

SmartMX2 P40 family

P40C040/072

Secure smart card controller

Rev. 1.3 — 5 November 2013
262813

Objective short data sheet
COMPANY PUBLIC

1. Introduction

P40C040/072 is a secure microcontroller designed and manufactured by NXP Semiconductors. It is part of the Smart-IC family of secure micro-controllers. The SmartMX2 P40 product family is built around a proven and powerful RISC core.

End-to-end data and code encryption and integrity protection ensures that user data and application code cannot be retrieved from the device, nor corrupted during execution.

The dedicated crypto coprocessors for symmetric and asymmetric cryptography provide outstanding power efficiency. The DES/AES engine is protected by mathematically proven countermeasures. The PKC (Public Key Crypto) coprocessor provides DPA resilience and serves asymmetric crypto algorithms with a flexible RSA key length of up to 2048 bits and up to 384 bits for elliptic-curve cryptography (ECC).

NXP's SmartMX2 P40 security architecture is built on more than 15 years of experience in this area. The SmartMX2 P40 product family provides embedded firmware forming a hardware abstraction layer (HAL). The use of this HAL makes it easier to efficiently develop embedded software for the device.

The SmartMX2 P40 product family supports the easy implementation of native operating systems in market segments such as banking, E-Government, ID cards, Health cards, secure access as well as Trusted Platform Modules (TPM).

Table 1. Feature table

Product type	EEPROM [KB]	User ROM [KB]	Total RAM [B]	RAM allocation CPU/PKCC	Coprocessor			ISO/IEC 7816 IO pads	Interface option
					PKC	DES	AES		
P40C040	40	260	6144	dynamic	yes	yes	yes	1	ISO 7816
P40C072	72	260	6144	dynamic	yes	yes	yes	1	



2. General description

2.1 General remarks

This document offers an introduction into the features and the architecture of the P40 SmartMX2 products P40C040/072.

The product data sheet and other detailed documentation, e.g. for Card Operating System development are available through NXP's portal for secured documentation. Access to such documents is granted on a need-to-know basis. Contact NXP sales for registration and access.

2.2 Naming conventions

Table 2. Naming conventions

P40xeee	
x	Interface and feature configuration identifier, as currently defined, e.g.: x = C: Asymmetric and symmetric cryptography implemented, ISO/IEC 7816 contact interface
eee	Indication of the Non-Volatile memory size in KB eee = 072: For example: 72 KB EEPROM implemented

2.3 Contact interfaces

Operating in accordance with ISO/IEC 7816, the SmartMX2 P40 contact interface is supported by a built-in Universal Asynchronous Receiver/Transmitter (UART). P40 UART enables data rates of up to 688 kbit/s allowing for the automatic generation of all typical baud rates and supports transmission protocols T=0 and T=1.

2.4 Public Key Crypto (PKC) coprocessor

The PKCC is speeding up the computation of public-key cryptographic operations within the P40C040/072.

The PKC coprocessor flexible interface provides programmers with the freedom to implement their own cryptographic algorithms. A Common Criteria certified crypto library from NXP providing a large range of required functions is available for all devices listed in [Table 4](#) in order to support customers in implementing public key-based solutions.

2.5 Coprocessor for DES and AES

The DES algorithm, widely used for symmetric encryption, is supported by a dedicated, high performance, highly attack-resistant hardware coprocessor. Relevant standards (ISO/IEC, ANSI, FIPS) are fully supported. A secure crypto library element for DES is available.

The same coprocessor supports secure AES as well. The implementation is based on FIPS197 as standardized by the National Institute for Standards and Technology (NIST), for key lengths of 128 bit, 192 bit, and 256 bit with performance levels comparable to DES. AES is the next generation for symmetric data encryption and recommended successor to DES providing significantly improved security level. A secure crypto library element for AES is available.

2.6 Security features

Advanced 0.09 μm CMOS technology, with seven metal layers, provides enhanced protection against reverse engineering and probing attacks, and produces a highly protective mesh of active and dynamic multi-threaded shielding.

SmartMX2 P40 incorporates a wide range of both inherent and OS-controlled security features as a countermeasure against all types of attacks. NXP Semiconductors apply their extensive knowledge of chip security, very dense CMOS technology and active shielding methodology.

As attacks evolve over time, the multi-dimensional approach of the SmartMX2 P40 security architecture allows for more proactive and continuous enhancements of the security mechanisms compared to alternative and less versatile approaches. This makes SmartMX2 P40 a future-proof secure micro-controller platform neutralizing all side channel and fault attacks as well as reverse engineering efforts.

