SmartMX

P5CC036

Secure PKI Smart Card Controller

Rev. 1.0 — 2004 March 26 Short Form Specification

1. General description

1.1 Family description

Philips Semiconductors Smart*MX* (**M**emory e**X**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 Smart*MX* family manufactured in most advanced CMOS 0.18 µm 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.

Smart*MX* 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 Smart*MX* platform features please refer to the "Smart*MX* platform features" short form specification.

1.2 Description P5CC036 device

- 36 Kbytes EEPROM
- 128 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

The P5CC036 is a Secure PKI Smart Card Controller of the Smart*MX* platform featuring 128 Kbytes of ROM, 4608 bytes of RAM and 36 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.

Bi-directional communication with the contact interface of the device is performed through a serial IO, which is under full control of the application software in order to allow conditional controlled access to the different internal memories.

PHILIPS

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 P5CC036 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 with a single 1.8V, 3 V or 5 V power supply (voltage classes C, B, A) at a maximum external clock frequency of 10 MHz supplied by the contact pads. The internal clock frequency generated by an independent oscillator can go up as high as 30 MHz.

2. Features

2.1 Product Specific Features

- 36 Kbytes EEPROM (including 192 bytes reserved manufacturer/security area)
- 128 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
- **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)

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
- **Memory protection** (encryption and physical measures) for RAM, EEPROM and ROM
- **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
- 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
  - Bytewise EEPROM programming and read access
  - EEPROM endurance: minimum 100.000, typical 250.000 programming cycles
  - EEPROM data retention time: 10 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

2.4 Design-in Support

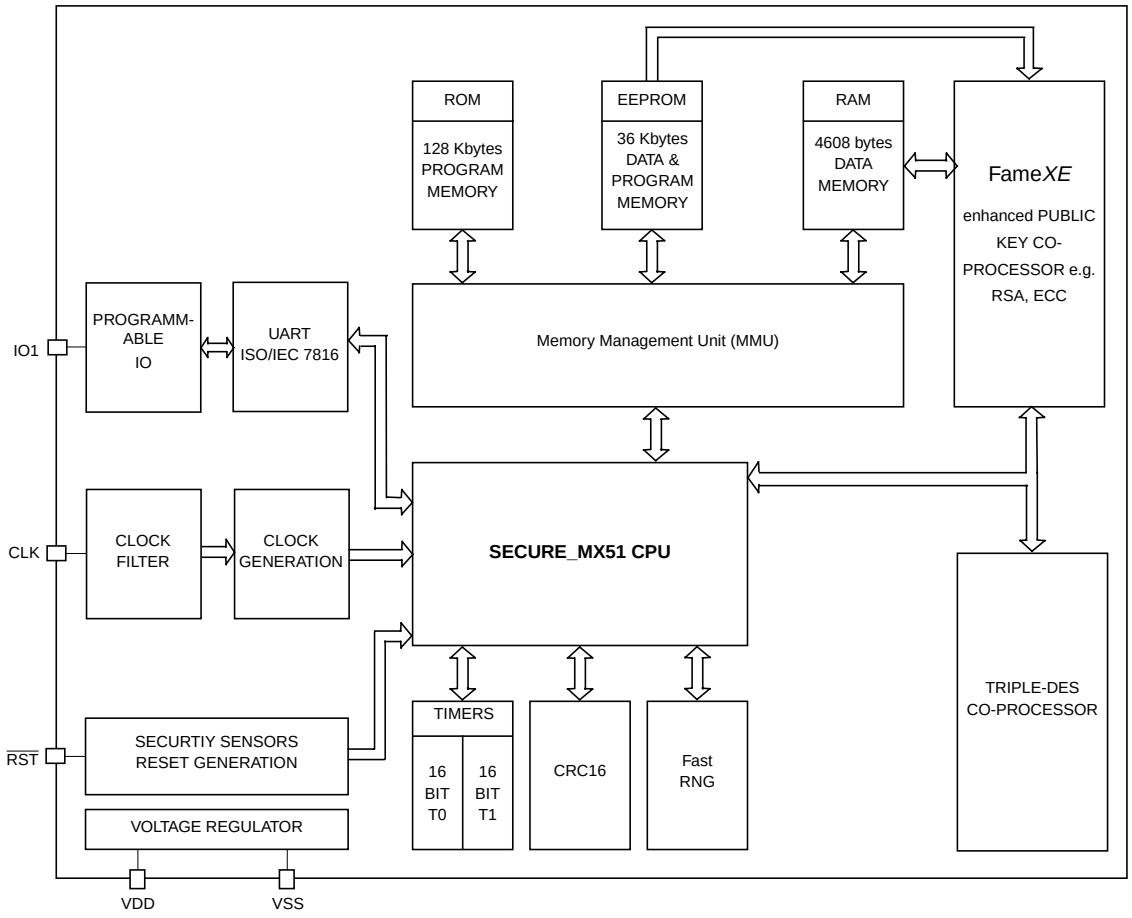
- Approved Development Tool Chain
  - Keil PK51 development tool package incl. Vision2/dScopeC51 simulator, additional specific hardware drivers incl. simulation of contactless interface and ISO/IEC 7816 card interface board. A “Smart*MX* DBox” allows software debugging and integration tests. (www.keil.com)
  - 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)
  - 8 Contact dummy modules OM6722 (PCM 1.1 - SOT658) for testing the implanting process.
- Software Libraries
  - EEPROM Read / Write routines
  - Tutorial library with source code example routines

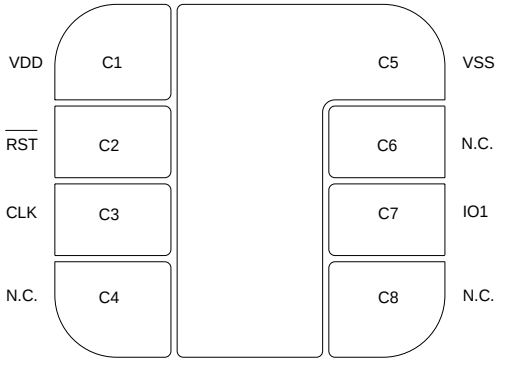
3. Ordering information

Table 1: Ordering information

Type number	Package		
	Name	Description	Version
P5CC036EW1/Tvsrrffo	FFC	sawn wafer 150 µ on film frame carrier	
P5CC036EV0/Tvsrrffo	Module	8 contact Modules on super 35 mm format (8-contact)	SOT658

4. Block diagram





ISO 7816		("Standard")	P5CC036
CONTACTS	**Symbol**	**Symbol**	**Description**
C1	VCC	VDD	Power supply voltage input
C2	RST	$\overline{\text{RST}}$	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

Fig 1. Block diagram and pinning information P5CC036.

5. Limiting values

Table 2: 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		-	± 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 3: 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		-25		+85	°C

6. 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.

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**

10. Tables

11. Figures

12. Contents

Date of release: 2004 March 26
Document order number: 9397 750 XXXXX

Published in The Netherlands