SmartMX2 family P60C080 and P60C144

Secure high-performance contact interface smart card controller

Rev. 1 — 21 October 2010 Objective short data sheet
198210 PUBLIC

1. Introduction

The new NXP Semiconductors SmartMX2 P60 family was created in order to cover all important market requests for state-of-the-art security chip controllers:

- Innovative and unique security measures, Common Criteria certified
- Superior transaction and personalization time
- Broadest portfolio of memory configurations with contact, dual-interface and contactless on a single platform
- Proven SmartMX reliability, interoperability and RF excellence for shortest time-to-market
- Market benchmark in view of cost-performance ratio

Further feature improvements in comparison to the existing approved SmartMX P5 family:

- Significant increases in controller and crypto performance
- Further extended CPU instructions for Java and C code
- Comprehensive hardware support for efficient and secure OS implementation
- Highest transaction and personalization speed
- Excellent power efficiency
- New-generation Fame2 crypto coprocessor for RSA/ECC
- New-generation Symmetric Block Cipher (SBC) crypto coprocessor for DES/AES
- Advanced 90 nm CMOS technology

Other important SmartMX2 P60 differentiators in the market are:

- New development tool suite, totally revised and based on an optimized close-to-product true bond-out chip emulation approach
- Broadest portfolio of certified package variations

2. General description

The P60C080 and P60C144 devices are members of the new SmartMX2 Family and offer with their two different EEPROM size variations a common set of functional blocks and interfaces, supporting high-performance, high-security contact applications. Figure 1 shows the block diagram of the modular controller architecture consisting of the following blocks and features:

- SmartMX2 CPU with enhanced application instruction set supporting 32-/24-/16-/8-bit move, logical and arithmetic functions
- Fame2 coprocessor based on innovative power-efficient and fast architecture for optimized RSA/ECC cryptography
- SBC coprocessor interface with multiple data/key register sets now supporting both AES and Triple-DES
- ISO/IEC 7816 data transfer improved with enhanced protocol support for T=0 and T=1 protocols
- New Copy Machines supporting direct memory access (DMA) to memories and all SFRs
- Cyclic Redundancy Check (CRC) coprocessors 16-bit/32-bit
- Memory Management Unit (MMU) with 16 cache segments
- New security features especially targeting combined laser light attacks and integrity of code execution and data fetch
- Development tool suite based on approved suppliers Keil and Ashling
  - μVision4 user interface
  - New and high-performance emulation hardware “SmartICE series”
- High-memory SoftMasking device for code development purposes
- Common Criteria security certified high-performance crypto library supporting various algorithms
- Consequent family concept with regard to all future platforms of the P60 family

3. Features and benefits

3.1 Product specific features

- EEPROM: choice of 80 KB or 144 KB
  - Data retention time: 25 years minimum
  - Endurance: 500000 cycles
  - Versatile EEPROM programming: 1 B to 256 B at a time
- ROM: 384 KB
- RAM: 8.125 KB (8320 B)
  - 5632 B CXRAM (including 256 B IRAM) usable for CPU
  - 2688 B FXRAM usable for Fame2 or CPU
- SmartMX2 CPU
  - orthogonal instruction set offering 32-/24-/16-/8-bit instructions optimized for secured and low power smart card applications
- Enhanced high-performance secured Public Key Infrastructure (PKI) coprocessor (RSA, ECC) Fame2
- Enhanced high-performance secured hardware support for symmetric block cipher (SBC) algorithms
  - Secured dual/triple-DES coprocessor
  - Secured AES coprocessor
  - Multiple key and data register sets supporting parallel data/key loading and calculation
- True Random Number Generator (compliant to AIS-31)
- 16-bit and 32-bit CRC coprocessor supporting fast memory verify functionality
- Memory Management Unit (MMU)
  - 16 segment cache entries and performance improvements
  - supporting integral concept for secure code fetch and execution
- Copy Machines offering data transfer between all Special Function Registers and all memory instances without CPU interaction
- Watchdog Timer supporting secure code execution
- Time Stamp Counter, Real Time Clock
- ISO/IEC 7816 contact interface (UART)
  - ISO/IEC 7816 contact interface (UART) offering hardware support for ISO/IEC 7816 T=0 and T=1 protocol stack implementation
  - Hardware support for automatic WTX generation for both ISO/IEC 7816 UART
  - continuos operation from 1.62 V up to 5.5 V supported
- −25 °C to +85 °C ambient temperature

