Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0939-V3-2018

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-V3-2018 (*)

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 ASE_TSS.2, ALC_FLR.1

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 Scheme Interpretations, 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 recognition for components up to EAL 2 and ALC_FLR only

Bonn, 17 December 2018

For the Federal Office for Information Security

Thomas Gast
Head of Branch

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.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- 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[4] [1] also published as ISO/IEC 15408.

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

2 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

3 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

- 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]

3. 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.

3.1. European Recognition of 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.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. 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 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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. 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 current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

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

4. 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-V2-2016. Specific results from the evaluation process BSI-DSZ-CC-0939-V2-2016 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 26 November 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] 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.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this 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-assessment or 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 would 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 17 December 2018 is valid until 16 December 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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.

6. 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] NXP Semiconductors Germany GmbH
Troplowitzstrasse 20
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.

The TOE also includes documentation describing the Instruction Set and the usage. Within this document the TOE will be abbreviated by P60D024/016/012yVB(Y/Z/A)/VF or short P60D024/016/012y.

The IC hardware platform NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/VF is a microcontroller incorporating a central processing unit, memories accessible via a Memory Management Unit, cryptographic coprocessors, 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.

Except for the y=P configuration the P60D024/016/012yVB(Y/Z/A)/VF includes Emulation Software MIFARE Plus MF1PLUSx0 and/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 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 ASE_TSS.2 and ALC_FLR.1.

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	
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation

TOE Security Functionality	Addressed issue
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
TOE components for P60D024/016/012P configurations				
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)

Type	Identifier	Release	Date	Form of Delivery
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 configurations				
IC Hardware	NXP Secure Smart Card Controller P60D024/016/012MVB(Y)	VB(Y)	20 September 2011	Wafer, module, inlay, package (dice have nameplate 9047A)
	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	Boot-ROM Software	08.0C	22 April 2013	Boot-ROM on the chip acc. to 9047A_BJ094_TESTROM_v1_btos_08v0C_fos_8v00.hex

Type	Identifier	Release	Date	Form of Delivery
Support Software	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
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	5.2	27 June 2014	Electronic Document
Document	Instruction Set for the SmartMX2 family, Secure smart card controller, NXP Semiconductors	3.1	02 February 2012	Electronic Document
Document	Information on Guidance and Operation, NXP Secure Smart Card Controller P60D024/016/012 VB/VF, NXP Semiconductors	2.4	24 October 2018	Electronic Document
Document	Wafer and delivery specification SmartMX2 family P60D012/016/024 VB/VF, NXP Semiconductors	3.2	21 May 2014	Electronic Document
Document	Product data sheet addendum: SmartMX2 family Post Delivery Configuration (PDC), NXP Semiconductors	3.2	04 February 2013	Electronic Document
Document	Product data sheet addendum: SmartMX2 family Chip Health Mode (CHM), NXP Semiconductors	3.1	01 October 2014	Electronic Document
Document	Product Errata Sheet SmartMX2 family P60D012/016/024 VB/VF Secure high-performance smart card controller, NXP Semiconductors	1.2	24 October 2018	Electronic Document

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] chapter 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.

Please note that 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.

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:

- 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

The complete TOE reference is given by NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software (see [6] and [9], chapter 1.2) where y is a placeholder for:

- y = P: Plain configuration without Mifare software.
- y = M: The availability of MIFARE Plus MF1PLUSx0.
- y = D: The availability of MIFARE DESFire EV1.

These TOE configurations and their components are defined in [6] and [9], chapter 1.4

The TOE can be configured into (see [6] and [9]):

- Major configurations for example P60D016PVB(Y), P60D012PVB(Z), P60D024PVB(A) or P60D012DVF (chapters 1.2 and 1.4.1),
- Minor configurations (chapter 1.4.2.2),
- Post-delivery configurations (chapter 1.4.2.3) and
- Evaluated package types (chapter 1.4.2.4).

The memory sizes available for the IC Embedded Software depend on the major configuration of the TOE as described in [6] and [9] chapter 1.4.2.1.

The P60D024/016/012y 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].

The major configurations M and D 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.

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 ASE_TSS.2, ALC_FLR.1 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-V2-2016, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on life cycle and Penetration Testing.

