Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1072-V4-2021

for

NXP Secure Smart Card Controller P6021y VB* including 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-1072-V4-2021 (*)

Smartcard Controller

NXP Secure Smart Card Controller P6021y VB* including 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 extended EAL 6 augmented by ASE_TSS.2 and 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 5.

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, 24 June 2021

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

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

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

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

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

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

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

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]
- BMI Regulations on Ex-parte 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]

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 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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.sogis.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 P6021y VB* including IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1072-V3-2019. Specific results from the evaluation process BSI-DSZ-CC-1072-V3-2019 were re-used.

The evaluation of the product NXP Secure Smart Card Controller P6021y VB* including IC Dedicated Software was conducted by TÜV Informationstechnik. The evaluation was completed on 18 June 2021. TÜV Informationstechnik 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 24 June 2021 is valid until 26 June 2026. 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 Secure Smart Card Controller P6021y VB* including 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 P6021y VB* with IC Dedicated Software and documentation describing the Instruction Set and the usage. The * in the TOE name indicates that MIFARE emulations are not part of the TSF and do not implement any Security Functional Requirement. The evaluation scope of the MIFARE emulations is limited to not interfere with the functionality provided by the IC hardware platform. The short name P6021y VB will be used in the following sections.

The P6021y VB is a microcontroller incorporating a central processing unit, memories accessible via a Memory Management Unit, cryptographic co-processors, other security components and two communication interfaces. The central processing unit supports a 32-/24-/16-/8-bit instruction set optimized for smart card applications, which is a super set of the 80C51 family instruction set. On-chip memories are ROM, RAM and EEPROM. The non-volatile EEPROM can be used as data or program memory.

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

Except for the y=P configuration the P6021y VB includes Emulation Software MIFARE Plus MF1PLUSx0 and/or MIFARE DESFire EV1. MIFARE emulations are not part of the TSF and do not implement any Security Functional Requirement. The evaluation scope of the MIFARE emulations are limited to not interfere with the functionality provided by the IC hardware platform.

The P6021y VB can be used to assure authorized conditional access in a wide range of applications. Examples are identity cards, Banking Cards, Pay-TV, Portable communication SIM cards, Health cards and Transportation cards.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile 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 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. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SS.RNG	Random Number Generator
SS.TDES	Triple-DES coprocessor
SS.AES	AES coprocessor
SS.RECONFIG	Post Delivery Configuration

TOE Security Functionality	Addressed issue
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control
SF.FFW	Firmware Firewall
SF.FIRMWARE	Firmware Support
SF.PUF	Physically Unclonable Function

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 Secure Smart Card Controller P6021y VB* including IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
Developer documents for all configurations of the P6021y VB					
1	DOC	Product Data Sheet SmartMX2 family P6021y VB, Secure high-performance smart card controller, NXP Semiconductors, Business Unit Identification [11]	3.9	2019-08-22	Electronic Document

No	Type	Identifier	Release	Date	Form of Delivery
2	DOC	Instruction Set for the SmartMX2 family, Secure smart card controller, NXP Semiconductors, Business Unit Identification [12]	3.1	2012-02-02	Electronic Document
3	DOC	Information on Guidance and Operation, NXP Secure Smart Card Controller P6021y VB, NXP Semiconductors [13]	1.2	2018-11-21	Electronic Document
4	DOC	Product data sheet addendum - SmartMX2 P6021y VB, Wafer and delivery specification, NXP Semiconductors [14]	3.5	2019-07-24	Electronic Document
5	DOC	Product Data Sheet Addendum - SmartMX2P602xy VB family, Firmware Interface Specification, NXP Semiconductors [15]	3.7	2017-05-15	Electronic Document
6	DOC	Firmware Interface Specification Addendum - SmartMX2P602xy VB family, Firmware Interface Specification Addendum [16]	1.1	2016-05-23	Electronic Document
TOE components for P6021y VB					
8	HW	NXP Secure Smart Card Controller P6021P VB	VB	2015-02-19	wafer, module, inlay, package (dice have nameplate 9071C).
9	SW	Test-ROM Software	10.1D	2015-04-25	Test-ROM on the chip acc. to 9071C_LB010_TESTROM_v1_btos_10v1D_fos_Cv21.hex
10	SW	Boot-ROM Software	10.1D	2015-04-25	Boot-ROM on the chip acc. to 9071C_LB010_TESTROM_v1_btos_10v1D_fos_Cv21.hex
11	SW	Plain Firmware Operating System (FOS-Plain)	0C.21 / 0C.22 / 0C.60	2015-06 / 2016-01 / 2016-04	Firmware Operating System on the chip acc. to 9071C_LB010_TESTROM_v1_btos_10v1D_fos_Cv21.hex (0C.21 / 0C.22) / 9071C_BB027_TESTROM_v1_btos_10v1D_fos_Cv6.hex (0C.60)
Additional TOE deliverables for P6021M VB / P6021J VB					
12	SW	Emulation Firmware Operating System (FOS- Emu) with MIFARE Plus MF1PLUSx0 configuration	0C.21 / 0C.22 / 0C.60	2015-06 / 2016-01 / 2016-04	Firmware Operating System on the chip acc. to 9072A_LK097_TESTROM_v1_btos_10v1D_fos_Cv21rc5.hex

