SmartMX platform features

Secure Smart Card Controller Platform

Rev. 1.0 — 24 March 2004 Short Form Specification

1. General description

1.1 Platform description

Philips Semiconductorís 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 8051 instruction set. The Smart*MX* platform manufactured in most advanced CMOS 0.18µm 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.

As the first smart card controller platform of its kind the Smart*MX* portfolio incorporates three interface options as an integral part of a highly secure smart card controller portfolio – ISO/IEC 7816 Contact Interface, ISO/IEC 14443A Contactless Interface and USB 2.0 LS Interface.

Smart*MX* enables the easy implementation of state-of-the-art operating systems and open platform solutions including Java Card Global Platform and MULTOS and offers an optimized feature 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 Philips Semiconductors' unique security, power, and performance optimized design concept named TANGRAM technology. The platform supports Class "A", "B" and "C" voltage ranges (1.62 - 5.5V) as required by application standards such as 3G Mobile Communication (3GPP) and the credit/debit card standard (EMV).

Indicated platform members feature a state-of-the-art Memory Management Unit (MMU) to further enhance the security of the platform in a multi-application set up. All functions featured, including the operation of Fame*XE*, DES and AES, are also available and fully operational via the contactless interface.

1.1.1 The Smart*MX* Architecture

Philips Semiconductors' MX-concept offers linear addressing for all on-chip memories up to 16 Mbytes. Therefore paging / banking concepts are not necessary anymore. Along with a new instruction set this concept improves the code efficiency with C programming. MX development tools generate code that is up to 30% more condensed than for standard 8051 architectures, enabling higher performance at minimized memory space consumption. Certain product types within Smart*MX*-platform maintain 100% backward compatibility to Philips Semiconductors' well established WE family and enable an easy transition of existing software retaining available software assets of Philips WE-Family and MIFARE® ProX-family customers as well as other 8051-based software developments.

PHILIPS

A “WE-compatibility mode” allows for direct reuse of existing WE software within the Smart*MX* platform. Together with Philips advanced 0.18 µm technology and the high performing, power saving, TANGRAM design methodology, Smart*MX* operates at clock frequencies of up to 30 MHz, outperforming any other comparable platform.

1.2 Product Types

The members of the Smart*MX* smart card controller are split into two categories:

Security Controllers and **PKI Controllers**

Security Controllers do have a Triple-DES hardware co-processor as standard crypto processor whereas PKI controllers do have an additional PKI hardware co-processor called Fame*XE*. On dedicated PKI platform controllers there is also a state of the art hardware AES co-processor available.

The platform members of the Smart*MX* Contact and Dual Interface Security Controllers as well as Smart*MX* Contact and Dual Interface PKI Controllers (Public Key Infrastructure via Fame*XE* operation) are documented in a regularly updated Philips Semiconductors Identification “Product Line Sheet”.

1.2.1 Naming conventions

P5xyzzz	**Smart*MX* platform**
yyy	Amount of Non-Volatile memory (EEPROM + optionally Flash) in Kbyte, increasing count for further product options.
x	Type of category: **S** .. Security controller (Triple DES co-processor) **C** .. PKI controller Fame*XE* co-processor + AES co-processor on selected products
y	Interface options **C** .. contact interface - ISO/IEC 7816 **D** .. Dual Interface - ISO/IEC 7816 + ISO/IEC14443 Contactless Interface **T**.. Triple interface ISO/IEC 7816 + ISO/IEC14443 Contactless Interface + USB 2.0 LS **U** .. ISO/IEC 7816 + USB 2.0. LS Interface
Examples:	
xy = SU	Security Controller, ISO/IEC 7816 + USB 2.0 (LS) Contact Interface/ UARTs
xy = SD	Security Controller, ISO/IEC 7816 Contact + ISO/IEC14443 Contactless Interface / UARTs
xy = SC	Security Controller, ISO/IEC 7816 Contact Interface / UART
xy = CT	PKI Controller, ISO/IEC 7816 + USB 2.0 (LS) Contact + ISO/IEC14443 Contactless Interface / UARTs
xy = CD	PKI Controller, ISO/IEC 7816 Contact + ISO/IEC14443 Contactless Interface
xx = CC	PKI Controller, ISO/IEC 7816 Contact Interface / UARTs

1.3 The Cryptographic co-processors

1.3.1 The Hardware PKI co-processor Fame*XE*

Philips Semiconductors' solution to support public key cryptography based on finite fields of prime order – GF(p), has been enhanced from Fame*X* to become Fame*XE* within the Smart*MX* platform concept. Fame*XE* supports the trend of increasing RSA keys with faster execution speeds and Elliptic Curve Cryptography (ECC) based on GF(2n) at best performance. Fame*XE* supports RSA with an operand length of up to 5kBits and related standards (PKC#1[RSA], PKC#3 [Diffie-Hellman] and FIPS 186-2 [DSA&EC-DSA], IEEE P1363).

