NXP secure microcontroller SmartMX2 P60-Step-Up!

Step up security and innovation with next generation SmartMX2 products

P60-Step-Up!, as the latest SmartMX2 P60 generation, builds on the groundbreaking IntegralSecurity™ architecture. It delivers unprecedented security, extended memory footprint, and high performance across all application categories.

KEY FEATURES

▸ High-performance SmartMX2 CPU with enhanced 8- to 32-bit application instruction set

▸ MIFARE DESFireEV1™, MIFARE Plus™, MIFARE™ Classic certified as ready-to-use applications

▸ Payment M/Chip Advance transaction performance < 290ms

▸ eGov SAC + EACv1 ePP performance < 3.5s (40kB)

▸ Very High Bit Rate (VHBR) supporting up to 1.7 Mbit/s

▸ Optimized ISO/IEC 14443 interface, including full support for mid-size antenna dimensions (subset of class 2)

▸ Power-efficient, high-speed crypto coprocessors for RSA/ ECC and second generation of AES and 3DES

▸ Extended hardware support for global cryptographic schemes: OSCCA SM4 and SEED

▸ Common criteria EAL 6+ certificate (ETR approved early 2016)

▸ Physical Unclonable Function (PUF) as next-level security feature for advanced key protection

▸ Larger ROM, EEPROM, and RAM than current P60 products

▸ Advanced IntegralSecurity architecture providing high attack resistance

▸ Softmask Device (SMD) as advanced development tool for FLASH-based prototyping

KEY BENEFITS

▸ Best-in-class transaction performance in payment applications

▸ Faster transactions in eGov applications due to VBHR

▸ Latest security certification CC EAL 6+ for leading security

▸ Next-generation security for protection of customer assets (PUF)

▸ Faster time-to-market with SMD concept

▸ Enlarged memory footprint for flexible OS development

APPLICATIONS

eGovernment
- ePassports, electronic IDs and credentials, health and social-security cards, driver's licenses

Payment
- Debit, credit, loyalty, ePurse, ATM, prepaid
- Multi-application payment cards, with support for all major payment schemes

Transport & access management
- Stored-value tickets to national transport schemes
- 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 for secure access to service networks

Wearables
- Fitness tracker, smartwatches, tokens, eyewear, payment

IoT
- Smart cities, homes and buildings, intelligent logistics, M2M Industry 4.0

Secure multi-application formats have become widespread in the smart card industry. Choosing the right solution can reduce time-to-market and lower operating cost. NXP's P60-Step-Up! products, the next generation of the widely known P60 series, are high-end solutions that meet these market requirements.

A STEP-UP IN SECURITY

The architecture provides SmartMX2 with a major security enhancement including:
- First-time PUF support to secure the keys against new attack scenarios
- Hardware-supported cryptography for Chinese OSCCA SM4
- Hardware-supported cryptography for Korean SEED
- AES and DES coprocessors with innovative side-channel protection
- End-to-end encryption for high resistance to side-channel attacks
- CC EAL 6+ certificate (ETR approved early 2016)
- Support of well-known SmartMX2 security features, including NXP-patented SecureFetch™ and GlueLogic™

A STEP-UP IN APPLICATION USE CASES

The enlarged memory footprint opens up additional use cases:
- Larger ROM and EEPROM enable integration of multiple applications
- Larger RAM allows performance optimization with regard to transaction time for time-critical target applications

A STEP-UP IN TIME-TO-MARKET

The P60-Step-Up! toolchain includes a Softmask Device (SMD) development tool which significantly reduces time-to-market. It provides a simple, effective way to validate chip-card OS, to achieve first-time-right products by using the same hardware structure as the P60-Step-Up! In addition, the SMD can be used for customer demonstrations and prototypes.

DESIGN PRODUCTIVITY

SmartMX2 builds on the proven and reliable IntegralSecurity architecture, which demonstrates worldwide interoperability and standard compliance. SmartMX and SmartMX2 products have been used by 85% of countries with ePassports, and more than 5.5 billion have been shipped. The SmartMX family is the leading choice for payment cards, and the preferred technology for the secure element of NFC-enabled phones.

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.

	Product	EEPROM (kB)	ROM (kB)	RAM (kB)
Contactless & dual-interface	P60D145	144	512/586	11
	P60D081	80	384	9
	P60D042	40	384	9
	P60D025	24	384	9

Toolchain	Packaging
Ashling Smart ICE emulator with bondout device, SMD P60D289, Keil simulator, compiler, loader	Contact/contactless modules DIF modules Inlays

LICENSED DPA COUNTERMEASURES™

With DPA Countermeasures functionality
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.