RENESAS RA FAMILY

FEATURES FOR IOT

AUGUST 2022
DIEGO MORENO
RENESAS ELECTRONICS

RENESAS RA FAMILY OVERVIEW

RENESAS RA FAMILY SERIES LINE-UP

Series	Performance Range	Series Indicators	Series Memory Ranges	ASSP Extensions
Under development **RA8**	More than 240MHz	Highest Performance, HMI, Connectivity, Security, Analog	Highest Memory integration: **2MB** Flash, 1MB SRAM	HMI Motor/Inverter AI/ML
RA6	Up to 240MHz	Advanced performance, connectivity, Security and scalable	High memory integration: up to **2MB** Flash, 640kB SRAM	Motor/Inverter Wireless HMI AI/ML
RA4	Up to 100MHz	Excellent power high performance mix paired with Security	Medium memory integration: up to **1MB** Flash,128kB SRAM	Sensor Wireless Motor
RA2	Up to 60MHz	Low power	Small memory integration: **256kB** Flash, 32kB SRAM	Rich Analog Sensor

DO YOU NEED SECURITY?

SECURITY TOUCHES EVERYTHING

- Connected
- Upgradable
- Valuable information

Energy grid | Retail | Environmental | Home automation | Healthcare

Smart city | Building automation | Farming | Identity & tracking | Connected clothing | Appliances

Robotics | Sensors | Industrial | IoT | Smart lighting | Smart watch

HARDWARE SECURITY FEATURES

THE SECURE CRYPTO ENGINE (SCE)

The SCE is a subsystem managed and protected by dedicated control logic

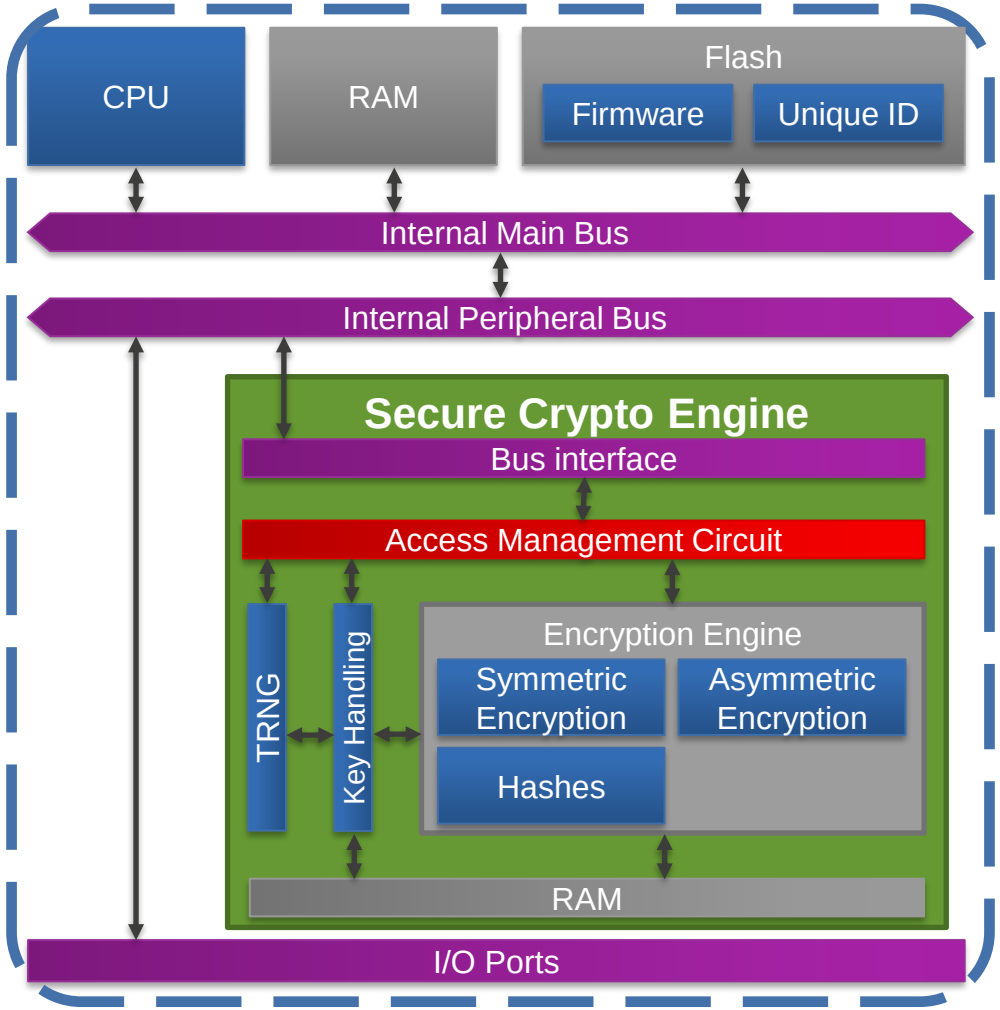
- A provided software driver handles the proper access sequence
- Improper access via the CPU or debugger locks the SCE Access Management Circuit until device reset

Crypto operations are physically isolated

- Dedicated SCE RAM
- No exposure of plaintext keys on any CPU-accessible bus

Advanced key handling capabilities

- Application keys are wrapped with the MCU unique HUK
- Wrapped keys enable simple, unclonable, secure storage
- Secure key installation mechanism



