Enhanced security, memory expansion and flexible I/O capabilities

Kinetis® K8x MCU Family

Based on the ARM® Cortex®-M4 core, the K8x microcontroller (MCU) family offers the security, scalability and flexibility to address the challenges of creating smart devices for the Internet of Tomorrow.

The K8x MCU family extends the Kinetis portfolio with advanced security capabilities including:

- Boot ROM to support encrypted firmware updates
- Automatic AES Decryption and execution from external serial NOR flash memory
- Hardware AES acceleration with side band attack protection
- Support for public key cryptography

Kinetis K8x MCUs offer symmetric cryptographic acceleration as a standard feature along with full-speed USB 2.0 On-The-Go (OTG), including options for crystal-less device functionality. K8x MCUs have 256 KB of embedded flash and 256 KB SRAM. In addition the integrated QuadSPI interface supports connections to non-volatile memory (serial NOR), allowing developers to expand beyond the boundaries of a traditional MCU.

TARGET APPLICATIONS

- Point-of-sale (POS)
- Building control
- Home automation and security
- IoT data concentrators
- Portable healthcare
- Smart energy gateways
- Wearables

BENEFITS

- CPU and system cache reduce latency of memory resources, lowering power consumption and improving performance
- Separate I/O power domain for up to 14 pins allow operations without the need for external level translators
- Flex™ I/O peripheral expands MCU capabilities by emulating serial, parallel, or custom interfaces using software drivers provided by the Kinetis SDK
- Low-power operation with state retention stop mode down to 5 µA with fast wake-up time and lowest power mode with only 330 nA

COMPREHENSIVE ENABLEMENT SOLUTIONS

Kinetis software development kit (SDK) **www.nxp.com/ksdk**

- Kinetis SDK is a collection of software enablement for NXP Kinetis microcontrollers that includes system startup, peripheral drivers, stacks and middleware, with new support for symmetric and asymmetric cryptographic acceleration
- Pre-integrated real-time operation systems (RTOS) kernels, including FreeRTOS™, Micrium® µC/OS-II® and µC/OS-III®
- All software is provided free-of-charge as assembly and C source code under permissive and open-source licensing
- Includes software examples demonstrating the usage of the HAL, peripheral drivers, middleware and RTOSes

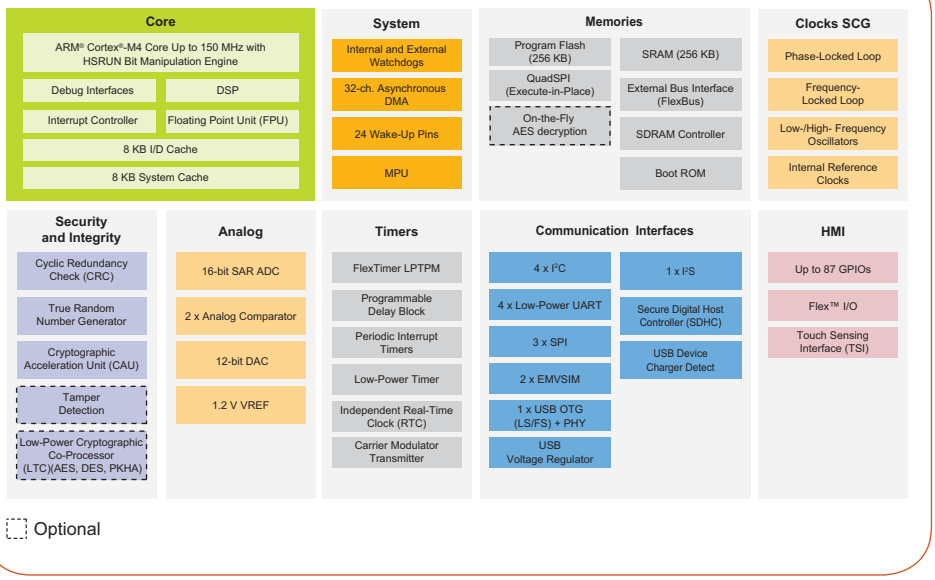
Processor Expert® software configuration tool

