P5Cx128/P5Cx145 family

Secure dual interface and contact PKI smart card controller

Rev. 3 — 1 August 2012
199530

Product short data sheet
COMPANY PUBLIC

1. General description

1.1 CMOS14 SmartMX family features overview

The CMOS14 SmartMX family members are a modular set of devices featuring:

- 128 KB to 144 KB EEPROM
- ROM memory size extended to 264 KB
- 7680 B RAM
- High-performance secure Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secure dual/triple-DES coprocessor
- Secure AES coprocessor
- Memory Management Unit (MMU)
- ISO/IEC 7816 contact interface
- Optional ISO/IEC 14443 A Contactless Interface Unit (CIU)
- 5-metal-layer 0.14 μm CMOS technology
- EEPROM with a minimum 500000 cycles endurance and a minimum of 25 years retention time
- Broad spectrum of delivery types
- Optional certified crypto library modules for RSA, ECC, DES, AES, SHA and PRNG
- Optional MIFARE 1 KB or 4 KB functionality

1.2 CMOS14 SmartMX family properties

The long-established approved Smart*MX* 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. In the P5Cx128/P5Cx145 product family, NXP's proven Secure_MX51 processor core has been further optimized over the P5Cx012/02x/040/073/080/144 family in 0.14 μm CMOS technology. Therefore, these products now offer improved CPU speed, leading to shorter overall transaction times. At the same time, the FameXE cryptography coprocessor has been optimized for even lower power operation, while keeping its performance at the same industry-leading level.

The availability of both contact interface and contactless or S^2C interface enable the easy implementation of native or open platform and multi-application operating systems in market segments like e.g. banking, E-passport, ID cards, Health Card, secure access, Java card as well as Trusted Platform Modules (TPM).

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 now further power-consumption reduced Fame*XE* 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 Fame*XE*, is only limited by the 2.5 KB size of the FXRAM. Fame*XE* runs up to 72 MHz, 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 widely used for 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 secure 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 to DES providing significantly improved security level. A secure crypto library element for AES is available.

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. Up to two additional I/Os 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 up to 848 kbit/s. A true anti-collision method (in accordance with ISO/IEC 14443-3) enables multiple cards to be handled simultaneously.

The optional MIFARE functionality provided in configurations B1 (MIFARE 1K implementation) and B4 (MIFARE 1K implementation) 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 customer code (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.

The MIFARE implementation on the SmartMX makes use of the approved true random number generator and thus is not susceptible to attacks based on the predictability of random numbers. This emulation is separated from the rest of the SmartMX by a firewall that is part of the Common Criteria evaluation.

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.

The input capacitance can be factory configured for either standard loop antennas or for smaller antennas (such as "ID1/2" antennas). This is accomplished by setting the device input capacitance to either the standard value or to a higher value.

1.5.3 SmartMX S^2C interface

The S^2C interface is intended for use with NXP Semiconductors NFC circuits (e.g. PN544) in order to build 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 and the S^2C interface.

The S^2C interface is connected to the internal ISO/IEC 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 front-end can be enabled. As the S^2C interface is connected to the CIU, the power to the P5CN145 must be supplied via the VDD and VSS pads in order to use the S^2C interface. The S^2C interface does not need any software adaptation compared to normal contactless operation.

When connected to the S^2C interface of a NFC front-end, the device is compatible with existing MIFARE reader infrastructure and the optional emulation modes of MIFARE 1K or MIFARE 4K 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.

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, in User mode the privileges are limited. User mode restrictions are configurable by software running in System mode.

Secure Fetch technology will significantly enhances the chip hardware security for a certain class of light attacks to the chip hardware. More specifically, Secure Fetch offers increased protection against attacks with higher spatial resolution and against both those with shorter and with longer light pulses; both with single and with multiple pulses. It protects both the device memory and code fetching operations from ROM, RAM and EEPROM, greatly increasing the probability that fault injection attacks are detected.

This unique security technology offers increased protection against future attack scenarios with light and laser sources, facilitating the development of highly secure software applications for customers.

The SmartMX security features are acknowledged by most of the NXP Semiconductors' customers for their outstanding properties. The countermeasures against light attacks are regarded as "best-in-class".

1.7 Security evaluation and certificates

Hardware security certification in accordance with CC EAL5+ is attained. Also, third-party approval such as 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 relevant information and documentation needed to execute subsequent composite evaluations of implemented applications.