FLASH ACCESS WINDOW
RA FAMILY MCUs WITH CORTEX-M23 AND M4 CORES

The Flash Access Window (FAW) creates regions of write-once flash

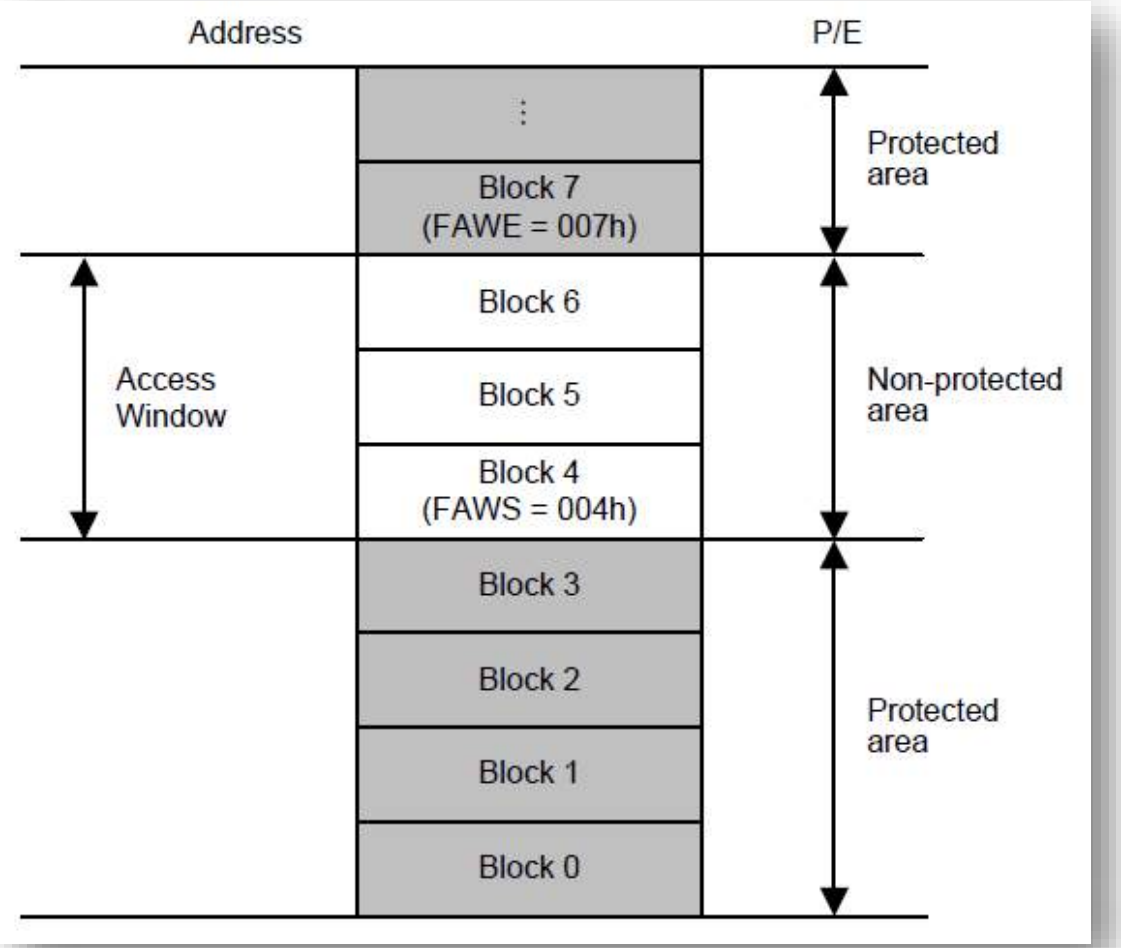
- The FAW start and end addresses (AWS.FAWS and AWS.FAWE) define the area of flash that is not protected
- All other flash is protected

Protection can be temporary or permanent

- Set with the AWS.FSPR bit
- Temporary protection is used for development
- Permanent protection is recommended for production

Use the FAW to protect permanent assets

- Create an immutable bootloader
- Store permanent root keys and certificates



FLASH BLOCK PROTECTION
RA FAMILY MCUs WITH CORTEX-M33 CORE

Block Protect creates regions of write-once flash

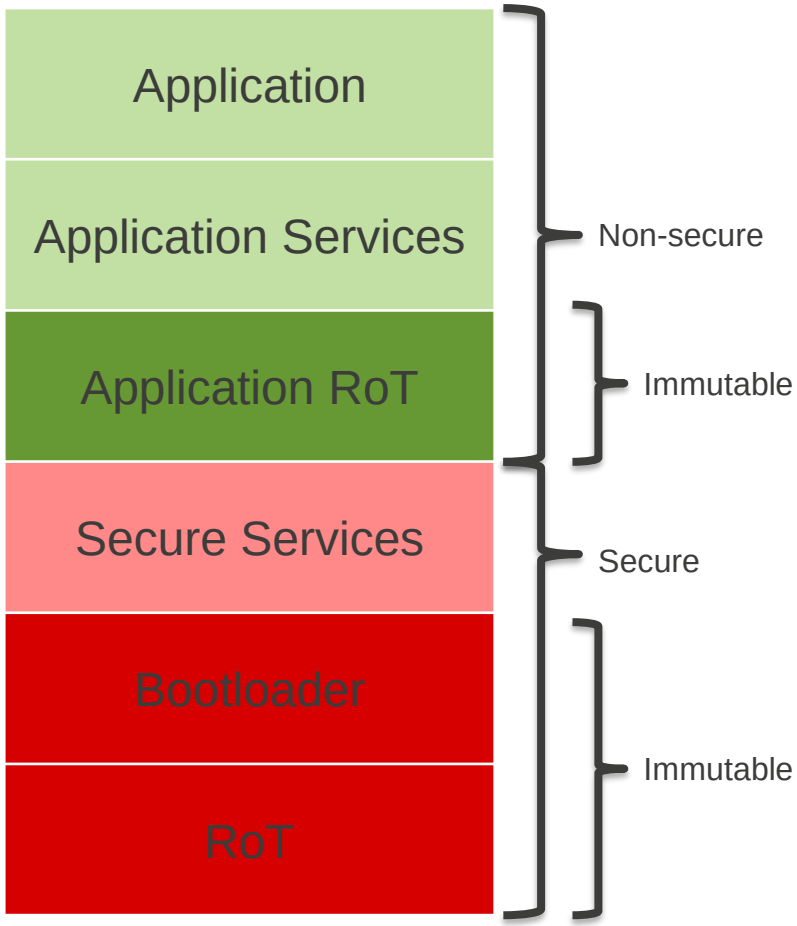
- Each flash block is set individually (8K/32K)
- Separate registers for protecting secure and non-secure flash regions

Protection can be temporary or permanent

- Temporary protection is used for development
- Permanent protection is recommended for production

Use Block Protect to protect permanent assets

- Create an immutable bootloader
- Store permanent root keys and certificates



Available on Renesas RA Family Cortex-M33 MCUs

TIME-STAMPED TAMPER DETECTION

USING THE TIME CAPTURE EVENT INPUT PINS OF THE RTC

Up to three “tamper pins” (package-dependent)