No	Type	Identifier	Release	Date	Form of Delivery
Additional TOE deliverables for P6021D VB / P6021J VB					
13	SW	Emulation Firmware Operating System (FOS-Emu) with MIFARE DESFire EV1 configuration	0C.21 / 0C.22 / 0C.60	2015-06 / 2016-01 / 2016-04	Firmware Operating System on the chip acc. to 9072A_LK097_TESTROM_v1_btos_10v1D_fos_Cv21rc5.hex

Table 2: Deliverables of the TOE

Document delivery to the customer is realised via a web tool, the DocStore. Customers and developer only have access to the documentation that is necessary according their status. Only registered and identified customers are provided with the necessary information. Furthermore all documents are protected and personalised based on certificates.

Delivery of the TOE is addressed in [14]. Here, identification of a certified product as well as the different forms and ways of delivery are described as follows:

- If the TOE is provided as wafer, it is shipped by the specified distribution center Malaysia Global Distribution Center (MYGDC), or directly from one of the specified NXP Wafer Test sites (ATBK or ATKH) (cf. [14] chapter 4.3).
- If the TOE is provided as module, it is shipped by the specified distribution center MYGDC, or directly from ATBK (cf. [14] chapter 4.4).
- If the TOE is provided as inlay, it is shipped directly from ATBK or via the MYGDC or via the W&D Hamburg (cf. [14] chapter 4.5).

Identification is also possible using the read-only security and manufacturer data area ([11] chapter 31.2.1) or the Chip Health Mode. Each major configuration has a dedicated device coding and type coding is described in [11] chapter 31.2.3.

The * in the TOE name indicates that MIFARE emulations are not part of the TSF and do not implement any Security Functional Requirement. The evaluation scope of the MIFARE emulations is limited to not interfere with the functionality provided by the IC hardware platform. For the configurations containing the MIFARE Plus MF1PLUSx0 and/or MIFARE DESFire EV1, additional documentation will be provided by NXP.

3. Security Policy

The security policy enforced 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.

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.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) appropriately. The IC Embedded Software Developer gets sufficient information on how to protect user data adequate in the security guidelines [13].
- 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. This is necessary 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 IC Embedded Software Developer is informed in the security guidelines [13].
- OE.Check-Init states that the TOE provides specific functionality that allows the unique identification of the TOE in form of FabKey-Data. The IC Embedded Software Developer gets sufficient information in the security guidelines [13].

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

5. Architectural Information

The TOE consists of the following hardware:

- CPU / coprocessors:
  - 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 coprocessor, 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 coprocessor (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 coprocessor, called Fame2 coprocessor, 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 (no security functionality),

- a CRC coprocessor, providing the CRC generation polynomials CRC-16 and CRC-32 for hardware cyclic redundancy check calculations (no security functionality).

- Memory / Memory Controller:
  - Read-Only Memory (ROM): the TOE incorporates 544 kByte of ROM, where 1 kByte = 1024 Byte. The ROM is partitioned by a Memory Management Unit (MMU) into 384 kByte Application-ROM for the Security IC Embedded Software, while 160 kByte are reserved for the Test-ROM,
  - Random Access Memory (RAM): 9.344 Byte of RAM, which is parted into RAM available to the Firmware Operating System only (576 Byte in case pf P6021P and 1152 Byte in case of P6021M/D/J), FXRAM assigned to the Fame 2 coprocessor (2.688 Byte), 640 Byte of PUF RAM, and RAM available to the IC Embedded Software (5440 Byte in case of P6021P and 4864 Byte in case of P6021M/D/J) called CXRAM,
  - Electrically Erasable Programmable Read Only Memory (EEPROM): Provides an overall maximum of 80 kByte of EEPROM, where 1024 Byte are always reserved for IC Dedicated Support Software for FOS control data, 512 Byte for the manufacturer area, 768 Byte for the PUF Block and the remaining part is reserved for MIFARE software part of the IC Dedicated Support Software,
  - Memory Controller: A Memory Management Unit (MMU) controls access to all of the three above mentioned memory types, and
  - Copy Machine: a device providing direct memory access for the Security IC Embedded Software without CPU interactions.
- Internal Peripherals:
  - a True Random Number generator,
  - a PUF (Physically Unclonable Function) block (optional), whose availability is subject to specific choice of Customer Reconfiguration Options,
  - a Watchdog timer, configurable by the Security IC Embedded Software to protect program execution,
  - 16 bit timers (T0 and T1),
  - Reset generator.
- Physical protection:
  - Secure shielding,
  - Security sensors (light, voltage, temperature, and frequency 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 pads I/O1,

- Single external power supply of 1.8V, 3V or 5V 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.

