End-To-End Secure LoRaWAN: Secure Devices with Key Management from Provisioning to Operations

Tony Rosati – ESCRYPT (a Bosch Company) and Erik Wood – Cypress Semiconductor Corp.

Introduction

Low-Power Wide Area Networks (LPWAN) offer low-cost, reliable connectivity at distances over 10 kilometers. LoRaWAN has emerged as the dominant open specification in 2018 with more than 500 ecosystem vendors and 60 service providers globally. It is optimized for low power consumption, security, and scalability.

LPWANs are used to transform many industrial applications. For example, smart cities are using LPWAN to lower operating costs by automating metering, control and monitor infrastructure, and offer new services such as parking availability and reservations. Building managers are using LPWAN in automation systems to optimize energy consumption 24x7. Agricultural applications use LPWAN for 24x7 monitoring of livestock and crops.

Industrial applications rely on large-scale sensor data to make mission-critical decisions. More importantly, these decisions may be fully automated, so security is paramount. This means that no one has access to root keys, devices cannot be copied (cryptographically), and device owners are the only entities that have access to sensor data.

LoRaWAN Security

The LoRaWAN specifications offer the fundamental building blocks for securely joining networks, and end-to-end encrypted communications using the state of the art NIST cryptographic standard AES. The LoRaWAN security whitepaper from the LoRa-Alliance provides an overview of security services offered. [https://lora-alliance.org/sites/default/files/2018-04/lora_alliance_security_whitepaper.pdf]

However, there are aspects of security that are outside the scope of the LoRaWAN specifications; namely, key management, device key provisioning, and protection. This issue must be addressed for LoRaWAN networks to scale. This whitepaper describes these fundamental security requirements and best practices.

In the following security model, no one has access to root keys, the LoRaWAN service provider only has access to network session keys for device authentication, and the owners only have access to the application session key to retrieve sensor data.

Key Management and Hardware Security for LoRaWAN

LoRaWAN uses symmetric-key cryptography. Root keys are used to derive session keys both for packet-level authentication and end-to-end encryption. This means that a root key that is stored in a sensor must also be made available to the network in order to generate session keys.

Key management for LoRaWAN can be broken down into three components: The key management system (KMS), device key provisioning, and the on-chip security of the end device. The architecture of a LoRaWAN network with KMS and factory-key provisioning is shown in Figure 1.

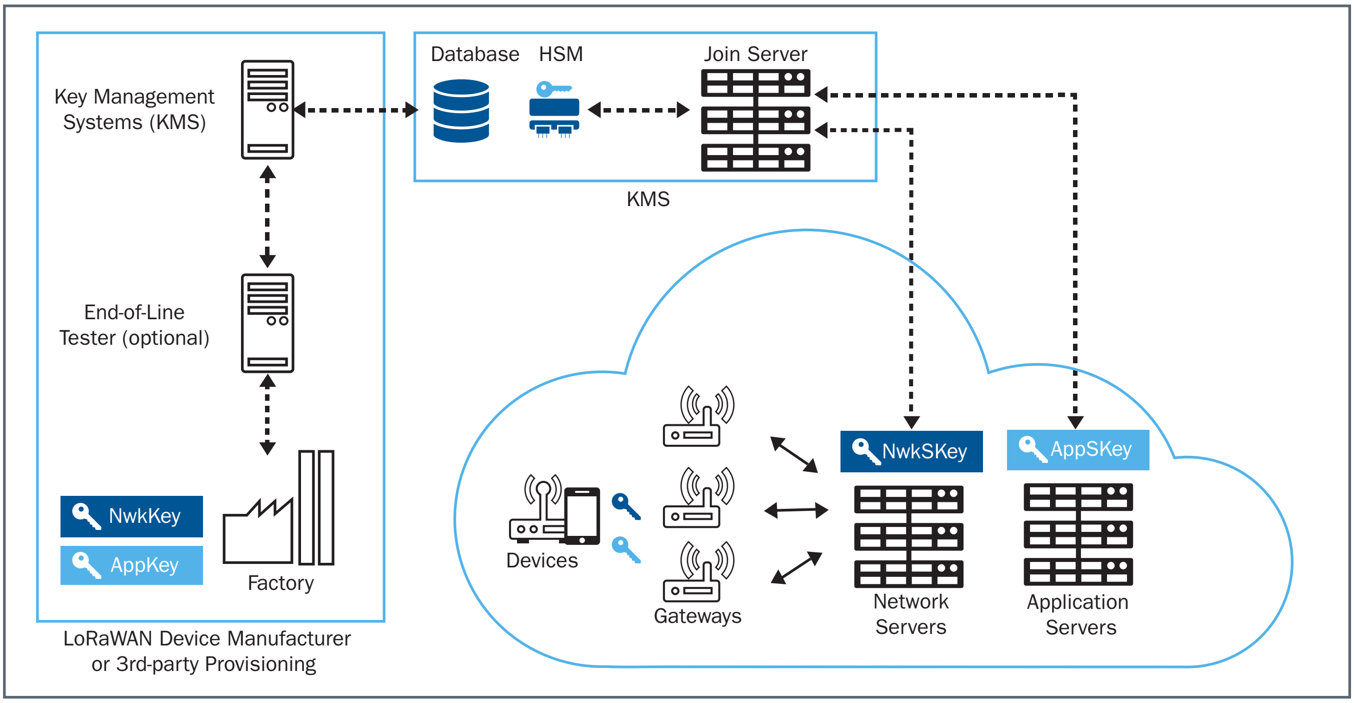
Key Management Systems (KMS)
End-of-Line Tester (optional)
NwkKey
AppKey
Factory
LoRaWAN Device Manufacturer or 3rd-party Provisioning
Database
HSM
Join Server
KMS
Devices
Gateways
NwkSKey
AppSKey
Network Servers
Application Servers