3. Features and benefits

3.1 Standard P40C040/072 features

- EEPROM: 40 or 72 KB
- ROM: 260 KB
- RAM: 6144 B split into area usable for CPU and PKC coprocessor. The split is configurable at runtime.
- Dedicated, RISC based Smart Card CPU
- ISO/IEC 7816 contact interface (UART)
- PKC coprocessor
 - ◆ Boolean operations for acceleration of major Public Key Cryptography (PKC) systems such as RSA and ECC
 - ◆ 2048 bits maximum key length for RSA with randomly chosen modulus
 - ◆ 32 bit operand input/output interface
- High speed DES/AES coprocessor
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalization up to 688 kbit/s
- High speed 8-, 16- or 32-bit CRC engine according to ITU-T polynomial definition
- Low power Random Number Generator (RNG) in hardware, AIS-31 compliant once NXP HAL functions are used
- 1.62 V to 5.5 V extended operating voltage range for class C, B and A (depending on product)
- -25 °C to +85 °C ambient temperature

3.2 Security features

- 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 (incl. integrated memory light sensor functionality)
- Electronic fuses for safeguarded operating mode control
- Active shielding
- Unique ID for each die
- Clock input filter for protection against spikes
- Optional programmable card disable feature
- Memory security (encryption and physical measures) for RAM, NV memory and ROM

4. Applications

- Banking
- Multi-application cards
- ID cards
- Health cards
- Electronic driving licences
- Digital Signature
- High-security access management
- Authentication
- Trusted Platform Modules (TPM)

5. Quick reference data

Table 3. 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

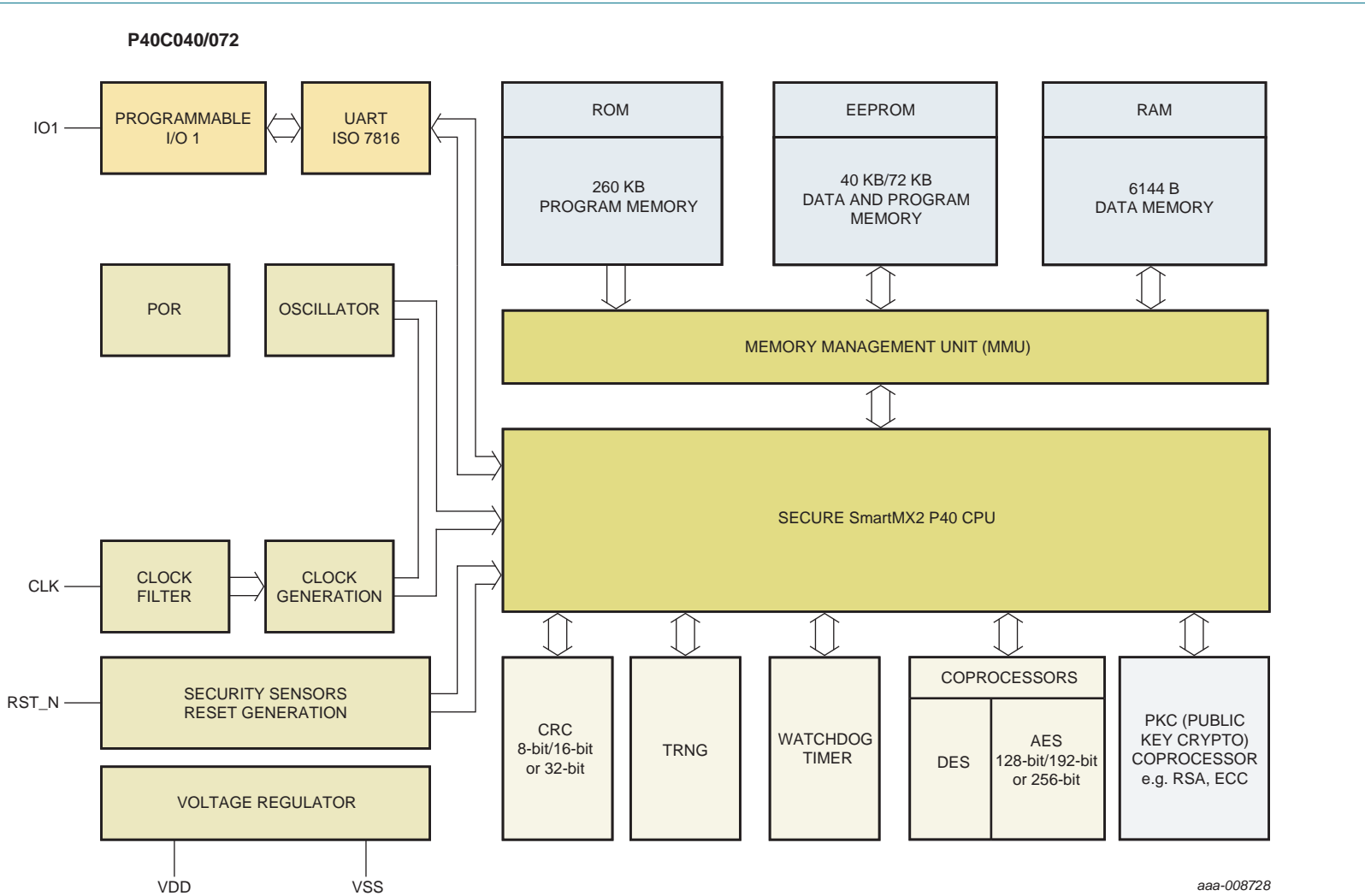
[1] **Remark:** continuous operation from 1.62 V up to 5.5 V supported

