Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0939-V2-2016

for

NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software

from

NXP Semiconductors Germany GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, 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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0939-V2-2016 (*)

Smartcard Controller

NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software

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 6 augmented by ALC_FLR.1 and ASE_TSS.2

SOGIS
Recognition Agreement

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 CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 18 February 2016

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (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:

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- 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 SOGIS Technical Domains only.

---

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 Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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.

As this certificate is a re-certification of a certificate issued according to CCRA-2000 this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ADV_FSP.5, ADV_IMP.2, ADV_INT.3, ADV_SPM.1, ADV_TDS.5, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_DPT.3, ATE_FUN.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 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 P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0939-2015. Specific results from the evaluation process BSI-DSZ-CC-0939-2015 were re-used.

The evaluation of the product NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 08 January 2016. TÜV Informationstechnik 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.

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 or in the CC itself.

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 order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 18 February 2016 is valid until 17 February 2021. Validity can be re-newed by re-certification.

[6] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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 P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software 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

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 IC hardware platform NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software and documentation describing the Instruction Set and the usage. Within this document the TOE will be abbreviated by P60D024/016/012yVB(Y/Z/A)/yVF.

The IC hardware platform NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF is a microcontroller incorporating a central processing unit, memories accessible via a Memory Management Unit, cryptographic co-processors, other security components and two communication interfaces. The central processing unit supports a 32-/24-/16-/8-bit instruction set optimized for smart card applications, which is a super set of the 80C51 family instruction set. On-chip memories are ROM, RAM and EEPROM. The non-volatile EEPROM can be used as data or program memory.

The IC Dedicated Software comprises IC Dedicated Test Software for test purposes and IC Dedicated Support Software. The IC Dedicated Support Software consists of Boot-ROM Software controlling the boot process of the hardware platform and Firmware Operating System which can be called by the Security IC Embedded Software.

Some configurations of the P60D024/016/012yVB(Y/Z/A)/yVF include Emulation Software MIFARE Plus MF1PLUSx0 or MIFARE DESFire EV1. The Mifare Software does not implement any Security Functional Requirements. The evaluation scope of MIFARE emulations is limited to being non-interfering with the TSF.

The P60D024/016/012yVB(Y/Z/A)/yVF can be used to assure authorized conditional access in a wide range of applications. Examples are identity cards, Banking Cards, Pay-TV, Portable communication SIM cards, Health cards and Transportation cards.

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 [8].

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 6 augmented by ALC_FLR.1 and ASE_TSS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], 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
Security Services	
SS.RNG	Random Number Generator
SS.HW_DES	Triple-DES coprocessor
SS.HW_AES	AES coprocessor
SS.RECONFIG	Post Delivery Configuration
Security Features	

TOE Security Functionality	Addressed issue
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

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], 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 [9], 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 for those cryptographic algorithms and their implementation suitable for encryption and decryption (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 P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software

The following table outlines the TOE deliverables:

Type	Identifier	Release	Date	Form of Delivery
Developer documents valid for all major configurations				
Document	Product data sheet SmartMX2 family P60D012/016/024 VB/VF Secure high-performance smart card controller, NXP Semiconductors Document Number 196752	5.2	27 June 2014	Electronic Document
Document	Instruction Set for the SmartMX2 family, Secure smart card controller, NXP Semiconductors, Document Number 1478**	3.1	02 February 2012	Electronic Document