For the TOE firmware, as given in [6] and [9] section 1.4.1.3 or Table 5, one has:

- Security IC Dedicated Test Software, which is stored in 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 including:
  - Boot-ROM Software, executed during start-up or reset, and
  - Firmware Operating System used as interface for firmware provided by the manufacturer.

In case of the major configurations P6021M VB, P6021D VB, and P6021J VB, the TOE comes with MIFARE software. MIFARE emulations are not part of the TSF and do not implement any Security Functional Requirement. The evaluation scope of the MIFARE emulations are limited to not interfere with the functionality provided by the IC hardware platform.

The smartcard embedded software is not part of the evaluation.

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 and
- 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 test result confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

The P6021y hardware platform was tested including all major configurations as well as all minor configuration options that can be selected based on [6] and [9] section 1.4.2.2. The major and all minor configurations were available to the evaluator. The major configuration does not have varying 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 [11] and [13].

The major and minor configurations cannot be influenced by the customer. They are selected by the customer according to the Order Entry Form [17]. This configuration cannot be changed in the Application Mode after delivery of the TOE.

Please note that the MIFARE emulations are not part of the TSF and do not implement any Security Functional Requirement. The evaluation scope of the MIFARE emulations is limited to not interfere with the functionality provided by the IC hardware platform.

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 EAL 5 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 37).

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

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

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

- All components of the EAL 6 package including the class ASE as defined in the CC (see also part C of this report)
- The components ASE_TSS.2 and 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-1072-V3-2019, re-use of specific evaluation tasks was possible.

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 ASE_TSS.2 and 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) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1.	Cryptographic Primitives	3-key Triple DES	[SP800-67]	168	Yes	-
2.		AES	[FIPS-197]	128,192, 256	Yes	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
3.		Physical RNG PTG.2	[13], Conformant to [AIS31]	N/A	Yes	Supports cryptographic implementations
4.	Confidentiality	Encryption and decryption with 3-key Triple-DES in ECB mode	[SP800-67], [SP800-38A]	168	No	ECB without padding
5.		Encryption and decryption with AES in ECB mode	[FIPS197], [SP800-38A]	128, 192, 256	No	ECB without padding
6.		AES encryption and decryption in CBC mode using PUF key	[FIPS197], [SP800-38A], [PUF]	128	Yes	Proprietary standard [PUF]
7.	Integrity	AES MAC generation and verification in CBC-MAC mode	[FIPS197], Algorithm 1 in [ISO_9797-1], [PUF]	128	No	Proprietary standard [PUF]
8.	Key Derivation	Proprietary PUF key derivation	[PUF]	128	Yes	Proprietary standard [PUF]

Table 3: TOE cryptographic functionality

Reference of Legislatives and Standards quoted above:

[SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[SP800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

[FIPS-197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), November 2001, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.

[PUF] P602x Family PUF Key Derivation – Specification, Version 1.0, 2015-01-16

[ISO 9797-1] ISO/IEC 9797-1-2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 2011.

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 [Auswahl im Einzelfall: 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. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES Advanced Encryption Standard

AIS Application Notes and Interpretations of the Scheme

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CRC	Cyclic redundancy check
cPP	Collaborative Protection Profile
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
ETR	Evaluation Technical Report
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MMU	Memory Management Unit
NIST	National Institute of Standards and Technology
OS	Operating system
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random number generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality

13.2. 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.

14. 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-1072-V4-2021, NXP Secure Smart Card Controller P6021y VB – Security Target, Version 1.11, 2019-08-23, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report BSI-DSZ-CC-1072-V4-2021, Version 3, 2021-06-16, 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 BSI-DSZ-CC-1072-V4-2021, NXP Secure Smart Card Controller P6021y VB – Security Target Lite, Version 1.11, 2019-08-23, NXP Semiconductors (sanitised public document)

[10] Evaluation Technical for Composite Evaluation (ETR COMP) for the P6021y VB, version 3, 2021-06-16, TÜV Informationstechnik GmbH (confidential document)

[11] SmartMX2 family P6021y VB Secure high-performance smart card controller, Objective data sheet, Version 3.9, 2019-08-22, NXP Semiconductors

