

## 1. General description

---

### 1.1 Family description

Philips Semiconductors SmartMX (**M**emory **eX**tension) multiple interface option platform features a significantly enhanced smart card IC architecture. New powerful opcodes are available beyond the compatible classic 80C51 instruction set. The SmartMX family manufactured in most advanced CMOS 0.18  $\mu\text{m}$  5 metal layer technology is positioned to service high volume, mono- and multi-application markets such as eGovernment (e.g. Smart Passport), banking/finance, mobile communications, public transportation, pay TV, conditional access and network access.

SmartMX enables the easy implementation of state-of-the-art operating systems and open platform solutions including Java Card Global Platform and MULTOS by offering optimized features like linear addressing and an enhanced instruction set together with the highest levels of security. Within its targeted segments, the new platform is the most advanced solution available, combining exceptionally powerful co-processors for public and secret key encryption supporting RSA, ECC, DES and AES, with the high security, ultra low power, performance optimized design concept of Philips Semiconductors' handshaking technology. For further details on general SmartMX platform features please refer to the "SmartMX platform features" short form specification.

### 1.2 Description P5CT072 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
- ◆ AES co-processor
- ◆ ISO/IEC 7816 contact interface
- ◆ ISO/IEC 14443A contactless interface
- ◆ USB 2.0 Low Speed contact Interface
- ◆ EEPROM data retention time: 20 years minimum

The P5CT072 is a Secure PKI Smart Card Controller of the SmartMX 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. Additionally a USB 2.0 (Low Speed) interface is available thus the device is called a "Secure Triple Interface Smart Card Controller". 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 contactless mode (ISO/IEC 14443) 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 the contactless interface.

The field proven RF interface technology (according ISO/IEC 14443-2) is well established in all products of the MIFARE® interface platform and provides reliable communication and secure processing, even in electro-magnetically harsh environments like in buses or train stations. Compatibility 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.

Bi-directional communication with the contact interface of the device can be performed through three 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 P5CT072 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 power supply at a maximum external clock frequency of 10 MHz supplied by the contact pads (internally up to 30 MHz) or with a power supply generated from the RF-field emitted by an RF-reader.

### 1.2.1 The Contact Interface

Operating in accordance with ISO/IEC 7816, the SmartMX contact interface is supported by a built in UART, which enables data rates of up to 1Mbit/s allowing for the automatic generation of all typical baud rates and supports transmission protocols T=0 and T=1.

### 1.2.2 The USB 2.0 (Low Speed) Interface

SmartMX is the first product platform of its kind to provide a fully integrated USB interface based on the USB 2.0 (Low Speed) standard SmartMX making SmartMX based IC cards “Plug and Play” compatible with the whole PC world without the use of complex reader devices or extra external components. The USB interface uses the ISO contact module and works via a 4-wire connection to any PC supporting “hot Plug and Play”. The card automatically recognizes an ISO or USB environment and is able to work with external frequency of up to 6 MHz or internal clock generation. The use of USB interfaces on smart cards is currently in the process of becoming standardized within ISO/IEC 7816-12.

### 1.2.3 Different Configurations of the P5CT072

Depending on the application requirements the P5CT072 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.

#### 1.2.3.1 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.

#### 1.2.3.2 Configuration B1

In configuration **B1** the contactless MIFARE® Classic OS provided by Philips is implemented on the P5CT072. 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.

