SmartMX

P5CN072

Secure Dual Interface PKI Smart Card Controller

Rev. 1.0 — 2005 March 09 Short Form Specification
107710

1. General description

1.1 Description P5CN072 device

- 72 Kbytes EEPROM
- 160 Kbytes User ROM
- 4608 bytes RAM
- PKI (Public Key Infrastructure) co-processor (RSA, ECC)
- Dual / Triple key DES-3 co-processor
- ISO/IEC 7816 contact interface
- S^2C interface to enable secure contactless communication via Near Field Communication (NFC)
- EEPROM data retention time: 20 years minimum

The P5CN072 is a Secure Dual Interface PKI Smart Card Controller of the Smart*MX* platform featuring 160 Kbytes of ROM, 4608 bytes of RAM and 72 Kbytes of EEPROM, which can be used as data memory and as program memory. The non-volatile memory consists of high reliability memory cells to guarantee data integrity, which is especially important when the EEPROM is used as program memory.

Operated both in contact mode (ISO/IEC 7816) and in S^2C mode the user defines the final function of the chip with his chip operating system (COS). This allows the same level of security, functionality and flexibility for the contact interface as well as for S^2C interface.

The S^2C interface technology provides reliable digital communication to a member of the NFC IC family to enable secure contactless communication via NFC enabled devices such as mobile phones.

The S^2C interface is connected to the internal ISO14443 CIU. The CIU handles the demodulation and the modulation of the S^2C signals that a full contactless communication via this interface and the NFC IC can be enabled. As the S^2C interface is connected to the CIU the power of the P5CN072 has to be supplied via the VDD and VSS pins in S^2C mode.

The P5CN072 offers the same features of contactless and contact mode handling as other members of the Smart MX family.

Connected to the S^2C interface of a NFC IC the P5CN072 is compatible with existing MIFARE® reader infrastructure and the optional free of charge emulation modes of MIFARE® 1K and MIFARE® 4K enable fast system integration and backward compatibility of standard MIFARE® and ProX family based cards. The communication on the S^2C interface support the ISO/IEC14443 A- part 3 and ISO/IEC14443 part 4.

PHILIPS

Bi-directional communication with the contact interface of the device can be performed through two serial IOs. These IOs are under full control of the application software in order to allow conditional controlled access to the different internal memories.

The on-chip hardware is software controlled via Special Function Registers (SFRs). Their function and usage is described in the respective sections of this specification as the SFRs are correlated to the activities of the CPU, Interrupt, IO, EEPROM, Timers, etc.

The P5CN072 provides two power saving modes with reduced activity: the IDLE and the SLEEP or CLOCKSTOP Mode. These two modes are activated by software.

The device operates either with a single 1.8V, 3 V or 5 V (voltage classes C, B, A) power supply at a maximum external clock frequency of 10 MHz supplied by the contact pads (internally up to 30 MHz).

1.1.1 Different Configurations of the P5CN072

Depending on the application requirements the P5CN072 can be configured according to options described in the data sheet chapter “ORDER ENTRY FORM”.

There are three different configurations (A, B1 and B4) possible as shown in Table [1]. The MIFARE® option configuration has impact on the access conditions for the EEPROM and influences the User OS development.

Note that the contactless interface can be used in any of the following configurations to communicate via any protocol (T=CL as specified in ISO/IEC 14443-4 or a self defined protocol), also concurrently to the MIFARE® protocol available in configuration B1 and B4.

1.1.1.1 Configuration A

In configuration **A** all memory resources are available and under full control of the dual interface User OS. No MIFARE® functionality is available.

1.1.1.2 Configuration B1

In configuration **B1** the contactless MIFARE® Classic OS provided by Philips is implemented on the P5CN072. 1 Kbyte of the EEPROM can be accessed by the MIFARE® Classic OS offering the same command set and functionality as a MIFARE® 1K hardwired logic chip. The access conditions for the user OS to the MIFARE® memory area can be configured via the so called ACM (Access condition matrix). The MIFARE® Classic OS offers a backward compatibility to support existing infrastructure based on the MIFARE® Classic functionality.

