P5Cx009/P5Cx072

Secure triple, dual and contact PKI smart card controller

Rev. 01 — 5 February 2010
181610

Product short data sheet
PUBLIC

1. General description

1.1 SmartMX CMOS18 features

The CMOS18 SmartMX family members are a modular set of devices featuring:

- 10 KB to 72 KB EEPROM
- 96 KB to 160 KB user ROM
- 4608 B RAM
- High-performance secure Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secure dual/triple-DES coprocessor
- Secured AES coprocessor (P5CC072 and P5CT072 only)
- Memory Management Unit (MMU)
- ISO/IEC 7816 contact interface
- 5-metal layer 0.18 μm CMOS technology
- EEPROM with up to 500 000 cycles endurance and a minimum of 20 years retention time
- Broad spectrum of delivery types
- Optional certified crypto library modules for RSA, DES, AES and ECC

1.2 CMOS18 SmartMX family properties

The long-established CMOS18 SmartMX family features an 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 SmartMX platform manufactured in CMOS 0.18 μm 5-metal layer technology offers many advantages in terms of security features, memory resources, crypto-coprocessor calculation speed for RSA/ECC as well as availability of secure hardware support for 2-key and 3-key Data Encryption Standard (DES) and Advanced Encryption Standard (AES) operations.

The contact interface availability, the optional contactless interface and the optional Universal Serial Bus (USB) 2.0 LS interface enable the easy implementation of native or open platform and multi-application operating systems in market segments such as banking, ID cards, health cards, conditional access (pay TV), Java cards, 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 S = triple-DES coprocessor
y	Interface options: C = contact interface - ISO/IEC 7816
zzz	Amount of non-volatile memory in KB (EEPROM and optional Flash), increasing count for further product options
Examples:	
xy = SD	Security controller, ISO/IEC 7816 contact and ISO/IEC 14443 contactless interface/ UARTs
xy = SC	Security controller, ISO/IEC 7816 contact interface/UART
xy = CU	PKI controller, ISO/IEC 7816 and USB 2.0 (LS) contact interface/UARTs
xy = CT	PKI controller, ISO/IEC 7816 and USB 2.0 (LS) contact and ISO/IEC 14443 contactless interface/UARTs
xy = CD	PKI controller, ISO/IEC 7816 contact and ISO/IEC 14443 contactless interface
xy = CC	PKI controller, ISO/IEC 7816 contact interface/UARTs

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 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 cryptography solutions. A secure 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 a 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. An additional IO is available for proprietary use.

1.5.2 SmartMX USB 2.0 (Low Speed) interface

SmartMX offers a fully integrated USB interface based on the USB 2.0 Low Speed (LS) standard SmartMX, making SmartMX-based IC cards “Plug and Play” compatible with the whole PC world without the use of complex reader devices or extra external components. The USB interface uses the ISO contact module and works via a 4-wire connection to any PC supporting “hot Plug and Play”. The card automatically recognizes an ISO or USB environment and works with either an external frequency of 6 MHz or an internally generated clock. The use of USB interfaces on smart cards is defined within ISO/IEC 7816-12.

1.5.3 SmartMX contactless interface

The optional contactless interface is fully compatible with ISO/IEC 14443 type 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 (in accordance with 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 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 user Operating System (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.

1.6 Security features

SmartMX incorporates a range of both inherent and OS-controlled security features as a countermeasure against all types of attack. NXP Semiconductors apply their extensive knowledge of chip security, combined with handshaking circuit technology, 5-metal layer 0.18 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.

The SmartMX security features are acknowledged as having outstanding properties by most NXP Semiconductors' customers. 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 with the 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 operating system are covered under this license agreement with CRI. Further details can be obtained on request.

1.9 P5Cx009 and P5Cx072 device description

The device is a secure PKI smart card controller of the SmartMX platform featuring 96 KB to 160 KB of ROM, 4608 B of RAM and 10 KB to 72 KB of EEPROM, which can be used as data memory and as program memory. The device also has a USB 2.0 (LS) interface which is the reason why the device is called a "Secure triple interface smart card controller". The non-volatile memory consists of high reliability memory cells to guarantee data integrity, which is especially important when the EEPROM is used as program memory.