The Fame*XE* PKI co-processor also supports ECC key lengths of up to 192-bit, which according to the German BSI is comparable with 2048-bit RSA [1]. An ECC – GF(2n) based signature, using a 163-bit key can be executed in less than 30 ms providing a security level comparable to 1024-bit RSA. Fame*XE* is easy to use and understood by programmers. Its user friendly and flexible interface provides programmers with the freedom to implement their own know how without being obliged to use third party software. A crypto library providing a large range of required functions is available to support customers in implementing Public Key-based solutions.

1.3.2 The Hardware Triple DES (Digital Encryption Standard) Co-processor

The Digital Encryption Standard (DES) for symmetric encryption used in many applications today is supported by a dedicated, high performance, highly attack resistant hardware co-processor. Single DES and triple DES, based on two or three DES keys, can be executed within less than 50 µs. Relevant standards (ISO/IEC, ANSI, FIPS) and Message Authentication Code (MAC) are fully supported.

1.3.3 The Hardware AES (Advanced Encryption Standard) Co-processor

Smart*MX* is the first smart card micro-controller platform to provide a dedicated high performance 128 bit parallel processing co-processor to support Advanced Encryption Standard (AES). The implementation is based on the Rijndael algorithm, as recommended by the National Institute for Standards and Technology (NIST), and supports key lengths of 128-, 192-, and 256-bits with performance levels comparable to DES. AES is the next generation for symmetric data encryption and is the recommend successor of DES providing significantly improved security levels.

1.4 The Smart*MX* Interfaces

1.4.1 The Smart*MX* Contact Interface

Operating in accordance with ISO/IEC 7816, the Smart*MX* 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.

1.4.2 The Smart*MX* Contactless Interface

The contactless interface is available on all Philips Semiconductors' Dual Interface smart card controller ICs and is fully compatible with ISO/IEC 14443 A and with Philips Semiconductors' field proven MIFARE® technology. A dedicated hardware, the so called CIU (Contactless Interface Unit) manages and supports communication at data rates of up to 424 Kbit/s.

A true anti-collision method (acc. ISO/IEC 14443-3), enables multiple cards to be handled simultaneously.

The contactless interface can be used to communicate via any protocol

- T=CL protocol (acc.ISO/IEC 14443-4)
- MIFARE® protocol (configuration B1 and B4)
- Self defined contactless transmission protocol

The free of charge emulation modes of MIFARE® Classic provided in configurations B1 (1K MIFARE® functionality) and B4 (4K MIFARE® functionality) makes this interface compatible with any installed MIFARE® Classic infrastructure.
The ability to run the MIFARE® protocol concurrently with other contactless transmission protocols implemented by the User OS (T=CL or self defined) enables the combination of new services and existing applications based on MIFARE® (e.g. ticketing) on a single Dual Interface controller based smart card.

Smart*MX* together with the contactless interface once more proves the superiority of the ISO/IEC 14443 A interface option for high security smart card solutions.
A tutorial software library for ISO/IEC 14443-3 and ISO/IEC 14443-4 is available to support Philips Semiconductors' customers and enable the easy integration of the contactless technology into current system solutions.

1.5 Security Features

Smart*MX* incorporates a range of security features to counter measure side channel attacks like DPA, SPA etc. Philips Semiconductors' deep knowledge of chip security, proven by the design of the WE- and P8RF family, combined with Philips TANGRAM technology, the highly densed 0.18 µm five metal layer technology and Philips Glue logic methodology make typical attack paths invalid. The effectiveness of the TANGRAM methodology has been proven on the MIFARE® ProX platform.

Smart*MX*'s Memory Management Unit (MMU), which is designed to define various memory segments and assign security attributes accordingly, supports a strong firewall concept which keeps different applications separate from each other. Only a so-called System Mode has full access privileges to all memory space and on-chip peripherals, while the User Mode only has privileges defined upon card personalization and executed under the control of the System Mode.

1.6 Security Evaluation and Certificates

Philips Semiconductors will continue to drive forward third party security evaluations to provide its customers with the relevant information and documentation needed to execute subsequent evaluations of implemented applications.

Targeted certifications are CC EAL5+, VISA, MASTERCARD, MULTOS, SECCOS, ZKA depending on the application requirements.

2. Features

2.1 Platform Standard Features

- Dedicated Secure_MX51 Smart Card CPU (Memory eXtended / enhanced 80C51)
  - highly condensed 0.18 µm - 5 metal layer CMOS technology
  - operating in contact and contactless mode (dependent on platform type option)
  - featuring a 24 bit universal memory space
  - 24 bit program counter
  - combined universal program/data memory linear address range up to 16 Mbyte
  - additional instructions to improve
    - Pointer operations
    - Performance and code density of both C and Java source code
  - Saving of up to 30% memory space
- Low power / low voltage design using Philips TANGRAM technology
- Development support and portation support to existing P8WE family mask (Compatibility Mode)
- Development support and portation support to existing P8RF family masks
- Two 16-bit timers
- Multiple source vectorized interrupt system with four priority levels
- Error handling by customer defined exception interrupts
- Watch exception provides for software debugging facility
- Multiple source RESET system
- 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 classes A, B and C
- -25 to +85°C operating ambient temperature range

