P5Cx012/02x/40/73/80/144 family

Secure dual interface and contact PKI smart card controller

Rev. 03 — 24 January 2008 Objective short data sheet

1. General description

1.1 SmartMX family approach

The new CMOS14 SmartMX family members feature a modular set of devices with:

- 12 KB to 144 KB EEPROM
- 200 KB user ROM
- 6144 B RAM
- High-performance secured Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secured dual/triple-DES coprocessor
- Secured AES coprocessor
- Memory Management Unit (MMU)
- ISO/IEC 7816 contact interface
- Optional ISO/IEC 14443 A Contactless Interface Unit (CIU)
- Optional S^2C interface for NFC communication link
- 5-metal-layer 0.14 μm CMOS technology
- EEPROM with typical 500000 cycles endurance and minimum 20 years retention time
- Broad spectrum of delivery types
- Optional certified crypto library modules for RSA, ECC, DES, AES, SHA and PRNG

1.2 SmartMX family properties

The long-term approved SmartMX family features a significantly enhanced secure smart card IC architecture. Extended instructions for Java and C code, linear addressing, high speed at low power and a universal memory management unit are among many other improvements added to the classic 80C51 core architecture. The technology transfer step from 5-metal-layer 0.18 μm to 5-metal-layer 0.14 μm CMOS technology offers now even more advantages in terms of security features, memory resources, crypto coprocessor calculation speed for RSA and ECC as well as availability of secure hardware support for 2/3-key Digital Encryption Standard (DES) and Advanced Encryption Standard (AES) operations.

The availability of contact interface, optional contactless or S^2C interface enables the easy implementation of native or open platform and multi-application operating systems in market segments like e.g. banking, E-passport, ID card, Health Card, secure access, Java card, Near Field Communication (NFC) connectable mobile hand sets as well as Trusted Platform Modules (TPM).

NXP founded by Philips

1.3 Naming conventions

Table 1. Naming conventions

P5xyzzz	SmartMX platform
x	Type of category: C = PKI controller + Triple-DES coprocessor + AES coprocessor on selected products
y	Interface options: C = contact interface - ISO/IEC 7816 D = dual interface - ISO/IEC 7816 + ISO/IEC 14443 contactless interface N = ISO/IEC 7816 + S^2C Interface for NFC
zzz	Amount of non-volatile memory in KB, increasing count for further product options

1.4 Cryptographic hardware coprocessors

1.4.1 FameXE coprocessor

The approved and modular FameXE architecture supports the trend of increasing RSA keys with faster execution speeds as well as Elliptic Curve Cryptography (ECC) based on GF(p) or GF(2^n) at best performance. FameXE supports RSA with an operand length of up to 8-kbit (up to 4-kbit with intermediate storage in RAM only).

The FameXE PKI coprocessor supports 192-bit ECC key length that offers the same level of security as 2048-bit RSA. An ECC GF(2^n) based signature, using a 163-bit key can be executed in less than 30 ms providing a security level comparable to 1024-bit RSA. The operand size for ECC, supported by FameXE, is only limited by the 2.5 KB size of the FXRAM. FameXE is easy to use and the flexible interface provides programmers with the freedom to implement their own cryptology solutions. A secured and CC EAL5+ certified crypto library providing a large range of required functions will be available for all devices in order to support customers in implementing public key-based solutions.

1.4.2 Triple-DES coprocessor

The DES for widely used symmetric encryption is supported by a dedicated, high performance, highly attack resistant hardware coprocessor. Single DES and triple-DES, based on two or three DES keys, can be executed within less than 40 µs. Relevant standards (ISO/IEC, ANSI, FIPS) and Message Authentication Code (MAC) are fully supported. A secured crypto library element for DES is available.

1.4.3 AES coprocessor

SmartMX is the first smart card microcontroller platform to provide a dedicated high performance 128-bit parallel processing coprocessor to support secure AES. The implementation is based on FIPS197 as standardized by the National Institute for Standards and Technology (NIST), and supports key lengths of 128-bit, 192-bit, and 256-bit with performance levels comparable to DES. AES is the next generation for symmetric data encryption and recommended successor of DES providing significantly improved security level. A secured crypto library element for AES is available.

© NXP B.V. 2008. All rights reserved.

