SHC RISC-V Root of Trust Demo

Andes RISC-V SoC with FreeRTOS and Amazon IoT Core

Nov 4, 2020
SH Consulting Group

SHC Demonstration: Andes Corvette F1 RoT with AWS IoT Core

This demo shows a Secure IoT solution using a Corvette-F1 board, evaluation kit with full support for the 32-bit AndesCore N25 and the AndeShape AE250 Platform, runs Amazon FreeRTOS, which is an open source operating system for microcontrollers from Amazon Web Services (AWS). It uses an ESP32-WROOM board as an external Wi-fi module. ATECC608A-MAHDA chip is integrated such as Trusted Platform Module (TPM) to provide hardware-based endpoint device security. This integration ensures the private key used to establish device identity can be securely stored in tamper-proof hardware devices to prevent it from being taken out of the devices for impersonation and other malicious activities.

In IoT solution deployments, it is important to check the identity of the device that is communicating with the messaging gateway. For the first time running demo, TPM will generate key pairs for the devices, which are then used to authenticate and encrypt the traffic. The keys are generated inside the TPM itself and are thereby protected from being retrieved by external programs. In fact, even without harnessing the capabilities of a hardware root of trust and secure boot, the TPM is also valuable just as a hardware key store. The private keys are protected by the hardware and offer far better protection than a software key. This integration uses the PKCS#11 protocol as the interface to the TPM.

After generating key pairs, this demo uses the FreeRTOS MQTT library to connect to the AWS Cloud and then periodically publish messages to an MQTT topic hosted by the AWS IoT MQTT broker. A specific Android application developed by SHC also uses this topic to communicate with Corvette-F1 board to control its on-board LEDs.

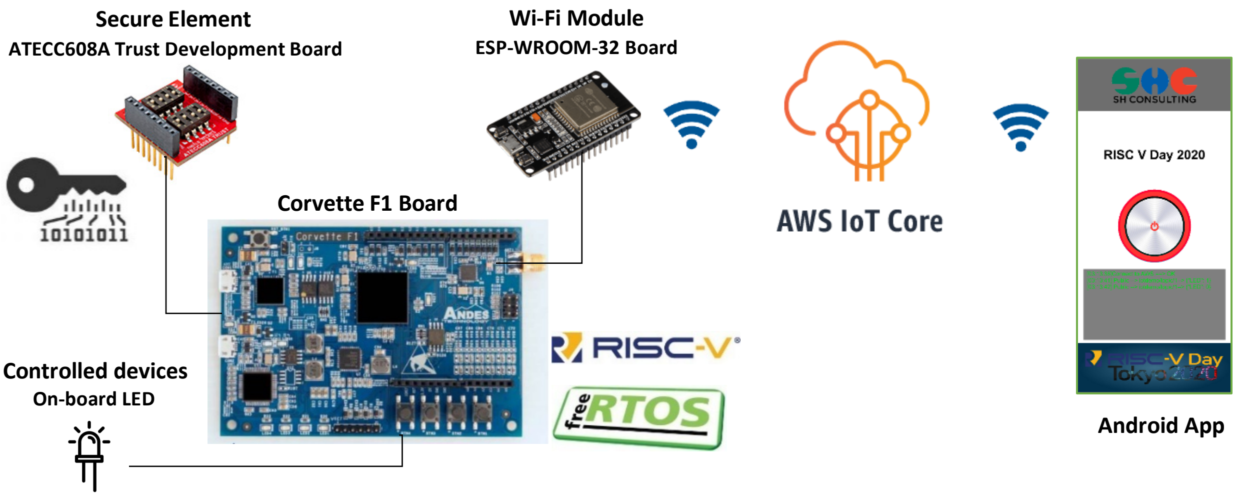


Figure 1: Corvette F1 Root of Trust and AWS IoT demonstration

Corvette F1 Board

General Description

Andes Technology is a leading supplier of high-performance low-power compact 32/64-bit RISC-V CPU cores and a founding member of the RISC-V Foundation. Its Corvette-F1 N25 platform is one of the first RISC-V platforms qualified for Amazon FreeRTOS. Amazon FreeRTOS is an open source operating system for microcontrollers from Amazon Web Services (AWS) that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage. Developers can take advantage of Amazon FreeRTOS features and benefits by using the RISC-V platform from Andes Technology.