2.2 Security Features

- **Enhanced Security Sensors**
  - Low / high clock frequency sensor
  - Low / high temperature sensor
  - Low / high supply voltage 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)** [1]
  - 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

1.dependent on selected product

2.3 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/IEC7816/ USB 2.0 (low speed) 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/IEC7816 / USB 2.0 (low speed) and ISO/IEC14443 card interface board. Code coverage and performance measurement software tools for real time software testing. (www.ashling.com)
  - Dual Interface dummy modules OM6711 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
  - Library with source code routines for random numbers, SHA-1 and the crypto co-processors DES, AES and Fame*XE*

3. Ordering information

Table 1: Ordering information

Type number [1]	Package		
	Name	Description	Version
P5xyzzzEW1/T0srrffo	FFC	sawn wafer 150 µ on film frame carrier [2]	-
P5xyzzzEV0/T0srrffo	Module	Dual Interface Modules on super 35 mm format (8-contact)	SOT658BA3
P5xyzzzEV1/T0srrffo	Module	Dual Interface Modules on super 35 mm format (8-contact) with Antenna connected to C4/C8	SOT658BA3
P5xyzzzEV3/T0srrffo	Module	pure contactless module MOB2 on super 35 mm format	SOT500AA3

[1] Refer also to data sheet chapter “ORDER ENTRY FORM”

[2] Delivered will be UV-Degradable Dicing Tape after UV exposure. See also “Data Sheet Addendum to the General Specification for 8” Wafer”.

4. Block diagram

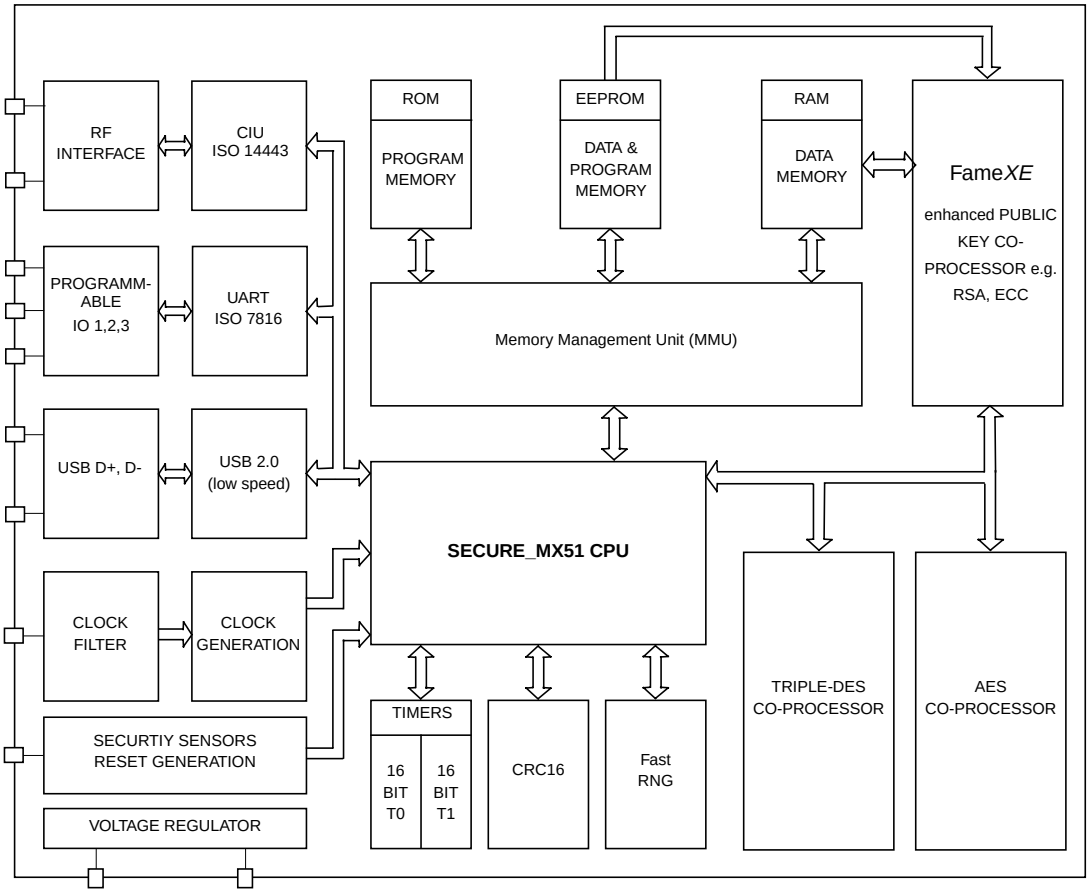

Fig 1. Block diagram P5xyzzz.

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, IO2, IO3		-	± 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
$V_{I(ai/o)}$	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 [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: 24 March 2004
Document order number: 9397 750 XXXXX

Published in The Netherlands