1.1.1.3 Configuration B4

In configuration **B4** the MIFARE® Classic OS provided by Philips Semiconductors offers the same functionality and command set as the MIFARE® 4K hardwired chip. This emulation offers the possibility to access 4 Kbytes of EEPROM memory using the MIFARE® command set. Access rights for the user OS and the MIFARE® 4K emulation on accessing the EEPROM memory can be configured via the so called ACM (Access Condition Matrix).

For secure separation of the user OS and the MIFARE® OS a dedicated built in hardware protection controls the access to the EEPROM, RAM and ROM.

For detailed explanation of MIFARE® 1K and MIFARE® 4K functionality please refer also to the following documents:

- MIFARE® MF RC500 Product Specification
- MIFARE® Standard IC MF1 ICS50 Functional Specification
- MIFARE® Standard 4 Kbytes Card IC MF1 ICS70

Table 1: Configurations of the P5CN072

Configuration	EEPROM
A	72 Kbytes for access with user OS
B1	35 Kbytes for access with user OS via EEPROM SFR
	1 Kbyte for access with MIFARE® Classic OS and user OS [1]
B4	32 Kbytes for access with user OS via EEPROM SFR
	4 Kbytes for access with MMIFARE® Classic OS and user OS [1]

[1] In configuration B1 and B4 the MIFARE® OS allocates 128 bytes of the RAM.

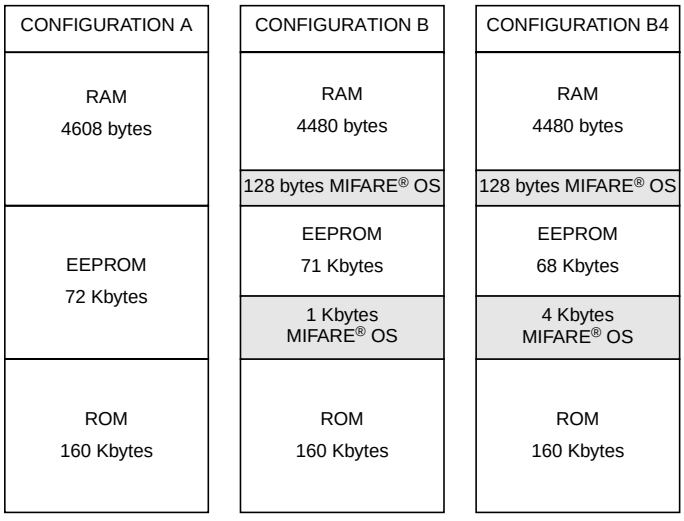


Fig 1. Configurations of the P5CN072.

2. Features

2.1 Product Specific Features

- 72 Kbytes EEPROM (including 192 bytes reserved manufacturer/security area)
- 160 Kbytes User ROM
- 4608 bytes RAM
  - 256 bytes + 3 Kbytes CXRAM
  - 1280 bytes FXRAM usable for Fame*XE*
- **Memory Management and Protection Unit** (MMU)
  - for more details see 2.2. Security Features
- S^2C Interface Unit
  - compatible with ISO/IEC14443A-3 via a NFC IC
  - fully supports the T=CL protocol acc. ISO/IEC14443-4
  - Data Transfer rates supported (106 Kbit/s)
- **High speed DES-3 co-processor** (64 bit parallel processing DES engine)
- **PKI Co-processor** Fame*XE*
  - The major Public Key Cryptosystems like RSA, El'Gamal, DSS, Diffie-Hellmann, Guillou-Quisquater, Fiat-Shamir and Elliptic Curve are supported
  - 4096 bits maximum key length for RSA with randomly chosen modulus
  - 32-bit interface
  - Boolean operations for acceleration of standard, symmetric cipher algorithms
  - Performance example: RSA Modular Exponentation (Straight forward) < 35 ms (2048 bit key length and 17 bit exponent)
- **Optional free of charge MIFARE® 1K and MIFARE® 4K functionality** supported by the S^2C interface
- **1 additional IO port IO2 for full-duplex serial data communication**

