn	Xn	Xn		Module (The letter “n” in” Xn” stands for a capital letter or a number, which identifies the module type)
A4	A4	A4		MOB4 module
A6	A6	A6		MOB6 module
Ai	Ai	Ai		Inlay (The letter ‘i” in “Ai” stands for a capital letter, which identifies both, the inlay type and the package type inside the inlay.)

Table 3: Supported package types

The requirements for the delivery of these package types are described in Chapter 2 of the Guidance and Operation Manual [16] and in P60D080/144 VA and P60C080/144 VA Wafer and delivery specification [17] and P60N144 VA Wafer and delivery specification [23]. For each delivery form of the hardware platform NXP BU ID offers two ways of delivery of the TOE:

1. The customer collects the hardware platform himself at the NXP BU ID site.

2. The hardware platform is sent to the customer by NXP BU ID with special protective measures.

The package type does not influence the security functionality of the TOE. It does only define which pads are connected in the package and for what purpose the TOE (with the appropriate package) can be used. The commercial type name is the name that the customer of NXP BU ID uses to order the TOE in the respective package. There is a separate Order Entry Form for each major configuration, refer to [24], [25] and [26]. The appendix for the definition of the FabKey is the same for all Order Entry Forms (cf. [27]). Note that the commercial type names contain placeholders for the customer specific parts (i.e. the ROM code number associated with the Security IC Embedded Software, the FabKey number and minor configuration options) of the TOE. A specification of the placeholders is given by the developer in section 1.4.2.4 of [6] and [8]. In consequence this means that a full commercial product name that fits in the variable forms described in table 3 determines that the hardware or the combination of hardware and software is an evaluated product. Note further that this gives no conclusion on the Security IC Embedded Software or whether the software uses the proper hardware configuration as described by section 1.3.1 of the Security Target [6] and [8].

The hardware version can be identified by the coded nameplate "9050B" on the surface of the hardware platform as described in sections 4.2 and 3.9.3 of the P60D080/144 VA and P60C080/144 VA Wafer and delivery specification and P60N144 VA Wafer and delivery specification [17, 23]. The nameplate is the same for all configurations. In addition each major configuration has a different device coding as described in [11], [22] and [28]. Identification is also possible using the Chip Health Mode. The identification string provided by the command 00h of the Chip Health Mode comprises also the device coding and the firmware version. Each major configuration has a dedicated device coding as listed in the following table.

	P60D144MVA	P60D080MVA	P60D144DVA	P60D080DVA	P60D144JVA	P60D080JVA	P60N144JVA
DC0	0010 0010	0010 0010	0010 0010	0010 0010	0010 0010	0010 0010	0100 0010
DC1	0000 1111	0000 1110	0000 1111	0000 1110	0000 1111	0000 1110	0001 0110
DC2	0XXX 0001	0XXX 0001	0XXX 0010	0XXX 0010	0XXX 0100	0XXX 0100	0XXX 0100
DC3	0001 0111	0001 0111	0001 0111	0001 0111	0001 0111	0001 0111	0001 0111
DC4	0000 000X	0000 000X	0000 000X	0000 000X	0000 000X	0000 000X	0000 000X

Table 4: Device coding of the major configurations

Note that “X” in the table above denotes 0 or 1 for the case of minor configuration options. All major configurations are unambiguously mapped by the representation in table 4. Both minor configurations of the antenna are part of the evaluation and can be selected by the customer. The software configuration can be identified by using the GET operations of the FVEC interface for MIFARE Post Delivery Configuration. The GET operation can also be used for identification of the TOE after applying the SET operation of the MIFARE Post Delivery Configuration. For details please refer to [11].

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. As the TOE is a hardware platform, the security policy of the TOE provides countermeasures against: leakage of information, physical probing, malfunctions, physical manipulations, access to code, access to data memory, abuse of functionality. Hence the TOE shall:

●maintain the integrity and the confidentiality of data stored in the memory of the TOE and

●maintain the integrity, the correct operation and the confidentiality of Security Functions (security mechanisms and associated functions) provided by the TOE.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Usage of Hardware Platform (OE.Plat-Appl)
- Treatment of User Data (OE.Resp-Appl)
- Protection during composite product manufacturing (OE.Process-Sec-IC)
- Check of initialisation data by the Security IC Embedded Software (OE.Check-Init)
- Check of the Originality Key of the MIFARE Software (OE.Check-OriginalityKey)
- Generation of secure values (OE.Secure-Values)
- Terminal support to ensure integrity, confidentiality and use of random numbers (OE.Terminal-Support)

Details can be found in the Security Target [6] and [8], chapter 4.2 and 4.3.