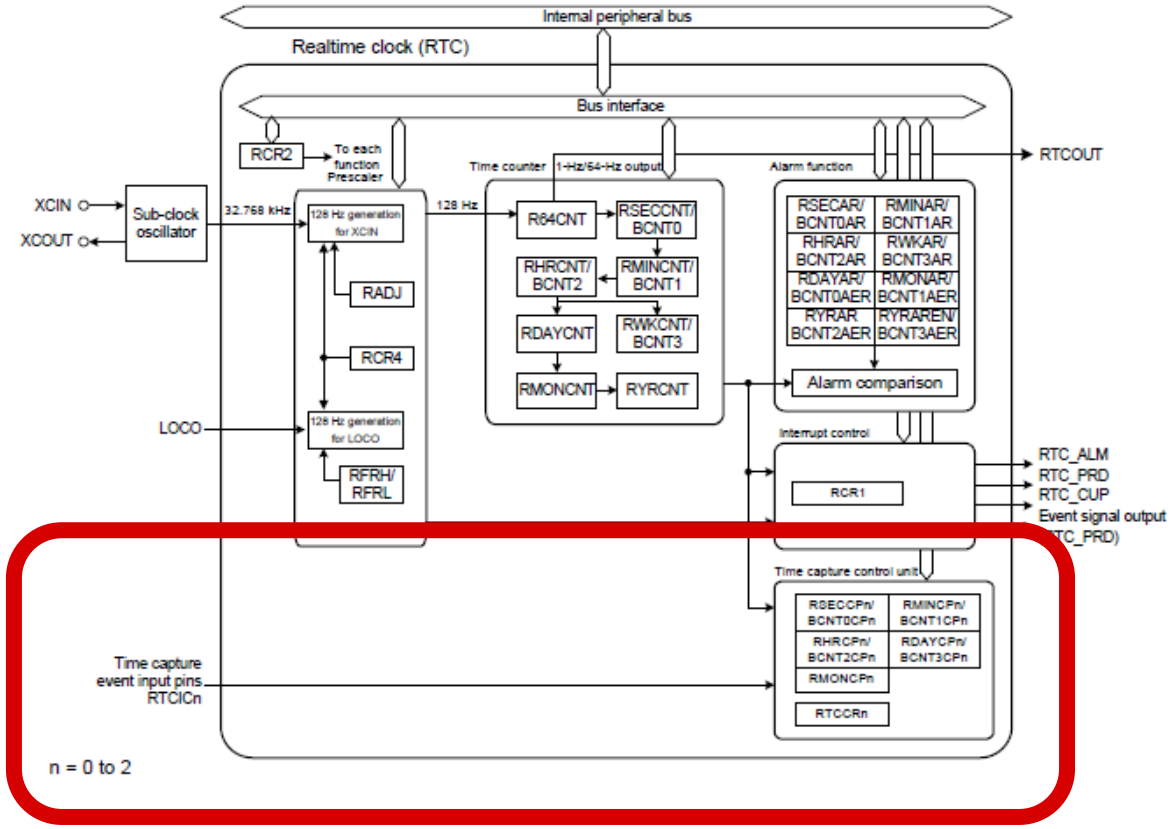
- When the pin is triggered, the current time is stored
- Pin can be triggered on falling edge, rising edge, or both

Time-stamp values are not cleared on reset

- Time stamp can be read even if attack resets the device

RTC can operate in all power modes

- Enables tamper detection as long as power is available
- VBATT support



WHAT IS TRUSTZONE?

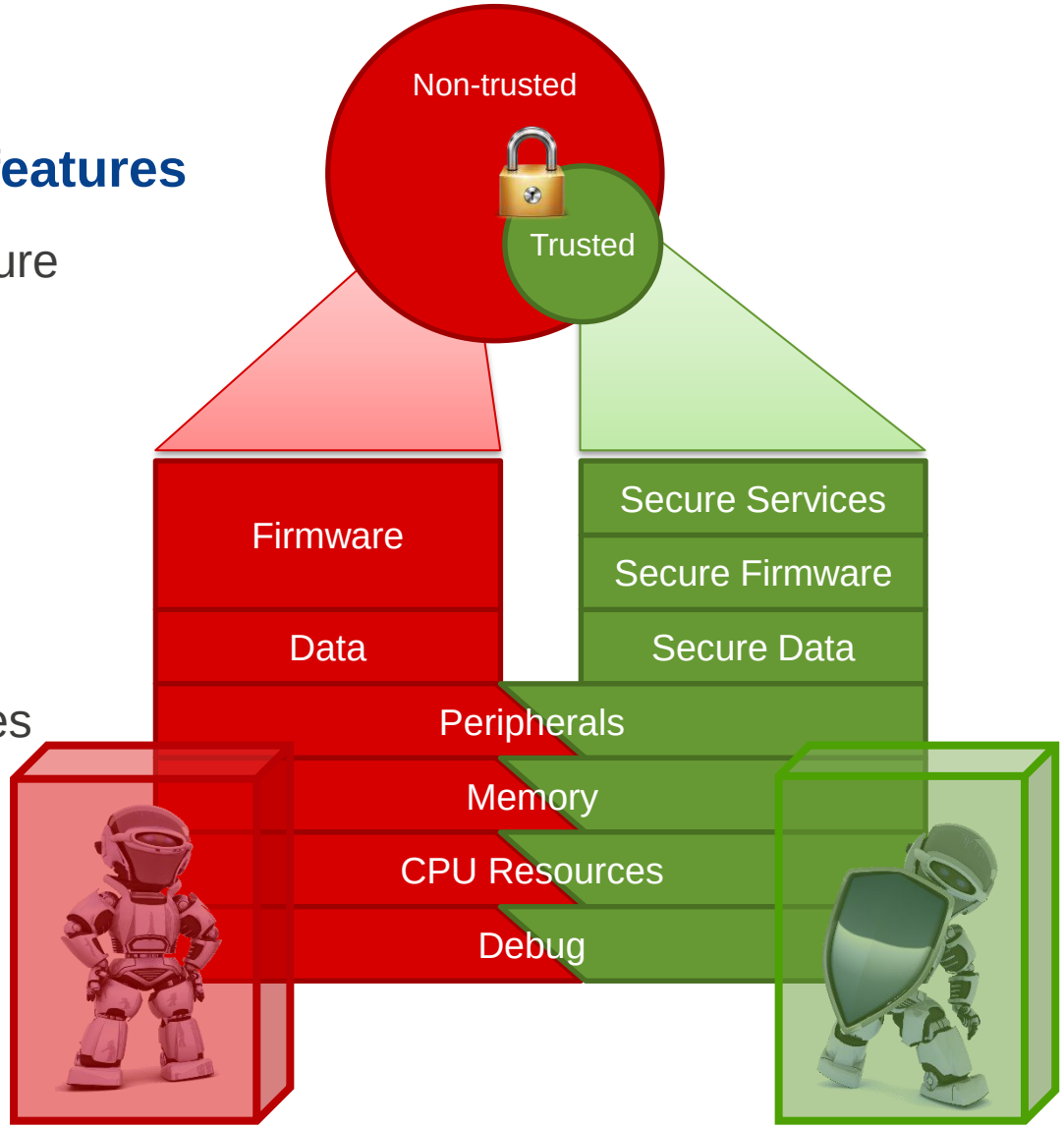
TrustZone is hardware-enforced separation of MCU features

- Introduced into Cortex-M devices with the Arm-v8M architecture
- Enables the creation of a protected environment

Capabilities can be split into two regions

- Secure world (SPE) - Trusted firmware and services
- Non-secure world (NSPE) - Non-trusted firmware and services