Type	Identifier	Release	Date	Form of Delivery
Document	Information on Guidance and Operation, NXP Secure Smart Card Controller P60D024/016/012 VB/VF, NXP Semiconductors	1.8	20 November 2015	Electronic Document
Document	Wafer and delivery specification SmartMX2 family P60D012/016/024 VB/VF, NXP Semiconductors, Document Number 2180**	3.2	21 May 2014	Electronic Document
Document	Product data sheet addendum: SmartMX2 family Post Delivery Configuration (PDC), NXP Semiconductors, Document Number 2250**	3.2	04 February 2013	Electronic Document
Document	Product data sheet addendum: SmartMX2 family Chip Health Mode (CHM), NXP Semiconductors, Document Number 2244**	3.1	01 October 2014	Electronic Document
TOE Components for P60D024/016/012P				
IC Hardware	NXP Secure Smart Card Controller P60D024/016/012PVB(Y)	VB(Y)	20 September 2011	Wafer, module, inlay, package (dice have nameplate 9047A)
	NXP Secure Smart Card Controller P60D024/016/012PVB(Z)	VB(Z)	12 September 2012	
	NXP Secure Smart Card Controller P60D024/016/012PVB(A)	VB(A)		
	NXP Secure Smart Card Controller P60D024/016/012PVF	VF	27 November 2013	Wafer, module, inlay, package (dice have nameplate 9047B)
Security IC Dedicated Test Software	Test ROM Software	08.07	21 September 2011	Test-ROM on the chip acc. to 9047A_BG002_TESTROM_v1_btos_08v07_fos_5v0.hex
Security IC Dedicated Support Software	Boot-ROM Software	08.07	21 September 2011	Boot-ROM on the chip acc. to 9047A_BG002_TESTROM_v1_btos_08v07_fos_5v0.hex
Security IC Dedicated Support Software	Firmware Operating System (FOS)	5.0/5.03	21 September 2011	Firmware Operating System on the chip acc. to 9047A_BG002_TESTROM_v1_btos_08v07_fos_5v0.hex
TOE Components for P60D024/016/012M				
IC Hardware	NXP Secure Smart Card Controller P60D024/016/012MVB(Y)	VB(Y)	20 September 2011	Wafer, module, inlay, package (dice have nameplate 9047A)

Type	Identifier	Release	Date	Form of Delivery
	NXP Secure Smart Card Controller P60D024/016/012MVB(Z)	VB(Z)	12 September 2012	
	NXP Secure Smart Card Controller P60D024/016/012MVB(A)	VB(A)		
	NXP Secure Smart Card Controller P60D024/016/012MVF	VF	27 November 2013	Wafer, module, inlay, package (dice have nameplate 9047B)
IC Dedicated Test Software	Test-ROM Software	08.0A	17 April 2012	Test-ROM on the chip acc. to 9047A_BM097_TESTROM_v1_btos_08v0A_fos_6v10.hex
IC Dedicated Support Software	Boot-ROM Software	08.0A	17 April 2012	Boot-ROM on the chip acc. to 9047A_BM097_TESTROM_v1_btos_08v0A_fos_6v10.hex
	Firmware Operating System FOS	06.12 / 06.13	17 April 2012	Firmware Operating System on the chip acc. to 9047A_BM097_TESTROM_v1_btos_08v0A_fos_6v10.hex
TOE Components for P60D024/016/012D				
IC Hardware	NXP Secure Smart Card Controller P60D024/016/012DVF	VF	27 November 2013	Wafer, module, inlay, package (dice have nameplate 9047B)
IC Dedicated Test Software	Test-ROM Software	08.0C	22 April 2013	Test-ROM on the chip acc. to 9047A_BJ094_TESTROM_v1_btos_08v0C_fos_8v00.hex
IC Dedicated Support Software	Boot-ROM Software	08.0C	22 April 2013	Boot-ROM on the chip acc. to 9047A_BJ094_TESTROM_v1_btos_08v0C_fos_8v00.hex
	Firmware Operating System FOS	08.00	22 April 2013	Firmware Operating System on the chip acc. to 9047A_BJ094_TESTROM_v1_btos_08v0C_fos_8v00.hex

Table 2: Deliverables of the TOE

The requirements for the delivery of TOE are described in chapter 31 of the [13]. For each delivery form of the hardware platform NXP offers two ways of delivery of the TOE:

1. The customer collects the product himself at the NXP site, or

2. the product is sent to the customer by NXP with special protective measures.

The TOE documentation is delivered in electronic form by the document control centre of NXP.

