NuMicro® Family
M2351 Series
Product Brief

For additional information or questions, please contact: Nuvoton Technology Corporation.

www.nuvoton.com

1 INTRODUCTION

NuMicro® M2351 Series – *a TrustZone® empowered microcontroller series focusing on IoT security.*

The rise of the internet of things (IoT) era has increased awareness for the integration of the physical world into digital systems. While the efficiency improvements and economic benefits coming behind the digitization of our everyday lives, it has also placed pressure on system designers to deliver the innovative products capable of connecting and exchanging data incessantly. Since security and power consumption are the key requirements of IoT applications, Nuvoton NuMicro® M2351 series is excellence in supporting the proliferation of intelligent connected devices.

The NuMicro® M2351 microcontroller series is powered by Arm® Cortex®-M23 core with TrustZone® for Armv8-M architecture, which elevates the traditional firmware security to the new level of robust software security.

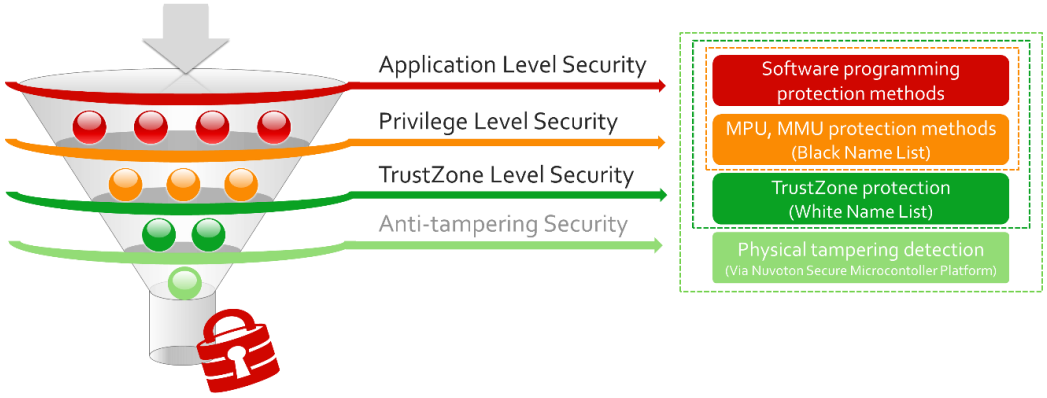

Figure 1-1 Design Concept of IoT Security Project

The low-power M2351 microcontrollers run up to 64 MHz with up to 512 Kbytes embedded Flash memory in dual bank mode, supporting secure OTA (Over-The-Air) firmware update and up to 96 Kbytes embedded SRAM. Furthermore, the M2351 series provides high-performance connectivity peripheral interfaces such as UART, SPI, I^2C, GPIOs, USB and ISO 7816-3 for smart card reader. Its secure and low-power features strengthen the innovation of IoT security.