1.5 SmartMX interfaces

1.5.1 SmartMX contact interface

Operating in accordance with ISO/IEC 7816, the SmartMX contact interface is supported by a built-in Universal Asynchronous Receiver/Transmitter (UART), which enables data rates of up to 1 Mbit/s allowing for the automatic generation of all typical baud rates and supports transmission protocols T = 0 and T = 1. Either one or two additional IOs are available.

1.5.2 SmartMX contactless interface

The optional contactless interface is fully compatible with ISO/IEC 14443 A as well as NXP Semiconductors field proven MIFARE technology. A dedicated Contactless Interface Unit (CIU) manages and supports communication using data rates of up to 848 kbit/s. A true anti-collision method (according to ISO/IEC 14443-3) enables multiple cards to be handled simultaneously.

The optional MIFARE functionality provided in configurations B1 (MIFARE 1 KB emulation) and B4 (MIFARE 4 KB emulation) safeguard the interface compatibility with any installed MIFARE 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.

A tutorial software library for ISO/IEC 14443-3 and ISO/IEC 14443-4 is available to support NXP Semiconductors customers for easy integration of the contactless technology into current system solutions.

1.5.3 SmartMX S^2C interface

The S^2C interface is intended for use with NXP Semiconductors NFC circuits (e.g. PN511, PN531) in order to configure a secure NFC system, e.g. in mobile hand sets.

Operated both in Contact mode (ISO/IEC 7816) and in S^2C mode the user defines the final function of the controller chip with its operating system. This allows the same level of security, functionality and flexibility for the contact interface as well as for S^2C interface.

The S^2C interface is connected to the internal ISO 14443 CIU. The CIU handles the demodulation and the modulation of the S^2C signals in a way that a full contactless communication via this interface and the NFC IC can be enabled. As the S^2C interface is connected to the CIU the power of the P5CN080/P5CN144 has to be supplied via the VDD and VSS pads to use the S^2C interface. The S^2C interface does not need any software adaptation compared to the normal contactless operation.

Connected to the S^2C interface of a NFC IC the device is compatible with existing MIFARE reader infrastructure and the optional emulation modes of MIFARE 1 KB or MIFARE 4 KB enable fast system integration and backward compatibility to MIFARE based cards. The communication on the S^2C interface supports both the ISO/IEC 14443 A part 3 and the ISO/IEC 14443 part 4.

© NXP B.V. 2008. All rights reserved.

1.6 Security features

SmartMX incorporates a big range of both inherent and OS controlled security features as counter measure against all types of attacks. NXP Semiconductors has used the deep knowledge of chip security, combined with the used handshaking circuit technology, the very dense 5-metal-layer 0.14 µm technology, glue logic and active shielding methodology for optimum results in CC EAL5+, EMVCo and other third party certifications and approvals.

SmartMX Memory Management Unit (MMU), designed to define various memory segments and assign security attributes accordingly, supports a strong firewall concept that keeps different applications separate from each other. Only the 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.

1.7 Security evaluation and certificates

The reached target of the certification is CC EAL5+. Also third party approvals like e.g. EMVCo (Visa, CAST), ZKA and others, depending on the application requirements, are available.

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

1.8 Optional crypto library

NXP Semiconductors will offer for all family types an optional crypto library:

- Various algorithms
  - AES encryption and decryption using the AES coprocessor
  - DES and Triple-DES encryption and decryption using the DES coprocessor
  - RSA encryption and decryption, signature generation and verification for straightforward and CRT keys up to 5024 bits
  - RSA key generation
  - ECC over GF(p) signature generation and verification (ECDSA) and Diffie-Hellman key exchange for keys up to 544 bits
  - ECC over GF(p) key generation
  - ECC over GF(2^n) signature generation and verification (ECDSA) and Diffie-Hellman key exchange for keys up to 571 bits
  - ECC over GF(2^n) key generation
  - SHA-1, SHA-224 and SHA-256 hash algorithm
  - Pseudo-Random Number Generator (PRNG)
- Easy to use API for all algorithms
- Secure operation in contact as well as in the contactless mode
- Latest built-in security features to avoid power (SPA/DPA), timing and fault attacks (DFA)

© NXP B.V. 2008. All rights reserved.

