SHORT FORM SPECIFICATION

High Speed DES Engine
64 Kbytes ROM / 16 Kbytes EEPROM / 1.3 Kbytes RAM
ISO7816 & ISO 14443 A Interface
Contact & Contactless Operation
Optional MIFARE® Emulation (1K or 4K)
TANGRAM Handshaking Technology

mifare® proX

P8RF6016

Secure Dual Interface Smart Card IC

Short Form Specification
Revision 1.0

November 2003

Philips
Semiconductors

Secure Dual Interface Smart Card IC P8RF6016

CONTENTS

Note: Specification may be changed without further notice.

Secure Dual Interface Smart Card IC P8RF6016

1 FEATURES

1.1 MIFARE® ProX FAMILY STANDARD FEATURES

- Enhanced ultra low power 80C51CPU, operates in contact and contactless mode
- TANGRAM handshaking technology
- High speed DPA resistant DES / DES3 engine
  - Triple-DES calculation time (incl. key load) <35 μs
  - Single-DES calculation time (incl. key load) <25 μs
- Memory Management Unit (MMU) allows:
  - secure separation of multi applications
  - memory mapping up to 1MByte Code memory
  - Extended memory addressing system (XMA) for fast memory access and data transfer
- True low power random number generator in hardware
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalisation at 1Mbit/s
- Contact configuration and serial interface according to ISO/IEC 7816: GND, VCC, CLK, RST, IO1
- contactless RF interface according to 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
  - 100% MIFARE®/ ISO/IEC14443 compatible
- Contactless Interface Unit (CIU) supporting the T=CL protocol according to ISO/IEC14443-4 including high speed option (212/424 kbit/s)
- optional free of charge MIFARE® functionality
- MIFARE® reader infrastructure compatibility
- High speed CRC engine according to CCITT
- Internal CPU / coprocessor clock up to 16 / 32 MHz
- Two 16-bit timers
- Multiple source vectorized interrupt system with two priority levels
- Error handling by customer definable exception interrupts
- Multiple source reset system
- Configurable external or internal CPU clocking
- external clock frequency range 1 MHz to 8 MHz
- High reliable EEPROM for both data storage and program execution
  - Bytewise EEPROM programming and read access
  - EEPROM endurance: minimum 100.000 programming cycles per byte
  - EEPROM data retention time: 10 years minimum
- Versatile EEPROM programming of 1 to 64 bytes at a time
- Typical EEPROM page erasing time: 1.6 ms
- Typical EEPROM page programming time: 1.6 ms
- 2.7 V to 5.5 V extended operating voltage range
- —25 to +85 °C operating ambient temperature range
- Power-saving IDLE Mode
  - Wake-up from IDLE Mode by Reset or any activated interrupt
- Power-saving SLEEP or CLOCKSTOP Mode
  - Wake-up from SLEEP or CLOCKSTOP Mode by Reset or External Interrupt
- Additional IO ports IO2 and IO3 for full-duplex serial data communication; can be left unconnected if only one IO is required.

1.2 SECURITY FEATURES

- Special Design measures against physical attacks
- Power-up / Power-down reset
- Low / high supply voltage sensor
- Low / high clock frequency sensor
- Low / high temperature sensor
- EEPROM programming:
  - no external clock
  - hardware sequencer controlled
  - on-chip programming voltage generation
- Electronic fuses for safeguarded mode control
- Unique 4 Byte long serial number for each die
- 16 bytes Write Once Security area in EEPROM
- 4 bytes Read Only Security area in EEPROM
- 64 EEPROM bytes for customer-defined security FabKey. Featuring batch-, wafer- or die-individual security data.
- Clock input filter for protection against spikes
- Memory protection for RAM, EEPROM and ROM
- Custom specific EEPROM initialisation possible

1.3 PRODUCT SPECIFIC FEATURES

- 64 Kbytes User ROM
- 256 bytes IDATA RAM
- up to 1024 bytes XDATA RAM
- 16 KBytes EEPROM
- optional free of charge MIFARE® 1K or MIFARE® 4K functionality

1.4 DELIVERY TYPES

- 180 μm sawn wafer on film frame carrier (FFC)
- Dual interface module with ISO 7816 contact pads on super 35 mm film (8-contact)
- Samples in SO28 package (for new rom codes in small quantities only)