5 Architectural Information

The NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 is an integrated circuit (IC) providing a hardware platform with IC Dedicated Support Software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target, [6] and [8]. The complete description of the hardware platform and the IC Dedicated Support Software as well as the complete instruction set of the NXP BU ID NXP Secure Smart Card Controller P60x144/080yVA can be found in the “Product Data Sheet, SmartMX2 family P60D080/144 and P60C080/144 VA, Secure high-performance smart card controller”, [11] (and its addendums [14], [15] and [17]) and the “Instruction Set for the SmartMX2 family”, [13]. The “Firmware Interface Specification”, [12] is an addendum to [11] including the description for the implemented versions FW06.11 and FW08.01 of the Firmware Operating System. The document ‘MIFARE Plus Functionality of implementation’ [18] serves as data sheet for the MIFARE PLUS MF1PLUSx0 software. The document ‘MIFARE DESFire EV1 Functionality of implementations’ [19] serves as data sheet for the MIFARE DESFire EV1 Software. In addition separate user guidance manuals are provided. The specific user guidance for the MIFARE PLUS MF1PLUSx0 is provided in ‘Guidance, Delivery and Operation Manual, MIFARE DESFire EV1’ [20]. The specific user guidance for the MIFARE DESFire EV1 is provided in ‘Guidance, Delivery and Operation Manual, MIFARE DESFire EV1’ [21]. If the configuration P60N144J is ordered, the document Product Data Sheet SmartMX2 family P60N144VA [22] (and the addendum [23]) is delivered additionally.

The hardware platform comprises the following components: a CPU supporting a 32-/24-/16-/8-bit instruction set and distinguishing five CPU modes, Triple-DES Co-Processor, AES Co-processor, CRC Coprocessor, Fame2 Co-Processor, Memory Management Unit, Copy Machines, Random Number Generator (RNG), Power Module and a module comprising Security Sensors and Filters. The hardware platform comprises a contact-based interface and either a contactless interface or a S2C interface. The different CPU Modes allow to separate different applications running on the TOE. One CPU Mode is reserved for the Firmware Operating System supporting specific functionality of the hardware platform. The security measures for physical protection of the hardware platform are realized within the layout of the whole circuitry.

The Special Function Registers that can be controlled by the Security IC Embedded Software provide one interface to the security functionality of the TOE. The NXP Secure Smart Card Controller P60x144/080yVA provides different levels of access control to the SFR with the different CPU Modes and additional – configurable – access control to Special Function Registers for the User Mode and the Firmware Mode.

The Fame2 does not provide a cryptographic algorithm itself. The modular arithmetic functions are suitable to implement different asymmetric cryptographic algorithms. The coprocessor implements security features to support the protection against fault attacks and timing attacks as described in [6] and [8].

The TOE executes the IC Dedicated Support Software (Boot Software) during the start up to configure and initialise the hardware. This software is executed in the Boot Mode. After the start-up is finished and the CPU Mode changed to System Mode it is not possible to re-enter the Boot Mode without forcing a reset.

The Firmware Operating System provides several functions to the Security IC Embedded Software. The functions can be grouped in: (i) support of EEPROM write operation, (ii) support for the contactless communication and (iii) start of the MIFARE Software (i.e.

MIFARE PLUS MF1PLUSx0 and/or MIFARE DESFire EV1). The EEPROM write support includes a re-trimming process in order to ensure the endurance of the EEPROM modules. The Firmware can be used to activate and maintain the contactless ISO 14443 protocol.

The MIFARE Software is also part of the Firmware Operating System and can be started by the Security IC Embedded Software. The Mifare application specific commands can be exchanged using the contactless interface or the so called remote interface. The remote interface requires a shared memory area in the RAM. A strict separation between the IC Dedicated Support Software and the Security IC Embedded Software is ensured based on the partitioning of the memories. The Firmware is executed in the Firmware Mode and has only access to the partitions of the Firmware. The System Mode and the User Modes have access to the partition of the Security IC Embedded Software. The System Mode can configure a shared memory area in the RAM to exchange data with software running in Firmware Mode for different Firmware vector calls (FVEC). The Firmware is able to access code and data stored in the EEPROM partition of the Security IC Embedded Software to support the EEPROM write operation. Code and data of the Firmware Operating System cannot be accessed by the Security IC Embedded Software running in System Mode or User Mode.