- Common criteria CC EAL5+ certification planned [except ECC over GF(2^n)] according to BSI-PP-0002 protection profile

2. Features

2.1 Standard family features

- EEPROM: choice of 12 KB, 20 KB, 40 KB, 72 KB, 80 KB or 144 KB
  - Data retention time: 20 years minimum
  - Endurance: 500000 cycles typical
- ROM: 200 KB
- RAM: 6144 B
  - 256 B IRAM + 3.25 KB standard RAM usable for CPU
  - 2560 B FXRAM usable for FameXE
- Dedicated Secure_MX51 Smart Card CPU (Memory eXtended/enhanced 80C51)
  - 5-metal-layer 0.14 µm 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 and data linear address range up to 16 MB
  - Additional instructions to improve:
    - Pointer operations
    - Performance
    - Code density of both C and Java source code
- ISO/IEC 7816 contact interface
- PKI coprocessor FameXE
- Support of major Public Key Cryptography (PKC) systems like RSA, Elgamel, DSS, Diffie-Hellman, Guillou-Quisquater, Fiat-Shamir and Elliptic Curves
  - 8192 bits maximum key length for RSA with randomly chosen modulus
  - 4096 bits maximum key length for calculation within RAM
  - 32-bit interface
  - Boolean operations for acceleration of standard, symmetric cipher algorithms
- High speed Triple-DES coprocessor (64-bit parallel processing DES engine)
  - Two or three keys loadable
  - DES3 performance < 40 µs
- High speed AES coprocessor (128-bit parallel processing AES engine)
- Memory Management Unit (MMU)
- Low power and low voltage design using NXP Semiconductors handshaking technology
- Multiple source vectorized interrupt system with four priority levels
- Watch exception provides 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

© NXP B.V. 2008. All rights reserved.

- Versatile EEPROM programming of 1 B to 64 B at a time or, optionally 1 B to 128 B at a time
- Typical EEPROM page erasing time: 1.7 ms
- Typical EEPROM page programming time: 1.0 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, VDD, CLK, RST_N, IO1
- ISO/IEC 7816 UART supporting standard protocols T = 0 and T = 1 as well as high speed personalization up to 1 Mbit/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 16-bit CRC engine according to ITU-T polynomial definition
- Low power Random Number Generator (RNG) in hardware, AIS-31 compliant
- 1.62 V to 5.5 V extended operating voltage range for class C, B and A
- Optional extended Class B operation mode (targeted for battery supplied applications)
- –25 °C to +85 °C ambient temperature
- Broad spectrum of delivery types:
  - Wafers
  - Modules

2.2 Product specific family features

- P5CC021, P5CC040, P5CC073, P5CC080 and P5CC144
  - ISO/IEC 7816 contact interface
  - Two additional IO ports IO2 and IO3 for full-duplex serial data communication
- P5CD012, P5CD020, P5CD040, P5CD080 and P5CD144
  - CIU fully compatible with ISO/IEC 14443 A:
    - Fully supports the T = CL protocol according ISO/IEC 14443-4
    - Data transfer rates supported: 106 kbit/s, 212 kbit/s, 424 kbit/s and 848 kbit/s
  - MIFARE contactless interface according ISO/IEC 14443-2:
    - 13.56 MHz operating frequency
    - Reliable communication due to 100 % ASK
    - High speed efficient frame support
    - True anticollision
  - MIFARE reader infrastructure compatibility
  - Optional MIFARE 1 KB and MIFARE 4 KB emulation
  - Two additional IO ports IO2 and IO3 for full-duplex serial data communication
- P5CN080 and P5CN144
  - S^2C interface
  - One additional IO port IO2 for full-duplex serial data communication

© NXP B.V. 2008. All rights reserved.

2.3 Security features

- Enhanced security sensors:
  - Low and high clock frequency sensor
  - Low and high temperature sensor
  - Low and high supply voltage sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors (included integrated memory light sensor functionality)
- Electronic fuses for safeguarded mode control
- Active shielding
- Unique ID for each die
- Clock input filter for protection against spikes
- Power-up and power-down reset
- Optional programmable card disable feature
- Memory security (encryption and physical measures) for RAM, EEPROM and ROM
- Memory Management Unit (MMU) including memory protection:
  - Secure multi application operating systems via two different operation modes: System mode and User mode
  - OS controlled access restriction mechanism to peripherals in User mode
  - Memory mapping up to 8-MB code memory
  - Memory mapping up to 8-MB (64-kbit) data memory
- 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-B or 128-B EEPROM for customer-defined Security FabKey. Featuring batch, wafer or die-individual security data, included encrypted diversification features on request
- 14 B user write protected security area in EEPROM (byte access, inhibit functionality per byte)
- 32 B write once security area in EEPROM (bit access)
- 32 B user read only area in EEPROM (byte access)
- Customer specific EEPROM initialization available

© NXP B.V. 2008. All rights reserved.

