0x5 HEX–Five Security

RA Ecosystem Partner Solution

MultiZone® Secure IoT Firmware

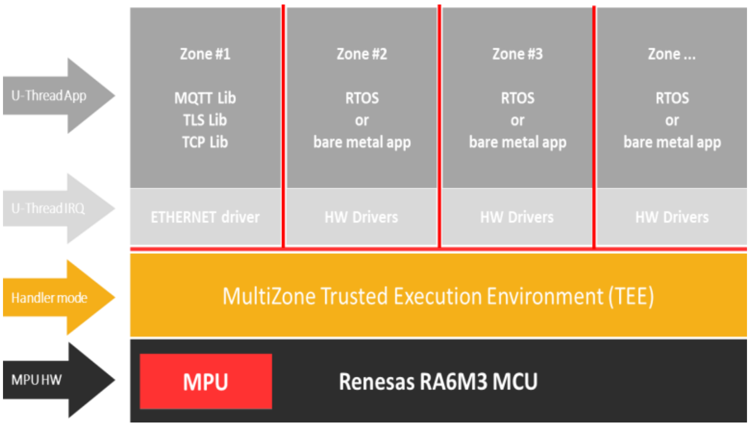
Solution Summary

The MultiZone® IoT Firmware is the quick and safe way to build secure IoT applications with RA6M3 microcontrollers. It provides secure access to IoT clouds, real-time monitoring, secure boot, and remote firmware updates. The built-in Trusted Execution Environment provides hardware-enforced separation to shields the execution of trusted applications from untrusted 3rd party libraries.

Features/Benefits

- Fully integrated with Renesas e^2 Studio and FSP (Flexible Software Package)
- Safe and quick way to add high-grade security and separation – up to 4 “secure worlds”
- Rapid development: pre-integrated TEE, TLS/ECC, TCP/IP, MQTT, RTOS, FSP
- Easy retrofit of existing hardware and software - no need for a system redesign
- Convenient MPU-based alternative to an Arm® TrustZone® upgrade
- Convenient software license priced per design – no royalties, no GPL contamination

Block Diagram



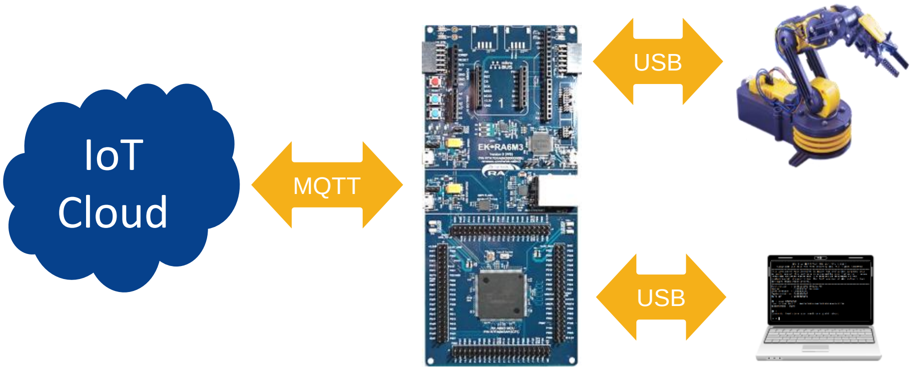
Hardware-Grade Security

Rapid Development

Easy Integration

Target Applications

- IoT
- Healthcare
- Meter
- Industrial
- Connectivity
- Building Automation



Reference Application on EK-RA6M3

__MultiZone__ is a registered trademark of Hex Five Security, Inc. - Patent pending US 16450826, PCT US1938774

2020.10

Technical Specs

IDE	▪ MultiZone IoT Firmware: MQTT, TLS, TCP/IP, RTOS, TEE, robot, terminal	
▪ Renesas e^2 Studio 7.8.0	▪ MultiZone SDK: TEE, USB Robot, uart terminal, bare metal buttons & leds	
▪ Hex Five's reference projects	▪ MultiZone Blinky: TEE, uart terminal, bare-metal buttons & leds	
	▪ MultiZone Minimal: TEE, 4 zones available for user applications	
FSP	▪ USB – optional, required for the robotic arm app	120KB
▪ Renesas FSP 1.1.0	▪ UART – optional, required for the MultiZone terminal app	32KB
▪ Hex Five's USB patch	▪ Ethernet – optional, required for MQTT / TLS access to cloud services	
TCP/IP library	▪ IP, ICMP, UDP, TCP, ARP, DHCP, DNS, SNTP, MQTT	40KB
▪ LWIP 2.1.1	▪ Light weight single threaded execution	16KB
▪ Hex Five security patches	▪ Fully integrated with SSL stack	
SSL library	▪ TLSv1.2, Cipher TLS_AES_128_GCM_SHA256	64KB
▪ mbed TLS 2.23.0	▪ ECC: prime256v1, Private Key NIST CURVE: P-256	32KB
▪ Hex Five secure configuration	▪ Mutual authentication, Cert expiration verification, TLS large fragment	
Real Time OS (optional)	▪ Secure unprivileged execution of kernel, tasks, and interrupt handlers	32KB
▪ FreeRTOS 10.3.0	▪ No memory shared with TCP/IP and SSL library code	16KB
▪ Hex Five integration with TEE	▪ No memory shared with other applications running in separate zones	
Trusted Execution Environment	▪ 4 separated Trusted Execution Environments (zones) enforced via MPU	4KB
▪ MultiZone Security TEE 2.0	▪ 8 memory-mapped resources per zone – i.e. ram, rom, i/o, uart, gpio, eth, …	4KB
▪ RA6M3 optimizations	▪ Secure inter-zone messaging – no shared memory, no buffers, no stack, etc	
	▪ Protected user-mode interrupt handlers mapped to zones – up to 128	

Use Cases

Secure access to private or public clouds

✓ Customer needs MQTT, TLS, ECC, mutual authentication optimized for MCU devices	▶ **MultiZone** provides built-in secure connectivity to commercial cloud providers like AWS, Azure, etc
✓ Customer is concerned about backdoors and lack of separation in 3rd party software	▶ **MultiZone** provides four separated execution environments, hardware enforced, software defined
✓ Customer can't afford time, cost and the technology risk of a complete system redesign	▶ **MultiZone** can retrofit existing hardware and software, works out-of-the-box, and it is available now

Remote device provisioning and firmware updates

✓ Product must comply with new IoT regulation requiring remote firmware updates - OTA	▶ **MultiZone** provides high-grade security OTA updates via open standard MQTT and TLS protocols
✓ Customer is concerned about time, cost, and security risk of developing a DIY solution	▶ **MultiZone** is commercial-grade, available immediately, and built from the ground up for security
✓ Customer is concerned about the vendor lock-in inherent in commercial cloud services	▶ **MultiZone** remote firmware updates work with any commercial or private IoT cloud

Safety critical applications

✓ Product must comply with safety critical regulations – i.e. medical devices, automotive	▶ **MultiZone** guarantees non interference and spatial and temporal separation of programs
✓ Customers needs to shield critical functionality from 100's of KB of untrusted 3rd party sw	▶ **MultiZone** provides high-grade security and separation for up to 8 execution environments
✓ Customer looking for low-cost alternatives to proprietary RTOS and hypervisors	▶ **MultiZone** offers a simple convenient license priced per customer's design – no royalties

__MultiZone__ is a registered trademark of Hex Five Security, Inc. - Patent pending US 16450826, PCT US1938774