The hardware platform comprises a contact based interface and either a contactless interface or a S2C interface. The contact interface and the contactless interface can be used independently from each other. If the S2C interface is used a contact based power supply is required. Based on a specific minor configuration and an associated clock configuration the interfaces could be used simultaneously.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The tests performed by the developer can be divided into the following categories:

1. tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE;

2. functional tests which are performed with special software to test all TSFIs including the Mifare software (MIFARE Plus MF1PLUSx0 and/or MIFARE DESFire EV1);

3. characterisation and verification tests to release the hardware platform for production including tests with different operating conditions as well as special verification tests for security services and security features of the hardware and the IC Dedicated Software;

4. functional tests at the end of the production process using IC Dedicated Test Software. These tests are executed for every chip to check its correct functionality and individually trim each device as last step of phase 3.

The developer tests cover all TSFIs identified in the functional specification as well as in the test documentation.

The evaluators were able to repeat the tests of the developer. The tests are repeated and verified against the test protocols provided by the developer. The tests of the developer are repeated by sampling. In addition the evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the evaluators comprise special tests and examination of the hardware platform and the Firmware using open samples. In addition the evaluators perform tests of the hardware platform and the Firmware using different major configurations according to table 5. Minor configuration options were characterised performing the same test under similar conditions for different minor configuration options.

The evaluation provides evidence that the actual version of the hardware platform provides the TOE Security Functionality as specified by the developer. The test results confirm the correct implementation of the TOE Security Functionality.

For penetration testing the evaluators took all TOE Security Functionality into consideration. Extensive penetration testing was performed to test the security mechanisms used to provide the Security Services and Security Features. The tests for the hardware platform and the Firmware comprise the use of bespoke equipment and expert knowledge. The penetration tests considered physical tampering of the hardware platform including information that can be gathered by reverse engineering to support other attacks. Further on attacks that do not modify the hardware platform physically such as side channel analysis for the coprocessors (AES, Triple-DES) and perturbation attacks were performed. The test of the hardware platform and the Firmware comprises attacks that must be averted by the combination of the hardware platform and the Security IC Embedded Software as well as attacks against the hardware platform and the Firmware directly. The penetration tests of the IC Dedicated Software include also logical attacks.

8 Evaluated Configuration

The TOE can be delivered with specific configurations for MIFARE Plus MF1PLUSx0 that are named P60D144MVA and P60D080MVA each with the same IC Dedicated Software and with specific configurations for MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 that are named P60D144JVA, P60D080JVA, P60D144DVA, P60D080DVA and P60N144JVA each with the same IC Dedicated Software. In short form the TOE is named P60x144/080yVA. ‘x’ is a placeholder for either ‘D’ or ‘N’. ‘D’ specifies availability of both ISO/IEC 7816 and ISO/IEC 14443 interface. ‘N’ specifies the use of pads for input of the digitized modulated ISO14443 signal and output of the envelope of the modulated ISO14443 signal for communication via an external RF Frontend (i.e. NFC IC) instead of using the internal RF interface for contactless communication. ‘144’ and ‘080’ specify the accessible EEPROM memory. Furthermore ‘y’ is a placeholder for either ‘M’, ‘D’ or ‘J’. ‘M’ specifies availability of MIFARE Plus MF1PLUSx0, ‘D’ the availability of MIFARE DESFire EV1 and ‘J’ the availability of MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1.

Note that all the major configurations of the hardware platforms are denoted in the most right column of the following table.

	P60D144yVA	P60D080yVA	P60N144yVA	Firmware Operating System	Major Configurations
ISO/IEC 7816 contact interface	available	available	available	-	-

	P60D144yVA	P60D080yVA	P60N144yVA	Firmware Operating System	Major Configurations
Contactless interface acc. ISO/IEC 14443 A	available	available	not available	-	-
S2C Interface	not available	not available	available	-	-
Supported configurations of MIFARE Plus MF1PLUSx0 or MIFARE DESFire EV1.For the accessible EEPROM space [bytes] of the minor configurations refer to the Security Target [6] and [8]. (Physical EEPROM of 24kBytes)	MP0	MP0	-	6.11	P60D144MVA, P60D080MVA
	MP2, MP4	MP2, MP4	MP2, MP4		
	D2, D4, D8	D2, D4, D8	D2, D4, D8	8.01	P60D144JVA, P60D080JVA, P60D144DVA, P60D080DVA, P60N144JVA
	MP0/D0	MP0/D0	MP0/D0		
	MP2/D2 MP4/D2 MP2/D4 MP4/D2 MP2/D8 MP4/D8	MP2/D2 MP4/D2 MP2/D4 MP4/D2 MP2/D8 MP4/D8	MP2/D2 MP4/D2 MP2/D4 MP4/D2 MP2/D8 MP4/D8		
Copy Machines	2	1	2	-	-