2.4 Design-in support

- Approved development tool chain:
  - Keil PK51 development tool package inclusive µVision3/dScope C51 simulator, additional specific hardware drivers inclusive simulation of contactless interface and ISO/IEC 7816 card interface board. A SmartMX DBox allows software debugging and integration tests.
  - Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO/IEC 7816 and ISO/IEC 14443 card interface board. Code coverage and performance measurement software tools for real time software testing.
  - Dual interface dummy modules OM6711 (PDM 1.1 - SOT658) 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 14443, part 3 and 4
  - EEPROM read/write routines

3. Applications

3.1 Application areas

- Banking
- Java cards
- E-passports
- ID cards
- Secure access
- Trusted platform modules

© NXP B.V. 2008. All rights reserved.

4. Quick reference data

Table 2. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{DD}	supply voltage	Class A: 5 V range		4.5	5.0	5.5	V
		Class B: 3 V range		2.7	3.0	3.3	V
		Class BE: 3 V range	[1]	2.2	3.0	3.3	V
		Class C: 1.8 V range		1.62	1.8	1.98	V

[1] In case of extended Class B (Class BE) operation mode (targeted for battery supplied applications), the class C is not supported.

5. Ordering information

Table 3. Ordering information

Type number	Package		
	Name	Description	Version
P5CC021UA	FFC	8 inch wafer (sawn; 150 µm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	<tbd>
P5CC040UA			
P5CC073UA			
P5CC080UA			
P5CC144UA			
P5CD012UA			
P5CD020UA			
P5CD040UA			
P5CD080UA			
P5CD144UA			
P5CN080UA			
P5CN144UA			
P5CD012UE	FFC	8 inch wafer (sawn; 75 µm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	<tbd>
P5CD020UE			
P5CD040UE			
P5CD080UE			
P5CD144UE			
P5CC021XS	PCM1.1	contact chip card module (super 35 mm format, 8-contact)	SOT658
P5CC040XS			
P5CC073XS			
P5CC080XS			
P5CC144XS			
P5CD012X1	PDM1.1	contactless chip card module (Plug-in type; super 35 mm format, 8-contact)	SOT658
P5CD020X1			
P5CD040X1			
P5CD080X1			
P5CD144X1			

© NXP B.V. 2008. All rights reserved.

Table 3. Ordering information *…continued*

Type number	Package		
	Name	Description	Version
P5CD012X0	PDM1.1	contactless chip card module (super 35 mm format, 8-contact)	SOT658
P5CD020X0			
P5CD040X0			
P5CD080X0			
P5CD144X0			
P5CD012A4	MOB4	plastic leadless module carrier package; 35 mm wide tape	SOT500-2
P5CD020A4			
P5CD040A4			
P5CD080A4			
P5CD144A4			
P5CD012A6	MOB6	plastic leadless module carrier package; 35 mm wide tape	SOT500-3
P5CD020A6			
P5CD040A6			
P5CD080A6			
P5CD144A6			

Table 4. Feature table

Product type	EEPROM [KB]	User ROM [KB]	Total RAM [KB]	CXRAM [KB]	FXRAM [KB]	Coprocessor			ISO 7816 IO pads	Interface option
						FameXE	DES	AES		
P5CD012	12	200	6	3.5	2.5	yes	yes	yes	3	dual interface
P5CC021	20	200	6	3.5	2.5	yes	yes	yes	3	contact
P5CD020	20	200	6	3.5	2.5	yes	yes	yes	3	dual interface
P5CC040	40	200	6	3.5	2.5	yes	yes	yes	3	contact
P5CD040	40	200	6	3.5	2.5	yes	yes	yes	3	dual interface
P5CC073	72	200	6	3.5	2.5	yes	yes	yes	3	contact
P5CN080	80	200	6	3.5	2.5	yes	yes	yes	3	contact + S^2C interface for NFC
P5CC080	80	200	6	3.5	2.5	yes	yes	yes	3	contact
P5CD080	80	200	6	3.5	2.5	yes	yes	yes	3	dual interface
P5CN144	144	200	6	3.5	2.5	yes	yes	yes	2	contact + S^2C interface for NFC
P5CC144	144	200	6	3.5	2.5	yes	yes	yes	3	contact
P5CD144	144	200	6	3.5	2.5	yes	yes	yes	3	dual interface

© NXP B.V. 2008. All rights reserved.

