Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1051-2019

for

NXP Smart Card Controller P61N1M3VD/VD-1/PVE-1 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-1051-2019 (*)

Smartcard Controller

NXP Smart Card Controller P61N1M3VD/VD-1/PVE-1 with IC Dedicated Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
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, 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 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, 15 March 2019

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

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 Smart Card Controller P61N1M3VD/VD-1/PVE-1 with IC Dedicated Software has undergone the certification procedure at BSI.

The evaluation of the product NXP Smart Card Controller P61N1M3VD/VD-1/PVE-1 with IC Dedicated Software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 8 February 2019. 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 15 March 2019 is valid until 14 March 2024. Validity can be re-newed by re-certification.

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

[5] Information Technology Security Evaluation Facility

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 Smart Card Controller P61N1M3VD/VD-1/PVE-1 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 TOE is the NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 including IC Dedicated Software. The TOE does not include a customer-specific Security IC Embedded Software.

The IC hardware is a microcontroller incorporating a central processing unit, memories accessible via a Memory Management Unit, cryptographic co-processors, other security components and several electrical communication interfaces. The central processing unit supports a 32-/24-/16-/8-bit instruction set optimized for smartcard applications, which is a superset of the 80C51 family instruction set. The first and in some cases the second byte of an instruction are used for operation encoding. On-chip memories are ROM, Flash, EEPROM and RAM. The ROM is reserved for IC Dedicated Software. Flash and EEPROM can be used by the Security IC Embedded Software for code and data. They consist of high reliable memory cells, which guarantee data integrity. Flash and EEPROM are optimised for applications that require reliable non-volatile data storage for data and program code. Dedicated security functionality protects the contents of all memories.

The IC Dedicated Software comprises IC Dedicated Test Software for test purposes and IC Dedicated Support Software. The IC Dedicated Support Software consists of the Boot-ROM Software, which controls the boot process of the hardware platform, the Firmware Operating System and the Bootloader Software. The Firmware Operating System serves a hardware control interface for Flash and EEPROM, which is accessible to the Security IC Embedded Software. The Bootloader Software is not accessible to the Security IC Embedded Software.

Users have the possibility to tailor the crypto co-processor part of the TOE during the manufacturing process by deselecting the Symmetric Block Cipher Interfaces. Hence the TOE can be delivered with or without the functionality of 3DES and AES, respectively. This is considered in the developer documentation and corresponding notes are added, where required. If the user decides not to use the Symmetric Block Cipher Interfaces, it can be deactivated during life cycle phases 5 and 6 and cannot be activated by the end consumer (i.e. after phase 6). In case of deactivation, the accompanying additional specific security functionality 3DES and AES is not provided to the end consumer by the TOE. Deselecting the Symmetric Block Cipher Interfaces has no impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the functionality. Also the Fame2 co-processor can be deactivated during the life cycle phases 5 and 6 (post-delivery configuration), which results in the fact that the dedicated hardware support for asymmetric calculations cannot be used. In either case, a software cryptographic library is not part of the TOE and thus not in scope of the evaluation. Besides the crypto co-processor blocking, the user has also the possibility to block the memory size of the EEPROM/Flash and RAM and choose between different interface options. This has no influence to the security policy of the TOE.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [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, ASE_TSS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6. 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 co-processor
SS.HW_AES	AES co-processor
Security Features	
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, 3.3 and 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 Smart Card Controller P61N1M3VD/VD-1/PVE-1 with IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
Developer documents valid for all base types				
1	Document	SmartMX2 P61N1M3 Secure high-performance mobile controller, Product data sheet	3.1, 2014-09-02	PDF via DocStore
2	Document	Instruction Set for the SmartMX2 family, Secure smart card controller	3.1, 2012-02-02	PDF via DocStore
3	Document	Chip Health Mode (CHM) for P61N1M3, data sheet addendum	1.2, 2013-08-09	PDF via DocStore
4	Document	P61N1M3 Firmware interface specification, data sheet addendum	1.6, 2013-10-31	PDF via DocStore
5	Document	NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 Information on Guidance and Operation	2.2, 2018-11-13	PDF via DocStore
6	Document	SmartMX2 family P61N1M3 VD/VE Wafer and delivery specification, data sheet addendum	1.5, 2013-10-31	PDF via DocStore
7	Document	Trust Provisioning – Trust Provisioning concept and security architecture	1.8, 2014-05-19	PDF via DocStore
8	Document	Key Delivery Procedures for Trust Provisioning	1.1, 2014-01-13	PDF via DocStore
9	Document	SmartMX2 family P61N1M3 Product errata sheet	1.2, 2018-11-13	PDF via DocStore
TOE Components for base types P61N1M3VD and P61N1M3VD-1				
10	IC Hardware	P61N1M3VD / P61N1M3VD-1	Identified by name plate 9068B and the NXP Content Number (NCN) which is “65” in case of P61N1M3VD and “67” in case of P61N1M3VD-1	Wafer with dice acc. to 9068B_BE_20130604. gds2.gz.
11	IC Dedicated Test Software	Test-ROM Software	Identified by NXP Content Number (NCN) which is “65” in case of P61N1M3VD and “67” in case of P61N1M3VD-1	ROM code on the IC acc. to 9068B_DA005_TESTROM_ v1_btos_0Ev13_fos_9v30rc 4.hex.
12	IC Dedicated Support Software	Boot-ROM Software		
		Firmware Operating System		
		Bootloader Software		ROM code on the IC acc. to phBootloader_P61_Crc.hex.
13	Document	P61N1M3 VD, NV Properties, data sheet addendum	1.0, 2013-11-22	
TOE Components for base type P61N1M3VE-1				