- Complimentary software configuration tool providing I/O allocation and pin initialization and configuration of hardware abstraction and peripheral drivers

Toolchain

- Atollic® TrueSTUDIO®
- IAR Embedded Workbench®
- ARM Keil® Microcontroller Development Kit
- SOMNIUM® DRT Cortex-M IDE
- Kinetis Design Studio IDE
  - No-cost integrated development environment (IDE) for Kinetis MCUs
  - Eclipse and GCC-based IDE for C/C++ editing, compiling and debugging

BLOCK DIAGRAM



Bootloader

- Common bootloader for all Kinetis MCUs
- In-system flash programming over a serial connection: erase, program, verify
- ROM-based bootloader with open-source software and host-side programming utilities

Development Hardware

- FRDM-K28F: Freedom development board
  - Low cost
  - Arduino® R3 compatible
- TWR-K80F150M: Tower® System modular development platform
  - Rapid prototyping and evaluation
  - Interchangeable modules
- TWR-PoS-K81: Point-of-sale (POS) development kit

STANDARD KEY FEATURES

Standard key features UART, I²C, I²S, SPI, 16-bit ADC, 12-bit DAC, timers, comparators, True RNG, CRC and GPIO	CPU	Memory	Packages	Comms	Security			
	ARM® Cortex®-M4 with Floating Point Unit (FPU)			USB Full-speed	Symmetric Crypto Accelerator (mmCAU)	256-bit AES/192-bit 3DES/public key Crypto Co-processor (LTC)	On-the-Fly 128-bit AES decryption from external Serial NOR	Anti-tamper
K80	150 MHz	256 KB Flash, 256 KB SRAM, 8 KB System + 8 KB I/D cache, XIP QuadSPI, SDRAM Controller	MAPBGA, LQFP	x	x			
K81				x	x	x	x	x
K82				x	x	x	x	

ADVANCED SECURITY ARCHITECTURE KEY FEATURES*

Products	Features	Benefit	Feature details
K80, K82, K81	Encrypted firmware updates boot ROM	Secure firmware update with built in ROM routines to reduce software overhead and complexity	• Firmware is encrypted by an AES 128-bit key • Fully supports internal flash security, including ability to mass erase or unlock security via the backdoor key • Multiple options for executing the bootloader either at system start-up or under application control at runtime • The ability to configure the QuadSPI interface is based on a configuration block located in the external QuadSPI
K80, K82, K81	Flash access control (FAC) configurable memory protection scheme designed to allow end users to utilize software libraries while offering programmable restrictions to these libraries	Protection of software IP	• Non-volatile control registers to set access privileges of on-chip flash resources • Supervisor or execute-only access can be set for up to 64 different segments
K82, K81	Hardware and software mechanisms for acceleration of symmetric cryptography and hashing functions	• Reduces CPU loading for cryptographic functions • Simplifies the implementation of higher level security functions nad network security standards • For firmware updates, hashing of firmware can be used with encryption keys to ensure that the firmware is trusted	• Hardware implementation of security operations symmetrical cryptography • Supports DES, 3DES, AES, MD5, SHA 1 and SHA 256 algorithms
K82, K81	Cryptographic co-processor for AES, DES and public key cryptography	• Offload CPU and reduced software footprint • Acceleration for RSA2048, ECDSA and ECDH reduces the latency for authentication	
K82, K81	On-the-fly AES decryption from external serial NOR flash	Easily secure off-chip firmware	Hardware module supporting AES128 counter mode decryptions on external flash data fetched by the QuadSPI
K81	Tamper detect module with up to eight tamper pins	Reduce external circuits needed to support anti-tamper mechanisms	• Secure key storage space with asynchronous erasure when external tamper events occur • Tamper detection for pin, temperature, voltage and clock, as well as active tamper
K81	Secure session RAM	Memory scratch pad for secure functions	RAM memory block designed for storage of sensitive information (such as encryption session keys) which is automatically cleared in the event of the detection of a tamper event

*Security features within the Kinetis K8x MCU family are incremental. For a full list of security features offered with Kinetis MCUs, visit: **www.nxp.com/security**.

www.nxp.com/Kinetis/Kseries

Document Number: KNTSK8XFS REV 4