6. Functional diagram

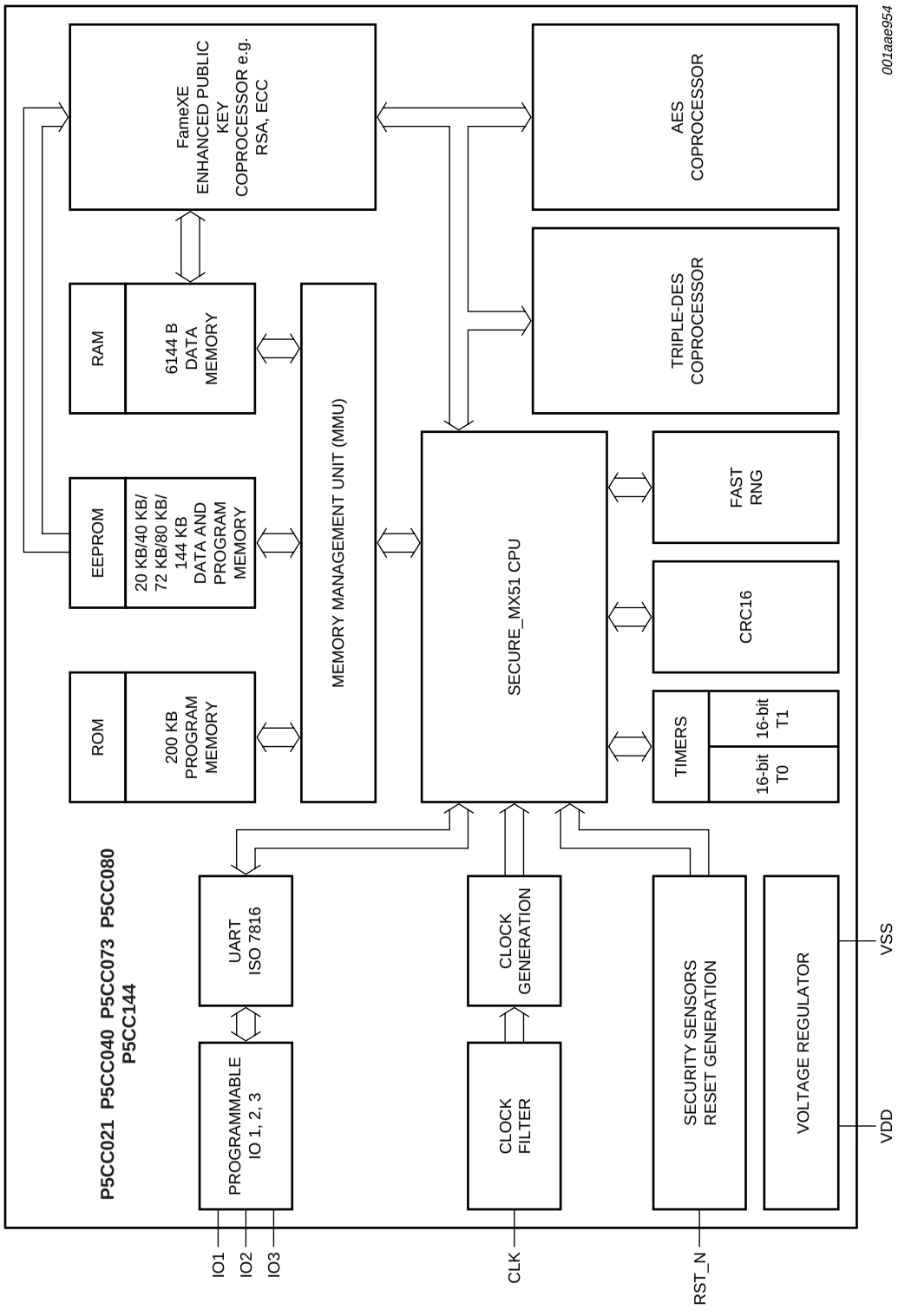

Fig 1. Functional diagram P5CC021/P5CC040/P5CC073/P5CC080/P5CC144

© NXP B.V. 2008. All rights reserved.