Table 5: Overview of major configurations

The configuration MP0 of the P60D144/080MVA does not provide any Security Service claimed for MIFARE PLUS MF1PLUSx0 since the Mifare software is disabled. The configuration MP0/D0 of the P60x144/080yVA does not provide any Security Service claimed for MIFARE PLUS MF1PLUSx0 and MIFARE DESFire EV1 since both Mifare components are disabled. The Security Features and Security Services claimed for the hardware platform and the emulation framework (support of EEPROM writing and support of the contactless protocol according to ISO/IEC 14443) are fully supported by these configurations.

The configuration MP2 and MP4 provide the Security Services claimed for MIFARE Plus MF1PLUSx0 in the Security Target only in Security Level 0 and Security Level 3. In Security Level 1 and Security Level 2 the configuration MP2 and MP4 support MIFARE classic functionality that does not support evaluated Security Services. However the Security Services and Security Features provided by the hardware platform cannot be violated by the MIFARE classic functionality. The configuration MP2 and MP4 allow to change from Security Level 1 and the Security Level 2 to the Security Level 3 (MIFARE Plus) in the field (phase 7). However this presumes that the related level switch keys are configured in Security Level 0 and the constraints described in the guidance manual [20], section 3.1 are considered.

The configurations D2, D4, D8 of MIFARE DESFire EV1 support different authentication procedures depending on the personalisation. The authentication using 3-key Triple-DES and AES are covered by the evaluation. The evaluation of the protected communication channel is limited to the cryptographic operation using AES. All options of the backward compatible mode as well as DES and 2-key Triple-DES for the "new authentication" do not provide evaluated Security Services.

The 'Joint' configurations MP2 / D2; MP4 / D2; MP2 / D4; MP4 / D4; MP2 / D8; MP4 / D8 provide the Security Services and Security Features claimed for MIFARE Plus MF1PLUSx0 in the Security Target in Security Level 0 and Security Level 3 as well as the Security Services provided by the MIFARE DESFire EV1.

The configurations MC1 and MC4 are limited to MIFARE classic functionality in Security Level 1. These configurations are fixed to Security Level 1. MC1 and MC4 do not implement any Security Functional Requirement for MIFARE Plus MF1PLUSx0 and the functionality provided by the IC Dedicated Software when configured to MC1 and MC4 is not part of the TOE. However the evaluators determine that the Security Services and Security Features provided by the hardware platform and the IC Dedicated Software (including FVEC7) cannot be violated by the MIFARE classic functionality.

The 'Joint' configurations MC1 / D2; MC4 / D2; MC1 / D4; MC4 / D4; MC1 / D8; MC4 / D8 provide the Security Services of MIFARE DESFire EV1. Using the MIFARE classic functionality MC1 and MC4, no Security Services are provided by the software. MC1 and MC4 do not implement any Security Functional Requirement for MIFARE Plus MF1PLUSx0 and the functionality provided by the IC Dedicated Software when configured to MC1 and MC4 is not part of the TOE. However the evaluators determine that the Security Services and Security Features provided by the hardware platform, the IC Dedicated Software (including FVEC7) and the MIFARE DESFire EV1 cannot be violated by the MIFARE classic functionality.

Note that the post delivery configuration as described in [11] and [22] allows to disable the AES coprocessor and thereby a security service provided by the TOE. In addition the Fame2 coprocessor can be disabled and the accessible size of the EEPROM and the accessible size of the CXRAM can be set by post delivery configuration. If a component is disabled the access to Special Function Registers or bits of Special Function Registers of this component will force an exception. According to [12] the FVEC0.15 can be used for the MIFARE Post Delivery Configuration, which allows reconfiguring of the MIFARE Software. This comprises the availability of the MIFARE Software and the memory space that is accessible by the related MIFARE application if it is enabled. Thereby FVEC0.15 also allows to disable security services provided by the TOE.

The documentation of the configuration comprises two parts. The configuration list is included in [28]. The customer specific configuration settings of a product according to the order entry form are listed in [29]. For the customer specific configuration information a configuration template (refer to [29]) is used which is adapted regarding the customer selectable configuration options.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards

(iii) Guidance, Smartcard Evaluation

(see [4], AIS 25, AIS 26, AIS 37).