The commercial type name is the identification used to order the TOE in the respective major configuration and with the evaluated package type. In consequence this means that a full commercial product name that fits in the variable forms described in [6] and [9] determines that the hardware platform is an evaluated product. In addition the hardware version can be identified by the coded nameplate "9047A" or “9047B” on the surface of the hardware platform as described in Chapters 4.2 and 3.9 of [16]. The nameplate “9047A” is

the same for all “VB” configurations and “9047B” for the configuration “VF”. In addition each major configuration has a different device coding described in [13, 31.2]. 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.

The major configurations P60D024/016/012M VB(Y/Z/A)/VF and P60D024/016/012D VF provide MIFARE functionality (MIFARE Plus MF1PLUSx0 or MIFARE DESFire EV1) which is not present in P60D024/016/012P VB(Y/Z/A)/VF. However, the MIFARE software does not contribute to the TSF. Therefore, all major configurations have to be considered as being identical, at least concerning their respective security functionality.

3. Security Policy

The security policy is defined by the selected set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The Security Policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement the symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a True Random Number Generator (TRNG).

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against 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 functionalities (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 and measures to be taken by the TOE environment, the user or the risk manager. The following topics are of relevance:

The objective OE.Plat-Appl states that the IC Embedded Software Developer must provide protection against disclosure of confidential data. Further, random numbers must be tested appropriately.

The objective OE.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) appropriately.

OE.Process-Sec-IC states that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

The objective OE.Check-Init states that the TOE provides specific functionality that allows the unique identification of the TOE in form of FabKey-Data.

Details can be found in the Security Target [6] and [9], chapter 4.2 and 4.3.

5. Architectural Information

The product is a single chip micro-controller unit designed by NXP Semiconductors Germany GmbH and built in 90 nm CMOS technology. A block diagram is given in the Security Target [6] and [9] chapter 1.4.1.

The TOE consists of the following hardware:

- CPU / co-processors:
  - a CPU implementation supporting a 32-/24-/16-/8 bit instruction set which is a superset of the 80C51 family instruction set and distinguishes four CPU modes,
  - a Triple-DES co-processor, supporting single DES and Triple-DES operations (in 2-key or 3-key operation, with two/three 56 bit keys (112-/168 bit)), where only Triple-DES operations are evaluated and considered as security functionality,
  - an Advanced Encryption Standard (AES) co-processor with key lengths of 128, 192 and 256 bits,
  - an arithmetic co-processor, called Fame2 co-processor, whose availability is subject to specific choice of Customer Reconfiguration Options. It supplies basic arithmetic functions to support implementation of asymmetric cryptographic algorithms by the Security IC Embedded Software; the Security IC Embedded Software is not part of the TOE,
  - a CRC co-processor, providing the CRC generation polynomials CRC-16 and CRC-32 for hardware cyclic redundancy check calculations,
- Memory / Memory Controller:
  - Read-Only Memory (ROM): the TOE incorporates 352 kBytes of ROM, where 1 kByte = 1024 Bytes. The ROM is partitioned by a Memory Management Unit (MMU) into 264 kBytes Application-ROM for the Security IC Embedded Software. 88 kBytes are reserved for the Test-ROM, Boot-ROM, and Firmware including emulations,
  - Random Access Memory (RAM): 8.125 kBytes of RAM, which is parted into RAM available to the Firmware Operating System only (512 Bytes). The remainder, which is available to the Security IC Embedded Software, is split into 2.625 kBytes for the Fame2 co-processor, called FXRAM and 5.0 kBytes general purpose RAM, called CXRAM,
  - Electrically Erasable Programmable Read Only Memory (EEPROM): An overall maximum of 24 kBytes of EEPROM, where 768 Bytes are always reserved for IC Dedicated Support Software, 512 Bytes for the manufacturer area and whose actual size is subject to specific choice of Major Configuration and Customer Reconfiguration Options,
  - Memory Controller: A Memory Management Unit (MMU) controls access to all of the three above mentioned memory types,
- Internal Peripherals:

- a True Random Number generator,
- reset generator,
- watch-dog timer, configurable by the Security IC Embedded Software to protect program execution,
- 16 bit timers (T0 and T1),

- Physical protection:
  - secure shielding,
  - security sensors with reset generator,
- Electrical interfaces:
  - ISO/IEC 14443 A contactless interface with pads LA and LB, whose availability is subject to a minor configuration option,
  - ISO/IEC 7816 contact interface with serial communication pad I/O,
  - single external power supply of 1.8 V, 3 V or 5 V nominal by the lines VDD and VSS, or supply by inductive coupling via the ISO/IEC 14443 A contactless interface,
  - clock input CLK with a clock filter and clock generator,
  - reset input RST_N.

