NXP SmartMX: 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 PayTV. It offers advanced attack resistance and high performance, with cryptographic coprocessors and ultra-low-power design.

Features

- Security certified according to CC EAL5+
- EEPROM: 10 to 144 KB
  - Data retention time: 20 to 25 years
  - Endurance: 100 000 to 500 000 cycles minimum
- ROM: 96 to 264 KB
- RAM: 2.25 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 emulation
- High-speed 3-DES coprocessor (64-bit parallel)
- High-speed AES coprocessor (128-bit parallel)
- PKI (RSA, ECC) coprocessor FameXE (32-bit parallel)

Application

- 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
- Mobile and set-top-box PayTV
- 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 more than half a billion ICs shipped – that delivers leading-edge performance in contactless operation along with reduced personalization time.

NXP founded by Philips

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.

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, MIFARE emulation supports a wide variety of automated fare collection (AFC) schemes for public transport.

Excellent security measurements

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.

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.
All SmarteID products come with a CRI license for improved DPA/SPA attack resistance features.

Excellent contactless performance: P5CD081 platform

NXP has been ranked number one in ABI's Contactless IC Vendor Ranking for two years running. Our P5CD081 platform, which includes the P5CD016, P5CD041, P5CD081, P5CD128, and P5CD145 products, features Secure Fetch™ technology and delivers Mchip4 transaction times under 400 ms. The platform is EMV-compliant, supporting antennas down to one half ID1, and offers an EAC reading time of only 3.5 seconds.

SmartMX

	Application		Type	EEPROM/ ROM (Kbyte)	Features
	Banking	eGovernment			
Contactless & Dual-Interface	DIF secure chip for mobile devices	Multi-application, high-end eID cards	P5CD145 *	144 / 264	▸CC EAL5+
			P5CD144	144 / 200	
			P5CD128 *	128 / 264	
	High-end DIF EMV/ATM cards	ePassport high-end eID cards	P5CD081	80 / 264	
			P5CD080	80 / 200	
			P5CD072	72 / 160	
	Low-end/mid-range EMV/ATM cards	Low-end/mid-range eID cards	P5CD041	40 / 264	
			P5CD040	40 / 200	
			P5CD036	36 / 160	
			P5CD021	20 / 264	
			P5CD020	20 / 200	
			P5CD016	16 / 264	▸MIFARE emulation **
			P5CD012	12 / 200	
Contact	Contact secure chip for mobile devices	Multi-application high-end eID cards	P5CC145 *	144 / 264	
			P5CC144	144 / 200	
			P5CC128 *	128 / 264	
	High-end EMV/ATM cards & PayTV	High-end health & eID cards	P5CC081	80 / 264	
			P5CC080	80 / 200	▸FameXE
			P5CC073	72 / 200	
			P5CC072	72 / 160	
			P5CC052	52 / 264	
			P5CC040	40 / 200	
	Low-end/mid-range EMV/ATM cards & PayTV	Low-end/mid-range health & eID Cards	P5CC037	36 / 200	
			P5CC036	36 / 128	▸EAL 5+ Certified crypto library
			P5CC024	24 / 160	
			P5CC021	20 / 200	
			P5CC020	20 / 160	
			P5CC018	18 / 128	
			P5CC012	12 / 160	
			P5CC009	10 / 96	

* under development ** for contactless product

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

founded by PHILIPS

Date of release: September 2009
Document order number: 9397 750 16823
Printed in the Netherlands