SHORT FORM SPECIFICATION

32-bit PKI Engine

High Speed DES Engine

64 Kbytes ROM / 16 Kbytes EEPROM / 2.3 Kbytes RAM

ISO7816 & ISO 14443 A Interface

Contact & Contactless Operation

Optional MIFARE® Emulation (1K or 4K)

TANGRAM Handshaking Technology

mifare® proX

P8RF5016

Secure Dual Interface Smart Card IC

Short Form Specification
Revision 1.4

May 2003

Philips
Semiconductors

PHILIPS

Secure Dual Interface Smart Card IC P8RF5016

CONTENTS

Note: Specification may be changed without further notice.

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 / co-processor 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 bytes 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
- 2048 bytes XDATA RAM
- 16 Kbytes EEPROM
- optional free of charge MIFARE® 1K or MIFARE® 4K functionality
- 32 bit PKI engine **Fame*X*** (Fast Accelerator for Modular Exponentiation-e*X*tended) optimized for public key cryptographic calculations
  - 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
  - < 40 ms typical signature generation time (Chinese Remainder Theorem) of 512-bit RSA
  - < 400 ms typical signature verification time of 1024-bit RSA
  - 32-bit key length increments
  - boolean operations for acceleration of standard, symmetric cipher algorithms

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 and PKI co-processors
  - Advanced PKI library

2 DESCRIPTION

The P8RF5016 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 P8RF5016 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 P8RF5016. 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 2.3 Kbytes RAM (data memory) and 16 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 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 P8RF5016 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.

The integrated PKI engine Fame*X* accelerates the encipherment for Public Key encryption algorithms. This widens the field of applications for this device, since it can be used as tamper-resistant security tool for secured and authentic communication in open networks and can be used both in contact and contactless operation.

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 P8RF5016 provides two power saving modes with reduced activity: the IDLE and the SLEEP or CLOCKSTOP Mode. These two modes are activated by software.

The P8RF5016 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.

Fig.1 P8RF5016 Dual Interface Card.

2.1 Different Configurations of the P8RF5016

Depending on the application requirements the P8RF5016 can be configured in three different ways. The configuration has impact on the access conditions for the EEPROM and influences the user OS development. Three different configurations (A, B1 and B4) are possible and shown in Table 1. The following section gives a rough idea of the different configuration.

2.1.1 Configuration A

In configuration **A** all memory resources are available and under full control of the dual interface User OS.

2.1.2 Configuration B1

In configuration B1 the contactless MIFARE® Classic OS provided by Philips is implemented on the P8RF5016. 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 in a special section of the ROM code with 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.

2.1.3 CONFIGURATION B4

Configuration B4 means that Philips provides MIFARE® Classic OS giving the same functionality and command set as given by the MIFARE® 4K chip. This emulation will be implemented in the ROM of the P8RF5016 and 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 in a special section of the ROM code (ACM .. Access Condition Matrix).

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

For detailed explanation of MIFARE® S 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 P8RF5016

CONFIGURATION	EEPROM
A	16 Kbytes for access with user OS
B1	15 Kbytes for access with user OS via EEPROM SFR 1 Kbyte for access with MIFARE® Classic OS and user OS (1) (2)
B4	12 Kbytes for access with user OS via EEPROM SFR 4 Kbytes for access with MIFARE® Classic OS and user OS (1) (2)

Notes

1. In configuration B1 and B4 the MIFARE® OS allocates 128 bytes of the CRAM at address 0480h to 04FFh
2. For secure access a password is needed that is checked every time the user operating system (User OS) wants to access MIFARE® password secured EEPROM data. The user system has to call the function **eePasswordRead** or **eePasswordWrite** by CVEC function calls.