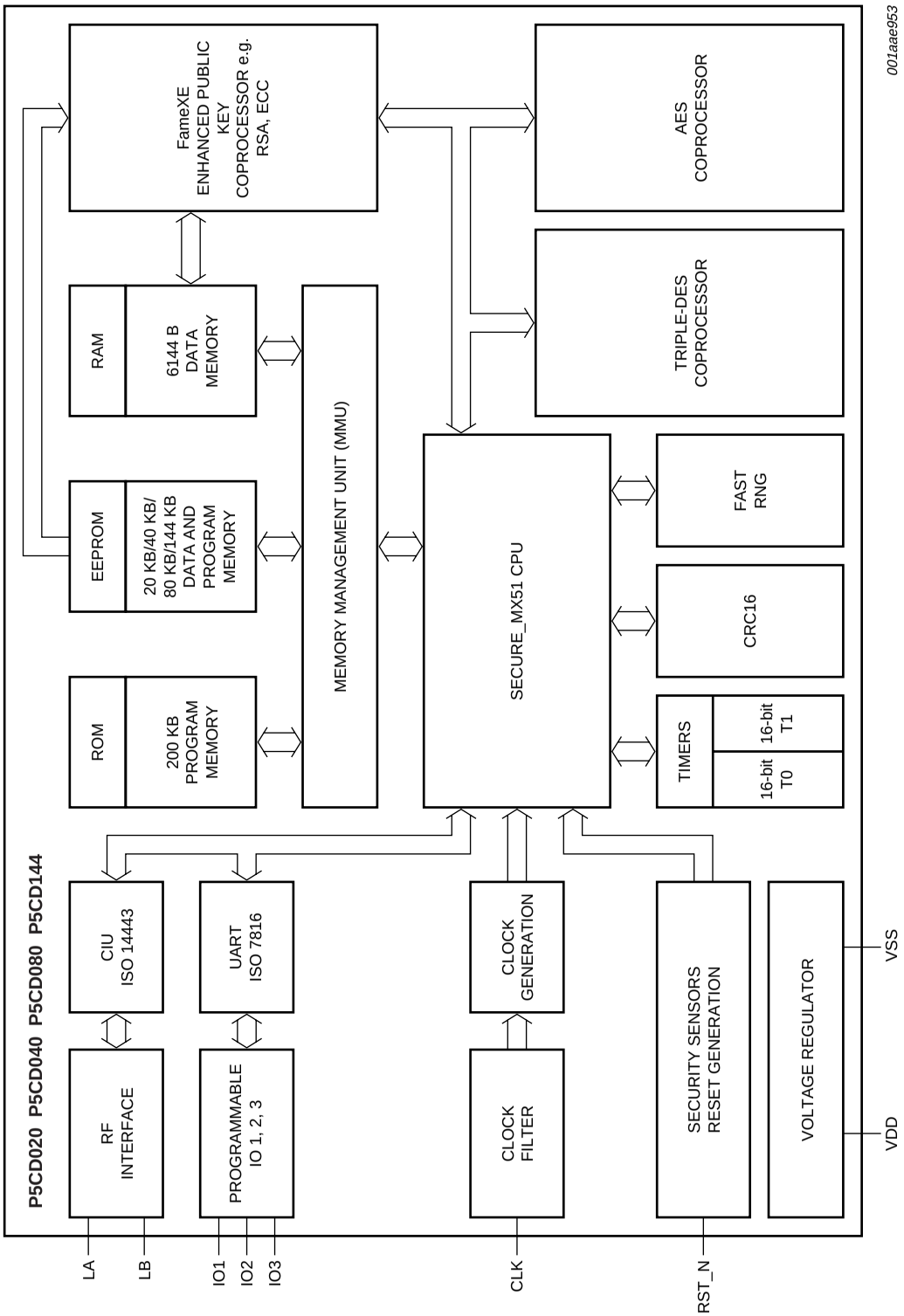

Fig 2. Functional diagram P5CD012/P5CD020/P5CD040/P5CD080/P5CD144

© NXP B.V. 2008. All rights reserved.