No	Type	Identifier	Release	Form of Delivery
14	IC Hardware	P61N1M3VE-1	Identified by name plate 9068C and the NXP Content Number (NCN) which is “84” in case of P61N1M3VE-1	Wafer with dice acc. to 9068C_20130808. gds2.gz.
15	IC Dedicated Test Software	Test-ROM Software	Identified by NXP Content Number (NCN) which is “85” in case of P61N1M3VE-1	ROM code on the IC acc. to 9068C_DA007_TESTROM_v1_btos_0Ev15_fos_9v3.hex.
16	IC Dedicated Support Software	Boot-ROM Software		
17		Firmware Operating System		
18		Bootloader Software		ROM code on the IC acc. to phBootloader_P61_Crc.hex.
19	Document	P61N1M3 VE, NV Properties, data sheet addendum	1.0, 2013-11-22	PDF via DocStore

Table 2: Deliverables of the TOE

Customers have to make sure that they always order and receive a security controller in a configuration and a package type, which was evaluated according to the related description within the Guidance and Operation Manual [16] chapter 2.

The requirements for the delivery of TOE are described in the “Product Data Sheet” [12] chapter 33 and the requirements for the delivery itself are given in the “Wafer and delivery specification” [17] chapter 4. 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. The delivery is protected by special measures.

3. Security Policy

The Security Policy is expressed by the 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.

Specific details concerning the above mentioned security policies can be found in chapter 7 of the Security Target [6] and [9]

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.Process-Sec-IC, OE.Lim_Block_Loader and OE.Check-Init. Details can be found in the Security Target [6] and [9], chapter 4.3.

5. Architectural Information

The TOE comprises the hardware of the above mentioned smart card security controllers and part of the associated firmware / software required for operation. All other software is called Security IC Embedded Software, which is not part of the TOE.

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 five 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 AES co-processor (key sizes 128, 192 or 256 bit), whose availability is subject to specific choice of Customer Reconfiguration Options, supporting AES operations with three different key lengths,
  - 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 (i.e. ROMinized Flash): the TOE incorporates up to 184 kBytes of ROM, where 1 kByte = 1024 Bytes. The ROM is partitioned by a Memory Management Unit (MMU) into 32 kBytes Application-ROM for the Security IC Embedded Software. 152 kBytes are reserved for the Test-ROM ([6] and [9], chapter 1.4.3.1),
  - Random Access Memory (RAM): 34.625 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 31.5 kBytes general purpose RAM, called CXRAM,

- Electrically Erasable Programmable Read Only Memory (EEPROM): An overall maximum of 128 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,
- Flash NVM: 1216kB of Flash NVM are available, partitioned by a Memory Management Unit (MMU) into 32 kB chunks,
- Memory Controller: A Memory Management Unit (MMU) controls access to all of the three above mentioned memory types,
- Copy Machine: a device providing direct memory access for the Security IC Embedded Software without CPU interactions.

- Internal Peripherals:
  - a True Random Number generator,
  - reset generator,
  - a 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 7816 compliant interface by use of ISO/IEC 7816 UART,
  - I/O interface by use Special Function Registers,
  - Serial Peripheral Interface (SPI),
  - ETSI TS 102 613 compliant SWP interface,
  - SWP interface in dual pad configuration by use of ETSI TS 102 613 protocol,
  - S²C interface by use of ISO/IEC 14443 protocol.

Furthermore, 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, bipartite 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. The P61N1M3PVD/VD-1/VE-1

provides eight firmware vectors (FVEC) and 32 system call vectors (SVEC). These vectors have to be explicitly called by the Security IC Embedded Software. A jump to a firmware vector forces Firmware Mode and starts execution of the Firmware Operating System, a jump to a system call vector forces System Mode.

6. Documentation

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

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

7. IT Product Testing

The tests performed by the developer were divided into five categories:

- Simulation tests (design verification),
- Qualification tests,
- Verification tests,
- Security Evaluation tests,
- Production tests.

The developer tests cover all security functionalities and all security mechanisms as identified in the functional specification.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developer's site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. For the developer tests repeated by the evaluators other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically. The penetration tests results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

The customer selects logical and physical configuration options of each base type without modification of its physical scope, as described in section 1.4.1 of [6] and [9]. Logical configuration options are structured in major configuration options according to section 1.4.2.1 and minor configuration options according to section 1.4.2.2 of [6] and [9].