#### 1.2.3.3 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.

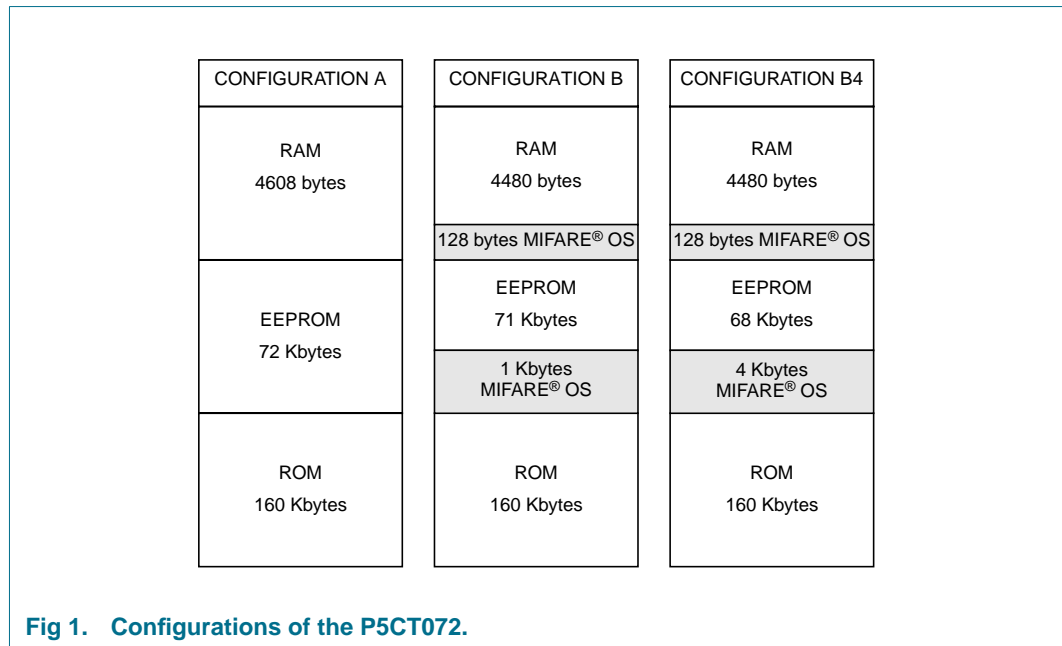
For detailed explanation of MIFARE® 1K and MIFARE® 4K functionality please refer also to the following documents:

- MIFARE® MF CM500 Product Specification
- MIFARE® Standard IC MF1 ICS50 Functional Specification
- MIFARE® Standard 4 Kbytes Card IC MF1 ICS70

**Table 1: Configurations of the P5CT072**

Configuration	EEPROM
A	72 Kbytes for access with user OS
B1	71 Kbytes for access with user OS via EEPROM SFR 1 Kbyte for access with MIFARE® Classic OS and user OS [1]
B4	68 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.



## 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 IRAM + 3 Kbytes CXRAM
  - ◆ 1280 bytes FXRAM usable for FameXE
- **Memory Management and Protection Unit**
  - ◆ for more details see 2.2. Security Features
- **USB 2.0 (Low Speed)** contact interface acc. ISO/IEC7816-12
- **Contactless Interface Unit (CIU)** fully compatible with ISO/IEC14443A
  - ◆ fully supports the T=CL protocol acc. ISO/IEC14443-4
  - ◆ Data Transfer rates supported (106/212/424 kbit/s)
- **MIFARE® RF contactless interface** acc. ISO/IEC14443-2
  - ◆ 13.56 MHz operating frequency
  - ◆ Reliable communication due to 100% ASK
  - ◆ High speed (106/212/424 kbit/s, efficient frame support)
  - ◆ True anticollision
  - ◆ High speed CRC co-processor according to CCITT
- **MIFARE® reader infrastructure compatibility**
- **High speed DES-3 co-processor** (64 bit parallel processing DES engine)
- **High speed AES co-processor** (128 bit parallel processing AES engine)
- **PKI Co-processor** FameXE
  - ◆ 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 Exponentiation (Straight forward) < 35 ms (2048 bit key length and 17 bit exponent)
- **Optional free of charge MIFARE®1K and MIFARE® 4K functionality**
- **2 additional IO ports IO2 and IO3 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 peripherals 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  $\mu$  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
- Development and portation support of existing P8WE / P8RF family masks
- 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
  - ◆ Byte-wise 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  $\mu$ s
- 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

## 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 “SmartMX DBox” allows software debugging and integration tests. ([www.keil.com](http://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](http://www.ashling.com))
  - ◆ Dual Interface dummy modules OM6711 (PDM 1.1 - SOT658) with special antenna bonding on C4 and C8 for testing the implanting process and antenna connection.
- Software Libraries
  - ◆ Libraries supporting contactless communication according to ISO/IEC 14443, Part 3 and 4
  - ◆ USB 2.0 (Low Speed) Basic Library Support
  - ◆ EEPROM Read / Write routines