1.8 Security licensing

In addition to the various intellectual properties regarding attack resistance of the NXP Semiconductors owned SmartMX family, NXP Semiconductors has obtained a patent license for SPA and DPA countermeasures from Cryptography Research Incorporated (CRI). This license covers both hardware and software countermeasures. It is important to customers that countermeasures within the operation system are covered under this license agreement with CRI. Further details can be obtained on request.

1.9 Optional crypto library

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

- 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)
- Common criteria CC EAL5+ certification available [except ECC over GF(2^n)] in accordance with BSI-PP-0035-2007 pprotection profile

2. Features and benefits

2.1 Standard family features

- EEPROM: choice of 128 KB or 144 KB
  - Data retention time: 25 years minimum
  - Endurance: 500000 cycles minimum
- ROM: 264 KB
- RAM: 7680 B
  - 256 B IRAM + 4.75 KB standard RAM usable for CPU
  - 2560 B FXRAM usable for FameXE
- Dedicated, Accelerated 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
- ISO/IEC 14443 contactless interface
- PKI coprocessor FameXE
- Support of major Public Key Cryptography (PKC) systems such as 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) with increased number of 8 cache segments
- 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
- Highly reliable EEPROM for both data storage and program execution
- Bytewise EEPROM programming and read access
- 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
- Contact configuration and serial interface in accordance with ISO/IEC 7816
- Power-saving Sleep (power-down) mode or Clockstop mode
- 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 62 MHz with synchronous operation
  - Internal clocking independent of externally applied frequency
- High speed 16-bit CRC engine in accordance with 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 (2.2 V to 5.5 V targeted for battery supplied applications)
- –25 °C to +85 °C ambient temperature
- Broad spectrum of delivery types:
  - Wafers
  - Modules
  - Packages
  - Inlays

2.2 Product specific family features

- P5CC128/P5CC145
  - ISO/IEC 7816 contact interface
  - Two additional IO ports IO2 and IO3 for optional proprietary use
- P5CD128/P5CD145
  - CIU fully compatible with ISO/IEC 14443A
    - 13.56 MHz operating frequency
    - fully supports the T=CL protocol according ISO/IEC 14443-4
    - factory configurable for higher input capacitance to match smaller loop antennas
    - supported data transfer rates: 106 kbit/s, 212 kbit/s, 424 kbit/s and 848 kbit/s
    - MIFARE reader infrastructure compatibility via optional MIFARE 1B or 4K emulation including built-in anticollision support
  - Two additional IO ports: IO2 and IO3 for optional proprietary use

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)
- Secure Fetch technology, protecting ROM, RAM and EEPROM code fetch operations
- 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 operating 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 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

2.4 Design-in support

- Approved development tool chain:
  - Keil PK51 development tool package including μVision3/dScope C51 simulator, additional specific hardware drivers including 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 in accordance with ISO/IEC 14443, part 3 and 4
  - T=1 communication in accordance with ISO/IEC 7816, part 3
  - EEPROM read/write routines

3. Applications

3.1 Application areas

- Banking
- ID cards
- Java cards
- Trusted Platform Modules
- USIM

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	-	5.5	V
		Class C: 1.8 V range		1.62	1.8	1.98	V
EEPROM characteristics							
t_{ret}	retention time (EEPROM data)	T_{amb} = +55 °C		25	-	-	years
$N_{endu(W)}$	write endurance	under all operating conditions		5×10^5	-	-	cycles

[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
P5CC128UA	FFC	8 inch wafer (sawn; 150 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	not applicable
P5CC145UA			
P5CD128UA			
P5CD145UA			
P5CN145UA			
P5CD128UE	FFC	8 inch wafer (sawn; 75 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	not applicable
P5CD145UE			
P5CC128HN	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 × 5 × 0.85 mm	SOT617-3
P5CC145HN			
P5CN145HN			
P5CD128A6	MOB6	contactless chip card module (super 35 mm tape format, module thickness 250 μm)	SOT500-3
P5CD145A6			
P5CC128XS	PCM1.1	contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5CC145XS			
P5CD128X0	PDM1.1	dual interface chip card module (super 35 mm tape format, 8-contact)	SOT658-3
P5CD145X0			
P5CD145X1	PDM1.1	dual interface chip card module (Plug-in type; super 35 mm tape format, 8-contact)	SOT658-3
P5CD128Ai	Inlay	chip module embedded in custom inlay; inquire at NXP sales for detail; i = inlay type, can be any letter	not applicable
P5CD145Ai			

