NXP secure microcontroller SmartMX3 P71D320

Improved security and flexibility for contactless & dual-interface apps

The third generation of NXP's proven and reliable SmartMX microcontroller family delivers exceptionally high security, flexible memory usage, and outstanding performance across all intended applications.

KEY FEATURES

Flexibility

- Unique FlexMem memory architecture combining Flash and ROM memory to provide flexibility and performance
- Large memory for code and data (444K total)
- Depending on customer code size (e.g. 220K), user memory can be available up to 225K
- Future-proof family concept across SmartMX3 microcontroller units
- Softmask Device (SMD) for fast prototyping
- ROM enables high NV memory density

Security

- Advanced IntegralSecurity architecture 2.0
- New Vertical Firewall technology
- Physical Unclonable Function (PUF)
- Full featured cryptography: RSA 4096, ECC640
- Common criteria EAL 6+ certification (2017) taking latest attacks on security into account

Performance

- Enhanced eGov SAC ePP performance < 2s
- Payment M/Chip transaction time improved by 30% < 230ms
- ROM memory enables enhanced seek time to storage
- High-performance MRK3-SC 16/32-bit CPU
- 4th generation of power-efficient, high-speed crypto coprocessors for RSA/ECC
- Very High Bit Rate (VHBR) supporting up to 3.2 Mbit/s

KEY BENEFITS

- Faster ROI with flexibility, product compatibility & quicker time-to-market
- Strong security protection of OS and data
- Consumer-friendly performance with faster-than-required transaction time

APPLICATIONS

- eGovernment
- Payment
- Transport
- Access management
- Mobile transactions
- Wearables
- Device authentication
- IoT

NXP SmartMX

FLEXIBILITY

The NXP FlexMem concept combines the best of flash memory and ROM, and improves production life-cycle management. FlexMem makes the customer's operating system code more flexible, yet maintains high performance in terms of read access and transaction speed. ROM can be used to extend the ample flash memory, in support of crypto libraries, Java virtual machines, and other code elements.

SECURITY ENHANCEMENT

The increased reliance on mobile-based services, smartphone apps, and centralized services in the cloud increases the need for security and trust in system endpoints. The SmartMX family is an anchor of hardware trust, and provides high degree of confidence. With the P71D320, endpoints now have a next-generation solution that offers continuity and reliability, for years of highly secure operation.

IntegralSecurity Architecture 2.0

- Security against known and most recent template attacks
- End-to-end protection by blinded data paths
- Configurable memory encryption
- No hard-macro design

Vertical firewall

- Certified isolation of NXP and customer code (firmware) mechanism for resource management and inter-OS communication

Latest certificates

- EMVCo & CC EAL 6+ certificates based on latest requirements for protection against side channel & fault injection attacks
- CC certified against PP 0084 with Package 2 loader

Unique protection layer

- Physical Unclonable Function (PUF) creates silicon fingerprint and enhances protection of customer assets (keys, sensitive data, etc.)

Full-featured cryptography

- RSA 4096, ECC640 at very high performance; sufficient headroom for longer keys and more complex protocols

Glue logic

- Spatial decorrelation of logic functions; strong protection against reverse engineering; no hard macros used in layout

BRAND VALUES

SmartMX3 products build on the proven and reliable IntegralSecurity architecture, which demonstrates worldwide interoperability and standard compliance. SmartMX products have been used in more than 100 countries, for EMV payment cards and eGovernment solutions, and more than 6 billion SmartMX ICs have shipped. The SmartMX microcontroller family is the leading choice for secure applications, including ePassports, eIDs, eHealthcards, eDriver's licenses, access management, and payment. It is the preferred technology for the secure element of NFC-enabled phones, too.

NXP LEADERSHIP

NXP is the world leader in contactless technology. NXP invented MIFARE and has been a 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.

P71D320 Platform				
Product	**Type**	**Flash (KB)**	**ROM (KB)**	**RAM (KB)**
Contact & dual-interface	P71D320/240	up to 336KB	100KB/108KB	10

Toolchain	Packing
License-free NXP toolchain using the Eclipse IDE; HW-based debug and prototyping with SMD	Contact/Contactless modules, DIF module, Inlays

*The P71D320 will also be available with NXP's proven JCOP3 JavaCard Operating System.

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.

www.nxp.com

Date of release: February 2017
Document order: SIS_SMX3_v1
Printed in the Netherlands