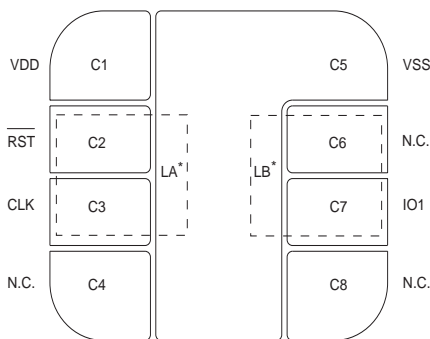
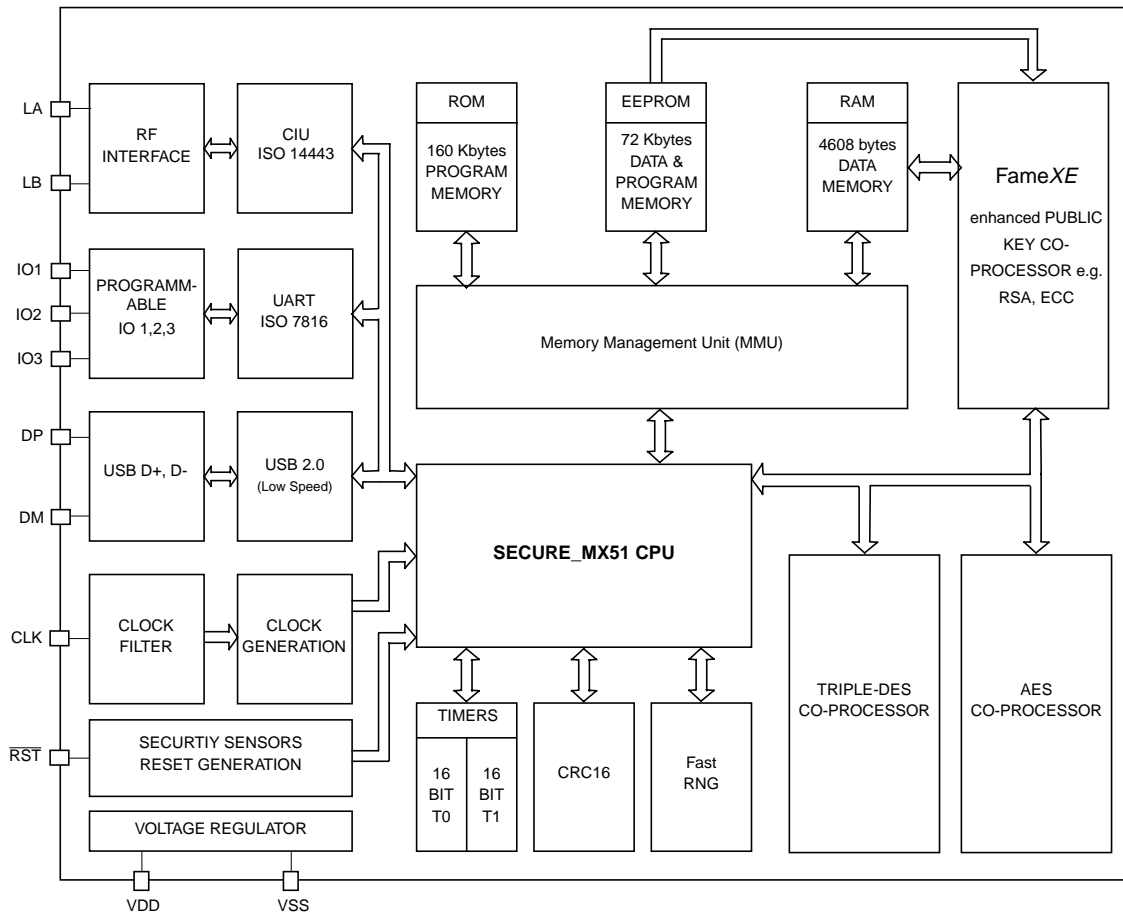
## 3. Ordering information