As more and more technologies have been deployed to the internet, the IoT market grows with a wide variety of diversified applications. The RISC-V Instruction Set Architecture (ISA) provides enhanced flexibility, extensibility, and scalability that can help generate new possibilities for the IoT and making it easier to design compact IoT hardware to take advantage of this growing market. By combining the RISC-V platform with solutions like Amazon FreeRTOS, AWS IoT Greengrass, and AWS IoT Core, Andes Technology can help developers to create comprehensive and competitive RISC-V-based IoT systems.

The Corvette-F1 N25 platform is one of the first RISC-V platforms qualified for Amazon FreeRTOS. The Corvette-F1 N25 platform is an FPGA-based Arduino-compatible evaluation platform. It comes with a 32-bit RISC-V AndesCore™ N25 running at 60MHz, 4MB Flash, 256KB instruction SRAM and 128KB data SRAM, and AndeShape™ AE250 Platform IP with a rich set of peripherals including GPIO, I2C, PWM, SPI, and UART. Users can easily build the prototypes and applications of IoT devices under Arduino standard IDE and full-featured AndeSight™ IDE.

ATECC608A Chip

Features

- Cryptographic Co-Processor with Secure Hardware-based Key Storage:
  - Protected Storage for up to 16 Keys, Certificates or Data
- Hardware Support for Asymmetric Sign, Verify, Key Agreement:
  - ECDSA: FIPS186-3 Elliptic Curve Digital Signature
  - ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman
  - NIST Standard P256 Elliptic Curve Support
- Hardware Support for Symmetric Algorithms:
  - SHA-256 & HMAC Hash including off-chip context save/restore
  - AES-128: Encrypt/Decrypt, Galois Field Multiply for GCM
- Networking Key Management Support:
  - Turnkey PRF/HKDF calculation for TLS 1.2 & 1.3
  - Ephemeral key generation and key agreement in SRAM
  - Small message encryption with keys entirely protected
- Secure Boot Support:
  - Full ECDSA code signature validation, optional stored digest/signature
  - Optional communication key disablement prior to secure boot
  - Encryption/Authentication for messages to prevent on-board attacks
- Internal High-Quality NIST SP 800-90A/B/C Random Number Generator (RNG)
- Two High-Endurance Monotonic Counters
- Guaranteed Unique 72-bit Serial Number
- Two Interface Options Available:
  - High-speed Single Pin Interface with One GPIO Pin
  - 1 MHz Standard I2C Interface
- 1.8V to 5.5V IO Levels, 2.0V to 5.5V Supply Voltage
- <150 nA Sleep Current
- 8-pad UDFN and 8-lead SOIC Packages

Applications

- Network/IoT Node Endpoint Security

Manage node identity authentication and session key creation & management. Supports the entire ephemeral session key generation flow for multiple protocols including TLS 1.2 (and earlier) and TLS 1.3

- Secure Boot

Support the MCU host by validating code digests and optionally enabling communication keys on success. Various configurations to offer enhanced performance are available.

- Small Message Encryption

Hardware AES engine to encrypt and/or decrypt small messages or data such as PII information. Supports AES-ECB mode directly. Other modes can be implemented with the help of the host microcontroller. Additional GFM calculation function to support AES-GCM.

- Key Generation for Software Download

Supports local protected key generation for downloaded images. Both broadcast of one image to many systems, each with the same decryption key, or point-to-point download of unique images per system is supported.

- Ecosystem control and Anti-Counterfeiting

Validates that a system or component is authentic and came from the OEM shown on the nameplate.

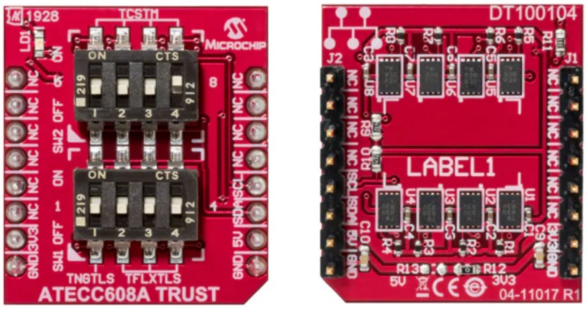


Figure 2: ATECC608A Trust Development Board (top view and bottom view)

Cryptographic Operation

The ATECC608A implements a complete asymmetric (public/private) key cryptographic signature solution based upon Elliptic Curve Cryptography and the ECDSA signature protocol. The device features hardware acceleration for the NIST standard P256 prime curve and supports the complete key life cycle from high quality private key generation, to ECDSA signature generation, ECDH key agreement, and ECDSA public key signature verification.

The device is designed to securely store multiple private keys along with their associated public keys and certificates.