1.5 DESIGN IN SUPPORT

- **Development Tools**
  - Keil PK51 and DK51 development tool package incl. μVision2/dScope C51 simulator, additional specific hardware drivers incl. simulation of contactless interface and ISO7816 card interface board. (*www.keil.com*)
  - Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO7816 and ISO14443 card interface board. Code Coverage and Performance Measurement software tools for real time software testing. (*www.ashling.com*)
  - Raisonance, RKitP51, RKitE51 Development Suite (includes RIDE, C-Compiler, Assembler, Simulator, Realtime Emulator and ISO7816 and ISO14443 card interface board). (*www.raisonance.com*)
  - EvalOS Cards and Modules for chip evaluation and production setup testing available in small quantities.
  - Dual Interface Dummy Modules OM6711 in SOT658BA1 package for implantation process testing available.
- **Application Support**
  - Application Notes and dedicated customer application support engineers.
  - Customer trainings on Dual interface controllers and ISO14443 related topics on request
- **Software Libraries**
  - Libraries supporting contactless communication according to ISO 14443, Part 3 and 4
  - EEPROM Read / Write routines
  - Tutorial libraries / example routines for DES engine

2 DESCRIPTION

The P8RF6016 is an ultra low power secure 8-bit dual interface smart card controller combining contactless smart card technology based on the ISO14443A / MIFARE® contactless interface platform and contact smart card technology on a single chip. It is designed to support both high level languages like Java and multi application operating systems. To meet the requirements of new open e-purse standards like CEPS high security features are implemented combined with the convenience and transfer speed that is needed in contactless applications such as electronic ticketing.

The device is manufactured in a most advanced CMOS process and is designed for embedding into chip cards according to ISO 7816. Compared to a contact only card an antenna has to be added in the peripheral zone of the card body (see Figure 1). The antenna consists of a few turns of a printed, etched or wired coil which is directly connected to the two contactless interface pads of the dual interface smart card module.

To provide the highest possible degree of protection against hostile attacks the Philips Dual Interface Smart Card ICs are designed for security which requires continuous ongoing improvements. Philips is committed to this policy. Special attention was drawn to the design of the security architecture, in order to achieve the highest degree of protection against fraudulent attacks. Each security measure is designed to act as an integral part of the complete system in order to strengthen the design as a whole.

The P8RF6016 is based on the 80C51 microcontroller family extended by additional functionality to support high speed memory access. This extended memory addressing system (XMA) is a special hardware block working like a co-processor and offering 16 bit functionality for the P8RF6016. It supports all data manipulating instructions of the 8051 core and can be used without additional special instructions.

The device includes 64 Kbytes of ROM, up to 1.3Kbytes RAM (data memory) and 8 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. This is especially important when the EEPROM is used as program memory.

The Triple-DES co-processor speeds up the calculation time for Triple-DES encryption by about three orders of magnitude compared to software solutions and can be used both in contact and contactless operation. Together with the fast contactless interface it offers high security and high speed for contactless smart card applications.

The field proven MIFARE® RF interface technology (ISO14443-2) is used 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 emulation modes of MIFARE® 1K or MIFARE® 4K enables fast system integration and backward compatibility of P8RF6016 based cards.

PHILIPS offers a unique feature free of charge on its Dual interface controllers, the MIFARE® 1K or 4K emulation providing the same functionality and performance as the hardwired logic contactless memory cards. The MIFARE® functionality can be used concurrently with ISO/IEC14443 (T=CL) protocol based applications. This gives customers maximum flexibility.

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

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 P8RF6016 provides two power saving modes with reduced activity: the IDLE and the SLEEP or CLOCKSTOP Mode. These two modes are activated by software.

The P8RF6016 operates either with a single 3 V or 5 V power supply at a maximum clock frequency of 8 MHz supplied by the contact pads or with a power supply generated from the electromagnetic field emitted by a reader antenna.

Operated both in contact and in contactless mode the users define the final function of the card with their operating system (OS). This allows the same level of security and flexibility for the contact (ISO 7816) interface as well as for the contactless (ISO 14443) interface.

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.