The TOE consists of the following firmware:

- Security IC Dedicated Test Software, which is stored to the Test-ROM and used by the manufacturer of the Security IC during production test; it includes the test operating system, test routines for the various blocks of the circuitry, control flags for the status of the EEPROM's manufacturer area and shutdown functions,
- Security IC Dedicated Support Software, according to:
  - Boot-ROM Software, executed during start-up,
  - the Firmware Operating System (FOS) provides an interface for the Security IC Embedded Software. This interface is called FVEC. There are several FVECs defined, namely FVEC0.x, FVEC1.x, FVEC3.x and FVEC7.x. The letter „x" is a placeholder for the sub functions of the FVECs. „x" can be a number between 1 and 255. Please note not all sub numbers are valid.

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 can be divided into the following categories:

7.1. Developer's Test according to ATE_FUN

Testing has been performed by the developer according to a documented testing approach, covering well defined TOE configurations and various categories of tests, thereby covering the whole TOE security functionality.

The developer's testing results demonstrate that the TOE in general and its TSFs behave as expected and specified.

TOE test configuration and developer's testing approach:

- The tests are performed with the TOE in different test environments and configurations depending on the test categories.
- All TSF and related security mechanisms, subsystems and modules are tested in order to assure complete coverage of all SFR.

Test categories:

- Production testing on wafers using test functions implemented in the IC Dedicated Software. These test functions are accessed via test commands, which are issued by the production tests. Test functions respond signatures to the production tests. Production tests also apply signals to and/or measures signals at any contact of the device. Final test or module test therefore is limited to a verification of electrical connections like checking the pins of the package for shorts and opens.
- Simulation tests are performed to verify functionality, which is not visible at the accessible interfaces of the TOE. These simulation tests are a subset of those, which were performed during development of the device to ensure a proper design of its modules.

  During run-time of a simulation an automated regression test continuously compares pre-defined internal signals (probe list) like data and address buses, control signals, register contents and microcode information against a "golden reference". Test results are automatically listed in log files and a summary, i.e. discrepancies occurred (yes/no), is output to the user interface.

  Manual simulation tests are performed in case an automated result comparison based on executable code is not possible.
- Characterization tests verify the electrical properties of the device, which are specified with regard to limiting values, thresholds and timings of several electrical parameters like voltages, currents, frequencies, capacitors, resistances and latches. For this purpose a number of devices for test are taken from production.
- Verification tests are performed on single samples of the device to verify specific security functionality, which is not testable for each device during production test or within the scope of characterization testing. Such tests include standard tests of the Random Number Generator, AES coprocessor and Triple-DES coprocessor.
- Test of configurations: Configuration data are stored to EEPROM based on the customer's choices in the Order Entry Form at later stages of the production test. For this purpose production test implements special test steps relying on an according test strategy to verify the required configuration. Special parts of verification tests explicitly test the configuration options of the device.

7.2. Independent Testing according to ATE_IND

As a result, the evaluator’s testing results demonstrate that the TOE in general and its TSFs behave as expected and specified.

The independent testing was partly performed in the developer’s testing environment and partly at TÜViT GmbH, information security department, in Essen. The same platforms and tools as for the developer tests were used (see ATE_FUN one section above).

Testing approach:

- The evaluator's objective regarding this aspect was to test the functionality of the TOE, and to verify the developer's test results by repeating developer's tests and additionally add independent tests.
- In the course of the evaluation of the TOE the following classes of tests were carried out:
  - Module tests,
  - Simulation tests,
  - Emulation tests,
  - Tests in user mode,
  - Tests in test mode,
  - Hardware tests.