Table 4. Feature table

Product type	EEPROM [KB]	User ROM [KB]	Total RAM [KB]	CXRAM [KB]	FXRAM [KB]	Coprocessor			ISO/IEC 7816 IO pads	Interface option
						Fame*XE*	DES	AES		
P5CC128	128	264	7.5	5	2.5	yes	yes	yes	3	contact
P5CD128	128	264	7.5	5	2.5	yes	yes	yes	3	dual interface
P5CC145	144	264	7.5	5	2.5	yes	yes	yes	3	contact
P5CD145	144	264	7.5	5	2.5	yes	yes	yes	3	dual interface
P5CN145	144	264	7.5	5	2.5	yes	yes	yes	3	contact + S^2C interface for NFC

6. Functional diagram

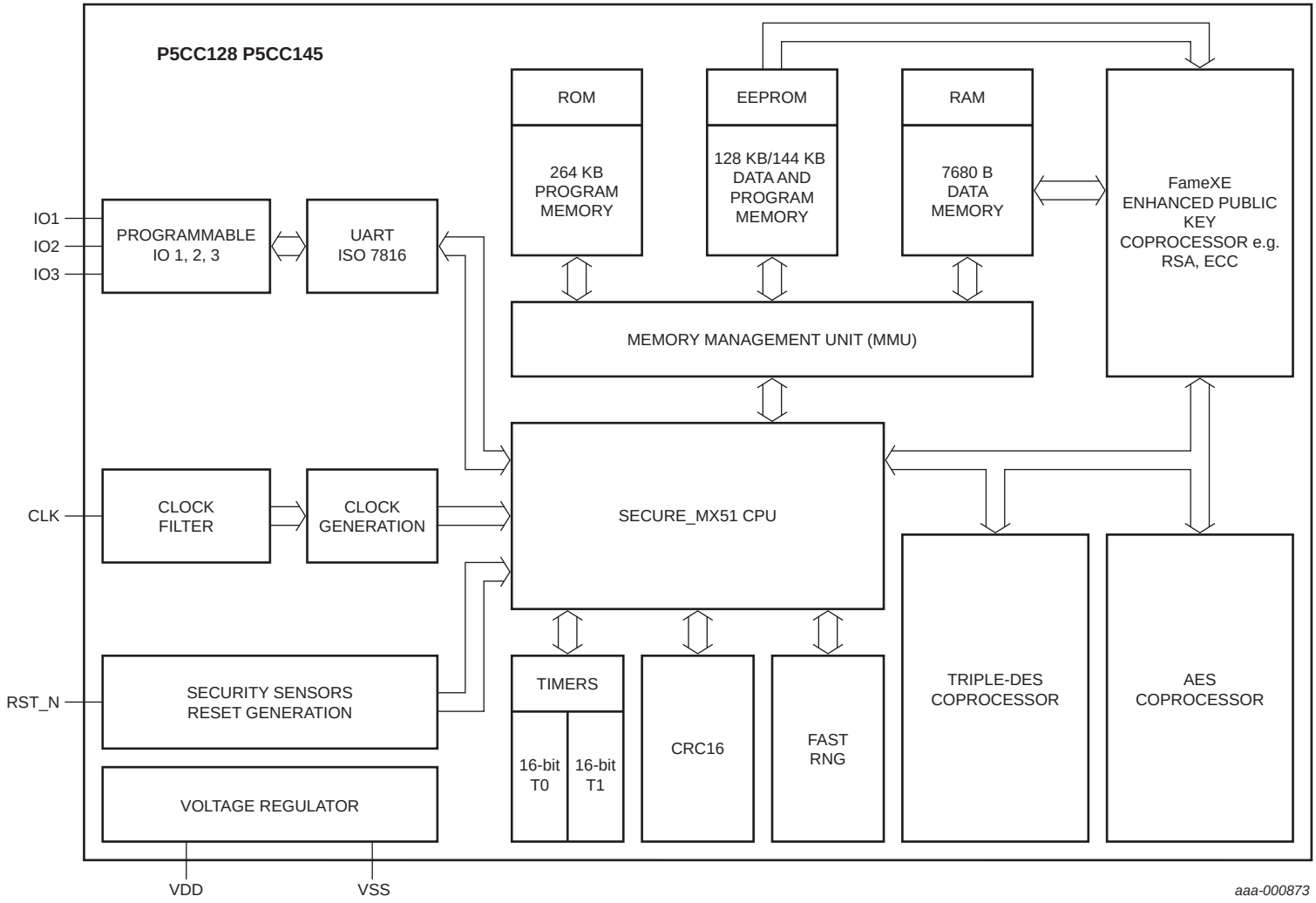

Fig 1. Functional diagram P5CC128/P5CC145

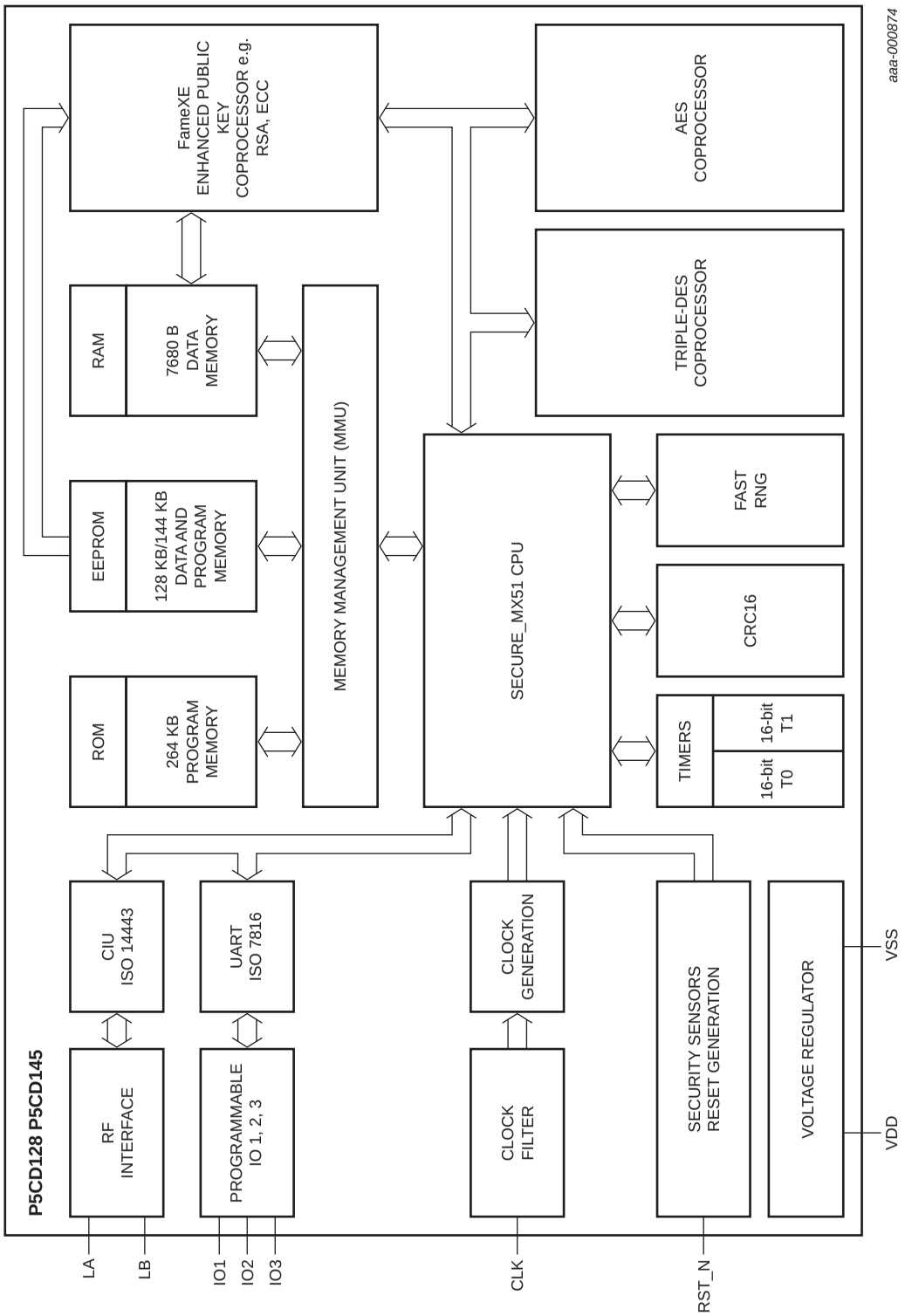

Fig 2. Functional diagram P5CD128/P5CD145

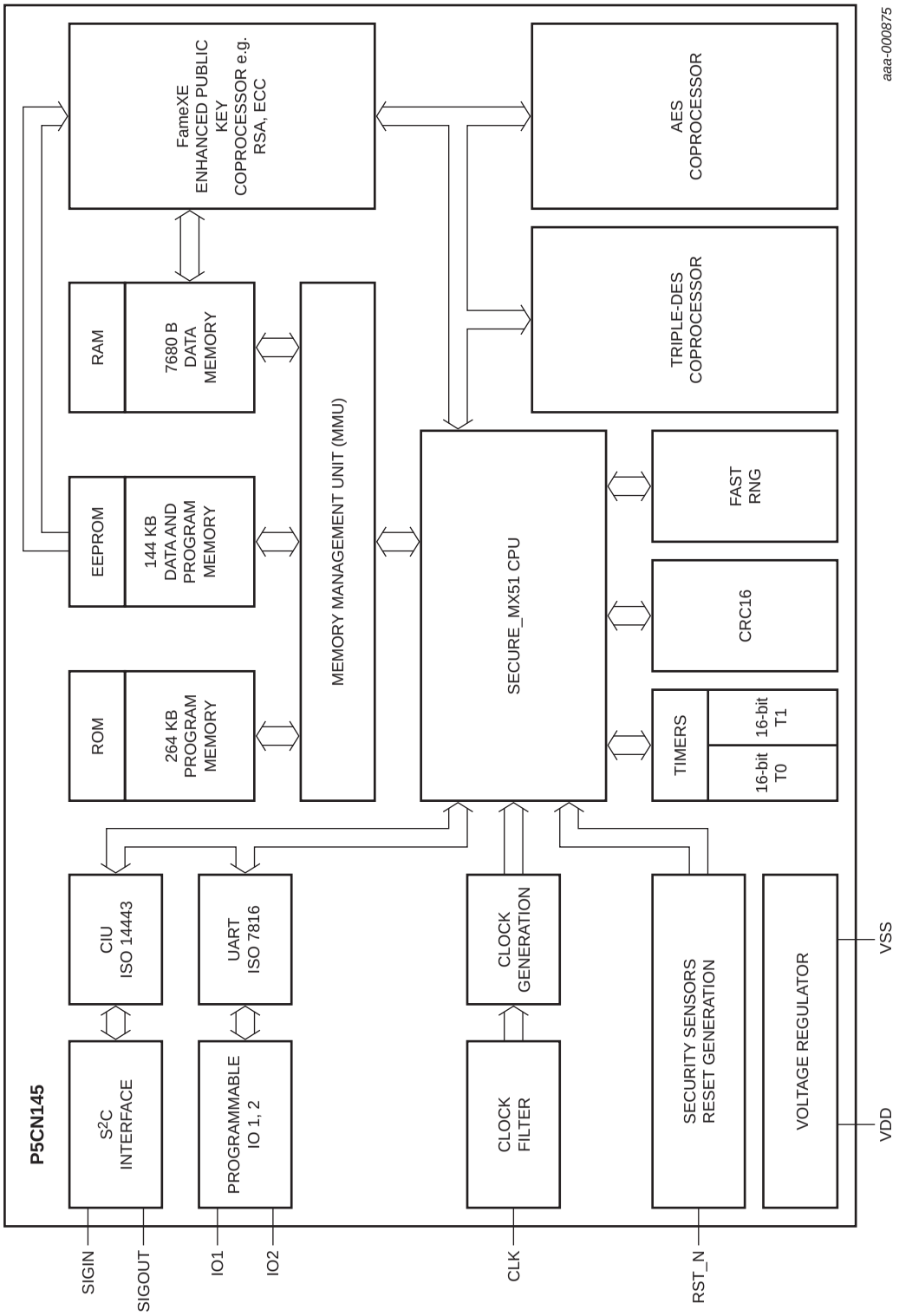

Fig 3. Functional diagram P5CN145

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]	-	-	°C

[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" Wafers* 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
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
I/O	Input/Output
MAC	Message Authentication Code
MMU	Memory Management Unit
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
P5Cx128_P5Cx145_FAM_SDS v.3	20120801	Product short data sheet	-	-
	• Initial version			

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.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

10.3 Disclaimers

Limited warranty and liability — 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

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 life support, life-critical or safety-critical systems or 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 and its suppliers accept 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.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial 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, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

10.4 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

10.5 Trademarks

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

FabKey — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

SmartMX — is a trademark of NXP B.V.

11. Contact information

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

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

12. Tables

13. Figures

14. Contents

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

Date of release: 1 August 2012
199530

Document identifier: P5Cx125_P5Cx145_FAM_SDS