One major configuration is target of evaluation for each base type, which is denoted by name P61N1M3PVD for base type P61N1M3VD, P61N1M3PVD-1 for base type P61N1M3VD-1 and P61N1M3PVE-1 for base type P61N1M3VE-1. The major configuration is chosen by the customer via Order Entry Forms [23] and [24] as detailed in Table 3

Major configuration	Base type
P61N1M3P	P61N1M3VD
	P61N1M3VD-1
	P61N1M3VE-1

Table 3: Evaluated Configurations

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, ASE_TSS.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [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, 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).

The table in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. 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) only.

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.

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

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
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 NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 BSI-DSZ-CC-1051-2019, Version 2.11, 2019-01-10, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report P61N1M3P VD/VD-1/VE-1, Version 3, 2019-01-28, TÜV Informationstechnik GmbH, (confidential document)

[8] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014

[9] Security Target Lite NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 BSI-DSZ-CC-1051-2019, Version 2.11, 2019-01-10, NXP Semiconductors (sanitised public document)

[10] ETR for composite evaluation P61N1M3P VD/VD-1/VE-1, 2019-01-28, TÜV Informationstechnik GmbH (confidential document)

[11] NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 Configuration List, Version 1.19, 2019-01-10, NXP Semiconductors (confidential document)

[12] SmartMX2 P61N1M3 Secure high-performance mobile controller Product Data Sheet, Version 3.1, 2014-09-02, NXP Semiconductors

[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

[13] Instruction Set for the SmartMX2 family, Secure smart card controller, Version 3.1, 2012-02-02, NXP Semiconductors

[14] Chip Health Mode (CHM) for P61N1M3, data sheet addendum, Version 1.2, 2013-08-09, NXP Semiconductors

[15] P61N1M3 Firmware interface specification, data sheet addendum, Version 1.6, 2013-10-31, NXP Semiconductors

[16] NXP Secure Smart Card Controller P61N1M3PVD/VD-1/VE-1 Information on Guidance and Operation, Version 2.2, 2018-11-13, NXP Semiconductors

[17] SmartMX2 family P61N1M3 VD/VE Wafer and delivery specification, data sheet addendum, Version 1.5, 2013-10-31, NXP Semiconductors

[18] Trust Provisioning – Trust Provisioning concept and security architecture, Version 1.8, 2014-05-19, NXP Semiconductors

[19] Key Delivery Procedures for Trust Provisioning, Version 1.1, 2014-01-13, NXP Semiconductors

[20] SmartMX2 family P61N1M3 Product errata sheet, Version 1.2, 2018-11-13, NXP Semiconductors

[21] P61N1M3 VD, NV Properties, data sheet addendum, Version 1.0, 2013-11-22, NXP Semiconductors

[22] P61N1M3 VE, NV Properties, data sheet addendum, Version 1.0, 2013-11-22, NXP Semiconductors

[23] Order Entry Form P61N1M3PVD/E, Version 0.67, 2014-03-19, NXP Semiconductors

[24] Order Entry Form P61N1M3PVD-1/E-1, Version 1.1, 2014-08-26, NXP Semiconductors

[25] SITE TECHNICAL AUDIT REPORT (STAR) Production Environment (Mask production) Toppan Photomasks Korea Ltd., Korea Icheon, Version 1, 2018-10-22, TÜV Informationstechnik GmbH

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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1051-2019

Evaluation results regarding development and production environment

The IT product NXP Smart Card Controller P61N1M3VD/VD-1/PVE-1 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 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 15 March 2019, 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)

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
Digital Realty	120 East Van Buren St, Phoenix, AZ 85004, United States	TOE database

Name of site / Company name	Address	Function
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	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 7: 25, Li-Hsin Rd., Hsinchu Science Park, Hsinchu, 300-78, Taiwan, R.O.C.	Mask data preparation, Mask and wafer production
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

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

Name of site / Company name	Address	Function
Production Site		
Toppan Icheon (refer to STAR [25])	Toppan Photomasks Korea Ltd. 91, Wonjeok-ro 290 beon-gil, Sindun-myeon Icheon-Si, Gyeonggi-do 467-842 South Korea	Mask production

Table 5: Sites audited in the course of the evaluation, but not part of the life-cycle

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.

Annex C of Certification Report BSI-DSZ-CC-1051-2019

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Cryptographic Primitives	2-key Triple DES (ECB)	[NIST SP800-67] (legacy use) [NIST SP800-38A]	|k| = 112	No
2		3-key Triple DES (ECB)	[NIST SP800-67] [NIST SP800-38A]	|k| = 168	No
3		AES (ECB)	[FIPS-197]	|k| = 128 / 192 / 256	No
4		Physical RNG PTG.2	[AIS31]	N/A	Yes

Table 6: TOE cryptographic functionality

Note: End of report