[12] Instruction set for the SmartMX2 family Secure smart card controller, Product data sheet, Version 3.1, 2012-02-02, NXP Semiconductors

[13] NXP Secure Smart Card Controller P6021y VB Information on Guidance and Operation, Version 1.2, 2018-11-21, NXP Semiconductors

[14] SmartMX2 P6021y VB Wafer and delivery specification, Preliminary data sheet addendum,Version 3.5, 2019-07-24, NXP Semiconductors

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- 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 39, Formal Method, Version 3.0, 24.10.2008
- AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013.
- AIS 47, Version 1.1, Regelungen zu Site Certification

[15] SmartMX2 P602xy VB family Firmware interface specification, Version 3.7, 2017-05-15, NXP Semiconductors

[16] SmartMX2 P602xy VB Family Firmware Interface Specification Addendum, Version 1.1, 2016-05-23, NXP Semiconductors

[17] Order Entry Form, Version 1.32, 2019-11-18, NXP Semiconductors

[18] NXP Secure Smart Card Controller P6021y VB Evaluation Reference List, Version 2.7, 2021-05-04, NXP Semiconductors (confidential document)

[19] NXP Secure Smart Card Controller P6021y VB Configuration List, Version 1.5, 2019-08-09, NXP Semiconductors (confidential document)

[20] Site Technical Audit Report (STAR), Taiwan Semiconductor Manufacturing Company Ltd, Taichung Fab15A, Version 2, 2021-06-16, 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 detailed 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-1072-V4-2021

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller P6021y VB* including 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, 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 24 June 2021, 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_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	NXP Semiconductors Germany GmbH Troplowitzstraße 20 22569 Hamburg, Germany	Development and IT support Wafer testing and wafer treatment Flaw Remediation Delivery
NXP Eindhoven	NXP Semiconductors Eindhoven HTC-46.3 West Building 46, High Tech Campus 5656AE, Eindhoven, Netherlands	Development
NXP Nijmegen	NXP Semiconductors Nijmegen B.V. Gerstweg 2, 6534AE Nijmegen, Netherlands	Development support (sample preparation, design data verification) Failure analysis lab
NXP Gratkorn	NXP Semiconductors Austria GmbH Mikron-Weg 1, 8108 Gratkorn, Austria	Document control
NXP IT Eindhoven Secure Room	Building 60, High Tech Campus Secure Room 131 5656AE, Eindhoven, Netherlands	IT support (admin room)

Name of site / Company name	Address	Function
Sii Gdansk	Olivia Prime (10th floor) Sii Sp.Zo.o Grunwaldzka 472C, 80-309 Gdansk, Poland	SW development
NXP Bangalore	NXP India Private Limited Manyata Tech Park Nagawara Village, Kasaba Hobli, Bangalore 560045, India	SW development
Colt Hamburg	Colt Hamburg Obenhauptstrasse, 22335 Hamburg, Germany	IT support (TOE database)
Akquinet Hamburg	Akquinet Hamburg Ulzburger Strasse 201, 22850 Norderstedt, Germany	IT support (TOE database)
Digital Reality Phoenix	Digital Realty Data Center 120 East Van Buren St, Phoenix, AZ 85004 United States of America	IT support (TOE database)
Datacenter Equinix Singapore	EQUINIX 20 Ayer Rajah Crescent, IBX SG1, Level 5 Unit 5, Ayer Rajah Industrial Park 139964 Singapore	Data center
NXP Bucharest	NXP Semiconductors Romania Campus 6, Bulevardul Iuliu Maniu 6L, 061103 Bucuresti Romania	IT engineering and support
NXP Guadalajara	NXP Guadalajara Periferico Sur #8110 Col. El Mante JALISCO, 45609 Tlaque-paque Mexico	IT engineering and support
Production Sites		
Chipbond, Hsin-Chu City	Chipbond Technology Corporation No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping

Name of site / Company name	Address	Function
TSMC Tainan and Hsinchu	Taiwan Semiconductor Manufacturing Company Limited 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 production and diffusion
NXP ATBK	NXP Semiconductors Thailand (ATBK) 303 Moo 3 Chaengwattana Rd. Laksi Bangkok 10210 Thailand	Wafer testing, wafer treatment, assembly, and Final Test Test program development Failure analysis lab Delivery
NXP ATKH	NXP Semiconductors Taiwan Ltd (ATKH) #10, Jing 5th Road, N.E.P.Z Kaohsiung 81170 Taiwan R.O.C	Wafer testing, wafer treatment, assembly, and Final Test Test program development Failure analysis lab Delivery
Linxens Ayutthaya	AY1, Linxens (Thailand) Co Ltd. 142 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In 13160 Ayutthaya Thailand	Inlay assembly

Table 4: Development and production sites for the TOE

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