3.2 Security features

- Outstanding Glue Logic chip layout approach:
  - Most efficient and proven protection against reverse engineering
  - Based on avoidance of any logical layout block recognition
- Secure Fetch (Code and Data)
- Active and dynamic shielding
- 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
- Clock input filter for protection against spikes
- Power-up and power-down reset
- Memory security (encryption and physical measures) for RAM, EEPROM and ROM
- Memory Management Unit (MMU) including memory protection:
  - Secure multi application operating systems via two different operation modes: System mode and User mode
  - OS controlled access restriction mechanism to peripherals in User mode
  - Memory mapping up to 8-MB code memory
  - Memory mapping up to 8-MB data memory
- Built-in integral concept for secure code execution covering code fetch, MMU and CPU
- Optional disabling of ROM read instructions by code executed in EEPROM
- Optional disabling of any code execution out of RAM
- Optional Unique ID for each die
- Optional programmable card disable feature
- EEPROM programming:
  - Hardware sequencer controlled
  - Enhanced error correction mechanism
- 128-B or 264-B EEPROM for customer-defined Security FabKey:
  - Featuring batch, wafer or die-individual security data
  - Encrypted diversification features available on request
- 14 B user write protected security area in EEPROM (byte access, inhibit functionality per byte)
- 32 B write once protected security area in EEPROM (bit access)
- 32 B user read only protected security area in EEPROM (byte access)
- Total useable EEPROM for customer OS (including optional FabKey areas)
  - P60C080: 81408 bytes + above 78 bytes within protected security area
  - P60C144: 146944 bytes + above 78 bytes within protected security area
- Customer specific EEPROM initialization available

4. Applications

- ID cards
- Health cards
- Electronic driving licences
- Contact banking
- Digital Signature
- Conditional Access (Pay TV)
- High-security access management
- Authentication
- Trusted platform modules
- Multi-application cards

5. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions [1]		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 C: 1.8 V range		1.62	1.8	1.98	V

[1] **Remark:** continuos operation from 1.62 V up to 5.5 V supported

6. Ordering information

Table 2. Feature table (EEPROM and RAM sizes without applied implementation of MIFARE Plus and/or DESFire EV1)

Product type	EEPROM [KB]	user ROM [KB]	total RAM [KB]	CXRAM [KB]	FXRAM [KB]	Coprocessor			MMU	Copy machines	ISO/ IEC 7816 IO pads	interface option
						Fame2	DES	AES				
P60C080	80	384	8.125	5.5	2.625	yes	yes	yes	yes	2	3	ISO/IEC 7816
P60C144	144	384	8.125	5.5	2.625	yes	yes	yes	yes	2	3	ISO/IEC 7816

Table 3. Ordering information

Type number	Package		
	Name	Description	Version
P60C080PU15	FFC	12 inch wafer (sawn; 150 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	NAU000
P60C144PU15			
P60C080PHN	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 × 5 × 0.85 mm	SOT617-1
P60C144PHN			
P60C080PX80	PCM1.1	contact chip card module (super 35 mm tape format, 8-contact, dual source)	SOT658-1
P60C144PX80			
P60C080PX81	Pd-PCM1.1	palladium plated contact chip card module (super 35 mm tape format, 8-contact, dual source)	SOT658-1
P60C144PX81			

