SmartMX

P5CD036

Secure Dual Interface 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 P5CD036 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
- AES co-processor
- ISO/IEC 7816 contact interface
- ISO/IEC 14443A contactless interface

The P5CD036 is a Secure Dual Interface 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.

PHILIPS

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 P5CD036 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) or with a power supply generated from the RF-field emitted by an RF-reader.

1.2.1 Different Configurations of the P5CD036

Depending on the application requirements the P5CD036 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.

1.2.1.1 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.

1.2.1.2 Configuration B1

In configuration **B1** the contactless MIFARE® Classic OS provided by Philips is implemented on the P5CD036. 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.

1.2.1.3 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 CM500 Product Specification
- MIFARE® Standard IC MF1 ICS50 Functional Specification
- MIFARE® Standard 4 Kbyte Card IC MF1 ICS70

Table 1: Configurations of the P5CD036

Configuration	EEPROM
A	36 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.

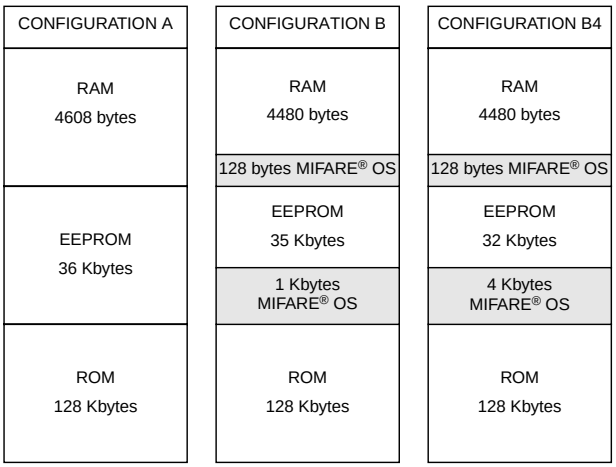

Fig 1. Configurations of the P5CD036.

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
- **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** 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**
- **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 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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.