SPE Services can be called by the NSPE



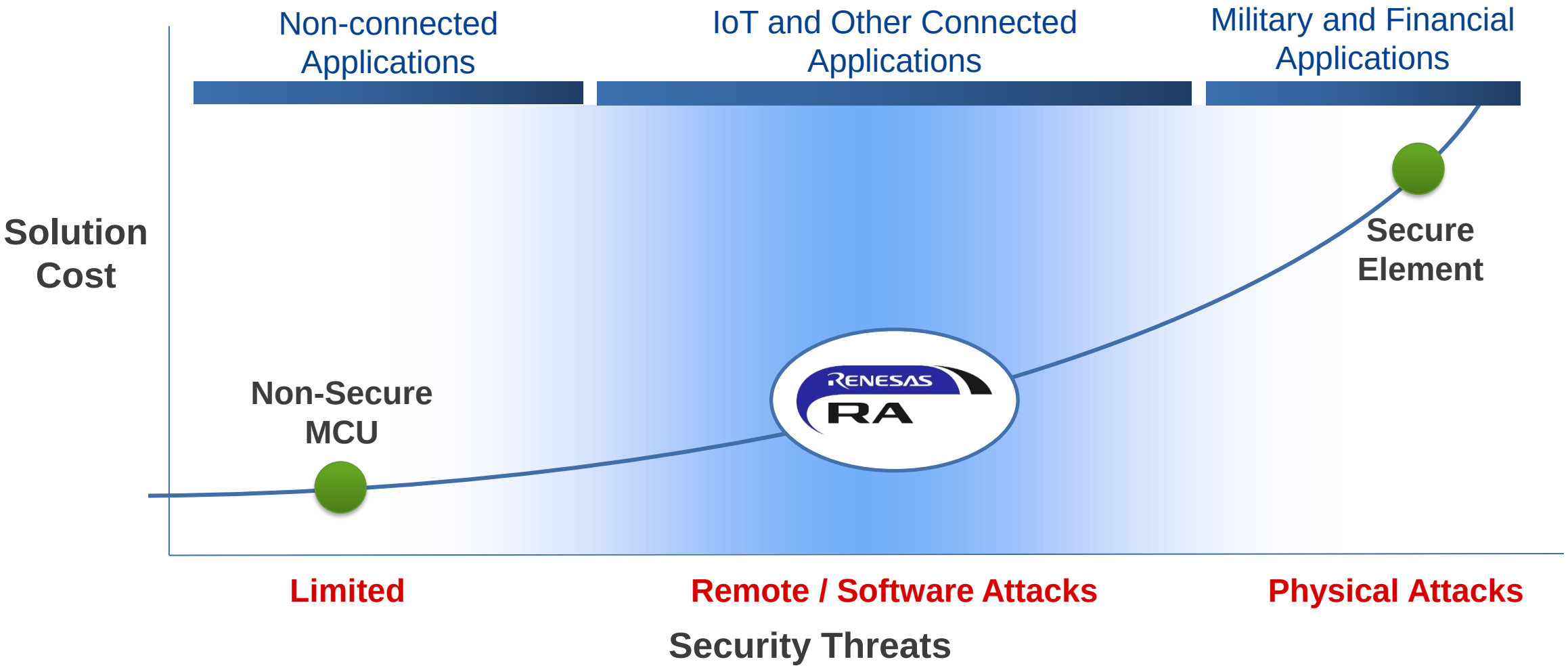
RA FAMILY HARDWARE PROTECTION FEATURES

Functions	RA8 Series	RA6M4, RA6M5 RA4M2, RA4M3	RA6M1, RA6M2, RA6M3, RA6T1	RA6T2	RA6E1 RA4E1	RA4M1, RA4W1	RA2 Series
Identity	Coming soon!						
Chip Unique ID		128-bit	128-bit	128-bit	128-bit	128-bit	128-bit
Isolation							
Flash and RAM		Arm TrustZone®	Security MPU	Arm TrustZone®	Arm TrustZone®	Security MPU	Security MPU
Peripherals		TrustZone, Bus Master MPU	Bus Master/Slave MPUs	TrustZone, Bus Master MPU	TrustZone, Bus Master MPU	Bus Master/Slave MPUs	-
Pins		Arm TrustZone	-	Arm TrustZone	Arm TrustZone	-	-
Arm Core MPU		S and NS	Y	S and NS	S and NS	Y	Y
Crypto Engine		SCE9	SCE7	SCE5_B	-	SCE5	-
Key Handling							
Secure Key Installation		Programmer, FSP	FSP(1)	FSP(1)	-	FSP(1)	-
Secure Key Storage		Wrapped w/ 256-bit HUK	Wrapped	Wrapped w/128-bit HUK	-	Wrapped	-
Plaintext Key Support		Y	Y	Y	-	Y	Y
Integrated Wrapped Key Support		Y	Y	Y	-	Y	-
Code Protection and Lifecycle							
Flash Program/Erase Protection		Per Block	Window	Per Block	Per Block	Window	Window
Code Encryption		-	-	-	-	-	-
Advanced DLM		Y	-	Y	Y	-	-
Debug and Program I/F Protection		Authentication w/key	Unlock ID Code	Authentication w/key	Authentication w/key	Unlock ID Code	Unlock ID Code
Physical Protection							
Tamper Pins		3	3	3	3	3	-
SPA/DPA Resistance		Included	Under evaluation	-	-	-	-

