NXP secure microcontroller family SmartMX2$^{\text{TM}}$

SmartMX2 unleashes secure multi-applications without compromise

This all-new family of secure microcontrollers is built on the groundbreaking IntegralSecurity$^{\text{TM}}$ architecture. Based on a versatile platform concept, the SmartMX2 family delivers unprecedented levels of security and performance for all types of applications.

Key benefits

- Unique security architecture meets current and future security requirements
- Multi-applications capability offers more value to your solutions
- Outstanding performance enables differentiation in terms of user convenience and transaction speed
- Fast time-to-market and smooth implementation

Key features

- IntegralSecurity$^{\text{TM}}$ architecture for best-in-class attack protection, CC EAL 6+
- High-performance SmartMX2 CPU with enhanced 8- to 32-bit application instruction set
- Power-efficient, high-speed crypto coprocessors for RSA/ECC and DES/AES
- Optimized ISO/IEC 14443 interface, including support for small antenna dimensions
- MIFARE DESFire$^{\text{TM}}$, MIFARE Plus$^{\text{TM}}$, and MIFARE$^{\text{TM}}$ Classic for applications convergence

Applications

- eGovernment
  - Passports, electronic IDs and credentials, health and social-security cards, driver's licenses
- Banking
  - Debit, credit, loyalty, ePurse, ATM
  - Different payment schemes combined with transport
- Transport
  - From stored value tickets to national transport schemes
- Access management
  - Access to buildings, logical access to PCs
- Mobile transactions
  - Payment, couponing, transport, access management
- Device authentication
  - Counterfeit protection of hardware, software and content
  - Cyber Security solutions to get access securely to service networks

As identification markets evolve and converge to secure multi-applications, the ability to move to the next level is instrumental, since it can impact time-to-market and operating cost. SmartMX2 is your best investment for secure identification solutions.

Security

NXP is the leader in security, with experience gained from developing more than five generations of certified secure microcontrollers. With the all-new SmartMX2, NXP introduces the IntegralSecurity architecture. It is designed to protect the integrity and confidentiality of user data and applications targeting CC EAL6+ certification. The IntegralSecurity architecture is a unique security design built on over 100 dedicated security mechanisms which create a dense protection shield with redundancy and multiple layers. The security mechanisms are orchestrated in a manner that provides a comprehensive response to the wide variety of modern security attacks. As attacks evolve over time, the non-monolithic approach of IntegralSecurity allows for more proactive and continuous enhancements of the security mechanisms compared to alternative and less versatile approaches. This makes the IntegralSecurity architecture a future-proof concept that neutralizes side channel and fault attacks as well as reverse engineering efforts. The architecture provides SmartMX2 with a major security enhancement including:

- NXP-patented SecureFetch™: the most advanced defense mechanism against light and laser attacks, now also covering data other than software code.
- NXP-patented GlueLogic™: the most advanced protection against reverse-engineering attacks.
- Completely re-designed MMU (memory management unit) with superior firewalling capabilities for multi-application set-ups.
- Hardened Fame2 crypto coprocessor with outstanding power efficiency, providing even more DPA resilience and serving the full range of RSA/ECC crypto algorithms with a flexible RSA key length of up to 4,096 bits.
- Advanced 0.09 µm CMOS technology, with seven metal layers, provides enhanced protection again reverse engineering and probing attacks, and produces a highly protective mesh of active and dynamic multi-threaded shielding.
- Highly secured RAM and additional Stealth-NV-Memory with advanced detection capabilities to protect against advanced and combined attack scenarios.
- Secure, hardware-based copy machine for safe and fast execution of recurring software routines.
- Upcoming products will support PUF (Physically Uncloneable Function).

Convenience & performance

According to a Dhrystone* benchmark, SmartMX2 delivers CPU and crypto performance – on both contact and contactless interfaces – that is up to 5.7x faster than its highest performing SmartMX™ predecessor, while consuming less energy.