Random private key generation is supported internally within the device to ensure that the private key can never be known outside of the device. The public key corresponding to a stored private key is always returned when the key is generated and it may optionally be computed at a later time.

The ATECC608A can generate high-quality random numbers using its internal random number generator, that is designed to meet the requirements documented in the NIST 800-90A, 800-90B and 800-90C documents.

These random numbers can be employed for any purpose, including usage as part of the device's crypto protocols. Because each random number is guaranteed to be essentially unique from all numbers ever generated on this or any other device, their inclusion in the protocol calculation ensures that replay attacks (i.e. re-transmitting a previously successful transaction) will always fail.

Root of Trust with Microchip's Trust Platform

In the age of the IoT, hardware-based security is the only way to protect secret keys from physical attacks and remote extraction. However, extensive security expertise, development time, and costs are required to configure and provision each device. Microchip has developed a key security service, called Microchip's Trust Platform for its CryptoAuthentication family, that provides an easy way for OEMs, small or large, to implement secure authentication for hardware devices. The service provides a secure system to manufacture device keys and a supply chain to generate custom part numbers

Based on the ATECC608A secure element, the Trust Platform is available in three tiers to meet the needs of users ranging from out-of-the-box pre-provisioned to fully customizable. The ATECC608A provides Common Criteria

Joint Interpretation Library (JIL) “high”-rated secure key storage, giving customers confidence that devices implement industry-proven security practices and the highest level of secure key storage. Hardware-based root of trust storage and cryptographic countermeasures protect the device against the widest classes of known physical attacks.

The three tiers are Trust&GO, TrustFLEX, and TrustCUSTOM.

- Trust&GO (ATECC608A-TNGTLS) for the mass market, provides zero-touch pre-provisioned secure elements with a minimum orderable quantity (MOQ) as low as 10 units. Device credentials are pre-programmed, shipped and locked inside the ATECC608A for automated cloud or LoRaWAN authentication onboarding.
- TrustFLEX (ATECC608A-TFLXTLS) offers the flexibility to use the customer’s certificate authority while benefiting from pre-configured use cases. These use cases include baseline security measures such as Transport Layer Security (TLS) hardened authentication for connecting to any IP-based network using any certificate chain, LoRaWAN authentication, secure boot, Over-the-Air (OTA) updates, IP protection, user data protection, and key rotation.
- TrustCUSTOM (ATECC608A-MAHDA) enables complete customization, providing customer-specific configuration capabilities and custom credential provisioning.

Microchip worked with Amazon Web Services (AWS) to enable a straightforward and simplified on-board process into AWS IoT services for products designed with all variants of the Microchip Trust Platform. The ATECC608A secure element can be paired with any microcontroller and microprocessor.

Amazon IoT Core

Easily and securely connect devices to the cloud. Reliably scale to billions of devices and trillions of messages.

What is AWS IoT Core?

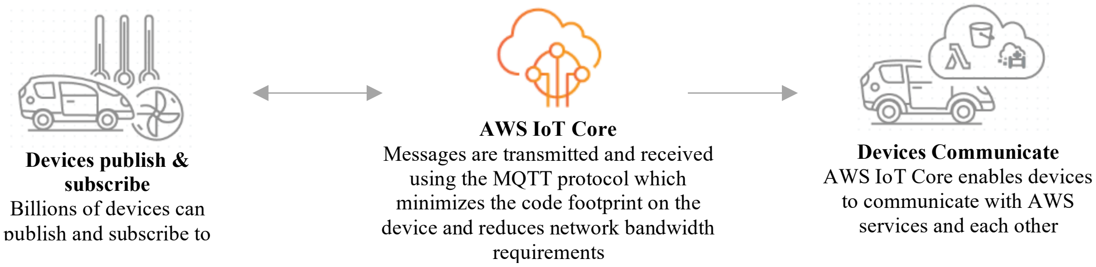
AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT Core, your applications can keep track of and communicate with all your devices, all the time, even when they aren’t connected.

AWS IoT Core also makes it easy to use AWS and Amazon services like AWS Lambda, Amazon Kinesis, Amazon S3, Amazon SageMaker, Amazon DynamoDB, Amazon CloudWatch, AWS CloudTrail, Amazon QuickSight, and Alexa Voice Service to build IoT applications that gather, process, analyze and act on data generated by connected devices, without having to manage any infrastructure.

How does AWS IoT Core work?

Connect and manage your devices

AWS IoT Core allows you to easily connect any number of devices to the cloud and to other devices.