(1) FSPv4.0.0

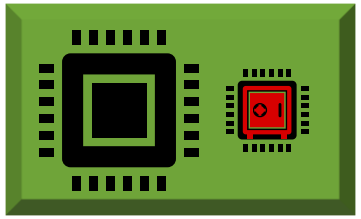
CERTIFICATIONS

COST VERSUS NEED

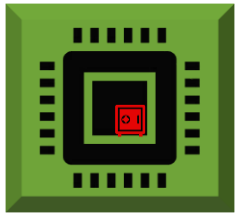


DETACHED VERSUS INTEGRATED SECURITY

MCU with Secure Element

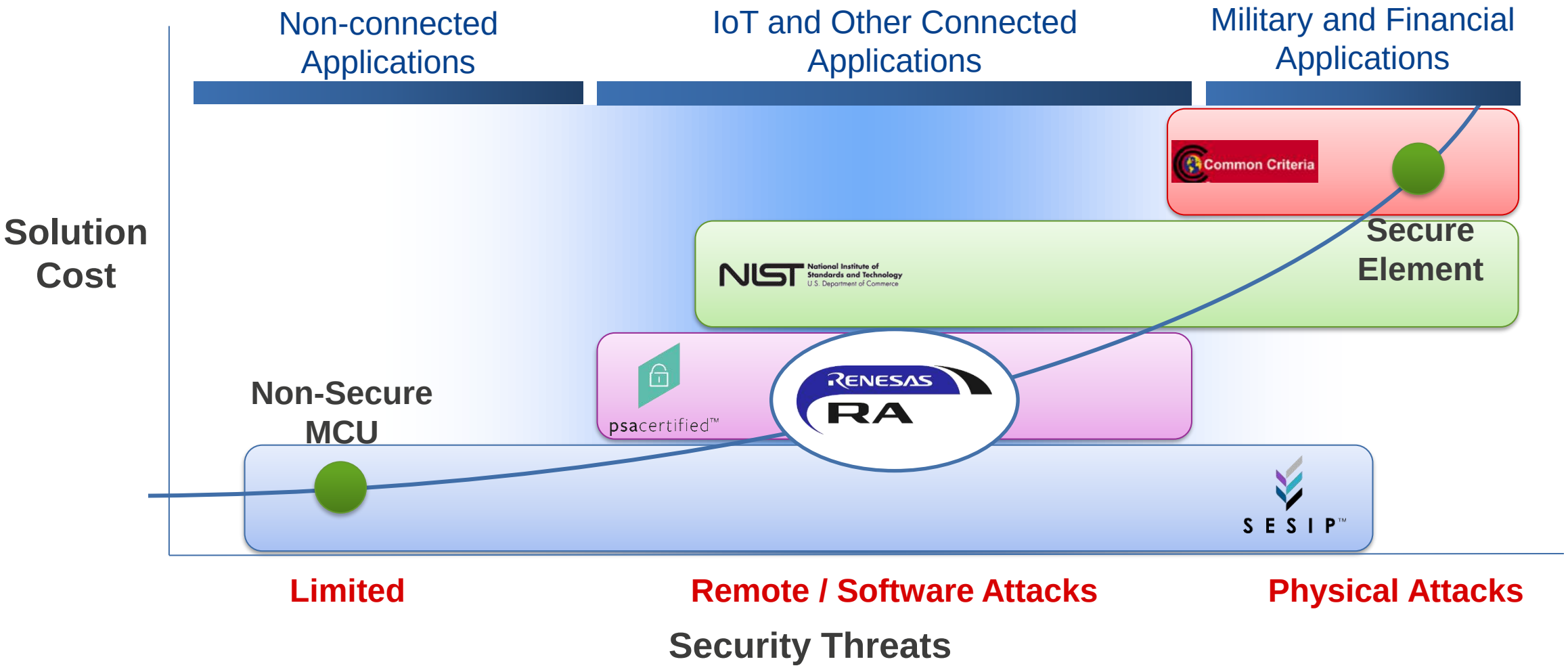


MCU with Integrated Crypto Engine



Feature	Secure Element	Integrated Crypto Engine
Identity	Secure Factory Provisioning	Factory or Field Provisioning, or MCU Unique ID
High-speed encrypted comms	Serial bus limited – MCU receives and processes the data, but SE has the keys to encrypt/decrypt	No bus limitation, no extra data movement
Low Power	Two devices	Single device
Low Cost	Two devices	Single device
Upgradeable	Sometimes, and must be updated separately via the MCU	Yes, with main application
Flexible	Only specific algorithms, fixed number of keys	Algorithms can be added easily, unlimited key storage
Certifications	Often NIST CMVP (FIPS 140-2) or CC	NIST CAVP

CERTIFICATION VERSUS APPLICATION



RA FAMILY CERTIFICATIONS AND EVALUATIONS

- Achieved
- In process
- Planned

Certification or Evaluation	RA6M5	RA6M4	RA6M3	RA6M2	RA6M1	RA6T2	RA6T1	RA6E1	RA4M3	RA4M2	RA4M1	RA4W1	RA4E1	RA2A1	RA2E1	RA2E2	RA2L1
PSA Certified Level 1	Achieved	Achieved	Achieved	Achieved	Achieved		Achieved		Achieved	Achieved							
PSA Certified Level 2		Achieved															
SESIP1		Achieved	Achieved							Achieved							
NIST CAVP SCE7			Achieved	Achieved	Achieved		Achieved										
NIST CAVP SCE9	Achieved	Achieved							Achieved	Achieved							
NIST FIPS 140-3		Planned															
SP800-22 TRNG	Achieved	Achieved	Achieved	Achieved	Achieved	In process	Achieved	Achieved	Achieved	Achieved	Achieved	Achieved	Achieved	In process	Achieved	Achieved	In process

SOFTWARE AND SOLUTIONS

MCUBOOT
SECURE BOOTLOADER FOR ALL RA FAMILY MCUs

MCUboot support is included in the FSP for all RA Family MCU Groups

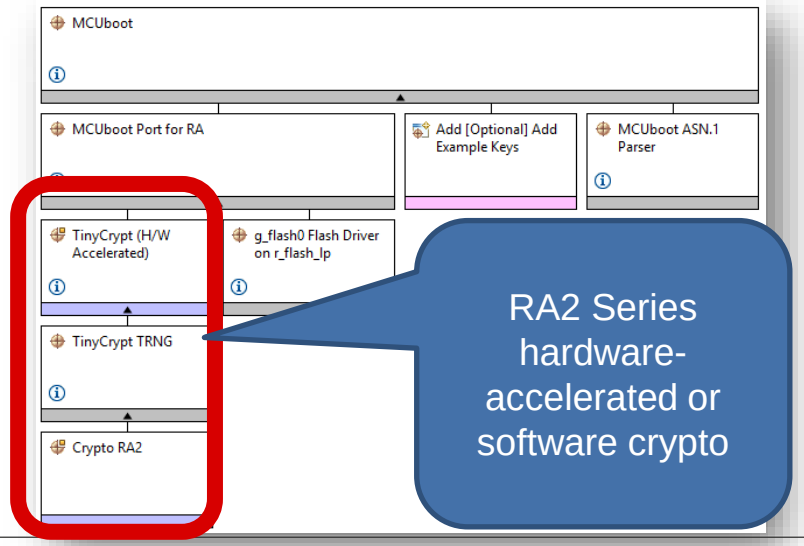
- Supports TrustZone and non-TrustZone use cases

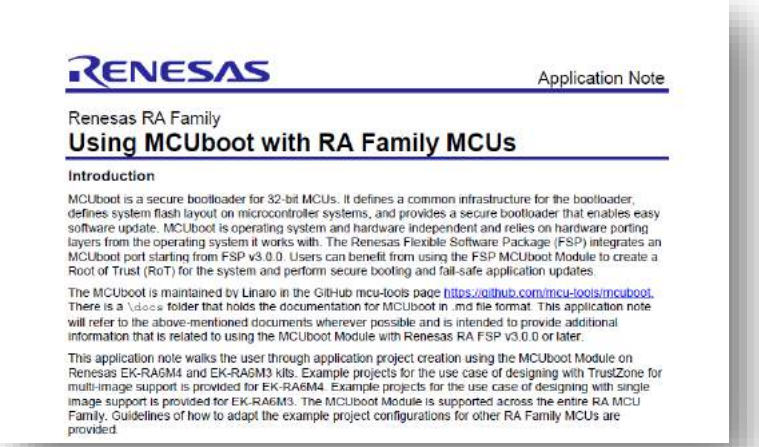
Supports hardware-accelerated cryptography

- SCE9 Protected Mode and Compatibility Mode support

Application Projects are available

- RA6M3 and RA6M4 (applicable to all RA6Mx MCU Groups)
- RA2 Series with optimisation guide