7. Functional diagram

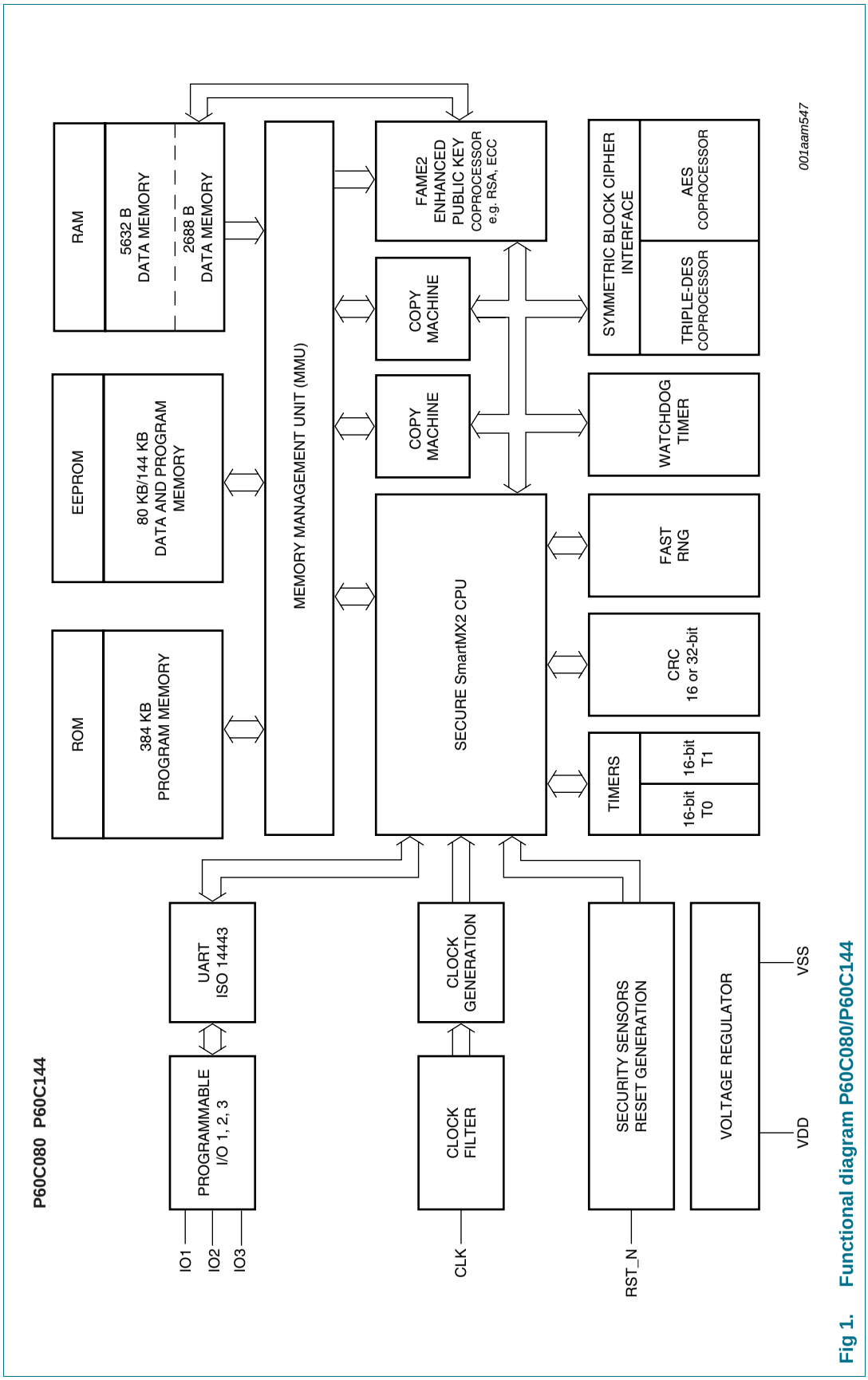

Fig 1. Functional diagram P60C080/P60C144

8. Abbreviations

Table 4. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
DES	Digital Encryption Standard
ECC	Elliptic Curve Cryptography
ICE	Integrated Circuit Emulator
RSA	Rivest, Shamir and Adleman
SECSII	Semiconductor Equipment Communications Standard 2
SFR	Special Function Register

9. Revision history

Table 5. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
SMX2_FAM_P60C080_C144_SDS v.1	20101021	Objective short data sheet	-	-

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 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 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.

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 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 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

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.

DESFire — is a trademark of NXP B.V.

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: 21 October 2010
198210