For RNG assessment the scheme interpretations AIS 31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities 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' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

Purpose	Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Authentication (MFP)	AES in CBC mode	[FIPS-197] (AES), [SP 800-38A] (CBC)	|K| = 128	yes
Authentication (DF)	AES in CBC mode	[FIPS-197] (AES), [SP 800-38A] (CBC)	|K| = 128	yes
	Three-key TDES in CBC mode	[FIPS-46-3] (DES), [SP 800-38A] (CBC)	|K| = 168	yes
Key Agreement (MFP)	FTP_TRP.1[MFP]	--	--	no
Key Agreement (DF)	FTP_TRP.1[DF]	--	--	no
Confidentiality (MFP)	AES in CBC mode	[FIPS-197] (AES), [SP 800-38A] (CBC)	|K| = 128	yes
Confidentiality (DF)	AES in CBC mode	[FIPS-197] (AES), [SP 800-38A] (CBC)	|K| = 128	yes
Integrity (MFP)	AES in CMAC mode	[FIPS-197] (AES), [SP800-38B] (CMAC)	|K| = 128	yes
Integrity (DF)	AES in CMAC mode	[FIPS-197] (AES), [SP800-38B] (CMAC)	|K| = 128	yes
Trusted Channel (MFP)	Mifare Plus MF1PLUSx0	--	--	no
Trusted Channel (DF)	Desfire EV1	--	--	no
Cryptographic Primitives	Two-key TDES	[FIPS-46-3] (DES)	|K| = 112	no
	Three-key TDES	[FIPS-46-3] (DES)	|K| = 168	yes
	AES	[FIPS-197] (AES)	|K| = 128, 192, 256	yes

Table 6: Cryptographic TOE Security Functionalities

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs 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 of 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 (see table 2) which contains guidelines for the developer of the Security IC Embedded Software as well as guidance for the devloper of the terminal for the Mifare software and guidance for the administrators of the Mifare Software. The requirements in these guidance must be followed 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 correctly 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 [10].

In addition, the following aspect needs to be fulfilled when using the TOE:

The implementation of the encryption/decryption operation of the MIFARE Plus MF1PLUSx0 may expose some bits of the XOR difference between pairs of plaintext using the principles of a watermark attack.This is addressed in [20], refer to REC.12.

11 Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DF	DESFire
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IEC	International Electrotechnical Commission

FVEC	Firmware Vector
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MFP	MIFARE Plus
OS	Operating System
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver Transmitter

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[11].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] NXP Secure Smart Card Controller P60x144/080yVA, Security Target, NXP Semiconductors, Business Unit Identification, Rev. 1.4, 10 September 2013 (confidential document)

[7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

[8] NXP Secure Smart Card Controller P60x144/080yVA, Security Target Lite, NXP Semiconductors, Business Unit Identification, Rev. 1.4, 10 September 2013

[9] Evaluation Technical Report BSI-DSZ-CC-0870, Version 1.4, 13 December 2013, T-Systems GEI GmbH (confidential document)

[10] ETR for composition according to AIS36, NXP P60x144/080yVA, T-Systems GEI GmbH, Version 1.1, 13.12.2013 (confidential document)

[11] Product Data Sheet, SmartMX2 family P60D080/144 and P60C080/144 VA, Secure high-performance smart card controller, NXP Semiconductors, Business Unit Identification, Rev. 4.0, 30 August 2013

[12] Product Data Sheet Addendum SmartMX2 family Firmware Interface Specification, (FIS), NXP Semiconductors, Rev. 3.8, 05 July 2013

[13] Instruction Set for the SmartMX2 family, Secure smart card controller, NXP Semiconductors, Business Unit Identification, Rev. 3.1, 02 February 2012

[11] specifically

- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

[14] Product Data Sheet Addendum, SmartMX2 family Chip Health Mode (CHM), NXP Semiconductors, Rev. 3.0, 11 May 2012

[15] Product Data Sheet Addendum, SmartMX2 family Post Delivery Configuration (PDC), NXP Semiconductors, Rev. 3.2, 04 February 2013

[16] Guidance and Operation Manual, NXP Secure Smart Card Controller P60x080VA/P60x144VA, NXP Semiconductors, Rev. 2.2, 15 July 2013