RENESAS Application Note

Renesas RA Family

Using MCUboot with RA Family MCUs

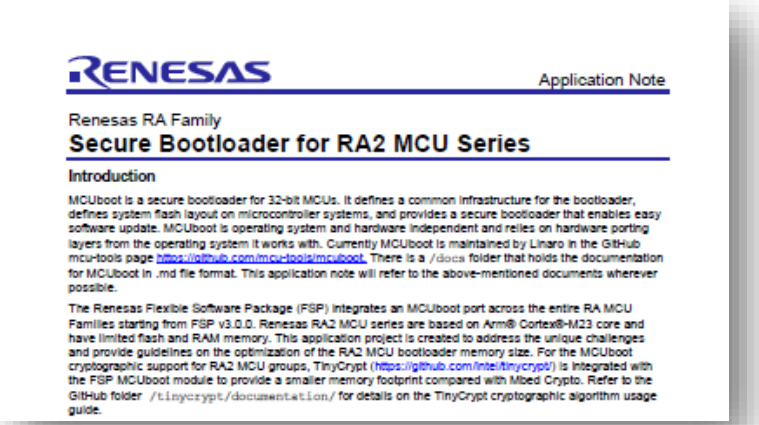
Introduction

MCUboot is a secure bootloader for 32-bit MCUs. It defines a common infrastructure for the bootloader, defines system flash layout on microcontroller systems, and provides a secure bootloader that enables easy software update. MCUboot is operating system and hardware independent and relies on hardware porting layers from the operating system it works with. The Renesas Flexible Software Package (FSP) integrates an MCUboot port starting from FSP v3.0.0. Users can benefit from using the FSP MCUboot Module to create a Root of Trust (RoT) for the system and perform secure booting and fail-safe application updates.

The MCUboot is maintained by Linaro in the GitHub mcu-tools page https://github.com/mcu-tools/mcuboot. There is a `\docs` folder that holds the documentation for MCUboot in .md file format. This application note will refer to the above-mentioned documents wherever possible and is intended to provide additional information that is related to using the MCUboot Module with Renesas RA FSP v3.0.0 or later.

This application note walks the user through application project creation using the MCUboot Module on Renesas EK-RA6M4 and EK-RA6M3 kits. Example projects for the use case of designing with TrustZone for multi-image support is provided for EK-RA6M4. Example projects for the use case of designing with single image support is provided for EK-RA6M3. The MCUboot Module is supported across the entire RA MCU Family. Guidelines of how to adapt the example project configurations for other RA Family MCUs are provided.

App Note and Sample Code



RENESAS Application Note

Renesas RA Family

Secure Bootloader for RA2 MCU Series

Introduction

MCUboot is a secure bootloader for 32-bit MCUs. It defines a common infrastructure for the bootloader, defines system flash layout on microcontroller systems, and provides a secure bootloader that enables easy software update. MCUboot is operating system and hardware independent and relies on hardware porting layers from the operating system it works with. Currently MCUboot is maintained by Linaro in the GitHub mcu-tools page https://github.com/mcu-tools/mcuboot. There is a `/docs` folder that holds the documentation for MCUboot in .md file format. This application note will refer to the above-mentioned documents wherever possible.

The Renesas Flexible Software Package (FSP) integrates an MCUboot port across the entire RA MCU Families starting from FSP v3.0.0. Renesas RA2 MCU series are based on Arm® Cortex®-M23 core and have limited flash and RAM memory. This application project is created to address the unique challenges and provide guidelines on the optimization of the RA2 MCU bootloader memory size. For the MCUboot cryptographic support for RA2 MCU groups, TinyCrypt (https://github.com/intel/tinycrypt/) is integrated with the FSP MCUboot module to provide a smaller memory footprint compared with Mbed Crypto. Refer to the GitHub folder `/tinycrypt/documentation/` for details on the TinyCrypt cryptographic algorithm usage guide.

App Note and Sample Code

FLEXIBLE SOFTWARE PACKAGE

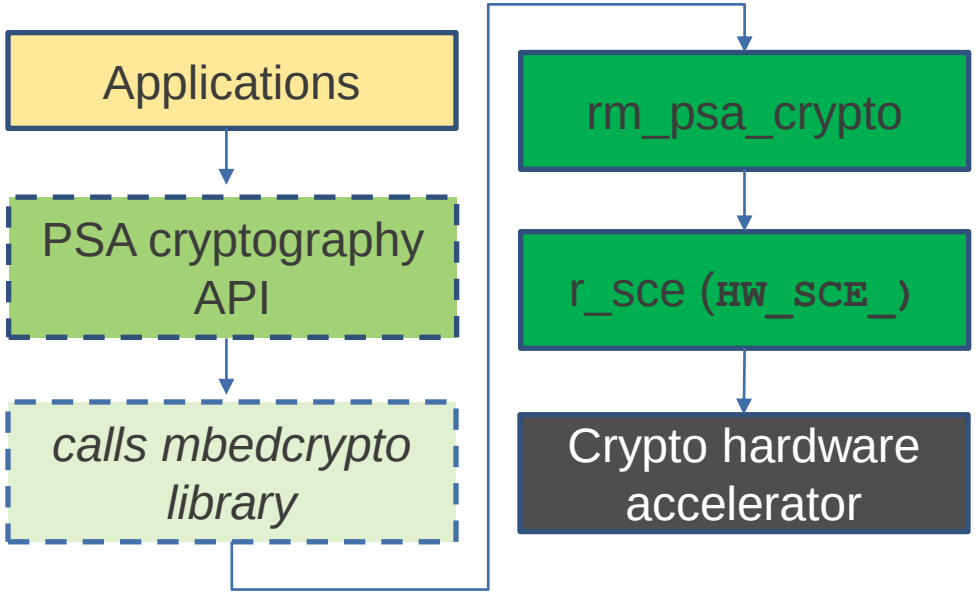
ENHANCED SECURITY OPTIONS WITH PSA CRYPTO & SCE

RA2A1	RA4M1	RA6M1	RA6T1
RA2L1	RA4M2	RA6M2	
RA2E1	RA4M3	RA6M3	
		RA6M4	
		RA6M5	

Based on Mbed Crypto v3.0

And mbedcrypto-2.0.0+renesas.0 tag

- **Includes software & hardware crypto with Mbed crypto**
  - Cryptographic APIs based on ARM PSA Crypto
  - Supports Software and Hardware crypto
  - Crypto support for AES128/256, TRNG, SHA256/SHA224 calculations, RSA2048, ECC
  - Supports wrapped and plain text key generation
  - Supports Persistent Key Storage
  - Easy tool options to configure Crypto modules
- Hardware acceleration for the Mbed Crypto implementation of the ARM PSA Crypto API

