P5CC008V1A and P5CC012V1A family

Secure contact PKI smart card controller

Rev. 3 — 22 August 2012
195430

Product short data sheet
COMPANY PUBLIC

1. General description

1.1 SmartMX family approach

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

- 8 KB or 12 KB EEPROM
- 196 KB user ROM
- 6144 B RAM
- High-performance secured Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secure dual/triple-DES coprocessor
- 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 (Common criteria version 3.1 EAL5+ in conformance to BSI-PP-0002 protection profile)
- Compliant to the EMV ICC Specification for Payment Systems

  Common Criteria version 3.1 level EAL5+ in conformance to BSI-PP-0035-2007 protection profile
- EMVCo security approval

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 now offers 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 Fame*XE* coprocessor

The security hardened 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 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 secured and CC EAL5+ certified crypto library will be available for all devices in order to support customers in implementing 3DES based solutions.

1.5 Smart*MX* interface

1.5.1 Smart*MX* 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.

1.6 Security features

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

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

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 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
  - 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 544 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 version 3.1 EAL5+ certification available (except ECC over GF(2^n)) in conformance to BSI-PP-0035-2007 protection profile

2. Features and benefits

2.1 Standard family features

- EEPROM: choice of 8 KB or 12 KB
  - Data retention time: 25 years
  - Endurance: 500000 cycles
- ROM: 196 KB
- RAM: 6144 B
  - 256 B IRAM + 3.25 KB Standard RAM usable for CPU
  - 2560 B FXRAM shared memory for Fame*XE* and 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/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 Fame*XE*
- High speed Triple-DES coprocessor (64-bit parallel processing DES engine)
  - Two or three keys loadable
  - Triple-DES calculation time < 40 μs
- 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
- 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
- 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 operand input/output 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

2.2 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 / Power-down reset
- Optional programmable card disable feature
- Memory security (encryption and physical measures) for RAM, EEPROM and ROM
- Optional disabling of ROM read instructions by code executed in EEPROM
- Optional disabling of any code execution out of RAM
- EEPROM programming:
    - No external clock
    - Hardware sequencer controlled
    - On-chip high voltage generation
    - Enhanced error correction mechanism

- 64 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 Smart*MX* 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
- E-Government
- Contact ID cards
- Secure access control
- Trusted platform modules
- Pay-TV
- Authentication

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		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), Class C is not supported

5. Ordering information

Table 3. Ordering information

Type number	Package		
	Name	Description	Version
P5CC012UA/... P5CC008UA/...	FFC	8 inch wafer (sawn; 150 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	not applicable
P5CC012XQ/... P5CC008XQ/...	PCM2.1	contact chip card module (super 35 mm tape format, 8-contact, transfer mould technology)	SOT658-1
P5CC012XR/... P5CC008XR/...	Pd-PCM2.1	palladium plated contact chip card module (super 35 mm tape format, 8 contacts, transfer mould technology)	SOT658-1
P5CC012XY/... P5CC008XY/...	PCM4.1	contact chip card module (super 35 mm tape format, 6-contact, transfer mould technology)	SOT455-1
P5CC012XZ/... P5CC008XZ/...	Pd-PCM4.1	palladium plated contact chip card module (super 35 mm tape format, 6-contact, transfer mould technology)	SOT455-1
P5CC012XS/... P5CC008XS/...	PCM1.1	contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5CC012XT/... P5CC008XT/...	Pd-PCM1.1	palladium plated contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5CC012XU/... P5CC008XU/...	PCM1.5	contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5CC012XV/... P5CC008XV/...	Pd-PCM1.5	palladium plated contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1

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		
P5CC008V1A	8	196	6	3.5	2.5	yes	yes	1	contact
P5CC012V1A	12	196	6	3.5	2.5	yes	yes	1	contact

