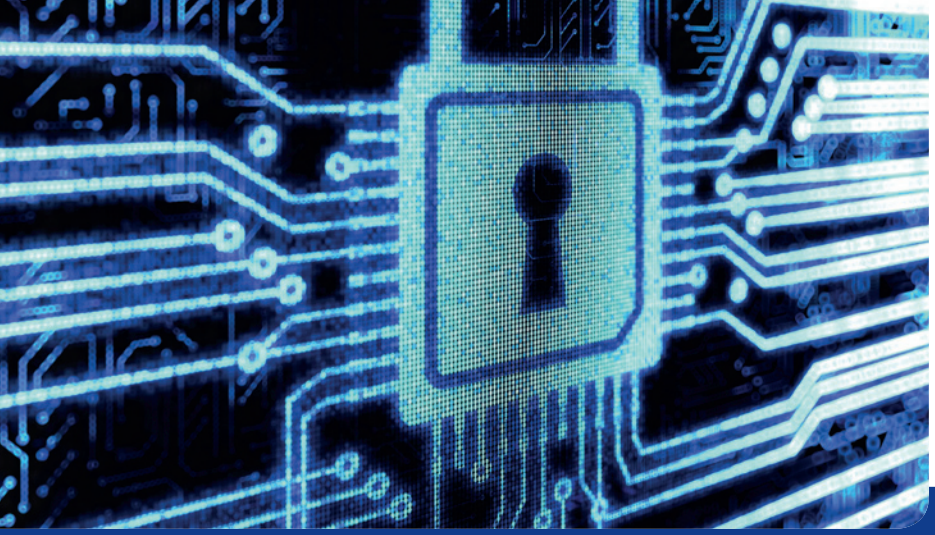

NXP chip card IC SmartMX2-P40 for eGov and Banking

Next-generation contact chip card ICs for advanced security in mass market applications

Building on a proven, high-performance RISC CPU and the IntegralSecurity™ architecture, these secure microcontroller ICs are optimized for fast, tamper-proof transactions in eGovernment, Banking, and other mass market deployments.

KEY FEATURES

- High-performance RISC platform for secure microcontroller
- IntegralSecurity™ architecture providing best-in-class attack protection
- ISO/IEC 7816 contact interface
- Dedicated crypto coprocessors for asymmetric RSA/ECC and symmetric DES/AES cryptography
- Certified to EMVCo, Common Criteria EAL5+

KEY BENEFITS

- Competitive solution for contact chip card applications
- Powerful, streamlined architecture for fast, tamper-proof performance
- Comprehensive protection against current and future attack scenarios
- Certified Hardware Abstraction Layer (HAL) and crypto library for fast time-to-market

APPLICATIONS

- eGovernment
  - eID cards, electronic health and social-security cards, eDriver's licenses
- Banking
  - Debit, credit, pre-paid, loyalty, ePurse, ATM

NXP has extended its industry-leading SmartMX2 portfolio to meet the needs of pure contact applications for payment and identification. The SmartMX2-P40 family is designed for mass market deployments and provides an ideal combination of speed and security. Using best-in-class analog and digital security functions, the ICs provide fast transactions while being able to withstand attack scenarios today and well into the future.

SECURITY

The IntegralSecurity architecture builds on 15 years of innovation and a comprehensive security concept. Produced in an advanced 0.09-µm CMOS technology with seven metal layers, the architecture produces a highly protective mesh of active and dynamic multi-threaded shielding that protects against probing and reverse engineering. NXP's patented GlueLogic™ adds an extra layer of protection against reverse engineering.

End-to-end data and code encryption with integrity protection ensures user data and application code cannot be retrieved from the device or corrupted during execution, while mathematically proven countermeasures protect the cryptographic coprocessors from side channel attacks.

CRYPTOGRAPHIC FUNCTIONALITY

The SmartMX2-P40 supports DES, AES, ECC, RSA cryptography, hash computation, and random-number generation. For asymmetric RSA and ECC cryptography, a dedicated coprocessor supports RSA key lengths up to 4,096 bits and ECC key lengths up to 521 bits. Coprocessors for symmetric ciphers support DES (single DES, 2-key 3DES, and 3-key 3DES), plus AES cryptography with bit lengths of 128, 192, or 256 bits. The Crypto Library provides ready-to-use, highly efficient software APIs for all cryptographic functions (RSA key length up to 2048 bits, ECC up to 384 bits).

PERFORMANCE

In Dhrystone benchmarks (available on request), the SmartMX2-P40 architecture demonstrates excellent performance in direct comparison to other secure microcontroller platforms. The memory configuration, which combines 260 kB ROM, 6 kB RAM, and up to 72 kB EEPROM, handles static code and dynamic data separately, and enables fast code execution from ROM.

DESIGN ADVANTAGES

Several features simplify the design process. Timing accurate simulation for the CPU and peripherals makes it easier to estimate and analyze performance from the function level to the instruction level. A soft-mask device, for customer OS verification in hardware, accurately reflects real-time behavior. The certified hardware abstraction layer (HAL) is a powerful, high-level programming interface that saves time for OS programming in order to achieve fast time to market and the toolchain uses the familiar Eclipse environment.

NXP LEADERSHIP

NXP is the world leader in contact and contactless secure microcontroller technology. NXP invented MIFARE™ contactless ICs and has been a leading contributor to many innovations, including NFC. NXP's proven end-to-end solutions include reader ICs, security ICs, and enabling technology for mobile transactions, infrastructure and end-user applications.

For nearly two decades, NXP technology has been central to thousands of contact and contactless chip card system roll-outs across the globe. These systems are ready to converge into multi-application formats that support more than one function. NXP's SmartMX2 platform lets these systems unleash their full potential for even higher value and convenience.

SmartMX2-P40 selection guide

Interface	Product	EEPROM (KB)	ROM (KB)	RAM (KB)	Features
Contact	P40C072	72	260	6	▸ Common Criteria EAL5+ certification
					▸ EMVCo approval
					▸ Memory data retention time: 25 years
	P40C040	40			▸ Endurance: 500,000 cycles (min)
					▸ Contact interface: ISO/IEC 7816
					▸ 16-bit RISC CPU
	P40C012	13			▸ Dedicated coprocessors for RSA/ECC and DES/AES cryptography
					▸ Certified hardware abstraction layer and crypto library
					▸ Certified delivery types (wafer, chip, module)

www.nxp.com

Date of release: October 2014
Document order number: 9397 750 17483
Printed in the Netherlands