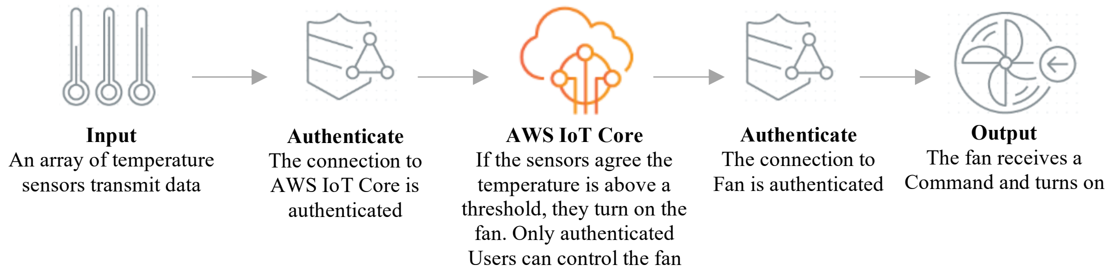
Devices publish & subscribe
Billions of devices can publish and subscribe to

AWS IoT Core
Messages are transmitted and received using the MQTT protocol which minimizes the code footprint on the device and reduces network bandwidth requirements

Devices Communicate
AWS IoT Core enables devices to communicate with AWS services and each other

Secure device connections and data

AWS IoT Core provides automated configuration and authentication upon a device’s first connection to AWS IoT Core, as well as end-to-end encryption throughout all points of connection, so that data is never exchanged between devices and AWS IoT Core without proven identity. In addition, you can secure access to your devices and applications by applying policies with granular permissions.



Input
An array of temperature sensors transmit data

Authenticate
The connection to AWS IoT Core is authenticated

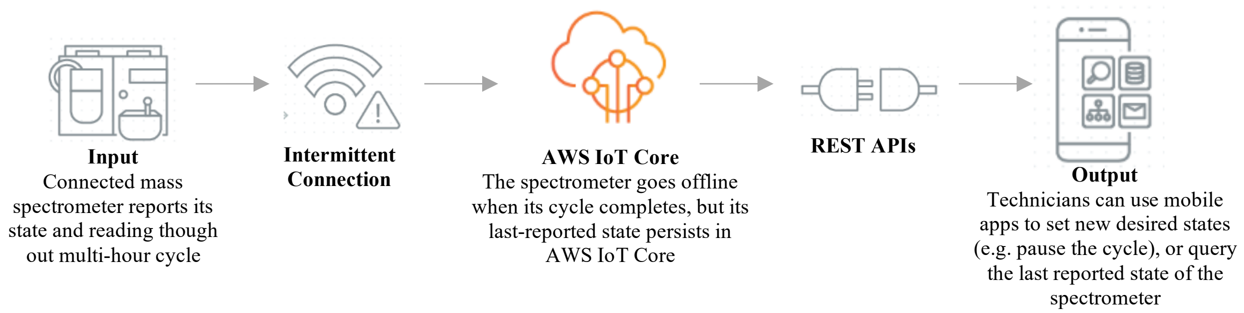
AWS IoT Core
If the sensors agree the temperature is above a threshold, they turn on the fan. Only authenticated Users can control the fan

Authenticate
The connection to Fan is authenticated

Output
The fan receives a Command and turns on

Read and set device state at any time

AWS IoT Core stores the latest state of a connected device so that it can be read or set at anytime, making the device appear to your applications as if it were online all the time.



Input
Connected mass spectrometer reports its state and reading though out multi-hour cycle

Intermittent Connection

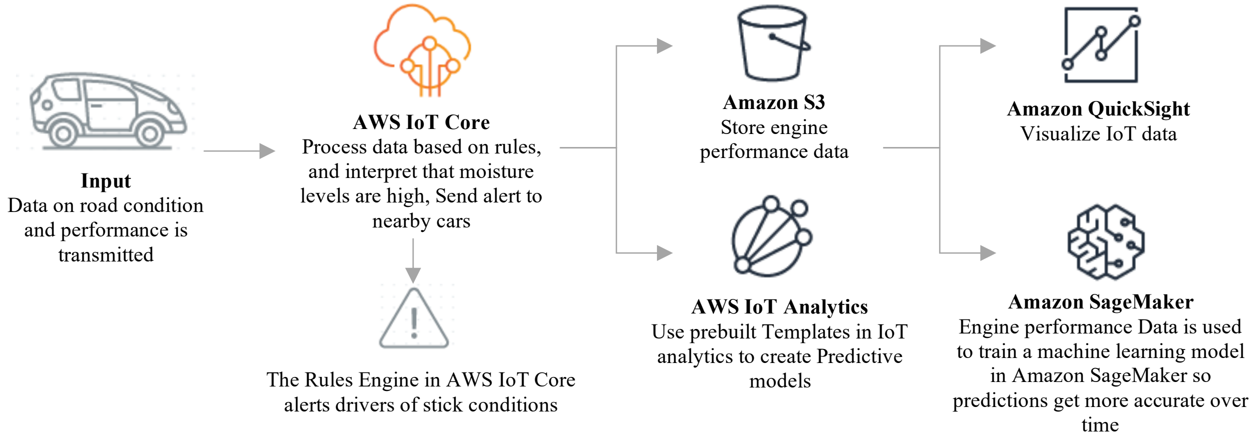
AWS IoT Core
The spectrometer goes offline when its cycle completes, but its last-reported state persists in AWS IoT Core