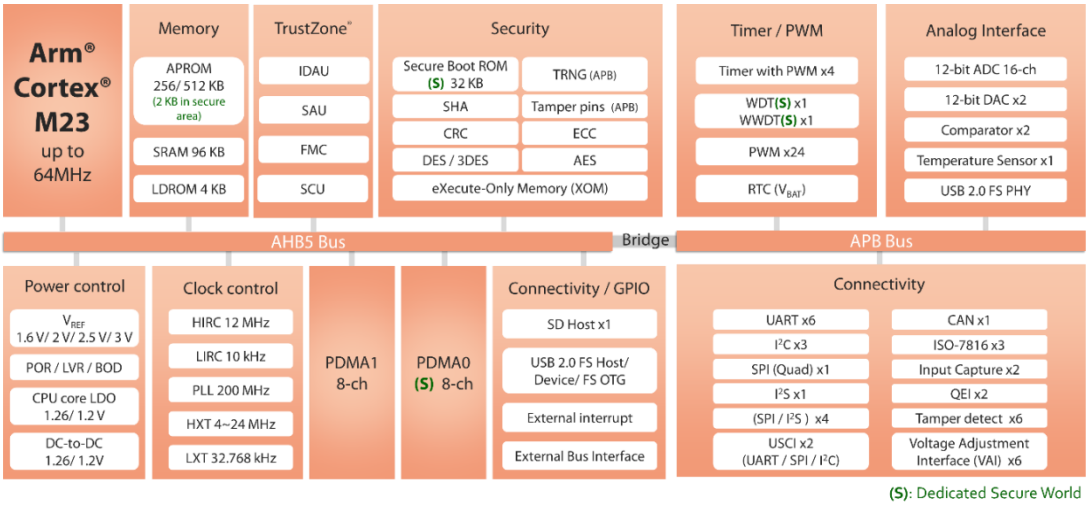

Figure 1-2 M2351 Series Block Diagram

TrustZone® for Arm®v8-M empowered

The NuMicro® M2351 series is empowered by Arm® TrustZone® for Armv8-M architecture. The TrustZone® technology is a System on Chip (SoC) and CPU system-wide approach to security. In addition to the firmware-level security, the M2351 series offers a more enhanced software-level security for more robust security and greater power efficiency.

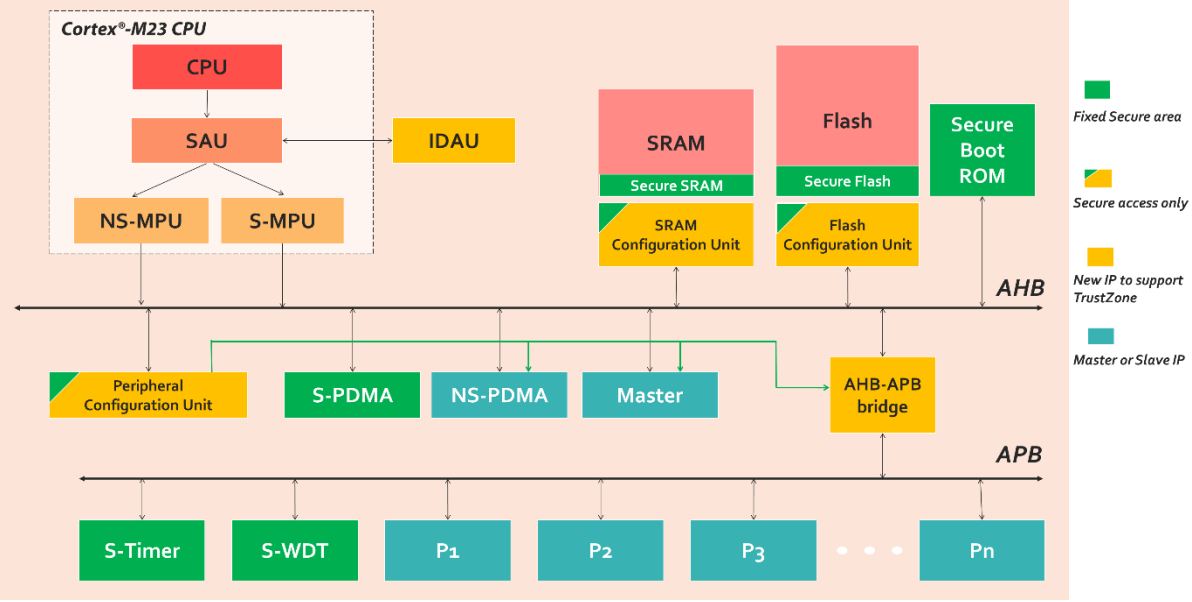

Figure 1-3 M2351 Series TrustZone® Architecture

In addition to the Cortex®-M23 core, the TrustZone® components of M2351 series include:

- Secure Attribution Unit (SAU, inside of Cortex®-M23 CPU)
- Implementation Defined Attribution Unit (IDAU)
- Flash Memory Controller (FMC)
- Security Configuration Unit (SCU, which supports SRAM and peripheral configurations)

As described in Figure 1-3, some functionalities are fixed to be secure attribution or secure resources accessible only for better software-level security assurance. Besides, other parts of the functionalities are designed to support TrustZone® implementation with bus master and bus slave IPs integration to realize the security functions.

