SmartMX3 family P71D320

Overview, pinning and electrical characteristics

Rev. 3.0 — 15 June 2017
295730

Product short data sheet
COMPANY PUBLIC

1. Introduction

SmartMX3 P71D320 is a secure microprocessor with full dual-interface crypto capability. It forms part of NXP's SmartMX family of products. The device is built around a proven and powerful secure RISC core. These products are ideally suited for eGovernment and payment applications requiring an economical but also tamper-proof solution, capable to withstand today's and future attack scenarios.

P71D320 offers the flexibility of Flash memory for code and data. At the same time, ROM is still available for customers that want to use it. The high contactless performance known for NXP secure microprocessors is maintained. Memory is managed by the device firmware, resulting in very solid endurance and retention on application level.

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. A secure hardware-based copy mechanism allows safe and fast execution of software routines dealing with copying of data.

The dedicated crypto co-processors for symmetric and asymmetric cryptography provide outstanding power efficiency and flexibility. The DES/AES engine is protected by mathematically proven countermeasures. The asymmetric crypto coprocessor provides DPA resilience and serves asymmetric crypto algorithms with a flexible RSA key length of up to 4096 bits and up to 544 bits for elliptic-curve cryptography.

NXP's SmartMX3 P71 security architecture is built on more than 15 years of experience. The platform provides an embedded firmware and a hardware abstraction layer that offers standard solutions for routine tasks.

The SmartMX3 P71 product 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	User Flash [KB]	User ROM [KB]	RAM [KB]	Asymmetric crypto coprocessor	DES/AES crypto coprocessor	Interface option
P71D320	up to 336	up to 192	10	yes	yes	ISO/IEC 7816, ISO/IEC 14443
P71D240	256	up to 108	10	yes	yes	

2. General description

P71D320 is a secure microprocessor for smart card-like applications. It represents NXP Semiconductors' ninth generation of secure microprocessors and forms the essence of more than fifteen years of experience - but many hundred R&D person years of chip architecture and design excellence.

With its FlexMem concept, P71D320 features unique flexibility characteristics in terms of memory usage and production lifecycle management support. Each code element can be put into ROM for highest speed and lowest power execution, or loaded into Flash for flexibility and possibility to update.

The NXP-provided embedded software that comes with P71D320 provides NXP shared OS libraries making operating system design more effective. An innovative firewall concept manages rights between separate software instances in a novel and much more flexible way than known so far. Two software instances can be run independently from each other. The P71D320 firewall makes sure that one cannot compromise the security of the other.

A modular crypto library is offered for P71D320 that provides proven and security certified cryptographic functions to operating system developers.

P71D320 shares the same CPU core and basic architecture used in NXP's SmartMX2 P40 products. However, system capabilities and performance have been considerably improved.

The development tool suite for P71D320 is based on a well-established integrated development environment. A softmasking device with debugging capabilities is available for in-system development and code verification.

3. Features and benefits

3.1 Product specific features

- High-performance dual-Interface secure microprocessor
  - MRK3-SC 16/32-bit RISC (reduced instruction set computing) CPU for high transaction performance, low power consumption and world-class security level
  - Code Signature ensures the integrity of instruction execution
- Top-level cryptography engines with "full key length" support
  - Dedicated cryptography functional unit for symmetric DES and AES algorithms
  - 56-bit key length DES, 112-bit 2DES, 168-bit triple-DES (TDES or 3DES), in various configurations
  - AES with 128, 192 and 256-bit key length
  - Asymmetric cryptography accelerator unit, supporting RSA, ECC and related algorithms
  - RSA cryptography with arbitrary key length up to 4096 bits
  - Elliptic-curve cryptography (ECC) with key length up to 571 bits
- True Random Number Generator, compliant to AIS31
- Deterministic Random Number Generator for faster execution in cases where lower RNG entropy is sufficient
- Cyclic redundancy check (CRC) functional unit for 16 and 32-bit operation
- Large memory for operating system design flexibility:
  - Read-only memory (ROM) for the storage of fixed code elements, or for maximum performance at minimum power supply; 0…192 K ROM available for customer use, depending on logical configuration and options selected
  - Flash memory for highest flexibility; minor parts of this memory may be reserved for NXP, depending on logical configuration and options selected; up to 336 K Flash are available for customer use, depending on logical configuration and options selected
  - 10 K RAM
- NXP FlexMem approach:
  - Single, contiguous logical memory addressing area across ROM and Flash memories
  - Flexibility to load code and data in ROM or Flash as required (ROM: fastest execution; Flash: post-production loading, update)
  - Full flexibility to partition Flash memory between code and personalization data
- Secure bootloader for initial loading or updates of Flash memory; suitable for use in secure manufacturing sites as well as in general environments. Various configuration options exist to manage and delegate rights for access and writing.
- Vertical Firewall technology
  - Full separation of SW instances, no trust required between SW instances - i.e., untrusted software cannot compromise security certified software
  - Security certified sharing / hand-over mechanism for managing HW resources between SW instances
- Dual-interface support with wide configuration range
  - ISO/IEC 7816 contact interface; standard data rates up to TA1 = 97h
  - ISO/IEC 14443 contactless interface