2.2 Security Features

- **Enhanced Security Sensors**
  - Low / high clock frequency sensor
  - Low / high temperature sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors
- **Electronic fuses** for safeguarded mode control
- **Unique ID for each die**
- **Clock Input Filter for protection against spikes**
- **Power-up / Power-down reset**
- **Optional programmable “Card Disable” feature**
- **Memory Security** (encryption and physical measures) for RAM, EEPROM and ROM
- **Memory Management and Protection Unit (MMU)**
  - Secure multi application operating systems via two different operation modes - System Mode and Application Mode
  - OS controlled access restriction mechanism to pheripherals in Application Mode
  - Memory mapping up to 8 Mbytes Code memory
  - Memory mapping up to 8 Mbytes (-64K) Data memory
- **Optional disabling of ROM read instructions by code executed in EEPROM**
- **Optional disabling of any code execution out of RAM**
- **EEPROM** programming:
  - No external clock
  - Hardware sequencer controlled
  - On-chip high voltage generation
  - Enhanced error correction mechanism
- **64 or 128 EEPROM bytes for customer-defined Security FabKey.** Featuring batch-, wafer- or die-individual security data, incl. encrypted diversification features on request
- **14 bytes User Write Protected Security area in EEPROM** (byte access, inhibit functionality per byte)
- **32 bytes Write Once Security area in EEPROM** (bit access)
- **32 bytes User Read Only area in EEPROM** (byte access)
- **Customer specific EEPROM initialization** optional

2.3 Family Standard Features

- Dedicated Secure_MX51 Smart Card CPU (Memory eXtended / enhanced 80C51)
  - 0.18 µ 5 metal layer CMOS technology
  - operating in contact and contactless mode (dependent on family type option)
  - featuring a 24 bit universal memory space, 24 bit program counter
  - combined universal program/data linear address range up to 16 Mbyte
  - additional instructions to improve
    - pointer operations
    - performance
    - code density of both C and Java source code
- Low power / low voltage design using Philips handshaking technology
- Multiple source vectorized interrupt system with four priority levels
- Watch exception provides for software debugging facility
- Multiple source RESET system
- Two 16-bit timers
- High reliable EEPROM for both data storage and program execution
  - Bytewise EEPROM programming and read access
  - EEPROM endurance: up to 500 k programming cycles per byte
  - EEPROM data retention time: 20 years minimum
- Versatile EEPROM programming of 1 to 64 byte at a time
- Typical EEPROM page erasing time: 2.5 ms
- Typical EEPROM page programming time: 1.5 ms
- Power-saving IDLE Mode
  - Wake-up from IDLE Mode by RESET or any activated interrupt
- Power-saving SLEEP (power down) Mode or CLOCKSTOP Mode
  - Wake-up from SLEEP or CLOCKSTOP Mode by RESET or External Interrupt
- Contact configuration and serial interface according to ISO/IEC 7816: GND, VCC, CLK, RST, IO1
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalization at 1Mbit/s
- External or internally generated configurable CPU clock
- 1 MHz to 10 MHz operating external clock frequency range
- Internal CPU clock up to 30 MHz with synchronous operation
  - Internal clocking independent of externally applied frequency
- High speed Triple-DES co-processor (two or three keys loadable)
- DES3 performance < 50 µs
- High speed 16 bit CRC Engine according to CCITT polynom definition
- Low power Random Number Generator (RNG) in hardware, FIPS140-2 compliant
- 1.62V to 5.5V extended operating voltage range for class C, B and A
- -25 to +85°C operating ambient temperature range (ISO7816 Mode)
- -15 to +85°C operating ambient temperature range (S^2C Interface Mode)

2.4 Design-in Support

- Approved Development Tool Chain
  - Keil PK51 development tool package incl. Vision2/dScopeC51 simulator, additional specific hardware drivers incl. simulation of contactless interface and ISO/IEC 7816 card interface board. A “Smart*MX* DBox” allows software debugging and integration tests. (www.keil.com)
  - Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO/IEC 7816 and ISO/IEC14443 card interface board. Code coverage and performance measurement software tools for real time software testing. (www.ashling.com)
- Software Libraries
  - Libraries supporting contactless communication according to ISO/IEC 14443, Part 3 and 4
  - EEPROM Read / Write routines