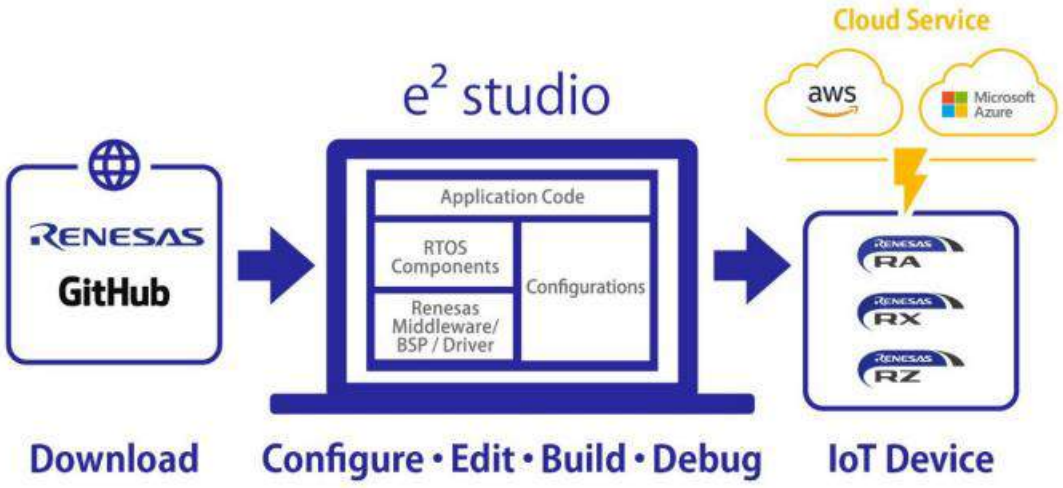


Simpler Development of IoT Devices Connectable with Amazon Web Services (AWS)

The e² studio supports the development of software for IoT devices to be connectable with Amazon Web Services (AWS) or Microsoft Azure Cloud Computing Service. The e² studio offers the following powerful functions for FreeRTOS or Azure RTOS.

- Quick building after downloading the latest version of FreeRTOS or Azure RTOS project directly from GitHub®
- Assisting in configuring RTOS, all required drivers, network stacks (TCP/IP, Wi-Fi, and MQTT), and component libraries (Device Shadow, Azure RTOS NetX duo and so on) Note1
- Embedding additional middleware and drivers (such as for USB and file-system support) in IoT devices

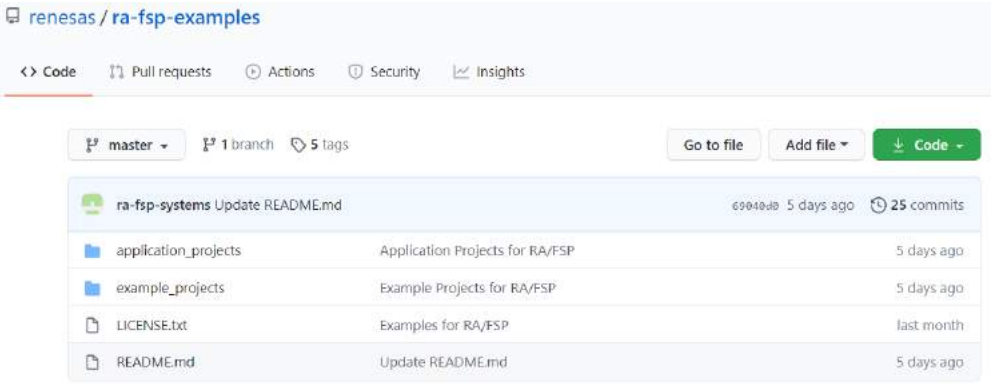
Note1
The settable components of RTOS are as follows: MQTT, Greengrass Discovery, Device Shadow, Azure RTOS NetX duo , Secure Sockets, and TCP/IP

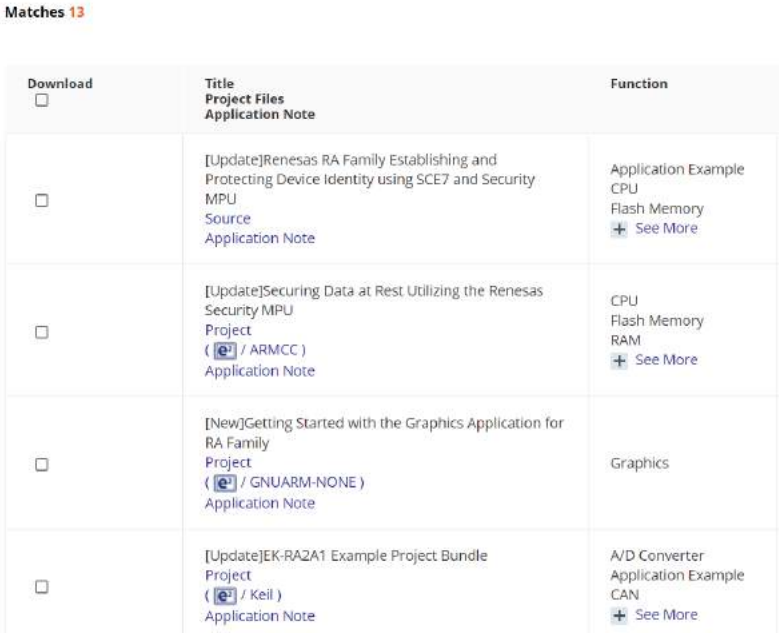


- AWS and Amazon Web Services are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. (https://aws.amazon.com/trademark-guidelines/)
- Azure is a trademark owned by Microsoft Corporation and its affiliated companies. (https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/)
- FreeRTOS is a trademark of Amazon Web Services, Inc. (https://freertos.org/copyright.html)
- GitHub® is a trademark of GitHub, Inc. (https://github.com/logos)