    - Type A interface for data rates up to 848 kbit/s, symmetric and asymmetric data rate configurations
    - support for very high bit rate (VHBR) configuration of contactless interface to minimize transaction time (3.4 Mbit/s in chip-to-reader direction)
- wide range of security-certified packaging options available directly from NXP - contact, dual-interface and contactless chip modules, various wafer delivery options
- hardware-based physically unclonable function (PUF) available for configuration through NXP firmware

3.2 Security features

- 90nm CMOS technology offers strong inherent protection against invasive attacks on logic and memories
- NXP Glue Logic concept effectively de-correlates the function and location of circuitry on the device: no functional blocks are recognizable in any physical layer of the device, adding another level of protection against active and passive invasive attacks
- No use of logical hardmacro blocks; all logics in the device - including CPU, coprocessors and all other functions - are synthesized into a single glue logic area.
- NXP PUF (physically unclonable feature) for additional protection of static secrets against even the most sophisticated reverse-engineering attacks

4. Applications

- ePassports (ePP) and residence permits (eRP)
- national ID cards
- Health cards
- Contact and dual-interface banking
- Electronic driving licenses
- Digital signature cards
- High security access management
- Machine-to-machine authentication
- Trusted platform modules
- Multi-application cards

5. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{DD}	Supply voltage[1]	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
H	Field strength	Contactless interface operation		1.5		7.5	A/m
T_{amb}	Operating ambient temperature[2]			-25		+85	°C

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

[2] All product properties and values specified within this data sheet are only valid within the operating ambient temperature range.

