P5xC012/020/024/037/052 family

Secure contact PKI smart card controller

Rev. 3.1 — 5 January 2010
138531

Product short data sheet
PUBLIC

1. General description

1.1 SmartMX family approach

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

- 12 KB to 52 KB EEPROM
- 160 KB to 264 KB user ROM
- 3584 B or 6144 B RAM
- High-performance secured Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secured dual/triple-DES coprocessor
- Memory Management Unit (MMU)
- ISO/IEC 7816 contact interface
- 5-metal-layer 0.14 μm CMOS technology
- EEPROM with minimum 500 000 cycles endurance and minimum 25 years retention time
- Broad spectrum of delivery types
- Optional certified crypto library modules for RSA and ECC

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 Data Encryption Standard (DES) operations.

The contact interface availability enables the easy implementation of native or open platform and multi-application operating systems in market segments such as banking, E-passport, ID card, secure access, Java card as well as Trusted Platform Modules (TPM) within extremely tiny SMD packages.

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, 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 EAL5+ CC 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.

1.5 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.

© NXP B.V. 2010. 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 in User mode the privileges are limited. User mode restrictions are configurable by software running in System mode.

The SmartMX security features are acknowledged by most of the NXP Semiconductors customers for their outstanding properties. The counter measures against light attacks are regarded as “best-in-class”.

1.7 Security evaluation and certificates

The reached target of the certification is CC EAL5+. Also third party approvals 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

Above and beyond the various intellectual properties regarding attack resistance of the SmartMX family owned by NXP Semiconductors, NXP Semiconductors has obtained a patent license for SPA and DPA countermeasures from Cryptography Research, Inc. (CRI). This license covers both hardware and software countermeasures. It is of special importance for the 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 will offer for all family types an optional crypto library:

- Various algorithms
  - 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-Hellmann key exchange for keys up to 544 bits
  - ECC over GF(p) key generation

© NXP B.V. 2010. All rights reserved.

  - ECC over GF(2^n) signature generation and verification (ECDSA) and Diffie-Hellmann 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
- Latest built-in security features to avoid power (SPA/DPA), timing and fault attacks (DFA)
- Common criteria EAL5+ certification available (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, 24 KB, 36 KB or 52 KB
  - Data retention time: 25 years minimum
  - Endurance: 500000 cycles minimum
- ROM: 160 KB, 200 KB or 264 KB (depending on EEPROM size)
- RAM for P5CC012/020/024/037/052: 6144 B
  - 256 B IRAM + 3.25 KB Standard RAM usable for CPU
  - 2560 B FXRAM usable for FameXE
- RAM for P5SC020: 3584 B
  - 256 B IRAM + 3.25 KB Standard RAM usable for CPU
- Dedicated Secure_MX51 Smart Card CPU (Memory eXtended/enhanced 80C51)
  - 5-metal layer 0.14 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
- 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

© NXP B.V. 2010. All rights reserved.

- High 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 according to ISO/IEC 7816: GND, VCC, CLK, RST, I/O
- One additional IO port 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 polynom 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 Security features

- Enhanced security sensors
  - Low/high clock frequency sensor
  - Low/high temperature sensor
  - Low/high supply voltage sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors (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

© NXP B.V. 2010. All rights reserved.

- Power-up/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, 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

2.3 Design-in support

- Approved development tool chain
  - Keil PK51 development tool package inclusive μVision3/dScope C51 simulator, additional specific hardware drivers inclusive 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 card interface board. Code coverage and performance measurement software tools for real time software testing.
- Tutorial C source libraries for
  - EEPROM read/write routines
  - T=1 communication according to ISO/IEC 7816, Part 3

3. Applications

3.1 Application areas

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

© NXP B.V. 2010. 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
t_{EER}	EEPROM data retention time	T_{amb} = +55 °C		25	-	-	years
N_{EEC}	EEPROM endurance (number of programming cycles)	under all operating conditions		5×10^5	-	-	cycles

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

5. Ordering information

Table 3. Ordering information

Type number	Package		
	Name	Description	Version
P5CC012HN	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 × 5 × 0.85 mm	SOT617-1
P5CC020HN			
P5SC020HN			
P5CC024HN			
P5CC037HN			
P5CC052HN			
P5CC012XS	PCM1.1	contact chip card module (super 35 mm format, 8-contact)	SOT658-1
P5CC020XS			
P5SC020XS			
P5CC024XS			
P5CC037XS			
P5CC052XS			
P5CC012XD	Pd-PCM1.1	paladium plated dual interface modules in super 30 mm format (8-contact)	SOT658-1
P5CC020XD			
P5CC024XD			
P5CC037XD			
P5CC052XD			