Operated both in Contact mode (ISO/IEC 7816) and in Contactless mode (ISO/IEC 14443) the user defines the final function of the chip with his Chip Operating System (COS). This allows the same level of security, functionality and flexibility for the contact interface as well as for the contactless interface.

The field proven RF interface technology (in accordance with ISO/IEC 14443-2) is well established in all products of the MIFARE interface platform and provides reliable communication and secure processing, even in electro-magnetically harsh environments such as buses or train stations. Compatibility with existing MIFARE reader infrastructure and the optional emulation modes of MIFARE 1 KB or MIFARE 4 KB emulation enable fast system integration and backward compatibility of MIFARE.

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

The on-chip hardware is software controlled via Special Function Registers (SFRs). Their function and usage is described in the respective sections of the product data sheet as the SFRs are correlated to the activities of the CPU, Interrupt, IO, EEPROM, Timers, etc.

The device has two power-saving modes for reduced activity: the Idle, and the Sleep or Clockstop mode. Both modes are activated by software.

The device operates either with a single 1.8 V, 3 V or 5 V (voltage Class C, B and A) power supply at a maximum external clock frequency of 10 MHz supplied via the contact pads (internally up to 31 MHz) or with a power supply generated from the RF-field emitted by an RF-reader applied to the antenna connections on pads LA and LB.

2. Features and benefits

2.1 Standard family features

- EEPROM: 10 KB to 72 KB
  - Data retention time: 20 years minimum
  - Endurance: up to 500 000 cycles per byte
- ROM: 96 KB to 160 KB
- RAM: 4608 B
  - 256 B IRAM + 3 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 0.18 μm CMOS technology
  - Operating in Contact mode
  - 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
- High speed triple-DES coprocessor (64-bit parallel processing DES engine)
  - Two or three keys loadable
  - Triple-DES calculation time < 40 μs

- High speed AES coprocessor (128-bit parallel processing AES engine, P5CC072 and P5CT072 only)
- USB 2.0 (LS) contact interface in accordance with ISO/IEC 7816-12
- 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
- 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
- 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 or Clockstop mode
- Wake-up from Sleep or Clockstop mode by RESET or external interrupt
- Contact configuration and serial interface in accordance with ISO/IEC 7816: GND, VCC, CLK, RST, I/O
- Up to three IO ports, IO3 for proprietary use
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalization up to 1 Mbit/s
- 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
- Externally or internally generated configurable CPU clock
- 1 MHz to 10 MHz operating external clock frequency range
  - 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 operating voltage range for Class C, B and A
- Optional extended Class B operation mode (2.2 V to 3.3 V targeted for battery supplied applications)
- −25 °C to +85 °C ambient temperature
- Broad spectrum of delivery types
  - Wafers
  - Modules
  - Tiny SMD packages

2.2 Product specific family features

- P5CC009
  - High-speed AES coprocessor (128-bit parallel processing AES engine)
  - One additional IO port: IO1
- P5CD009
  - CIU fully compatible with ISO/IEC 14443A
    - 13.56 MHz operating frequency
    - fully supports the T=CL protocol in accordance with ISO/IEC 14443-4
    - supported data transfer rates: 106 kbit/s, 212 kbit/s, 424 kbit/s and 848 kbit/s
    - MIFARE reader infrastructure compatibility via optional MIFARE 1 KB or 4 KB implementation including built-in anticollision support
  - One additional IO port: IO1
- P5CC072
  - High-speed AES coprocessor (128-bit parallel processing AES engine)
  - Two additional IO ports: IO2 and IO3 for full-duplex serial data communication
- P5CD072
  - CIU fully compatible with ISO/IEC 14443A
    - 13.56 MHz operating frequency
    - fully supports the T=CL protocol in accordance with ISO/IEC 14443-4
    - supported data transfer rates: 106 kbit/s, 212 kbit/s, 424 kbit/s and 848 kbit/s
    - MIFARE reader infrastructure compatibility via optional MIFARE 1 KB or 4 KB implementation including built-in anticollision support
  - Two additional IO ports: IO2 and IO3 for full-duplex serial data communication
- P5CT072
  - High-speed AES coprocessor (128-bit parallel processing AES engine)
  - USB 2.0 (LS) contact interface in accordance with ISO/IEC 7816-12
  - CIU fully compatible with ISO/IEC 14443A
    - 13.56 MHz operating frequency
    - fully supports the T=CL protocol in accordance with ISO/IEC 14443-4
    - supported data transfer rates: 106 kbit/s, 212 kbit/s, 424 kbit/s and 848 kbit/s
    - MIFARE reader infrastructure compatibility via optional MIFARE 1 KB or 4 KB implementation including built-in anticollision support
  - Two additional IO ports IO2 and IO3 for full-duplex serial data communication