6. Functional diagram

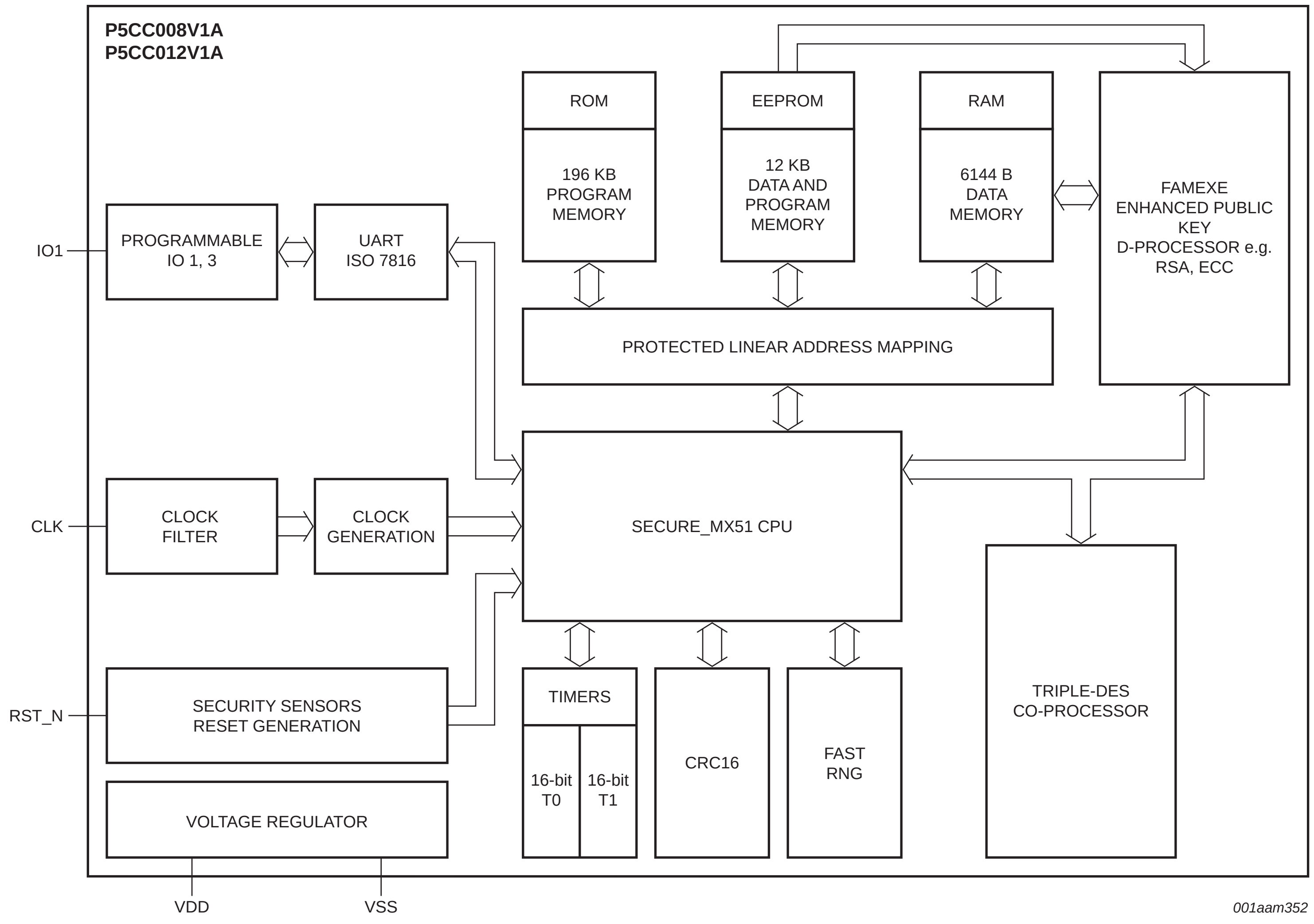

Fig 1. Functional diagram P5CC008V1A and P5CC012 V1A

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		-	±15.0	mA
I_O	output current	pad IO1		-	±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	[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 ” Wafers* and to *NXP Semiconductors Contact & Dual Interface Chip Card Module Specification*

8. Abbreviations

Table 6. Abbreviations

Acronym	Description
API	Application Programming Interface
B	byte/s[1]
CLK	External clock signal input contact pad
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
ESD	Electrostatic Discharge
Fame*XE*	Fast Accelerator for Modular Exponentiation -eXtended
GF	Galois Function
IO	Input Output
I/O	Input/Output[2]
MAC	Message Authentication Code
OS	Operating System
PKC	Public Key Cryptography

All information provided in this document is subject to legal disclaimers.

Table 6. Abbreviations *…continued*

Acronym	Description
PKI	Public Key Infrastructure
PRNG	Pseudo-Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
SFI	Single Fault Injection
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
UART	Universal Asynchronous Receiver/Transmitter

[1] e.g. “1 KB” = 1 Kbytes = 1024 bytes.

[2] Generic name for all existing I/O contact pads (I/O1, I/O2,) and their I/O line signals.

9. Revision history

Table 7. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
P5CC008V1A_P5CC012V1A_FAM_SDS v.3	20120822	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.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

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.

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

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

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

Date of release: 22 August 2012
195430
Document identifier: P5CC008V1A_P5CC012V1A_FAM_SDS