Scalable Memory Expansion, Enhanced Security and Flexible I/O Capabilities

Kinetis K8x MCU Family

The K8x MCU family offers the security, scalability, and flexibility to address the challenges of creating smart devices for the Internet of Tomorrow.

TARGET APPLICATIONS

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

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

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

These advancements are done while maintaining a high level of compatibility with previous Kinetis devices. K8x MCUs are performance efficient and offer industry-leading low power while providing significant BOM savings through smart on-chip integration. The Kinetis K series is supported by a comprehensive set of development tools, software and enablement.

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. The initial K8x MCUs range in total flash space up to 256 KB and have 256 KB of SRAM. In addition to the embedded memory resources, the integrated QuadSPI interface supports connections to non-volatile memory (serial NOR), allowing developers to expand beyond the boundaries of a traditional MCU. With the extended memory resources and new security features, developers can safely and quickly enhance their embedded applications with greater capability.

KINETIS K8x MCU 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
- FlexI/O peripheral expands MCU capabilities by emulating serial, parallel, or custom interfaces using software drivers provided by the Kinetis SDK
- Low-power operation with dynamic currents down to 210 uA/MHz, state retention stop mode down to 5 uA with fast wake-up time and lowest power mode with only 330 nA
- Faster time to market with comprehensive enablement solutions, including SDK (drivers, libraries, stacks), IDE, ROM bootloader, RTOS, online community, and more

COMPREHENSIVE ENABLEMENT SOLUTIONS

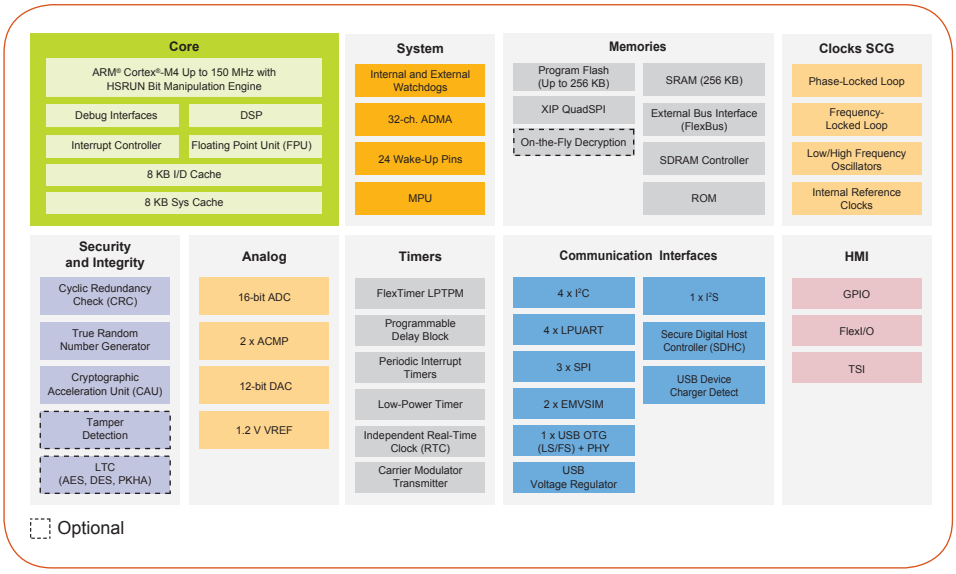
Kinetis Software Development Kit (SDK)

- Extensive suite of robust peripheral drivers, stacks and middleware, with new support for symmetric and asymmetric cryptographic acceleration
- Includes software examples demonstrating the usage of the HAL, peripheral drivers, middleware and RTOSes
- Operating system abstraction (OSA) for our proprietary MQX™ RTOS, FreeRTOS, and Micrium uC/OS kernels and baremetal (no RTOS) applications

Processor Expert Software Configuration Tool

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

KINETIS K8x MCU FAMILY BLOCK DIAGRAM



Integrated Development Environments (IDE)

- Atollic® TrueSTUDIO®
- IAR Embedded Workbench®
- ARM Keil® Microcontroller Development Kit
- 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
- Broad ARM ecosystem support through our Connect program partners

Proprietary MQX™ RTOS

- Commercial-grade MCU software platform at no cost with optional add-on software and support packages

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

- Tower System modular development platform
  - Rapid prototyping and evaluation
  - Low cost, interchangeable modules
- Freedom development platforms
  - Low cost (<$50 USD)
  - Arduino R3 compatible
  - mbed-enabled onselect boards
- TWR-K80F150M, FRDM-K82F, TWR-PoS-K81

KINETIS K8x MCUs: ADVANCED SECURITY ARCHITECTURE KEY FEATURES*

	Features	Benefit	Feature Details
K80	Encrypted firmware updates boot ROM	Secure firmware update with built in ROM routines to reduce software overhead and complexity	Firmware is encrypted by an AES128 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.
	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.
	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 and 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	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.	
	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.
	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 3