Nuvoton Security Functions Strengthened

In addition to the TrustZone® technology, the NuMicro® M2351 series is also equipped with rich functions to improve system security. The Secure Bootloader supports trusted boot feature. The hardware crypto accelerators, including ECC, support encryption and decryption operations to offload the main processor's computing power. The KPROM is a password protection mechanism to allow Flash memory write and erase. The XOM defines execute-only memory regions to protect critical program codes. The Flash lock bits are designed to disable external Flash read/write and debug interface. Tamper detection pins can detect the state transition on the tamper pins.

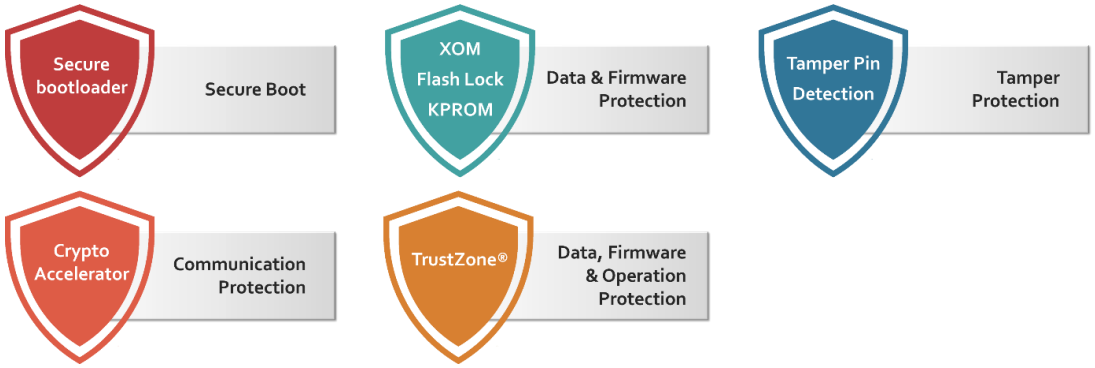

Figure 1-4 M2351 Series Security Functions

Low-Power Technology for IoT Innovation

Other than security, low power is also vital for IoT applications. Regarding the power consumption of the M2351 series, the normal run mode consumes 97 µA/MHz in LDO mode and 45 µA/MHz in DC-DC mode. The current consumption of Standby Power-down mode is 2.8 µA and the Deep Power-down mode without V_{BAT} is less than 2µA.

Feature / Power Consumption		Power Consumption			SRAM Data Retention		
		With SRAM Retention	Without SRAM Retention	Unit	System Bank 0	System Bank 1	Peripheral
Normal Run Mode (LDO)		96.8		µA/MHz	Yes		No
Normal Run Mode (DC-DC)		45.3		µA/MHz	Yes		No
Idle Mode (LDO)		36.0		µA/MHz	Yes		No
Idle Mode (DC-DC)		17.2		µA/MHz	Yes		No
Power-down Mode	Fast Wake-up Power-down Mode (FWPD)	128	107	µA	No		
	Normal Power-down Mode (PD)	40.3	20.2	µA	No		
	Low Leakage Power-down Mode (LLPD)	15.8	8.2	µA	No		
	Ultra Low Leakage Power-down Mode (ULLPD)	11.7	6.2	µA	No		
	Standby Power-down Mode (SPD)		2.8	µA	No		
	Deep Power-down Mode (DPD)		1.5	µA	No		
V_{BAT} supply for RTC		2.5		µA	No		

Table 1-1 M2351 Series Power Consumption Comparison

Arm® PSA with Nuvoton Secure Microcontroller Platform (NuSMP) Supported

The Platform Security Architecture (PSA) is a holistic set of threat models, security analysis, hardware and firmware architecture specifications, and an open source firmware reference implementation. The PSA is a contribution from Arm® to the entire IoT ecosystem, offering common ground rules and a more economical approach to building more secure devices.