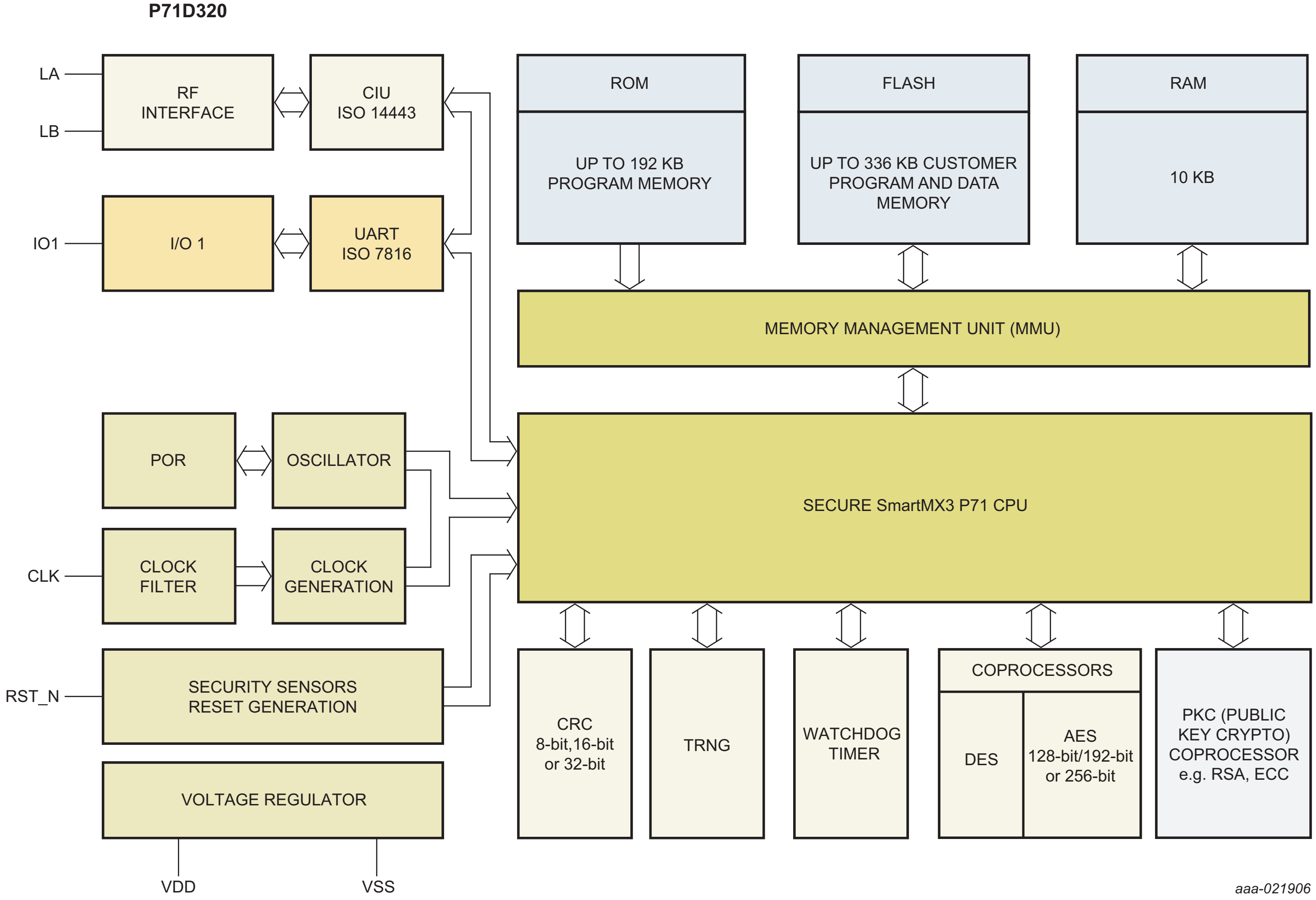
6. Ordering information

Table 2. Ordering information

Type number [1]	Package		
	Name	Description	Version
P71D240PU15 P71D320PU15 P70D144PU15	FFC	12 inch wafer (sawn; 150 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	NAU000
P71D240PU75 P71D320PU75	FFC	12 inch wafer (sawn; 75 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	NAU000
P71D240PA4 P71D320PA4	MOB4	contactless chip card module (super 35 mm tape format, module thickness 320 μm)	SOT500-2
P71D240PA6 P71D320PA6	MOB6	contactless chip card module (super 35 mm tape format, module thickness 250 μm)	SOT500-3
P71D240PX30 P71D320PX30	PDM1.1	dual interface chip card module (super 35 mm tape format, 8-contact); multi-source	SOT658-3
P71D240PX31 P71D320PX31	Pd-PDM1.1	palladium plated dual interface chip card module (super 35 mm tape format, 8-contact); multi-source	SOT658-3

[1] Contact your local NXP Sales office for additional delivery types and their release and related certification status.

7. Functional diagram


P71D320
LA
LB
RF INTERFACE
CIU ISO 14443
IO1
I/O 1
UART ISO 7816
ROM
UP TO 192 KB PROGRAM MEMORY
FLASH
UP TO 336 KB CUSTOMER PROGRAM AND DATA MEMORY
RAM
10 KB
MEMORY MANAGEMENT UNIT (MMU)
POR
OSCILLATOR
CLK
CLOCK FILTER
CLOCK GENERATION
SECURE SmartMX3 P71 CPU
RST_N
SECURITY SENSORS RESET GENERATION
VOLTAGE REGULATOR
VDD
VSS
CRC 8-bit,16-bit or 32-bit
TRNG
WATCHDOG TIMER
COPROCESSORS
DES
AES 128-bit/192-bit or 256-bit
PKC (PUBLIC KEY CRYPTO) COPROCESSOR e.g. RSA, ECC
aaa-021906

Remark: The diagram provides a generic overview of the architecture of the SmartMX3 P71 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 P71

8. Revision history

Table 3. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
295730	15 06 2017	Product short data sheet	-	295711
	• General update			
295711	25 01 2017	Objective short data sheet	-	-
	• General update			
295710	27 March 2016	Objective short data sheet	-	-
	• 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	
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.

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.
DPA™	

9.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

DESFire — is a trademark of NXP Semiconductors N.V.

FabKey — is a trademark of NXP Semiconductors N.V.

MIFARE — is a trademark of NXP Semiconductors N.V.

MIFARE FleX — is a trademark of NXP Semiconductors N.V.

MIFARE Plus — is a trademark of NXP Semiconductors N.V.

SmartMX — is a trademark of NXP Semiconductors N.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

12. Figures

13. 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: 15 June 2017
Document identifier: 295730