Table 2: Ordering information

Type number	Package		
	Name	Description	Version
P5CT072EW1/Tvsrrffo	FFC	sawn wafer 150 $\mu$ on film frame carrier	-
P5CT072EV0/Tvsrrffo	Module	Dual Interface Modules on super 35 mm format (8-contact)	SOT658 BA3
P5CT072EV1/Tvsrrffo	Module	Dual Interface Modules on super 35 mm format (8-contact) with Antenna connected to C4/C8	SOT658 BA3
P5CT072EV3/Tvsrrffo	Module	pure contactless module MOB2 on super 35 mm format	SOT500 AA3



### 4. Block diagram



\* Antenna contacts are placed on module backside

ISO 7816		Triple Interface ("Standard")	P5CT072
CONTACTS	Symbol	Symbol	Description
C1	VCC	VDD	Power supply voltage input
C2	RST	RST	Reset input, active LOW
C3	CLK	CLK	Clock input
C4	-	N.C.	not connected
C5	GND	VSS	Ground (reference voltage) input
C6	VPP	N.C.	not connected
C7	IO	IO1	Input/Output #1 for serial data
C8	-	N.C.	not connected
-	-	LA	antenna coil connection
-	-	LB	antenna coil connection

Note: IO2, IO3 and assignments on request.

Fig 2. Block diagram P5CT072.

## 5. Limiting values

**Table 3: 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		-	$\pm 15.0$	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, DP, DM		-	$\pm 4.0$	kV
	on all other pads		-	$\pm 2.0$	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 4: 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
$V_{I(ai/o)}$	DC input voltage on analog USB IO pads (DP/DM)		0		3.6	V
$T_{amb}$	Operating ambient temperature [1]		-25		+85	°C

- [1] Operation ambient temperature when using the Universal Serial Bus interface with internally generated USB clock:  $T_{amb} = 0$  to  $+50$  °C.

## 6. Data sheet status

Level	Data sheet status <sup>[1]</sup>	Product status <sup>[2]</sup> <sup>[3]</sup>	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.

## 7. 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.

## 8. 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.

## 9. 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](mailto:sales.addresses@www.semiconductors.philips.com)

## 10. Tables

Table 1: Configurations of the P5CT072 . . . . .	4	Table 3: Absolute maximum ratings <a href="#">[1]</a> . . . . .	10
Table 2: Ordering information . . . . .	8	Table 4: Recommended operating conditions . . . . .	10

## 11. Figures

Fig 1. Configurations of the P5CT072. . . . .	4	Fig 2. Block diagram P5CT072. . . . .	9
---	---	---------------------------------------	---

## 12. Contents

<b>1</b>	<b>General description . . . . .</b>	<b>1</b>
1.1	Family description . . . . .	1
1.2	Description P5CT072 device . . . . .	1
1.2.1	The Contact Interface . . . . .	2
1.2.2	The USB 2.0 (Low Speed) Interface . . . . .	2
1.2.3	Different Configurations of the P5CT072 . . . . .	3
1.2.3.1	Configuration A . . . . .	3
1.2.3.2	Configuration B1 . . . . .	3
1.2.3.3	Configuration B4 . . . . .	3
<b>2</b>	<b>Features . . . . .</b>	<b>5</b>
2.1	Product Specific Features . . . . .	5
2.2	Security Features . . . . .	6
2.3	Family Standard Features . . . . .	7
2.4	Design-in Support . . . . .	8
<b>3</b>	<b>Ordering information . . . . .</b>	<b>8</b>
<b>4</b>	<b>Block diagram . . . . .</b>	<b>9</b>
<b>5</b>	<b>Limiting values . . . . .</b>	<b>10</b>
<b>6</b>	<b>Data sheet status . . . . .</b>	<b>11</b>
<b>7</b>	<b>Definitions . . . . .</b>	<b>11</b>
<b>8</b>	<b>Disclaimers . . . . .</b>	<b>11</b>
<b>9</b>	<b>Contact information . . . . .</b>	<b>11</b>



© Koninklijke Philips Electronics N.V. 2003

All rights are reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

Date of release: 4 October 2004  
Document order number: 9397 750 XXXXX

Published in The Netherlands