Nuvoton has developed the Nuvoton Secure Microcontroller Platform (NuSMP) to support Arm® PSA. The NuSMP is a range of hardware and software mixture technologies for security requirements of general purpose and secure IoT microcontrollers. With NuSMP, developers can easily achieve the secure services with the M2351 series in coverage of: Trusted Boot (Root of Trust), Secure OTA (Over-The-Air) firmware update (including secure software download), Power Management APIs for non-secure world and PC side crypto related development software tool.

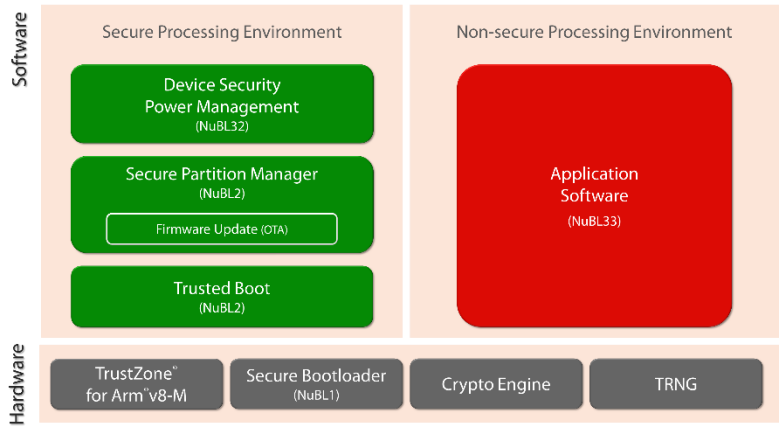

Figure 1-5 Nuvoton Secure Microcontroller Platform Architecture

The entire offering suite is constructed in compliance of Chain of Trust (CoT) with several secure booting layers named NuMicro® Boot Loader 1 (NuBL1, hardware level), Boot Loader 2 (NuBL2 first software level including trust boot code and memory partition manager with OTA update feature), Boot Loader 32 (NuBL32, for Secure World), and Boot Loader 33 (NuBL33, for Non-Secure World). With the CoT guarantee, all services and software tool can support most security requirements for MCU applications.

Easy to develop, easy to implement

Being committed to providing an easy development experience, Nuvoton offers a wealth of resources to work with the M2351 series. For compiler selection, the M2351 series supports the development on Arm® Keil MDK, IAR Embedded Workbench for Arm M2351 series m and GCC. Furthermore, the Keil MDK Nuvoton Edition for M2351 series is free to use. For supporting tools, the M2351 series offers considerate tools to aid the project progress. For example, the TrustZone Template Generator could assist the security state planning and the secure firmware building; the CryptoTool could support the cryptographic requirements of M2351 series, including key generation, key exchange, signature, encryption and decryption. For security project developing, Nuvoton offers integrated security technologies, NuSMP (Nuvoton Secure Microcontroller Platform). The application note, sample code and training videos for each technology would be available for developers to access and reference. Lastly, the Arm® Mbed OS for IoT solutions and the Segger emWin for interactive interfaces are both supported in the M2351 series.