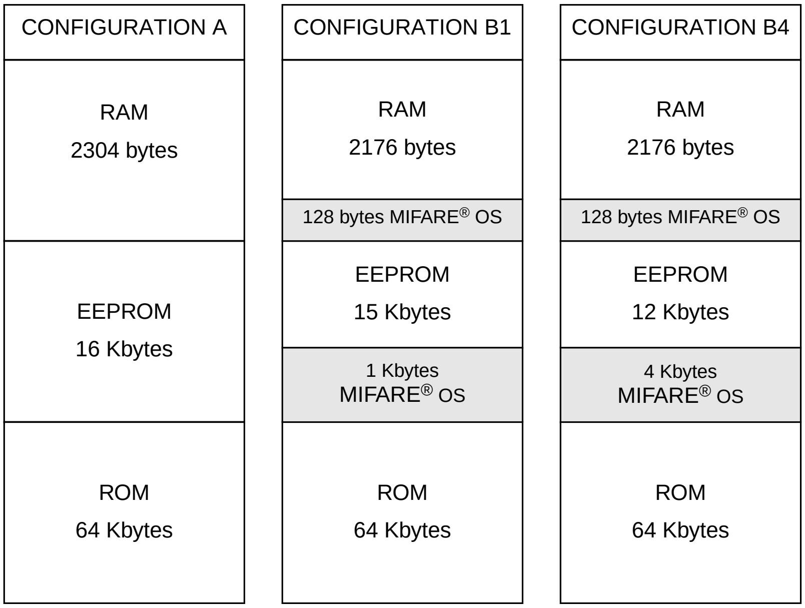


Fig.2 Configurations of the P8RF5016.

3 ORDERING INFORMATION

Table 2 Ordering Information of the P8RF5016

TYPE NUMBER[1]	PACKAGE			TEMPERATURE RANGE (°C)
	NAME	DESCRIPTION		
P8RF5016AEW/0xxyyWz	FFC	sawn wafer on film frame carrier	–	-25 to +85
P8RF5016AEV/0xxyyBz	Module	Dual Interface Modules on super 35 mm film (8-contact)	SOT658BA1	
P8RF5016AEV/0xxyyCz	Module Plug In Type	Dual Interface Modules on super 35 mm film (8-contact) with Antenna connected to C4 and C8	SOT658BA1	

4 BLOCK DIAGRAM

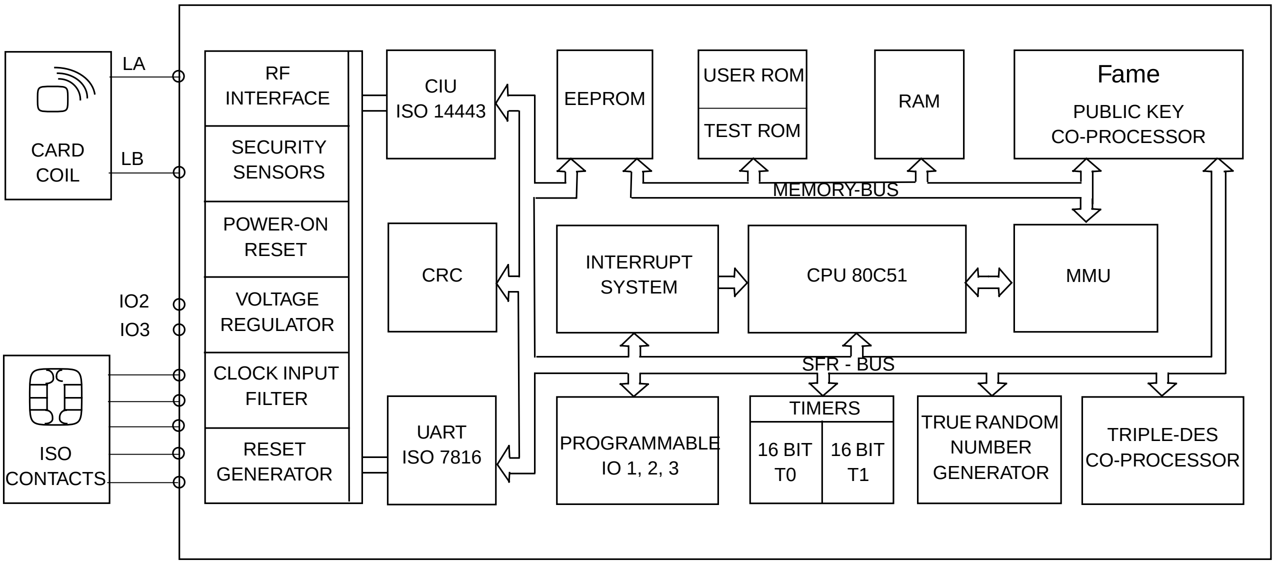
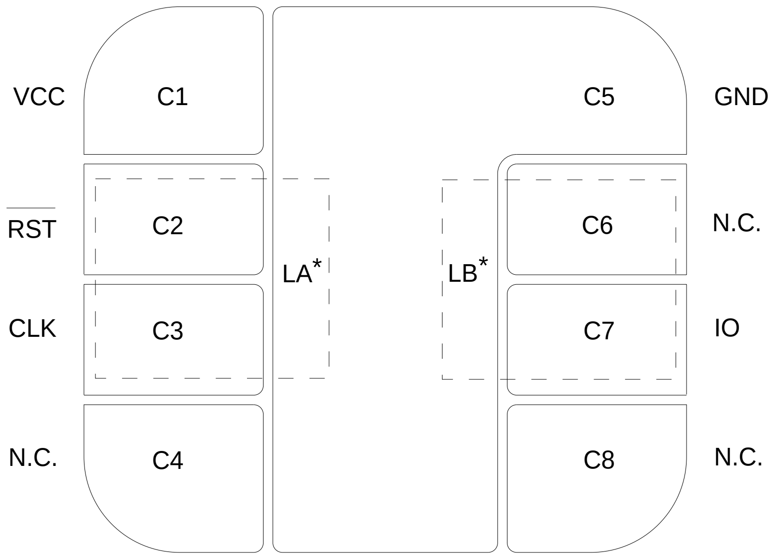