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 (including 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 system support 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 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 EEPROM for customer-defined security FabKey, featuring batch-, wafer- or die-individual security data, including 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.
- Tutorial C source libraries for:
  - contactless communication in accordance with ISO/IEC 14443, Part 3 and 4
  - T=1 communication in accordance with ISO/IEC 7816, Part 3
  - USB 2.0 (LS) basic library support
  - EEPROM Read/Write routines

3. Applications

3.1 Application areas

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

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
EEPROM							
t_{ret}	retention time	T_{amb} = +55 °C		20	-	-	years
$N_{endu(W)}$	write endurance	under all operating conditions		-	5×10^5	-	cycles

[1] In extended Class B (Class BE) operation mode (targeted for battery powered applications), Class C is not supported.

5. Ordering information

Table 3. Ordering information

Type number	Package		
	Name	Description	Version
P5CD009EV4	MOB4	contactless chip card module (super 35 mm tape format, module thickness 320 μm)	SOT500-2
P5CD072EV4			
P5CC009EV0	PCM1.1	contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5CC072EV0			
P5CC009EVD	Pd-PCM1.1	palladium plated contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5CC072EVD			
P5CD009EV0	PDM1.1	dual interface chip card module (super 35 mm tape format, 8-contact)	SOT658-3
P5CD009EV1	PDM1.1	dual interface chip card module (plug-in type; super 35 mm tape format, 8-contact)	SOT658-3
P5CD072EV1			
P5CD009EVD	Pd-PDM1.1	palladium plated dual interface chip card module (super 35 mm tape format, 8-contact)	SOT658-3
P5CD072EVD			

Table 3. Ordering information *…continued*

Type number	Package		
	Name	Description	Version
P5CD009ETS	SSOP20	plastic shrink small outline package; 20 leads; body width 4.4 mm	SOT266-1
P5CC072ETS			
P5CT072ETS			

Table 4. Feature table

Product type	EEPROM [KB]	User ROM [KB]	Total RAM [KB]	CXRAM [KB]	FXRAM [KB]	Coprocessor			USB	ISO/IEC 7816 IO pads	Interface option
						FameXE	DES	AES			
P5CC009	10	96	4	3	1.25	yes	yes	no	no	1	contact
P5CD009	12	96	4	3	1.25	yes	yes	no	no	1	dual
P5CC072	72	160	4	3	1.25	yes	yes	yes	no	3	contact interface
P5CD072	72	160	4	3	1.25	yes	yes	no	no	3	dual interface
P5CT072	72	160	4	3	1.25	yes	yes	yes	yes	3	dual interface