Figure 1-6 Multiple Support Resources of M2351 Series

Security Features

- Arm® Cortex®-M23 TrustZone® Technology
- 8 regions MPU_NS (for non-secure world)
- 8 regions MPU_S (for secure world)
- 8 regions Security Attribution Units (SAU)
- Implementation Defined Attribution Unit (IDAU)
- 2 KB OTP ROM with additional 1KB lock bits
- Hardware Crypto Accelerators
- CRC calculation unit
- Up to 6 tamper detection pins
- 96-bit Unique ID (UID), 128-bit Unique Customer ID (UCID)
- Arm® Platform Security Architecture (PSA) and Trusted Base System Architecture-M (TBSA-M) supported

Applications

- IoT Devices with Secure Connection
- Collaborative Secure Software Development Business Model
- Fingerprint Card, Fingerprint Lock
- Smart Home Appliance
- Smart City Facilities
- Wireless Sensor Node Device (WSND)
- Auto Meter Reading (AMR)
- Portable Wireless Data Collector
- Digital Currency Authentication
- Trusted Execution Environment (TEE) with Trusted Applications (TAs)

2 FEATURES

- **Security Core**
  - Arm® Cortex®-M23 core delivering 0.95 DMIPS per MHz
  - TrustZone® for ARM®v8-M
  - 32-bit Single-cycle hardware multiplier and 32-bit 17-cycle hardware divider
  - Up to 8 regions MPU_NS (for non-secure world)
  - Up to 8 regions MPU_S (for secure world)
  - 8 Security Attribution Unit (SAU) memory regions
- **Operating Characteristics**
  - Running up to 64 MHz
  - Voltage range: 1.7V to 3.6 V
  - Temperature range: -40°C to +105°C
  - Selectable core power voltage levels: 1.26V, 1.2V in run and idle mode
- **Memories**
  - Up to 512 KB of dual bank Flash memory. Dual bank Flash memory allows read-while-write programming
  - Up to 96 KB SRAM, first 32KB SRAM with hardware parity check
  - 4 KB Flash for user program loader (LDROM)
  - 2 KB OTP for general-purpose control use, (2 KB data + 1 KB lock bit) easy for PLM (Product Lifecycle Management) implementation
  - 32 KB Secure Boot ROM
  - ISP/ICP/IAP programming
  - External Bus Interface (EBI) supports maximum external address space of 1 M Bytes, up to 3 chip selects and 8/16-bit external data bus
- **Clocks**
  - 4 to 24 MHz crystal oscillator
  - 32 kHz oscillator for RTC
  - Internal 12 MHz RC oscillator (variation < ±2% at -40 ℃~105℃)
  - Internal 10 kHz RC with calibration
- **Power management**
  - Normal run: 97 µA/MHz (LDO); 45 µA/MHz (DC-DC)
  - Idle: 36 µA/MHz (CPU clock disabled, LDO); 17µA/MHz (CPU clock disabled, DC-DC)
  - Power-down: 20 µA
  - Standby power-down: 3.0 µA
  - Deep Power-down: 4.0 µA (with V_{BAT})
  - Deep Power-down: 1.5 µA (without V_{BAT})
  - V_{BAT} supply for RTC: 2.5 µA (80 bytes spare registers)
- **Timers**
  - Four 24-bit timers (Timer0~3), with up to 8 PWM complementary channels
  - Twelve 16-bit timers (PWM0~1) with up to 12 enhanced PWM channels
  - Two 16-bit timers(BPWM0~1), with up to 12 PWM channels,
  - Three 24-bit timers for smart card with ISO 7816-3
  - Two 24-bit SysTick timer: One is secure system timer and the other is Non-secure system timer
  - Two watchdog timers: independent and window
- **PDMA controller**
  - Two 8-ch PDMA controllers; PDMA0 is fixed to be secure PDMA and PDMA1 can be configured as secure or Non-secure PDMA.
- **Crypto and Security**
  - True random number generator (TRNG)
  - AES 256/ SHA 384/ 3-DES/ DES
  - The ECC accelerator is a fully compliant implementation for the prime field GF(p) and binary field GF(2^m) algorithms. The prime field GF(p) supports up to NIST P-521. The binary field GF(2^m) supports up to NIST B-571 and NIST K-163, K-233, K-283, K-409 and K-571.
  - CRC calculation unit
- **Analog**
  - One 12-bit, 3.76M SPS at 64MHz SAR ADC (with 6 fast channels, total up to 16 channels)
  - Two 12-bit, 1M SPS DACs
  - Two rail-to-rail comparators (CMP)
- **Communication interfaces**
  - Up to 11 UART interfaces (up to 10.66 MHz), with up to 3 ISO-7816-3 interfaces, 6 RS-485, 6 IrDA and 2 LIN interfaces
  - Up to 5 I^2C interfaces (up to 1 Mbps), with up to 3 I^2C with SM Bus/ PM Bus
  - Up to 7 SPI interfaces (up to 64 MHz), with 4 I^2S interfaces, additional 1 Quad-SPI interface
  - Up to 5 I^2S interfaces, 4 I^2S shared with 4 SPI
  - Secure Digital I/O (SDIO)(up to 50 MHz)
- **Advanced connectivity**
  - USB 2.0 full speed OTG controller with on-chip PHY
  - One CAN interface up to 1 Mbps (CAN 2.0A and 2.0B standard)
  - Support crystal-less
- **Motor interfaces**
  - Up to 2 quadrature encoder interfaces (QEI)
  - 2 input capture timers (ECAP)
- **Voltage Adjustable Interface**
  - Up to 6 I/O pins support VAI with supply V_{DDIO} from 1.7 to 3.6 V
- **Up to 80 I/O with interrupt capability**
  - 5V input tolerant I/O except analog pins
- **RTC with independent power domain with Calendar and Alarm including 80 bytes spare registers**
- **Up to 6 tamper detection pins**
- **96-bit Unique ID (UID)**
- **128-bit Customer ID (UCID)**
- **IEC-61967 compliant**
- **Packages (RoHS)**
  - LQFP 128-pin / 64-pin
  - QFN 33-pin
  - WLCSP 49