Fig.3 Block diagram P8RF5016.

5 PINNING INFORMATION

5.1 Smart Card contacts

5.1.1 Smart Card contacts Dual Interface “Standard Type”



* Antenna contacts are placed on module backside

Fig.4 Contact assignments for SOT658BA1 (Standard Type).

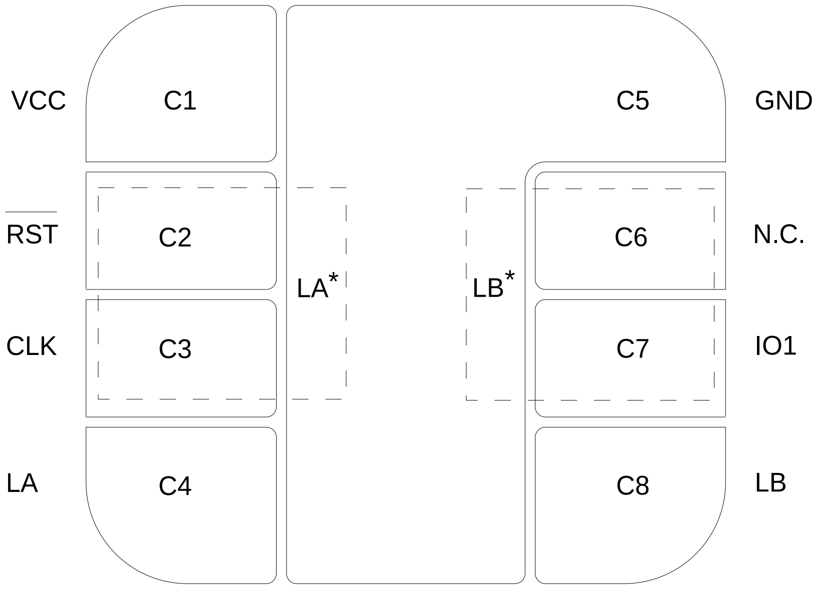
Table 3 Pin description

ISO 7816		P8RF5016	
CONTACTS	**SYMBOL**	**SYMBOL**	**DESCRIPTION**
C1	VCC	VCC	Power supply voltage input
C2	RST	$\overline{RST}$	Reset input, active LOW
C3	CLK	CLK	Clock input
C4	reserved	N.C.	not connected
C5	GND	GND	Ground (reference voltage) input
C6	VPP	N.C.	not connected
C7	IO	IO	Input/Output #1 for serial data
C8	reserved	N.C.	not connected
–	–	IO2	Input/Output #2 for serial data
–	–	IO3	Input/Output #3 for serial data
–	–	LA	antenna coil connection
–	–	LB	antenna coil connection

Note

1. IO2, IO3 assignment on request

5.1.2 Smart Card Contacts Dual Interface “Plug In Type”



* Antenna contacts are placed on module backside

Fig.5 ISO contact assignments for SOT658BA1 (Plug-In-Type).

Table 4 Pin description

ISO 7816		DUAL INTERFACE (“PLUG-IN TYPE”)	P8RF5016
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	reserved	LA	Antenna coil connection LA
C5	GND	VSS	Ground (reference voltage) input
C6	VPP	N.C.	not connected
C7	IO	IO1	Input/Output #1 for serial data
C8	reserved	LB	Antenna coil connection LB

Note

1. IO3 assignment on request

Philips Semiconductors – a worldwide company

Contact information

For additional information please visit **http://www.semiconductors.philips.com**. Fax: **+31 40 27 24825**
For sales offices addresses send e-mail to: **sales.addresses@www.semiconductors.philips.com**.

SCA74

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.

Let's make things better.

Philips
Semiconductors

PHILIPS

PHILIPS