With this kind of tests the entire security functionality of the TOE was tested.

7.3. Penetration Testing according to AVA_VAN

The penetration testing was partially performed using the developer’s testing environment, partially using the test environment of the evaluation body.

All configurations of the TOE being intended to be covered by the current evaluation were tested. The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential high was actually successful.

Penetration testing approach:

- Systematic search for potential vulnerabilities and known attacks in public domain sources, use of a list of vulnerabilities, and from a methodical analysis of the evaluation documents.
- Analysis why these vulnerabilities are unexploitable in the intended environment of the TOE.
- If the rationale is suspect in the opinion of the evaluator penetration tests are devised.
- Even if the rational is convincing in the opinion of the evaluator penetration tests are devised for some vulnerabilities, especially to support the argument of non-practicability of exploiting time in case of SPA, DPA and FI attacks.
- The tests are performed with the chip P60D024/016/012yVB(Y/Z/A)/yVF. For the tests different chip types are prepared with different patch. With the loaded patch

code the defined tests could be performed. The entire functionality is the same for all chips.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- P60D024/016/012P VB(Y/Z/A)/VF,
- P60D024/016/012M VB(Y/Z/A)/VF,
- P60D024/016/012D VF,

The major configurations M, D, and J provide MIFARE functionality. However, MIFARE emulation is explicitly excluded from the logical scope of the TOE for the current evaluation. The evaluation scope of both emulations is limited to being non-interfering with the TSF.

The P60D024/016/012yVB(Y/Z/A)/yVF hardware platform was tested including all minor configuration options that can be selected based on Table 8 in chapter 1.4.2.2 of [6] and [9]. The major configuration does not have dependencies to security features. All minor configuration options that are part of the evaluation were tested. The minor configuration options behave as specified and described in [13] and [15]. Therefore the results described in this document are applicable for all minor configurations described in [6] and [9].

These minor configuration options (and all others) for NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF can be selected by the customer via Order Entry Form. The Order Entry Form identifies all the minor configuration options, which are supported by the major configuration. However, only those minor configurations mentioned above correspond to different commercial product identifiers.

Further some minor configurations can be deselected once after the delivery via post-delivery configuration (PDC).

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] 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.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the EAL 6 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 and ASE_TSS.2 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0939-2015, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on life cycle and Side Channel Attacks.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [8]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 6 augmented by ALC_FLR.1 and ASE_TSS.2

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	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
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
Physical RNG PTG.2	[AIS31]	N/A	N/A	Supports cryptographic implementations

Table 3: TOE cryptographic functionality

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 this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the IC Dedicated Support Software and/or Embedded Software using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented 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 product layer on top. 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].

11. Security Target

For the purpose of publishing, the Security Target [9] 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
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FVEC	Firmware Verctor Call
IT	Information Technology
IC	Integrated Circuit
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITSEF	Information Technology Security Evaluation Facility
PDC	Post Delivery Configuration
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
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0939-V2, NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF, NXP Semiconductors, Version 4.1, 23 November 2015 (confidential document)

[7] Evaluation Technical Report, for the P60D024/016/012y VB(Y/Z/A)/VF, TÜV Informationstechnik GmbH, Version 2, 17 December 2015 (confidential document)

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

[9] Security Target Lite BSI-DSZ-CC-0939-V2, NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF, NXP Semiconductors, Version 4.1, 23 November 2015 (sanitised public document)

[10] Evaluation Technical for Composite Evaluation (ETR COMP) for the P60D024/016/012y VB(Y/Z/A)/VF, TÜV Informationstechnik GmbH, Version 2, 17 December 2015 (confidential document)

[8] 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 EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 38, Version 2, Reuse of evaluation results

[11] NXP Secure Smart Controller P60D024/016/012yVB(Y/Z/A)/ yVF Configuration List, NXP Semiconductors, Version 2.50, 20 November 2015 (confidential document)