6. Ordering information

Table 4. Ordering information

Type number	Package		
	Name	Description	Version
P40C040U15	FFC	12 inch wafer (sawn, 150 μ m thickness, on film frame carrier; electronic fail die marking according to SECSII format)	NAU000
P40C072U15			
P40C040U75	FFC	12 inch wafer (sawn, 75 μ m thickness, on film frame carrier; electronic fail die marking according to SECSII format)	NAU000
P40C072U75			
P40C040X84	PCM1.5	contact chip card module (super 35 mm tape format, 8-contact); multi-source	SOT658
P40C072X84			
P40C040X85	Pd-PCM1.5	palladium plated contact chip card module (super 35 mm tape format, 8-contact); multi-source	SOT658
P40C072X85			
P40C040X60	PCM3.1	contact chip card module (super 35 mm tape format, 8-contact)	SOT658
P40C072X60			
P40C040X61	Pd-PCM3.1	palladium plated contact chip card module (super 35 mm tape format, 8-contact)	SOT658
P40C072X61			

7. Functional diagram



Remark: The diagram provides a generic overview of the architecture of the SmartMX2 P40 product family. Functional blocks, pins and connections shown in this diagram are optional and represent a super-set of those elements actually implemented in a real product.

Fig 1. Functional diagram P40C040/072

8. Revision history

Table 5. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
P40C040_C072_SMX2_FAM_SDS v1.3	20131105	Objective short data sheet	-	P40C040_C072_SMX2_FAM_SDS v1.2
Modifications:				
				<ul style="list-style-type: none"> • Section 2 “General description” on page 2: corrections and rewording • Renamed Section 2.3 “Contact interfaces” on page 2 • Section 2.3 “Contact interfaces” on page 2 and Section 3.1 “Standard P40C040/072 features” on page 4: corrected P40 UART speed personalization to 688 kbit/s • Table 4 “Ordering information” on page 7: removed package of PCM1.1 and PD-PCM1.1
P40C040_C072_SMX2_FAM_SDS v1.2	20131011	Objective short data sheet		
				<ul style="list-style-type: none"> • Initial version

9. Legal information

9.1 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>.

9.2 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.

9.3 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 controlled classification (1) — The content of this document is subject to export controls. Export or supply to listed parties requires a prior authorization from the competent authorities. The Export Control Classification Number (ECCN) is 5E002.

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.

9.4 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.

9.5 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.

10. Contact information

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

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

11. Tables

Table 1.	Feature table	1
Table 2.	Naming conventions	2
Table 3.	Quick reference data	6
Table 4.	Ordering information	7
Table 5.	Revision history	9

12. Figures

Fig 1. Functional diagram P40C040/0728

13. Contents

1	Introduction	1
2	General description	2
2.1	General remarks	2
2.2	Naming conventions	2
2.3	Contact interfaces	2
2.4	Public Key Crypto (PKC) coprocessor	2
2.5	Coprocessor for DES and AES	2
2.6	Security features	3
3	Features and benefits	4
3.1	Standard P40C040/072 features	4
3.2	Security features	4
4	Applications	5
5	Quick reference data	6
6	Ordering information	7
7	Functional diagram	8
8	Revision history	9
9	Legal information	10
9.1	Data sheet status	10
9.2	Definitions	10
9.3	Disclaimers	10
9.4	Licenses	11
9.5	Trademarks	11
10	Contact information	12
11	Tables	13
12	Figures	14
13	Contents	15

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. 2013.

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 November 2013

Document identifier: P40C040_C072_SMX2_FAM_SDS