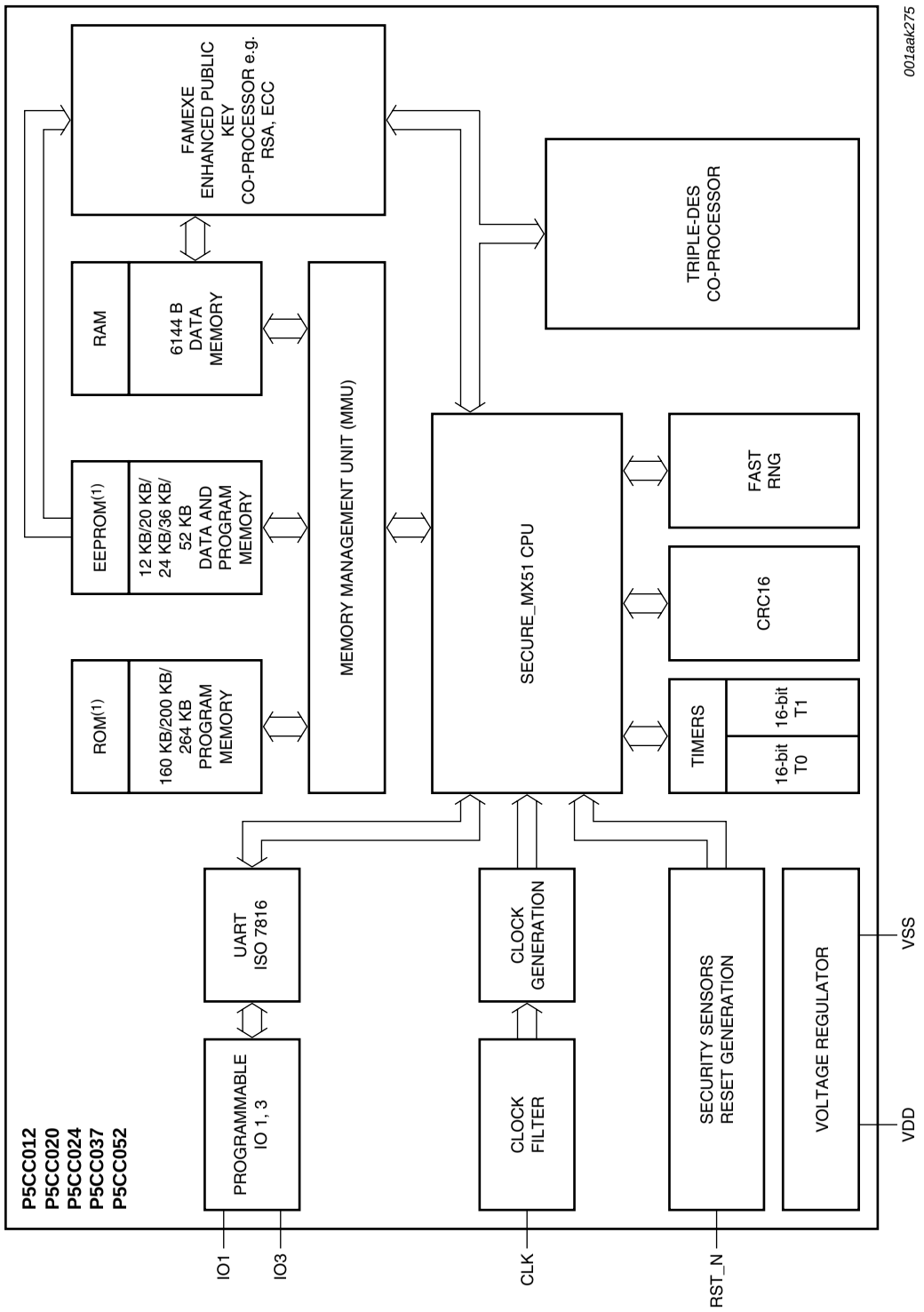
© NXP B.V. 2010. All rights reserved.

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
						FameXE	DES		
P5CC012	12	160	6	3.5	2.5	yes	yes	2	contact
P5SC020	20	160	3.5	3.5	-	no	yes	2	contact
P5CC020	20	160	6	3.5	2.5	yes	yes	2	contact
P5CC024	24	160	6	3.5	2.5	yes	yes	2	contact
P5CC037	36	200	6	3.5	2.5	yes	yes	2	contact
P5CC052	52	264	6	3.5	2.5	yes	yes	2	contact

© NXP B.V. 2010. All rights reserved.

6. Functional diagram



(1) Memory size dependent on Family type.

Fig 1. Functional diagram P5CC012/P5CC020/P5CC024/P5CC037/P5CC052

© NXP B.V. 2010. All rights reserved.