3 PARTS INFORMATION

3.1 M2351 Series Selection Code

M23	51	S	I	A	A	E
Core	**Line**	**Package**	**Flash**	**SRAM**	**Rev.**	**Temperature**
Cortex®-M23	**51:** Performance Line	**C:** WLCSP49 (3.2x3.2 mm) **Z:** QFN33 (5x5 mm) **S:** LQFP64 (7x7 mm) **K:** LQFP128 (14x14 mm)	**I:** 512 KB **G:** 256 KB **E:** 128 KB	**C:** 128 KB **A:** 96 KB **8:** 64 KB **6:** 32 KB		**E:** -40°C~105°C

Table 3-1 M2351 Series Selection Code

3.2 M2351 Series Selection Guide

PART NUMBER		M2351			
		ZIAAE	CIAAE	SIAAE	KIAAE
Flash (KB)		512	512	512	512
SRAM (KB)		96	96	96	96
ISP Loader ROM (KB)		4			
I/O		25	41	51	107
32-bit Timer		4			
Tamper		-	-	1	6
RTC		√			
Connectivity	LPUART	6			
	ISO-7816	3			
	Quad SPI	1			
	SPI/I²S	3	3	4	4
	I²S	1			
	I²C	3			
	USCI (UART/I²C/ SPI)	2			
	CAN	1			
	LIN	2			
	SDHC	1	2	2	2
Crypto	TRNG	√			
	DES / 3-DES / AES	√			
	ECC	√			
	SHA	√			
16-bit Enhanced PWM		12			
16-bit Basic PWM		12			
QEI		1	2	2	2
ECAP		-	1	1	1
USB 2.0 FS OTG		√			
12-bit ADC		10	12	16	16
12-bit DAC		2			
Analog Comparator		1	2	2	2
Cryptography		√			
External Bus Interface		-	√	√	√
Package		QFN 33	WLCSP 49	LQFP 64	LQFP 128

Table 3-2 NuMicro® M2351 Series Selection Guide

4 REVISION HISTORY

Date	Revision	Description
2018.08.31	1.00	Initial release

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.