P60D042_SDS

SmartMX2 Family P60D042y

Rev. 3.0 — 27 September 2016

Public product data sheet
COMPANY PUBLIC

1 General description

The P60D042 dual-interface secure microcontroller is part of the most recent P60-Step-Up! family generation and builds on the IntegralSecurity architecture. It delivers unprecedented security, extended memory footprint, and highest performance across all typical up-to-date requested fast transaction cases in Payment and eGov. Furthermore, it comes with comprehensive options of ready-to-use MIFARE™ functionality and certified crypto library modules and can be ordered in various advanced package options for contact, dual interface, and contactless operation.

2 Features and benefits

2.1 Key features

- User EEPROM: up to 40 KB
- User ROM: 384 KB
- User RAM: up to 8128 Bytes
- Dual Interface Type according to ISO/IEC 14443/7816
- Rich option choice of certified convergence implementations:
  - y = P (Plain, no convergence implementations)
  - y = M (MIFARE Plus/Classic implementation)
  - y = D (MIFARE DESFire EV1 implementation)
  - y = J (Joint, common MIFARE Plus/Classic/DESFire EV1 implementation)
- Contactless VHBR data rate up to 1.7 Mbit/s (card to reader)
- Hardware-based Physically Unclonable Function (PUF) implemented: provides strong protection for secret keys and data
- SmartICE Development tool chain with true bond-out chip and Softmasking Device allows faster time to market

2.2 Hardware features

- Economic and resilient ROM/EEPROM design
  - data retention time: 25 years minimum
  - endurance: 500000 cycles
  - versatile EEPROM programming: 1 B to 128 B at a time
- SmartMX2 CPU with orthogonal instruction set offering 32-/24-/16-/8-bit instructions optimized for secured and low-power smart card applications
- Dedicated high-performance secure coprocessor FAME2 for Public Key Infrastructure (PKI) cryptography (RSA, ECC)
- High-performance secured hardware support for symmetric block cipher algorithms:

  - Dual/triple DES and AES, all key lengths
  - Dedicated hardware support for SEED and OSCCA algorithms, multiple key and data register sets for 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 Machine 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
- Continuous operation from 1.62 V up to 5.5 V
- Operating ambient temperature from -25 °C to +85 °C
- Selection of optimized antenna adaptations for respectively Class 1 ("ID1") and Class 2 ("1/2 ID1") antenna dimensions; additional option of common adaptation for both Class1 and Class2

2.3 Security features

- Outstanding Glue Logic chip layout based on the IntegralSecurity™ architecture concept:
  - Most efficient and proven protection against reverse engineering
  - Impossible to recognize logical blocks by means of optical inspection
- Advanced security sensors on clock, temperature, supply voltage, light, and single fault injection
- Active and dynamic shielding
- Advanced memory security (encryption and physical measures) for RAM, EEPROM and ROM
- OS controlled access restriction mechanism to peripherals in user mode
- Programmable card disable feature
- Physically Unclonable Function hardware support to secure keys against new attack scenarios
- Metal layer design for highest attack resilience
- No general standard core or re-used hard macro applied
- No use of ROM-based micro code
- Selection of optimized antenna adaptations for respectively Class 1 (ID1) and Class 2 (1/2 ID1) antenna dimensions, additional option of common adaptation for both Class1 and Class2
- Certificates and approvals; Common Criteria up to EAL6+, EMVCo, and CUP
- One common certificate for controllers with or without MIFARE functionality offers high re-use for any composite certification

2.4 Additional features

- CC security certified crypto library as a commercial option:
  - Consists of easy to use APIs for all algorithms, allows for dynamic use of memory resources
  - Safeguards secure operation in both contact and contactless mode
  - Includes state-of-the-art and future-proof built-in security features to avoid power (SPA/DPA), timing and fault attacks (DFA)
  - Every module is available separately
  - RSA encryption and decryption (256 … 4096 bit key length)
  - RSA signature generation and verification (256 … 4096 bit key length)
  - RSA key generation (plain and CRT format, 256 … 4096 bit key length)
  - ECC over GF(p) signature generation and verification (128 … 576 bit key length
  - ECC over GF(p) key generation and Diffie-Hellman key exchange (128 … 576 bit key length)
  - ECC over GF(p) full point addition
  - SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 hash computation
  - DES encryption, decryption and MAC (S-DES and T-DES with 2 & 3 keys)
  - AES encryption, decryption and MAC calculation (128, 192, 256 bit key length)
  - Pseudo Random number generation based on a deterministic random number generator, generator of type K4
- Rich set of MIFARE™ Flex configuration options available as selectable mix of card data sizes:
  - MIFARE Classic/Plus (up to 4 KB)
  - MIFARE DESFire EV1 (up to 32 KB)
  - In-built functionality, no additional User ROM area needed
- Service on batch, wafer or die-individual security data, secure transport keys:
  - Various EEPROM initialization options available to facilitate customer's personalization
  - Comprehensive offer on NXP Trust Provisioning service options

3 Development tools

- Development tool chain, based on approved suppliers Keil and Ashling:
  - Well-perceived µVision user interface
  - Fast and efficient compiler, loader and timing-accurate simulator software
  - High-performance emulation hardware "SmartICE series"
  - Close-to-product emulation safeguarded via a true bond-out controller
- Dual Interface Softmask Device (SMD) P60D289 for fast Flash-based prototyping
- Tutorial Libraries with dedicated customer application support via local NXP Field Application Engineers

4 Packages and applications

- Rich selection of contact, dual interface, and contactless chip modules on tape:
  - Approved selection of gold-plated and palladium-plated chip modules (Figure 1)
  - Benchmark in thinnest contactless modules (Figure 2)
  - Benchmark in robust molded modules
  - Wafer deliveries in different thicknesses on Film Frame Carrier (FFC), Figure 3
- Full coverage of today's performance needs for:
  - Payment and eGov applications
  - Transport & access management
  - Device authentication
  - Wearables and Internet of Things (IoT)

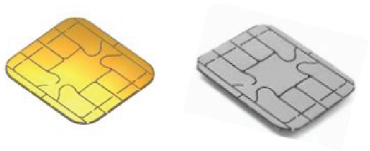

Figure 1. Gold-plated and palladium-plated modules

Figure 2. Contactless module

Figure 3. FFC

5 Revision history

Table 1. Revision history

Document ID	Release date	Data sheet status	Change notice	Supercedes
P60D042_SDS v.3	20160927	Product data sheet	-	-

6 Legal information

6.1 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.

6.2 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.

6.3 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.

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.

6.4 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.

6.5 Trademarks

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

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

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: 27 September 2016