[12] NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF Evaluation Reference List, NXP Semiconductors, Version 3.21, 14 December 2015 (confidential document)

[13] SmartMX2 family P60D012/016/024 VB/VF Secure high-performance smart card controller Product data sheet, NXP Semiconductors, Version 5.2, 27 June 2015 (confidential document)

[14] Instruction set for the SmartMX2 family Secure smart card controller Product data sheet, NXP Semiconductors, Version 3.1, 02 February 2012 (confidential document)

[15] NXP Secure Smart Card Controller P60D012/016/024 VB/VF Information on Guidance and Operation Guidance and Operation Manual, NXP Semiconductors, NXP Semiconductors, Version 1.8, 20 November 2015 (confidential document)

[16] SmartMX2 family P60D012/1016/024 VB/VF Wafer and delivery specification Product data sheet addendum, NXP Semiconductors, Version 3.2, 21 May 2014 (confidential document)

[17] SmartMX2 family Post Delivery Configuration (PDC) Secure high-performance smart card controller Product data sheet addendum, NXP Semiconductors, Version 3.2, 04 February 2013 (confidential document)

[18] Product data sheet addendum: SmartMX2 family Chip Health Mode (CHM), NXP Semiconductors, Document Number 2244**, NXP Semiconductors, Version 3.1, 01 October 2014 (confidential document)

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
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

Assurance Class	Assurance Components
	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.

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

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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”

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.”

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-0939-V2-2016

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software (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 Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 18 February 2016, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_FLR.1, ALC_LCD.1, ALC_TAT.3)

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

Development site	Task within the evaluation
NXP Semiconductors Hamburg Business Unit Security & Connectivity (BU S&C) Stresemannallee 101 22569 Hamburg Germany	Development, Delivery and customer support
NXP Semiconductors Development Center Eindhoven HTC-46.3 West Building 46, High Tech Campus 5656AE, Eindhoven The Netherlands	Development center
NXP Semiconductors Departments RQC, TOO and MM of NXP NXP Semiconductors Netherlands B.V. Gerstweg 2 6534AE Nijmegen The Netherlands	Development and Manufacturing, Regional Quality Center - Europe
NXP Semiconductors Austria GmbH Styria Business Unit Security & Connectivity (BU S&C) Mikron-Weg 1 8108 Gratkorn Austria	Document control
NXP High Tech Campus Building 60, High Tech Campus Secure Room 131 5656AE, Eindhoven	Tape Out Office, and Materials Management Department

Development site	Task within the evaluation
The Netherlands	
Atos Bydgoszcz Building BETA Secure Room B20S1 Biznes Park ul. Kraszewskiego 1 85-240 Bydgoszcz Poland	IT Engineering and Generic Support
TSMC, Fab 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 No. 1, Nan-Ke North Rd. Tainan Science Park Tainan, Taiwan 741, R.O.C.	Mask and wafer production
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	Module assembly and test center
Ardentec Corporation (T Site) No. 3, Gungye 3rd Rd. Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien Taiwan 30351, R.O.C	Wafer Testing
Ardentec Corporation (K Site)	Wafer processing

Development site	Task within the evaluation
No. 24, Wen-Huan Rd. Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien Taiwan 30351, R.O.C.	
NedCard (Shanghai) Microelectronics Co Ltd. Standardized Plant Building #8 No. 789 Puxing Road Caohejing Hi-Tech Park, EPZ 201114 Shanghai, People's Republic of China	Module assembly, final testing
NedCard B.V. Bijsterhuizen 25-29 6604 LM Wijchen The Netherlands	Module assembly, final testing
Smartflex Technology Pte Ltd 27, Ubi Road 4 #04-01 Singapore 408618	Module assembly, final testing
HID Global Teoranta Paic Tionscail na Tulaigh Balle na hAbhann Co. Galway Ireland	Inlay assembly
SMARTRAC Technology Ltd. Bangkok Street: 142 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In 13160 Ayutthaya Thailand	Inlay 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 [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.