- Contactless transaction speed up to 848 kbit/s in combination with an internal clock frequency of up to 150 MHz** in contact and contactless operation, even down to low field strength of 1.5 A/m.
- Support of simultaneous operation of both ISO/IEC 7816 and ISO/IEC 14443 interface for multi-applications, including mobile payment.
- Industry-standard I^{2}C (400 kbit/s) and SPI (2 Mbit/s) interfaces.
- Easy interface with NFC ICs.
- Dedicated hardware support for safe and fast execution of recurring software routines. For example, use of the copy machine between memories and registers, along with implemented support for UART protocols, saves significant lines of code and increases the copy execution speed.
- Enhanced 8-, 16-, 24- and 32-bit application instruction set minimizes the number of CPU cycles, for faster execution time and lower power consumption with maximum computing performance.
- Family concept with enhanced memory options: 264 to 500 KB ROM, 4 to 8.125 KB RAM, 24 to 144 KB EEPROM and 256 to 400 KB Page Flash on the same architecture and interface options.
- SmartMX2 supports all versions of MIFARE products like MIFARE Classic, MIFARE Plus and MIFARE DESFire EV1, the world's leading platform for automatic fare collection used in more than 650 cities and 50 countries worldwide.
- MIFARE FleX framework to manage selection of any MIFARE implementation per transaction. In addition, configuration flexibility of ID (UID, FNUID and random ID), activation parameters (ATQA, SAK, ATS) and exit conditions (timeout, UART activity, RF field absence).
- Available in industry-leading MOB6 package with 250 µm thickness, improving card robustness and allowing for additional physical security features in the card.

* Dhrystone is a CPU benchmark program developed in 1984 by R. P. Wecker.

** Based on a six clock/cycle machine.

Design productivity

SmartMX2 builds on proven and reliable technology that demonstrates worldwide interoperability and standard compliance. SmartMX2 is the next generation of SmartMX, which is currently used by 85% of the countries with electronic passports, is the leading choice for bank cards, and is the preferred technology for the secure element of NFC-enabled phones.

- Fast software development and safe time-to-market via available security certified crypto library.
- State-of-the-art tool chain support from Keil and Ashling. Developers use a true bondout chip for emulation, an innovative softmasking device, and a set of new, sophisticated debug facilities.
- Global Customer Application Support team with application notes, training, and customer-specific technical assistance.

NXP leadership

NXP is the world leader in contactless technology. NXP invented MIFARE and has been the leading contributor in the development of many contactless innovations, including NFC. By building on deep application insight, NXP offers unique end-to-end solutions that include reader ICs, security ICs, and enabling technologies for infrastructure and end-user products. For nearly two decades, NXP technology has been at the heart of the vast majority of thousands of contactless system roll-outs around the globe. Today, many of these systems are on the brink of converging into secure multi-applications.

SmartMX2 selection guide

	Product	EEPROM (KB)	ROM (KB)	RAM (KB)	Features
Contactless & Dual-interface	P60D144	144	384	8.125	‣ Security certified according to Common Criteria and FIPS ‣ EMVCo approval ‣ Memory data retention time: 25 years ‣ Endurance: 500,000 cycles (min) ‣ Contact interfaces: ISO/IEC 7816, I^{2}C, SPI ‣ Contactless interface: ISO/IEC 14443 ‣ Voltage class: C, B, A (1.62 to 5.5 V) ‣ SmartMX2 CPU with enhanced 8/16/24/32-bit instruction set ‣ High-speed Fame2 for RSA/ECC operation with up to 4,096-bit keys ‣ DES/AES coprocessor with multiple key loading ‣ MIFARE FleX framework ‣ MIFARE Classic, MIFARE Plus and MIFARE DESFire EV1 implementation ‣ Certified crypto library ‣ Certified delivery types (wafer, chip, module) and standard IC packages
	P60D080	80	384	8.125	
	P60D040	40	300	8.125	
	P60D024	24	264	8.125	
	P60D041	40	264	6.000	
	P60D017	17	264	6.000	
	P60D016	16	264	8.125	
	P60D012	12	264	8.125	
Contact	P60C144	144	384	8.125	
	P60C080	80	384	8.125	
	Product	**Page Flash (KB)**		**RAM (KB)**	
Contactless & Dual-interface	P61D500	500		8.125	
Contact	P61C500	500		8.125	

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.

SmartMX, SmartMX2, MIFARE, MIFARE DESFire, MIFARE Plus, MIFARE FleX
IntegralSecurity, GlueLogic, Secure Fetch are trademarks of NXP Semiconductors N.V.

www.nxp.com/smartmx2

SmartMX2

www.nxp.com

Date of release: August 2012
Document order number: 9397 750 17276
Printed in the Netherlands