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 ASE_TSS.2, ALC_FLR.1

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.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

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].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

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

- A new guidance document [19] was introduced to address specific behaviour of the memory management unit (MMU). This also causes an update of the access control policy defined in the security target [6] and [9].

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 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://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[7] 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-V3, NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF, Version 4.4, 29 October 2018, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report, for the P60D024/016/012yVB(Y/Z/A)/VF, Version 4, 26 November 2018, TÜV Informationstechnik GmbH (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-V3, NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF, Version 4.4, 29 October 2018, NXP Semiconductors (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 4, 26 November 2018 (confidential document)

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

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 9, 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 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1, Regelungen zu Site Certification

[12] NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF Evaluation Reference List, NXP Semiconductors, Version 3.26, 14 November 2018 (confidential document)

[13] Product Data Sheet SmartMX2 family P60D012/016/024 VB/VF Secure high-performance smart card controller, Version 5.2, 27 June 2014 (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] Information on Guidance and Operation, NXP Secure Smart Card Controller P60D012/016/024 VB/VF, NXP Semiconductors, Version 2.4, 24 October 2018 (confidential document)

[16] Product data sheet addendum: Wafer and delivery specification SmartMX2 family P60D012/016/024 VB/VF, 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, NXP Semiconductors, Version 3.1, 01 October 2014 (confidential document)

[19] Product Errata Sheet SmartMX2 family P60D012/016/024 VB/VF Secure high-performance smart card controller, NXP Semiconductors, Version 1.2, 24 October 2018 (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

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

Annex B of Certification Report BSI-DSZ-CC-0939-V3-2018

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 17 December 2018, 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:

Name of site / Company name	Address	Function
Development Sites		
NXP Hamburg	Business Unit Identification Troplowitzstraße 29 22569 Hamburg, Germany	Development, Delivery and customer support
NXP Eindhoven	Building 46, High Tech Campus 5656AE, Eindhoven, The Netherlands	Development center
NXP Nijmegen	NXP Semiconductors Netherlands B.V. Gerstweg 2 6534AE Nijmegen, The Netherlands	Development and Manufacturing, Regional Quality Center - Europe
NXP Gratkorn	Business Unit Identification Mikron-Weg 1 8108 Gratkorn, Austria	Document control
NXP High Tech Campus Building 60 Secure Room	Building 60, High Tech Campus Secure Room 131 5656AE, Eindhoven, The Netherlands	IT Engineering and Generic Support
Development Center NXP Bangalore	NXP Semiconductors India Private Limited Manyata Technology Park Nagawara Village,	TOE database

Name of site / Company name	Address	Function
	Kasaba Hobli, Bangalore 560045 India	
DC COLT– Obenhauptstrasse – 22335 Hamburg - Germany	Obenhauptstrasse, 22335 Hamburg - Germany	TOE Database
DC Akquinet – Ulzburger Strasse 201 – 22850 Norderstedt - Germany	Ulzburger Strasse 201, 22850 Norderstedt - Germany	TOE Database
Production Sites		
TSMC Tainan and Hsinchu	Fab 14A: 1-1, Nan-Ke North Rd., Tainan Science Park, Tainan 741-44, Taiwan, R.O.C., Fab 2 and 5: 121, Park Ave. 3, Hsinchu Science Park, Hsinchu 300-77, Taiwan, R.O.C., Fab 8: 25, Li-Hsin Rd., Hsinchu Science Park, Hsinchu, 300-78, Taiwan, R.O.C.	Mask data preparation, Mask and wafer production
Chipbond, Hsin-Chu Chity, Taiwan	No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping
Test Center Europe - Hamburg (TCE-H)	Troplowitzstraße 29 22569 Hamburg, Germany	Test Center, configuration of the Fabkey, and delivery
NXP ATBK	303 Moo 3 Chaengwattana Rd. Laksi, Bangkok 10210, Thailand	Test centre, wafer treatment, module assembly and delivery
NXP ATKH	#10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170 Taiwan, R.O.C	Test centre, wafer treatment, module assembly and delivery
HID Global Teoranta	Paic Tionscail na Tulaigh Balle na hAbhann Co. Galway, Ireland	Inlay assembly
Linxens (Thailand) Co Ltd.	Street: 142 Moo, Hi- Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In 13160 Ayutthaya, Thailand	Inlay assembly

Table 4: Relevant development/production sites for the respective TOE configurations

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.

Note: End of report