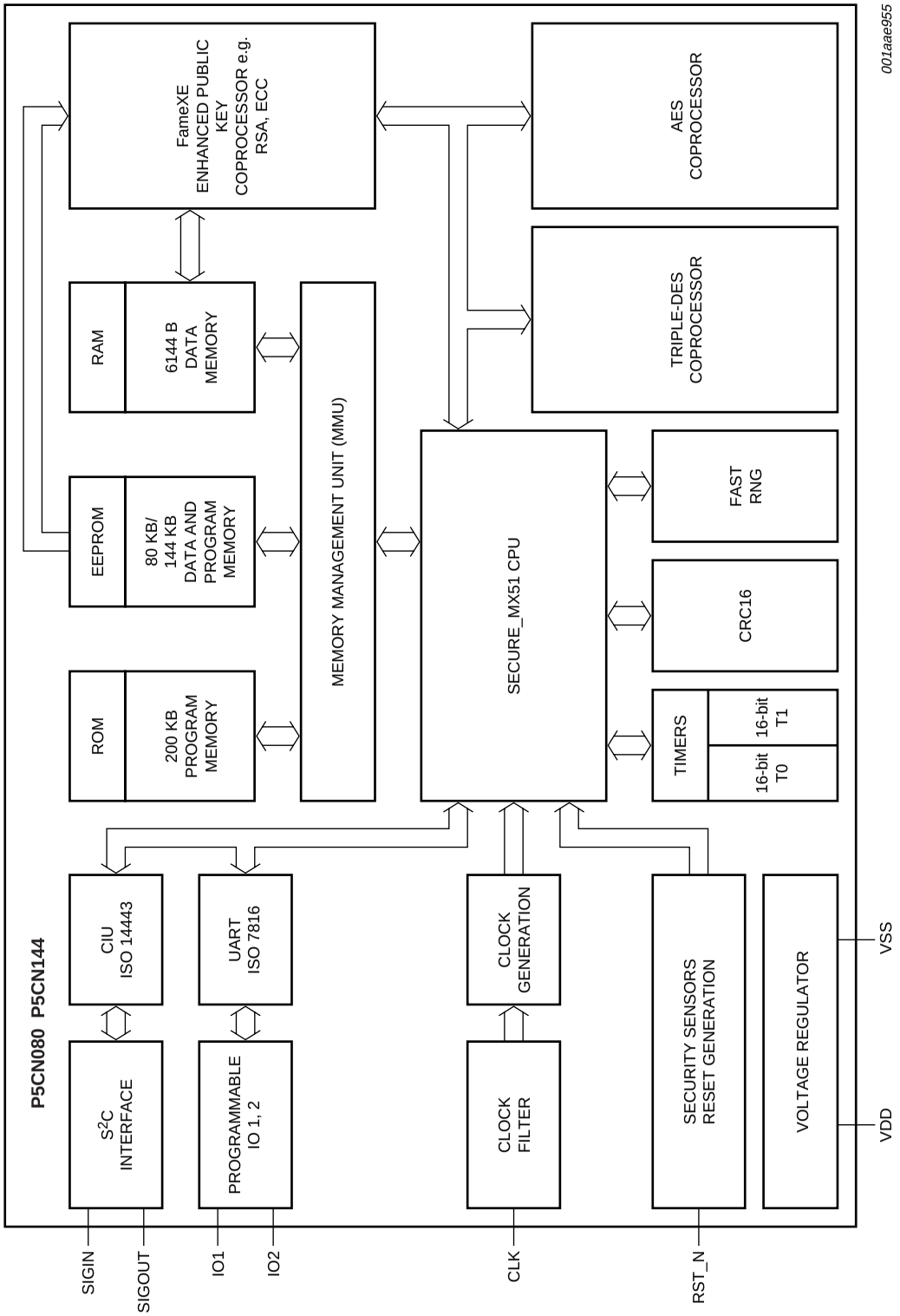

Fig 3. Functional diagram P5CN080/P5CN144

© NXP B.V. 2008. All rights reserved.

7. Limiting values

Table 5. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to VSS (ground = 0 V).

Symbol	Parameter	Conditions		Min	Max	Unit
V_{DD}	supply voltage			–0.5	+6.0	V
V_I	input voltage	any signal pad		–0.5	V_{DD} + 0.5	V
I_I	input current	pad IO1, IO2 or IO3		-	±15.0	mA
I_O	output current	pad IO1, IO2 or IO3		-	±15.0	mA
I_{lu}	latch-up current	V_I < 0 V or V_I > V_{DD}		-	±100	mA
V_{esd}	electrostatic discharge voltage	pads VDD, VSS, CLK, RST_N, IO1, IO2, IO3	[1]	-	±4.0	kV
		pads LA, LB	[1]	-	±2.0	kV
P_{tot}	total power dissipation		[2]	-	1	W
T_{stg}	storage temperature		[3]	-	-	

[1] MIL Standard 883-D method 3015; human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = –25 °C to +85 °C.