3. Ordering information

Table 2: Ordering information

Type number	Package		
	Name	Description	Version
P5CN072EW1/Txxx	FFC	sawn wafer 150 µ on film frame carrier	-
P5CN072ETS/Txxx	SMD	SSOP 20	SOT 266-1

4. Block diagram

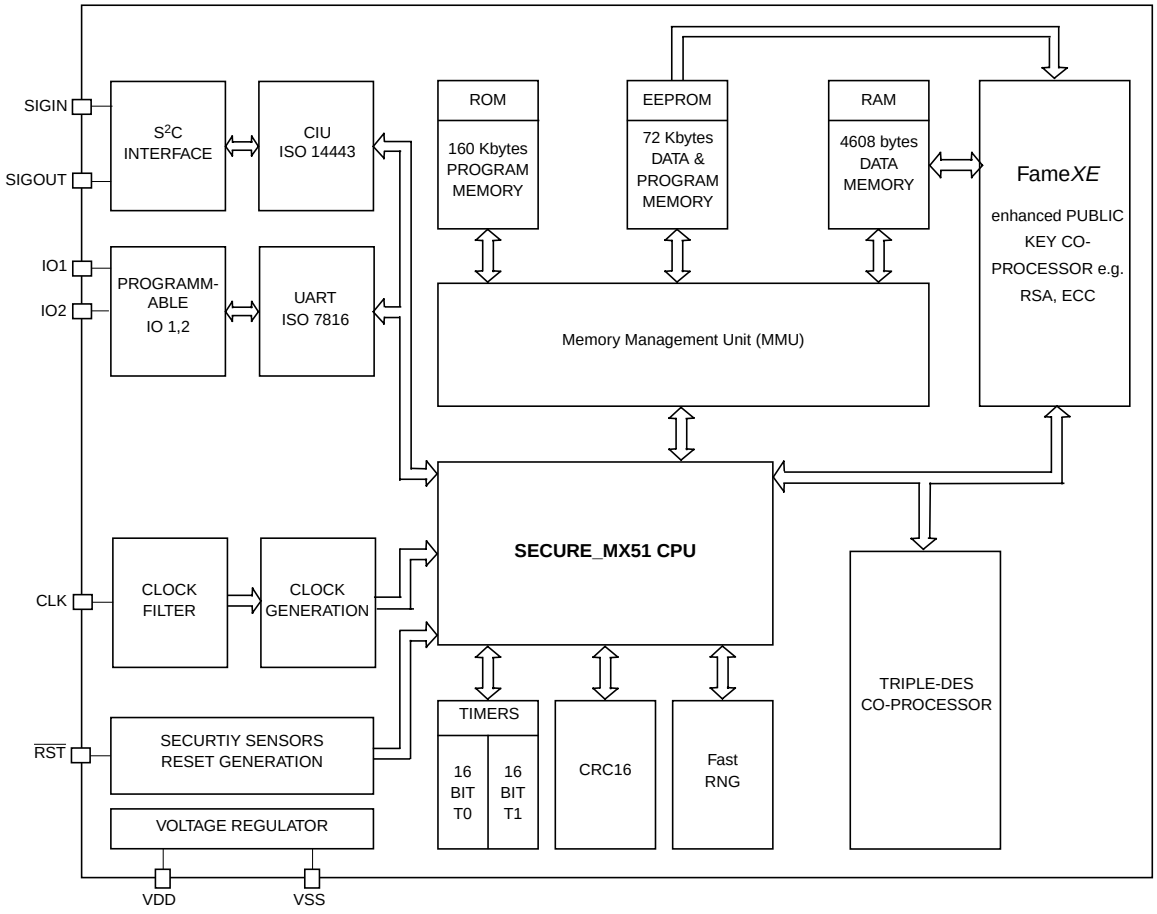
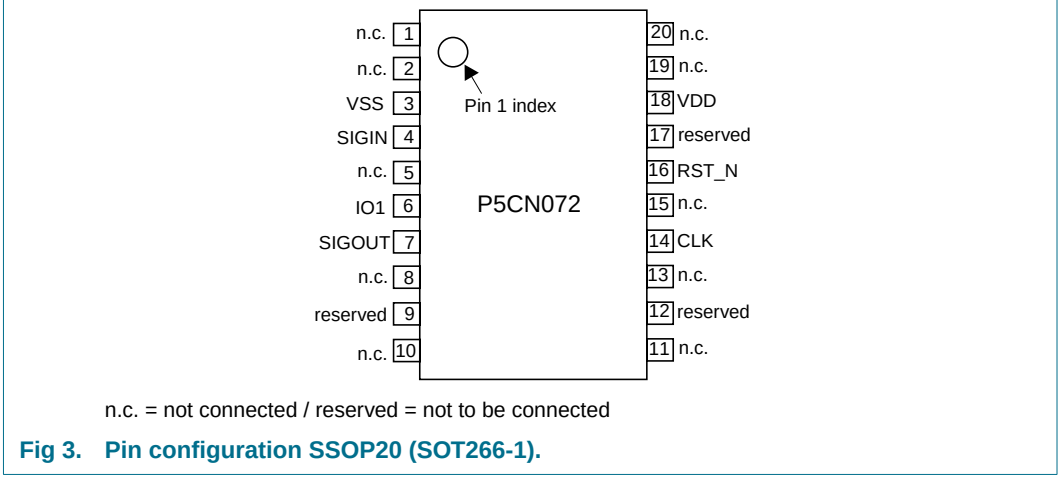