6. Functional diagram

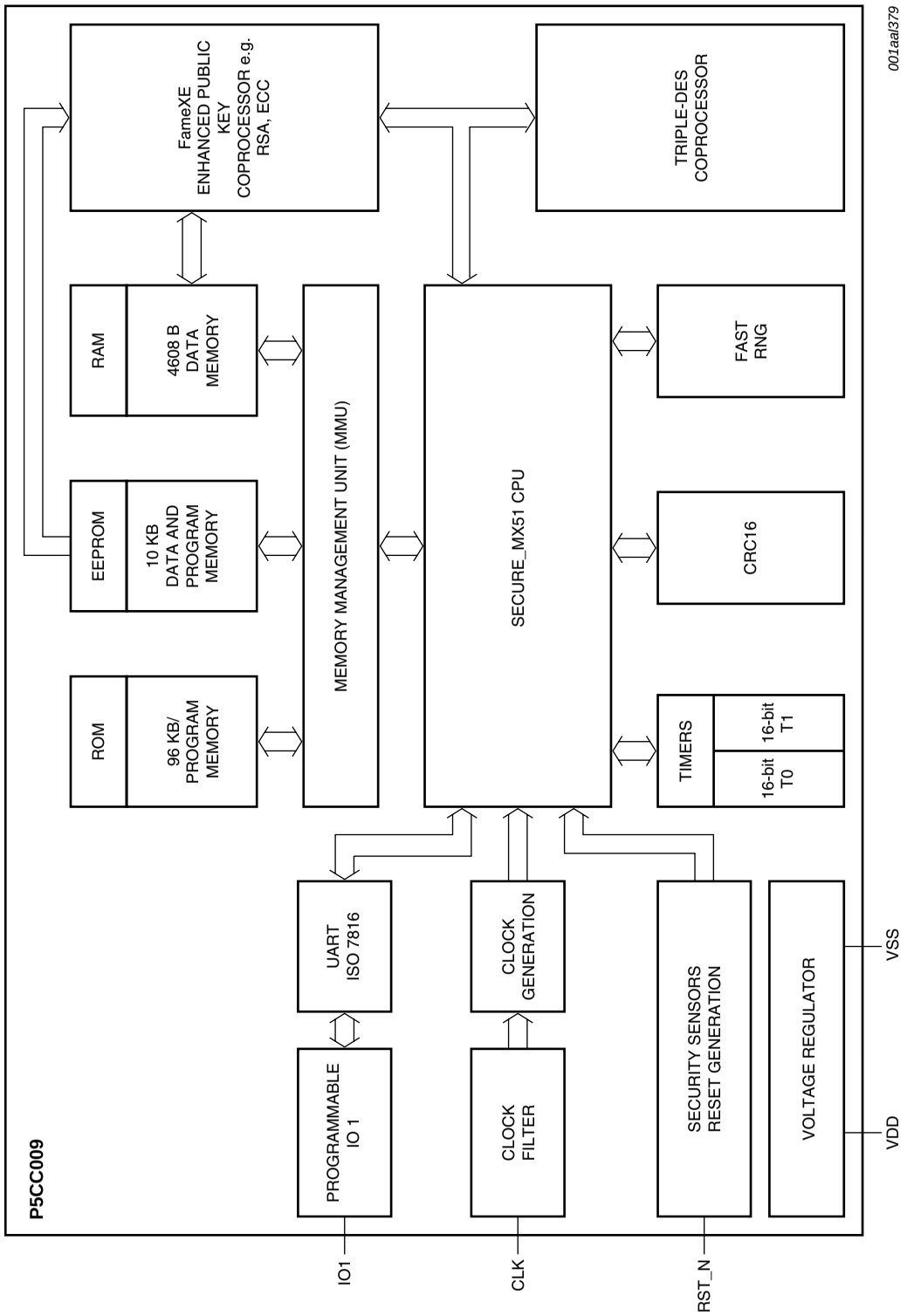

Fig 1. Functional diagram P5CC009

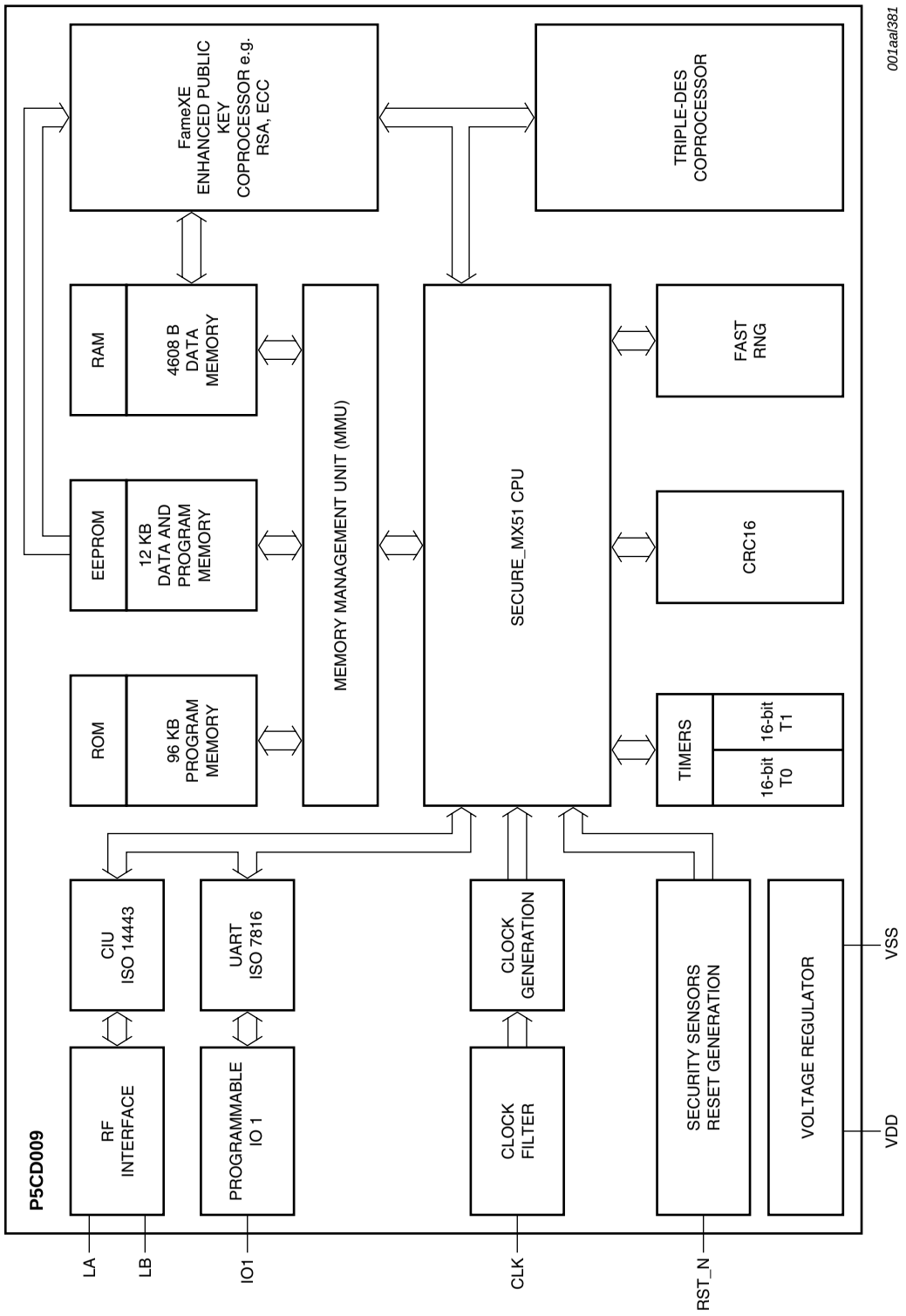

Fig 2. Functional diagram P5CD009

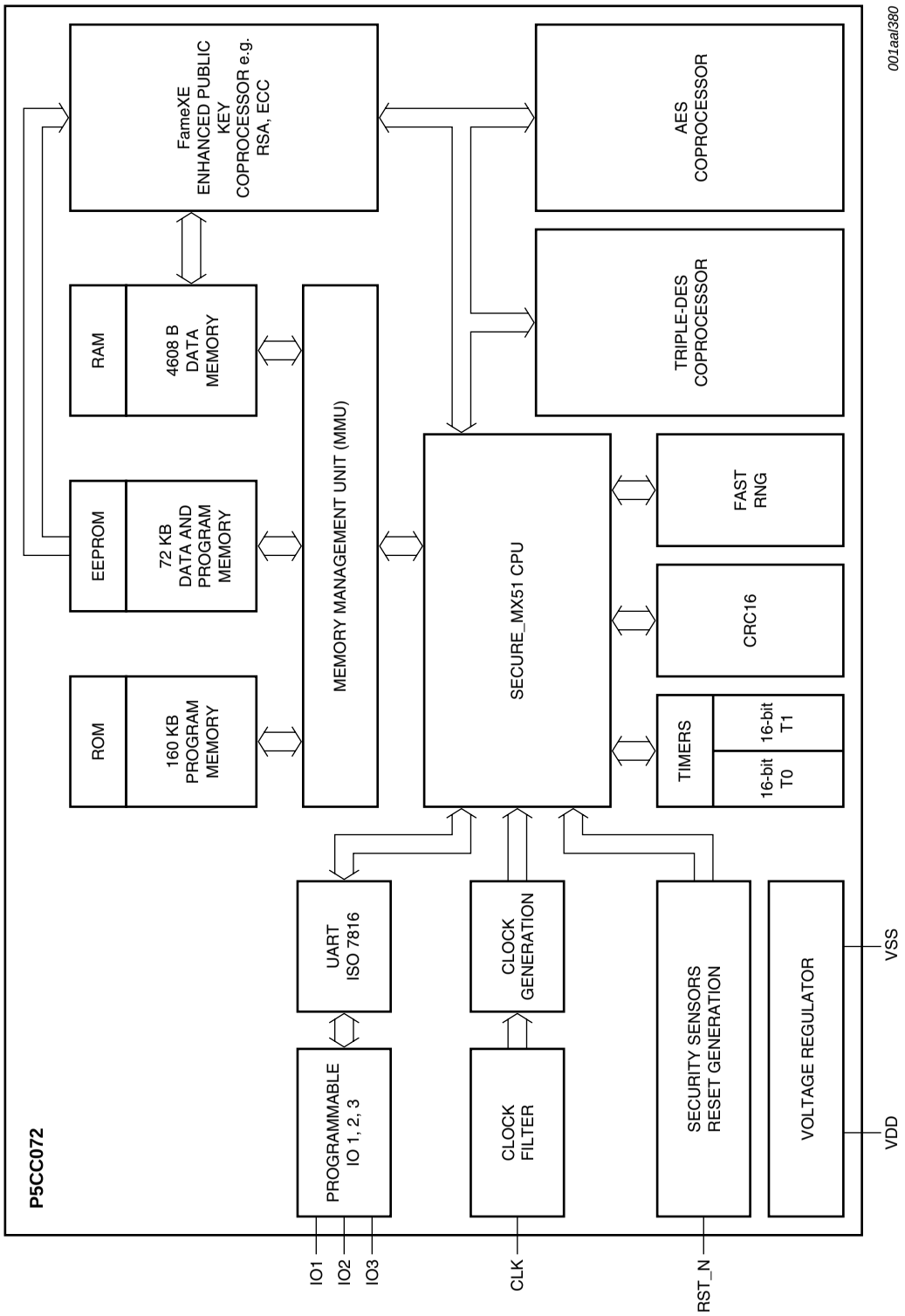

Fig 3. Functional diagram P5CC072

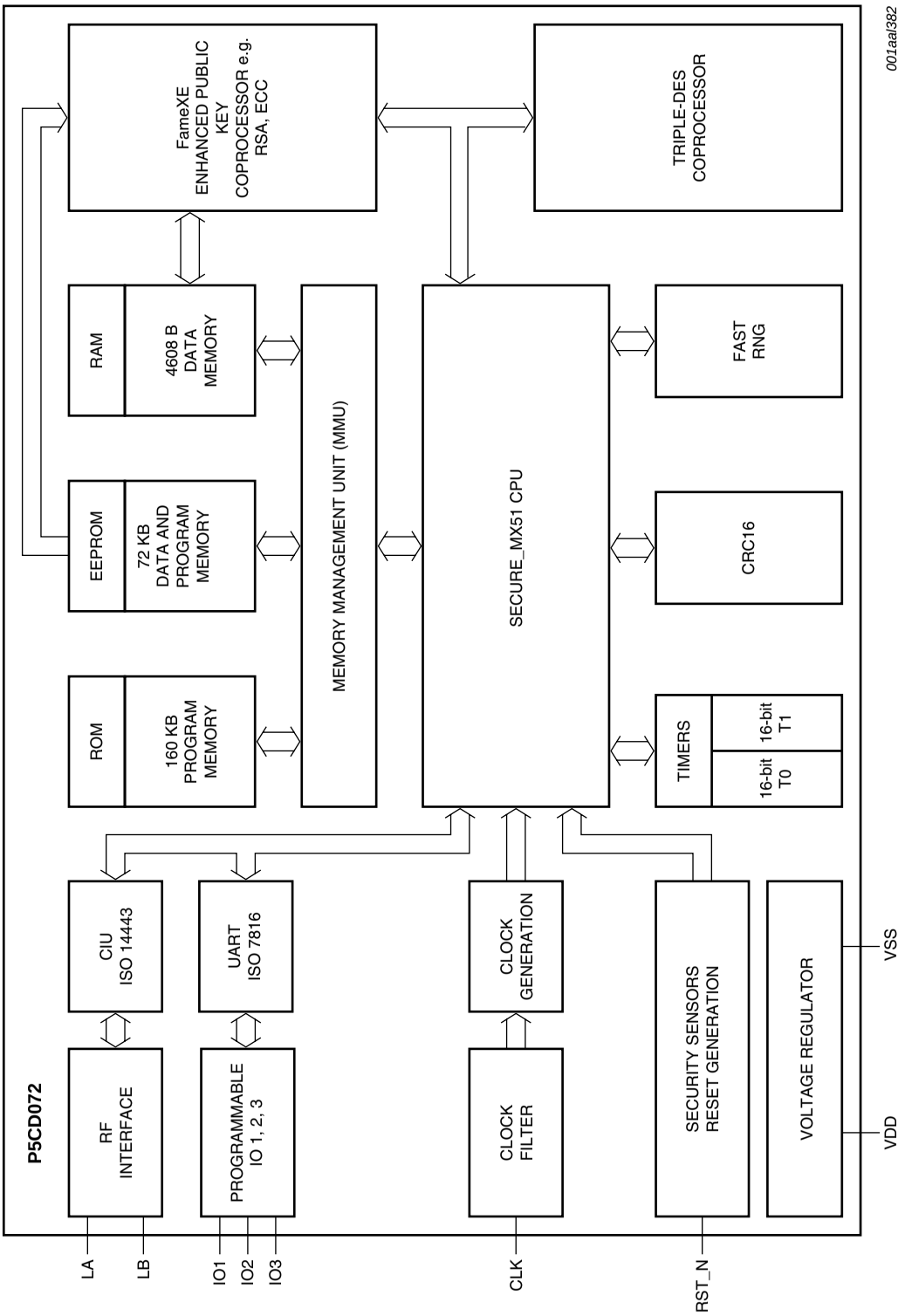

Fig 4. Functional diagram P5CD072

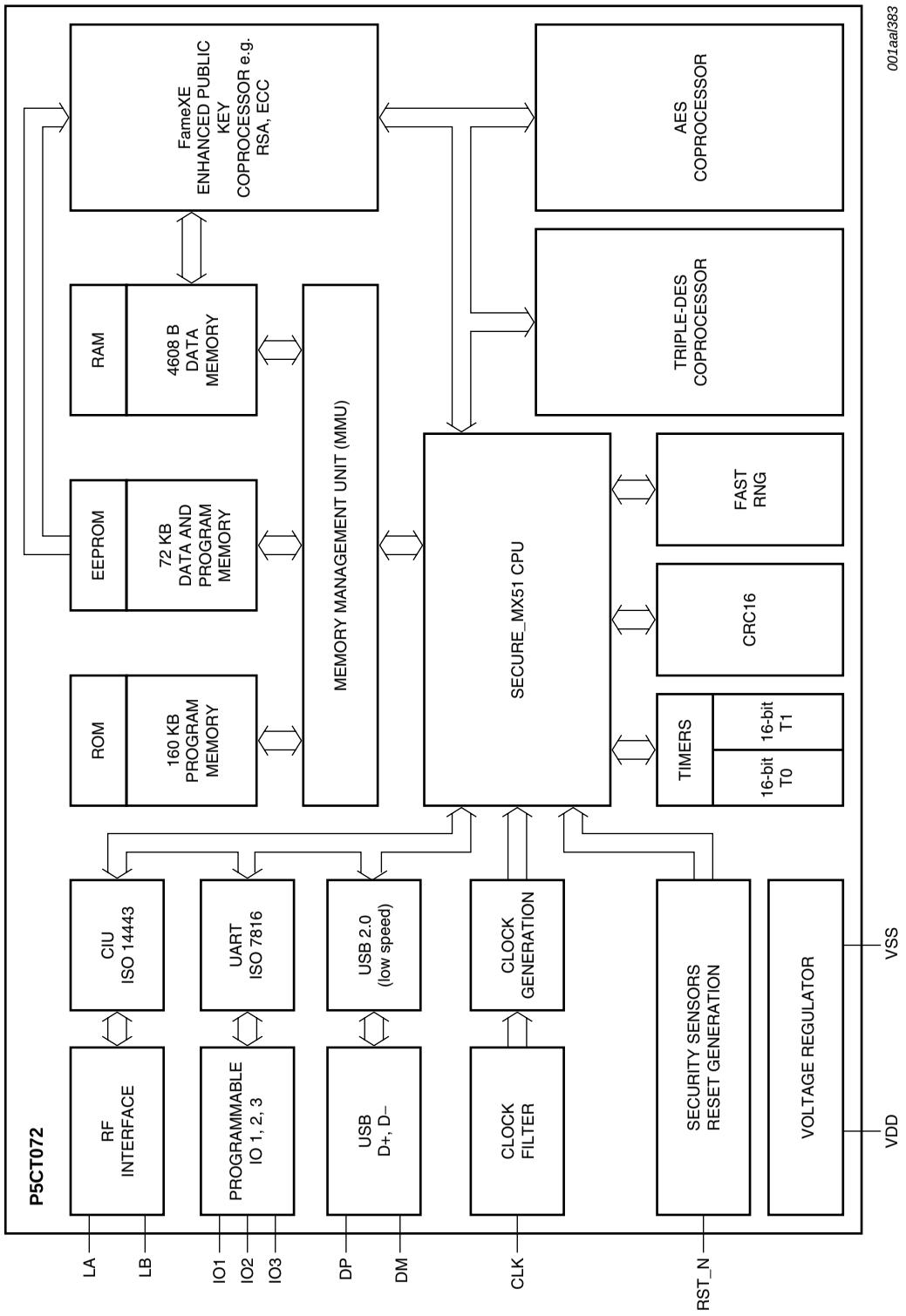

Fig 5. Functional diagram P5CT072

7. Limiting values

Table 5. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to V_{SS} (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}	[1]	-	±100	mA
