NXP SmartMX^{TM} high security microcontroller IC

SmartMX for programmable, high-security, multi-application smart cards

SmartMX, the platform of choice for secure and fast data transactions, is a proven solution for contact and contactless applications including eGovernment, banking and public transport. It offers advanced attack resistance and high performance, with cryptographic coprocessors and ultra-low-power design.

Features

- Security certified according to CC EAL5+
- EEPROM: 8 to 144 KB
  - Data retention time: 25 years
  - Endurance: 500 000 cycles minimum
- ROM: 160 to 264 KB
- RAM: 3.5 to 7.5 KB
- Interfaces
  - Contact interface according to ISO/IEC 7816
  - Contactless interface according to ISO/IEC 14443 A
- Voltage class: C, B, and A (1.62 to 5.5 V)
- Memory Management Unit (MMU)
- MIFARE DESFire^{TM} EV1 2K / 4K / 8K implementation
- MIFARE^{TM} Classic 1K / 4K implementation with MIFARE FleX^{TM} framework (configure ID, activation parameters, exit conditions)
- High-speed 3-DES coprocessor (64-bit parallel)
- High-speed AES coprocessor (128-bit parallel)
- PKI (RSA, ECC) coprocessor FameXE (32-bit parallel)
- Broad spectrum of delivery types
  - 150 µm and 75 µ sawn wafers
  - Contact, dual interface and contactless chip modules down to 250 µ width
  - Very tiny SMD packages

Application

- Public Transport
  - Powerful platform for national AFC schemes and convergence with banking or eGov
- eGovernment
  - ePassports, national ID cards, health and social-security cards, citizen cards and resident permits, driver's licenses, high-security physical/logical access control
- Banking
  - Debit, credit (MasterCard PayPass, VISA qVSDC), convergence (payment and public transportation), loyalty, mobile payment
- The SmartMX Family is steadily enhanced with regard to most recent CMOS process technology generations thus always offering best constraints for security and optimized transaction times.

The NXP SmartMX family meets the highest performance standards and forthcoming security requirements yet reduces overall cost. It is a proven, reliable solution for smart transactions – with almost one billion ICs shipped – that delivers leading-edge performance in contactless operation along with reduced personalization time.

Building on NXP's track record of innovation, the SmartMX platform is supported by a product roadmap that offers increasing levels of convenience and security.

Options include a broad spectrum of industry-leading and certified delivery types that enable optimized product implementation and reduced time to market. Faster personalization time lowers production costs, for an efficient price/performance ratio.

SmartMX also has a built-in Memory Management Unit (MMU) to support strong firewalls and enhance security levels within a multi-application set-up. All relevant cryptographic algorithms are supported with "hardened" IC blocks equipped with unique features. Cryptographic coprocessors support public key algorithms, and optimized, certified crypto libraries are available for interfacing the coprocessors and simplifying development of a secure OS.

To service a range of applications in eGovernment and banking, SmartMX supports proprietary operating systems as well as open-platform solutions such as Java and MULTOS. Its contact interface meets the international standard ISO/IEC 7816 and its contactless interface complies with ISO/IEC 14443. In addition, the MIFARE Classic and MIFARE DESFire EV1 implementations ensure compatibility with a widely deployed MIFARE infrastructure.

Excellent security measures

The product family is certified Common Criteria EAL 5+, so it protects against light attacks, invasive fault attacks, and side-channel attacks, and comes with a CRI license for improved DPA/SPA attack resistance features.

Steady extension of the SmartMX portfolio

NXP is the leader among Contactless IC vendors. The P5CD145 platform, which includes the dual interface types P5CD016, P5CD041, P5CD081, P5CD128 products, features Secure Fetch™ technology and delivers Mchip4 transaction times <400 ms. The platform is EMV-compliant, supporting antennas down to one half ID1, and offers an EAC reading time down to 3.5 seconds with a 50 kbyte dataset. All known crypto algorithms and protocols supported by SmartMX for multiple key lengths.

The proven SmartMX series fully supports multi application requirements. For the highest multi-application performance requirements, the first products of the highly anticipated family of SmartMX2 products are now available. Customers have reported the features and performance of these new devices to be the best in the Smartcard industry!

SmartMX

	MIFARE DESFire EV1 Type	Standard Type	EEPROM ROM (Kbyte)	Features
Contactless & Dual-Interface		P5CD145	144 / 264	▸ CC EAL5+ ▸ EMVCo Approval ▸ fast FameXE for up to 4096 bit keys ▸ MIFARE Classic implementation (for contactless products) ▸ EAL5+ certified crypto library
		P5CD144	144 / 200	
		P5CD128	128 / 264	
	P5CD081V1D*	P5CD081	80 / 264	
		P5CD080	80 / 200	
	P5CD041V1D*	P5CD041	40 / 264	
		P5CD040	40 / 200	
	P5CD021V1D*	P5CD021	20 / 264	
		P5CD020	20 / 200	
	P5CD016V1D*	P5CD016	16 / 264	
		P5CD012	12 / 200	
Contact		P5CC145	144 / 264	
		P5CC144	144 / 200	
		P5CC128	128 / 264	
		P5CC081	80 / 264	
		P5CC080	80 / 200	
		P5CC073	72 / 200	
		P5CC052	52 / 264	
		P5CC040	40 / 200	
		P5CC037	36 / 200	
		P5CC024	24 / 160	
		P5CC021	20 / 200	
		P5CC020	20 / 160	
		P5CC012	12 / 160	
		P5CC008	8 / 160	

* Device Type standard with 232KB ROM. MIFARE DESFire EV1 Type products are CC EAL4+ certified

SmartMX, MIFARE, MIFARE DESFire, MIFARE FleX, Secure Fetch are trademarks of
NXP Semiconductors N.V.

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.

www.nxp.com

Date of release: October 2011
Document order number: 9397 750 17192
Printed in the Netherlands