Fig 2. Block diagram and pinning information P5CN072.

5. Pinning information

5.1 Pin description SSOP20 (SOT266-1)



n.c. = not connected / reserved = not to be connected

Fig 3. Pin configuration SSOP20 (SOT266-1).

Table 3: Pin description

Symbol	Pin	Description
N.C.	1 to 2	not connected
VSS	3	Ground (reference voltage) input
SIGIN	4	S^2C signal from controller to NFC IC
N.C.	5	not connected
IO1	6	Input/Output #1 for serial data
SIGOUT	7	S^2C signal from NFC IC to controller
N.C.	8	not connected
reserved	9	not to be connected
N.C.	10 to 11	not connected
reserved	12	not to be connected
N.C.	13	not connected
CLK	14	Clock input
N.C.	15	not connected
RST_N	16	Reset input, active LOW
reserved	17	not to be connected
VDD	18	Power supply voltage input
N.C.	19 to 20	not connected

6. Limiting values

Table 4: Absolute maximum ratings [1]

In accordance with the Absolute Maximum Rating System (IEC 60134).

Symbol	Parameter	Conditions	Min	Max	Unit
V_{DD}	Supply voltage		-0.5	+6.0	V
V_I	Input voltage on any signal pad		-0.5	V_{DD} +0.5	V
I_I; I_O	DC input or output current on IO1, IO2 or IO3 pad		-	± 15.0	mA
$I_{latchup}$	Latch up current	$V_I < 0$ or $V_I > V_{DD}$	-	100	mA
V_{ESD}	Electrostatic discharge voltage [2]				
	on pads VDD, VSS, CLK, RST, IO1, IO2, IO3		-	± 4.0	kV
	on all other pads		-	± 2.0	kV
P_{tot}	Total power dissipation per package [3]		-	1	W
T_{stg}	Storage temperature range		Table note [4]	Table note [4]	

[1] Stresses beyond those listed may cause permanent damage to the device. These are stress ratings only and functional operation of the device at these or any other conditions beyond those indicated under “recommended operating conditions” is not implied. Exposure to absolute-maximum-rated conditions for extended periods may affect device reliability.

[2] MIL Standard 883-D method 3015; Human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = -25 to +85 °C.

[3] Depending on appropriate thermal resistance of the package.