V_{ESD}	electrostatic discharge voltage	pads VDD, VSS, CLK, RST_N, IO1, IO2, IO3, DP, DM	[2]		±4.0	kV
		pads VDD, VSS, CLK, RST_N, IO1, IO2, IO3, DP, DM with SSOP20 (SOT 266-1) package			±3.0	kV
		pads LA, LB	[2]		±2.0	kV
P_{tot}	total power dissipation		[3]	-	1	W
T_{stg}	storage temperature		[4]	-	-	

[1] USB pads DM and DP performed at maximum rating (6.0 V).

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

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

[4] 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
AIS	Automatic Identification System
CC	Common Criteria
CRC	Cyclic Redundancy Check
DES	Digital Encryption Standard
DPA	Differential Power Analysis
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-Only Memory
GF	Galois Function
IO	Input Output
IRAM	Intelligent Random Access Memory
MAC	Message Authentication Code

Table 6. Abbreviations *...continued*

Acronym	Description
MMU	Memory Management Unit
OS	Operating System
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SFI	Single Fault Injection
SMD	Surface Mounted Device
SPA	Simple Power Analysis
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus

9. Revision history

Table 7. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
P5Cx009_P5Cx072_FAM_SDS_1	20100205	Product short data sheet PUBLIC	-	-

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.

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 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.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on a weakness or default in the customer application/use or the application/use of customer's third party customer(s) (hereinafter both referred to as "Application"). It is customer's sole responsibility to check whether the NXP Semiconductors product is suitable and fit for the Application planned. Customer has to do all necessary testing for the Application in order to avoid a default of the Application and the product. NXP Semiconductors 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 national 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 the data sheet of an NXP Semiconductors product expressly states that the 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

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.

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: 5 February 2010
181610