EXAMPLES AND APPLICATIONS

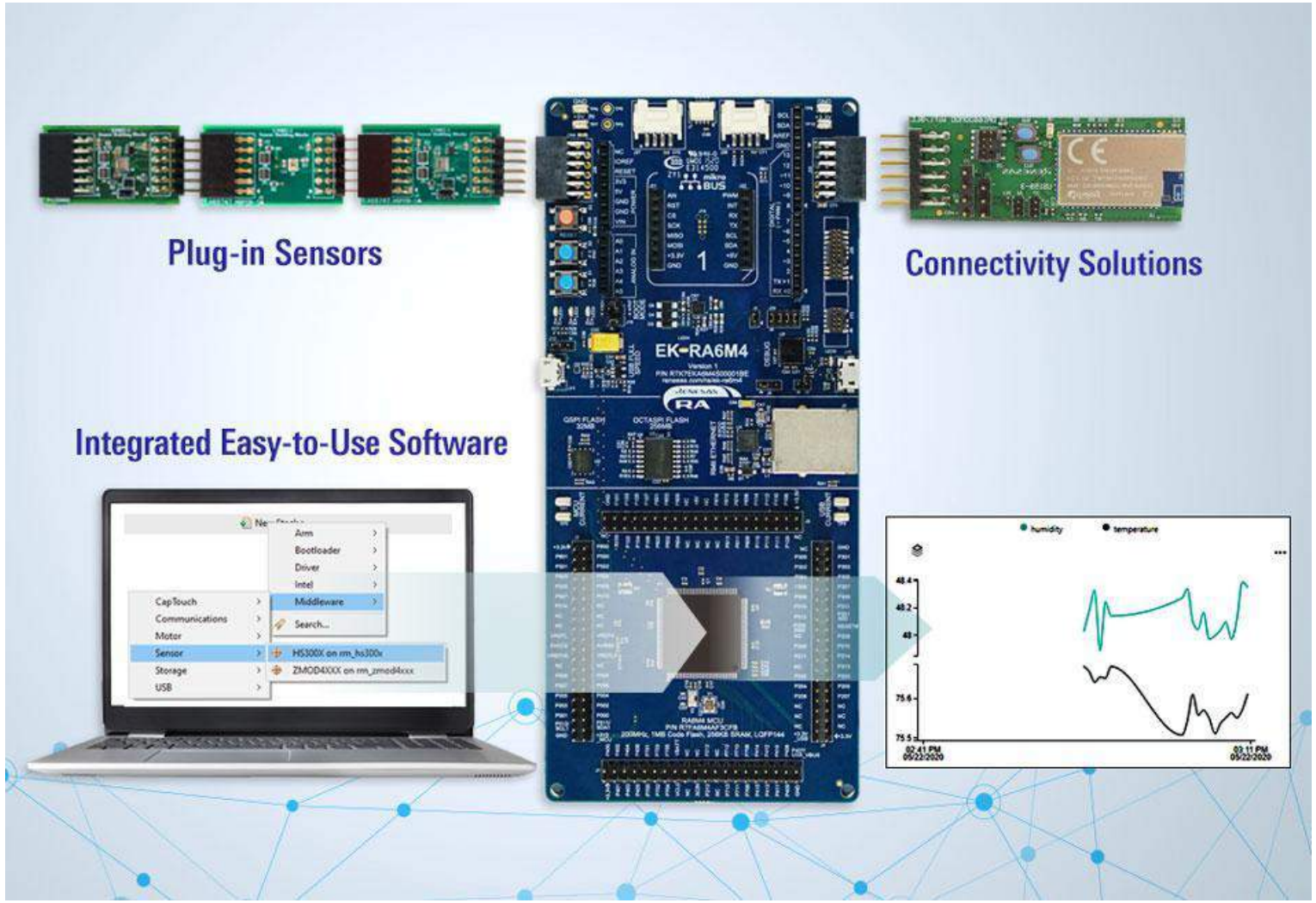
- Dedicated GitHub repository for Example Projects and Application Projects releases (https://github.com/renesas/ra-fsp-examples)
- Documentation and Sample Code
  - Azure Cloud Connectivity Solution
  - AWS Cloud Connectivity Solution





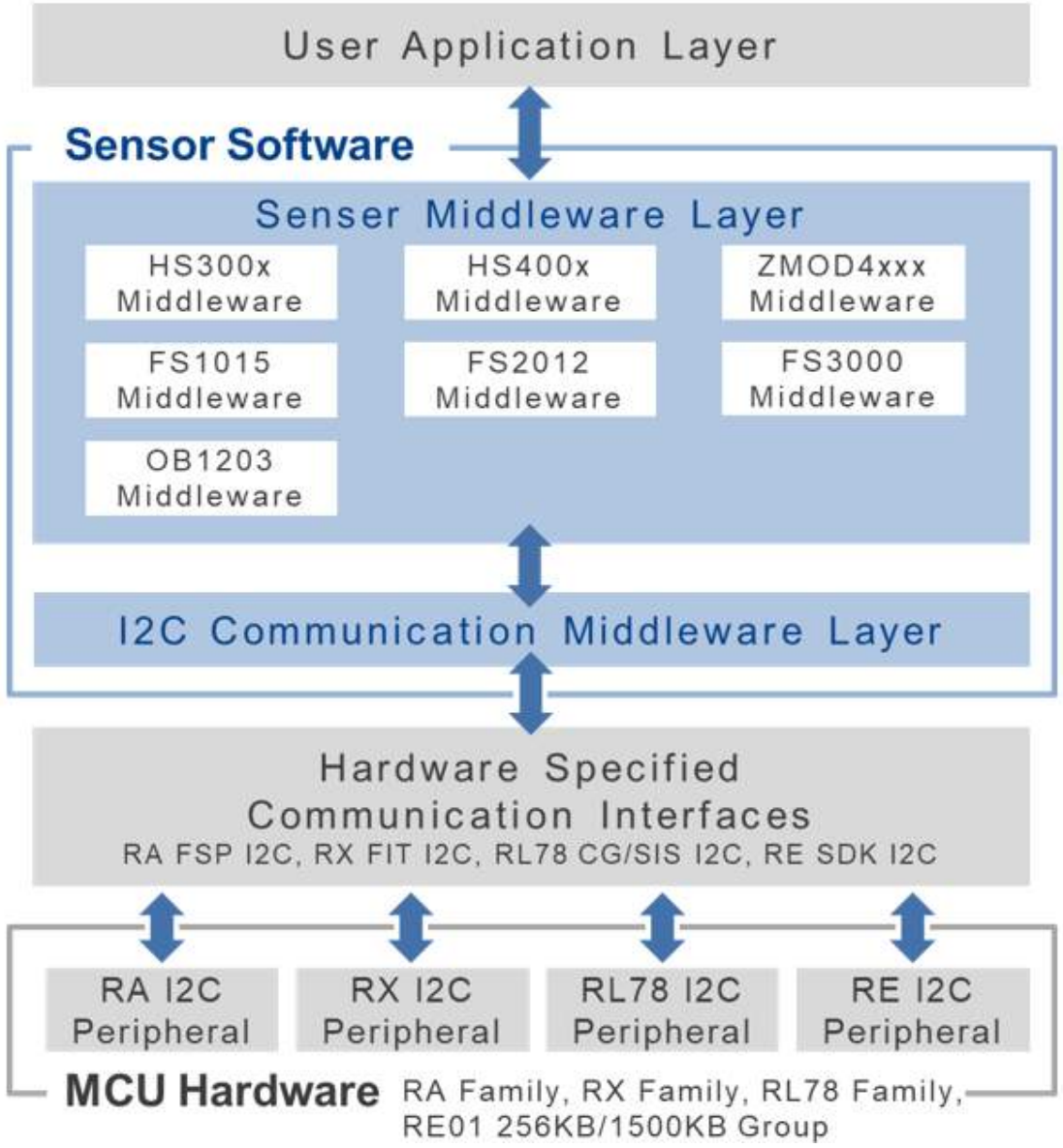
QUICK-CONNECT IOT

- Evaluation platform for fast prototyping by providing compatible hardware and software building blocks



QUICK-CONNECT IOT

- Sensor Software Modules
  - API functions to control sensors
  - I2C communication middleware layer
  - Documentation and Sample Code



renesas.com/ra