[4] Depending on delivery type, refer to “Philips General Specification for 8” Wafers” and to “Philips Contact & Dual Interface Chip Card Module Specification”.

Table 5: Recommended operating conditions

Symbol	Parameter	Conditions	Min	Typ.	Max	Unit
V_{DD} (5.0)	Supply voltage	5 V operation	4.5	5.0	5.5	V
V_{DD} (3.0)		3 V operation	2.7	3.0	3.3	V
V_{DD} (1.8)		1.8 V operation	1.62	1.8	1.98	V
V_I	DC input voltage on digital inputs and digital IO pads		0		V_{DD}	V
T_{amb}	Operating ambient temperature (ISO7816 Mode)		-25		+85	°C
	Operating ambient temperature (S^2C Interface Mode)		-15		+85	°C

7. Data sheet status

Level	Data sheet status [1]	Product status [2] [3]	Definition
I	Objective data	Development	This data sheet contains data from the objective specification for product development. Philips Semiconductors reserves the right to change the specification in any manner without notice.
II	Preliminary data	Qualification	This data sheet contains data from the preliminary specification. Supplementary data will be published at a later date. Philips Semiconductors reserves the right to change the specification without notice, in order to improve the design and supply the best possible product.
III	Product data	Production	This data sheet contains data from the product specification. Philips Semiconductors reserves the right to make changes at any time in order to improve the design, manufacturing and supply. Relevant changes will be communicated via a Customer Product/Process Change Notification (CPCN).

[1] Please consult the most recently issued data sheet before initiating or completing a design.

[2] The product status of the device(s) described in this data sheet may have changed since this data sheet was published. The latest information is available on the Internet at URL http://www.semiconductors.philips.com.

[3] For data sheets describing multiple type numbers, the highest-level product status determines the data sheet status.

8. Definitions

Short-form specification — The data in a short-form specification is extracted from a full data sheet with the same type number and title. For detailed information see the relevant data sheet or data handbook.

Limiting values definition — Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 60134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics sections of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.

Application information — Applications that are described herein for any of these products are for illustrative purposes only. Philips Semiconductors make no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

9. Disclaimers

Life support — These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips Semiconductors customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Philips Semiconductors for any damages resulting from such application.

Right to make changes — Philips Semiconductors reserves the right to make changes in the products - including circuits, standard cells, and/or software - described or contained herein in order to improve design and/or performance. When the product is in full production (status ‘Production’), relevant changes will be communicated via a Customer Product/Process Change Notification (CPCN). Philips Semiconductors assumes no responsibility or liability for the use of any of these products, conveys no licence or title under any patent, copyright, or mask work right to these products, and makes no representations or warranties that these products are free from patent, copyright, or mask work right infringement, unless otherwise specified.

10. Contact information

For additional information, please visit **http://www.semiconductors.philips.com**

For sales office addresses, send an email to: **sales.addresses@www.semiconductors.philips.com**

11. Tables

Table 1: Configurations of the P5CN072 3
Table 2: Ordering information 7
Table 3: Pin description 9
Table 4: Absolute maximum ratings [1] 10
Table 5: Recommended operating conditions 10

12. Figures

Fig 1. Configurations of the P5CN072. 3
Fig 2. Block diagram and pinning information P5CN072. 8
Fig 3. Pin configuration SSOP20 (SOT266-1). 9

13. Contents

1 General description 1
1.1 Description P5CN072 device 1
1.1.1 Different Configurations of the P5CN072 2
1.1.1.1 Configuration A 2
1.1.1.2 Configuration B1 2
1.1.1.3 Configuration B4 3
2 Features 4
2.1 Product Specific Features 4
2.2 Security Features 5
2.3 Family Standard Features 6
2.4 Design-in Support 7
3 Ordering information 7
4 Block diagram 8
5 Pinning information 9
5.1 Pin description SSOP20 (SOT266-1) 9
6 Limiting values 10
7 Data sheet status 11
8 Definitions 11
9 Disclaimers 11
10 Contact information 11

Date of release: 2005 March 09
Document order number: 107710

Published in The Netherlands