REST APIs

Output
Technicians can use mobile apps to set new desired states (e.g. pause the cycle), or query the last reported state of the spectrometer

Process and act upon device data

With AWS IoT Core, you can filter, transform, and act upon device data on the fly, based on business rules you define.



Input
Data on road condition and performance is transmitted

AWS IoT Core
Process data based on rules, and interpret that moisture levels are high, Send alert to nearby cars

The Rules Engine in AWS IoT Core alerts drivers of stick conditions

Amazon S3
Store engine performance data

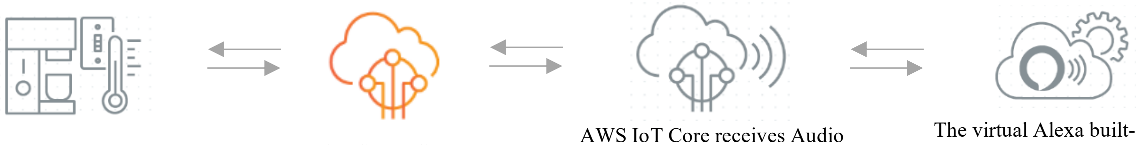
AWS IoT Analytics
Use prebuilt Templates in IoT analytics to create Predictive models

Amazon QuickSight
Visualize IoT data

Amazon SageMaker
Engine performance Data is used to train a machine learning model in Amazon SageMaker so predictions get more accurate over time

Cost-effectively scale to hundreds of millions of Alexa Built-in devices

The Alexa Voice Service (AVS) Integration for AWS IoT Core introduces a new virtual Alexa Built-in device in the cloud. It allows customers to send and receive audio messages over the reserved MQTT topics, interface with the device microphone and speaker, and manage the device-side state all while using the same secure IoT Core connection.



Produce devices using MCUs like Arm Cotex-M based devices with less than 1MB embedded RAM

AWS IoT Core
Securely and easily connect your devices to the cloud and to other devices with AWS IoT Core

AWS IoT Core receives Audio messages from the device and delivers them to AVS through secure MQTT topics

The virtual Alexa built-in device processes the audio data and sends the response back to the device through AWS IoT Core as an MQTT message

About SH Consulting Group

SH Consulting Group (SHC) has engineers in US, Vietnam and in Japan specialized in providing stability to RTOS, device drivers, and wireless connectivities for MCUs such as H8s, SHs, ARMs and RISC-Vs. It has been integrating OSes such as QNX, .NETMF, Linux, and Windows for MCUs and wireless solutions such as Lora, WiFi and Bluetooth for many years. They worked on Windows, Android and iOS platforms. In recent years SHC engineers enabled FreeRTOS for large semiconductor companies on ARM platforms and direct this effort to RISC-Vs.

SH CONSULTING K.K. (JAPAN)
Tokyo Head Office: 7-18-13-502 ginza, Chuo-ku, Tokyo, Japan 104-0061
Phone: 03-3833-3717
Tokyo Design Center: Yamamoto Building 5F, 3-23-12 Minami-cho, Kokubunji-shi, Tokyo 185-0021, Japan

SH CONSULTING VIETNAM COMPANY LTD. (VIETNAM)
(Local Name: CÔNG TY TNHH SH CONSULTING VIỆT NAM)
Quang Trung Software park, Tan Chanh Hiep
Ward, District 12 Ho Chi Minh City
Phone: 84-8-3715-0060

SOFTWARE HARDWARE & CONSULTING LLC (USA)
San Francisco Bay Area USA:
Software Hardware & Consulting LLC
1325A Church St, San Francisco, CA 94114-3900
Phone: +1-(408) 510-8221