[2] Depending on appropriate thermal resistance of the package.

[3] Depending on delivery type, refer to NXP Semiconductors *General Specification for 8" Wafer* and to NXP Semiconductors Contact & Dual Interface Chip Card Module Specification.

8. Abbreviations

Table 6. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
ASK	Amplitude Shift Keying
CIU	Contactless Interface Unit
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
DES	Digital Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
GF	Galois Function
MAC	Message Authentication Code
MMU	Memory Management Unit

© NXP B.V. 2008. All rights reserved.

Table 6. Abbreviations *...continued*

Acronym	Description
NFC	Near Field Communication
OS	Operating System
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PRNG	Pseudo-Random Number Generator
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
S^2C	SigIn-SigOut-Connection
SFI	Single Fault Injection
SHA	Secure Hash Algorithm
SMD	Surface Mounted Device
SPA	Simple Power Analysis
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver/Transmitter

9. Revision history

Table 7. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
P5CX012_02X_40_73_80_144_FAM_SDS_3	20080124	Objective short data sheet		P5CX02X_40_73_80_144_FAM_SDS_2
Modifications:	• Type number P5CD012 added • Table 3 “Ordering information” corrected and new type number added • Figure 2 added			
P5CX02X_40_73_80_144_FAM_SDS_2	20070424	Objective short data sheet	-	P5CX02X_40_80_144_FAM_SDS_1
P5CX02X_40_80_144_FAM_SDS_1	20070216	Objective short data sheet	-	-

© NXP B.V. 2008. All rights reserved.

10. Legal information

10.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

10.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

10.3 Disclaimers

General — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

Terms and conditions of sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

10.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

MIFARE — is a trademark of NXP B.V.

FabKey — is a trademark of NXP B.V.

11. Contact information

For additional information, please visit: **http://www.nxp.com**

For sales office addresses, send an email to: **salesaddresses@nxp.com**

© NXP B.V. 2008. All rights reserved.

12. Tables

Table 1. Naming conventions 2
Table 2. Quick reference data 9
Table 3. Ordering information 9
Table 4. Feature table 10
Table 5. Limiting values 14
Table 6. Abbreviations 14
Table 7. Revision history 15

13. Figures

Fig 1. Functional diagram P5CC021/P5CC040/P5CC073/P5CC080/ P5CC144 11
Fig 2. Functional diagram P5CD012/P5CD020/P5CD040/P5CD080/ P5CD144 12
Fig 3. Functional diagram P5CN080/P5CN144 13

continued >>

© NXP B.V. 2008. All rights reserved.

14. Contents

1 General description 1
1.1 SmartMX family approach 1
1.2 SmartMX family properties 1
1.3 Naming conventions 2
1.4 Cryptographic hardware coprocessors 2
1.4.1 FameXE coprocessor 2
1.4.2 Triple-DES coprocessor 2
1.4.3 AES coprocessor 2
1.5 SmartMX interfaces 3
1.5.1 SmartMX contact interface 3
1.5.2 SmartMX contactless interface 3
1.5.3 SmartMX S^2C interface 3
1.6 Security features 4
1.7 Security evaluation and certificates 4
1.8 Optional crypto library 4
2 Features 5
2.1 Standard family features 5
2.2 Product specific family features 6
2.3 Security features 7
2.4 Design-in support 8
3 Applications 8
3.1 Application areas 8
4 Quick reference data 9
5 Ordering information 9
6 Functional diagram 11
7 Limiting values 14
8 Abbreviations 14
9 Revision history 15
10 Legal information 16
10.1 Data sheet status 16
10.2 Definitions 16
10.3 Disclaimers 16
10.4 Trademarks 16
11 Contact information 16
12 Tables 17
13 Figures 17
14 Contents 18

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2008. **All rights reserved.**

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 24 January 2008

Document identifier: P5CX012_02X_40_73_80_144_FAM_SDS_3

founded by

PHILIPS