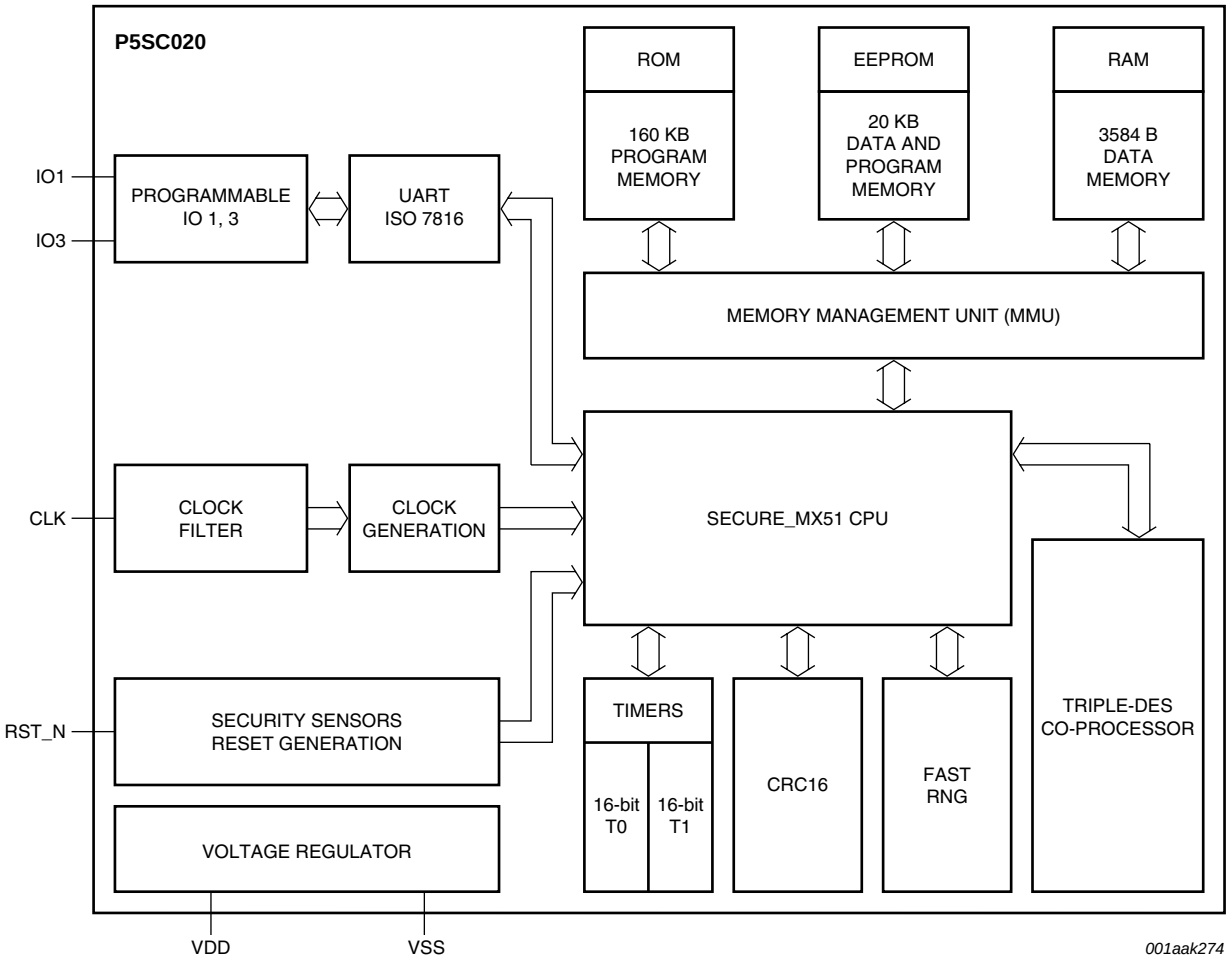


Fig 2. Functional diagram P5SC020

© NXP B.V. 2010. 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 or IO3		-	±15.0	mA
I_O	output current	pad IO1 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, IO3	[1]	-	±4.0	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
API	Application Programming Interface
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
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
SFI	Single Fault Injection

© NXP B.V. 2010. All rights reserved.

Table 6. Abbreviations *…continued*

Acronym	Description
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
P5XC012_02X_037_052_FAM_SDS_2	20100105	Product data sheet	-	P5XC012_02X_037_052_FAM_SDS_1
Modifications:	• BL-ID number corrected from 138511 to 138531			
P5XC012_02X_037_052_FAM_SDS_1	20090729	Product data sheet	-	-

© NXP B.V. 2010. 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.

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.

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.

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.

© NXP B.V. 2010. All rights reserved.

11. Contact information

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

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

© NXP B.V. 2010. All rights reserved.

12. Tables

13. Figures

© NXP B.V. 2010. All rights reserved.

14. Contents

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. 2010. **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: 5 January 2010
138531

Document identifier: P5XC012_02X_037_052_FAM_SDS_2

founded by

PHILIPS