[17] Product Data Sheet addendum: SmartMX2 family P60D080/144 VA and P60C080/144 VA Wafer and delivery specification, NXP Semiconductors, Rev. 3.6, 05 July 2013

[18] Product Data Sheet Addendum: MIFARE Plus Functionality of implementation on smart card controllers, NXP Semiconductors, Business Unit Identification, Rev. 3.2, 27 February 2013

[19] Product Data Sheet Addendum: MIFARE DESFire EV1 Functionality of implementations on smart card controllers, NXP Semiconductors, Business Unit Identification, Rev. 3.2, 22. July 2013

[20] Guidance, Delivery and Operation Manual, MIFARE Plus MF1PLUSx0, NXP Secure Smart Card Controller P60xeeey, NXP Semiconductors, Business Unit Identification, Rev. 1.5, 21. June 2013

[21] Guidance, Delivery and Operation Manual, MIFARE DESFire EV1, NXP Secure Smart Card Controller P60xeeey, NXP Semiconductors, Business Unit Identification, Rev. 1.3, 10. June 2013

[22] Product Data Sheet SmartMX2 family P60N144VA, Secure high-performance smart card controller, NXP Semiconductors, Business Unit Identification, Rev. 3.1, 03. July 2013

[23] Product Data Sheet Addendum: SmartMX2 family P60N144 VA Wafer and delivery specification, NXP Semiconductors, Business Unit Identification, Rev. 3.1, 18 June 2013

[24] Order Entry Form, P60D144, Release 2.12, NXP Semiconductors, Business Unit Identification, online document

[25] Order Entry Form, P60D080, Release 2.12, NXP Semiconductors, Business Unit Identification, online document

[26] Order Entry Form, P60N144, Release 3.0, NXP Semiconductors, Business Unit Identification, online document

[27] Appendix 1 to SmartMX2 P60 Family Order Entry Form – P60 FabKey Data Transfer Form, Version 1.1, January 31st, 2012, NXP Semiconductors

[28] NXP Secure Smart Card Controller P60x144eVA / P60x080eVA, Appendix of the Configuration List for composite evaluation, NXP Semiconductors, Rev. 02.20, 30 August 2013

[29] NXP Secure Smart Card Controller P60x144eVA / P60x080eVA, Customer specific Appendix of the Configuration List, NXP Semiconductors, Revision 2.20, 30 August 2013

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

"The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D."

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0870-2014

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller P60x144/080yVA including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 19 February 2014, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1 and ALC_TAT.2)

are fulfilled for the development and production sites of the TOE listed below:

Development site	Task within the evaluation
NXP Semiconductors Hamburg Business Unit Identification (BU ID) Stresemannallee 101 2569 Hamburg Germany	Development, Delivery and customer support
NXP Semiconductors India Private Limited Information Technology Park Nagawara Village, Kasaba Hobli, Bangalore 560045 India	Development
NXP Semiconductors Interleuvenlaan 80 B-3001 Leuven Belgium	Development support
TSMC, Fab 2 and 5 No. 121 Park Ave. III Hsinchu Science Park Hsinchu, Taiwan 300, R.O.C.	Mask data preparation
TSMC, Fab 7 No. 6, Creation Rd. II Hsinchu Science Park Hsinchu, Taiwan 300, R.O.C.	Mask data preparation
TSMC, Fab 6 and Fab 14	Mask and wafer production

Development site	Task within the evaluation
No. 1, Nan-Ke North Rd. Tainan Science Park Tainan, Taiwan 741, R.O.C.	
Chipbond Technology Corporation No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping
NXP Semiconductors GmbH Hamburg Test Center Europe - Hamburg (TCE-H) Stresemannallee 101 22569 Hamburg Germany	Test Center and configuration of the Fabkey
Assembly Plant Bangkok 303 Moo 3 Chaengwattana Rd. Laksi, Bangkok 10210 Thailand	Test Center, Delivery and Module assembly
Assembly Plant Kaohsiung NXP Semiconductors Taiwan Ltd #10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170 Taiwan, R.O.C	Test Center and Module assembly
HID Global Teoranta Paic Tionscail na Tulaigh Balle na hAbhann Co. Galway Ireland	Inlay assembly
NXP Semiconductors Austria GmbH Styria Business Unit Identification (BU ID) Mikron-Weg 1 8108 Gratkorn Austria	Document control
NedCard B.V. Bijsterhuizen 25-29 6604 LM Wijchen The Netherlands	Module assembly

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [8]) are fulfilled by the procedures of these sites.