Figure 1: ESCRYPT KMS/Join Server

The Key Management System (KMS)

The KMS is responsible for the issuance of device root keys. In LoRaWAN Specification 1.02, the root key is AppKey. In LoRaWAN Specification 1.1, there are two root keys AppKey and NwkKey. These root keys are unique 128-bit random numbers that must be stored securely in the LoRaWAN end device.

Root keys must also be available on the network side at the Join Server so that session keys can be derived from them when devices attempt to join a network. In the LoRaWAN specifications, session key NwkSKey is used to authenticate packets to a network server and AppSKey is used to encrypt the device payload. Ideally, data is encrypted from the device to an application server where sensor data is made available to the owner of the device.

The ESCRYPT KMS/Join Server for LoRaWAN offers all the required security services for the network, including factory-level device key provisioning.

Device Key Provisioning

Device key provisioning refers to injecting a root key from the KMS into a device. This can be done during device manufacturing or in the field, as devices are registered to join a LoRaWAN network. The KMS must be able to authenticate the entity doing the provisioning.

Eventually, those devices will be incorporated into a product and deployed in the field, at which point the sensor will be registered to an owner and service provider.

The ESCRYPT KMS enables device key provisioning through a local provisioning authority (LPA). Two-factor authentication is used to validate the provisioning agent to the KMS before root keys are generated and programmed.

Security of End Devices

Root keys issued to a device must be securely stored and protected during operation so that keys can't simply be read out of memory. Ideally, at the device key provisioning stage no one will have access to keys being programmed into the device.

During operation, the crypto computations must be protected as part of the LoRaWAN stack. Ideally, a microcontroller (MCU) would be locked down so that its image can't be replicated in any way. This is done using a secure MCU companion paired with the LoRa radio as an optimal way to limit end-device board space and bill of materials. Cryptographic acceleration is also an effective hardware-based security feature to significantly reduce transaction time and reduce power consumption.

Take, for example, the use of a Cypress PSoC® 6 secure MCU in this application.The PSoC 6 hardware-based security approach uses multiple levels of isolation in its asymmetric, dual-core architecture (a CM4 core plus a CM0+ core in one chip). PSoC 6 uses a highly secure M0+ core with memory and peripheral protection units to isolate the LoRa radio stack and the root keys from the M4 core in a client server architecture. It can even isolate the keys from the LoRa stack within the M0+ to further logically secure the root keys. This leaves the M4 core for non-secure customer applications.

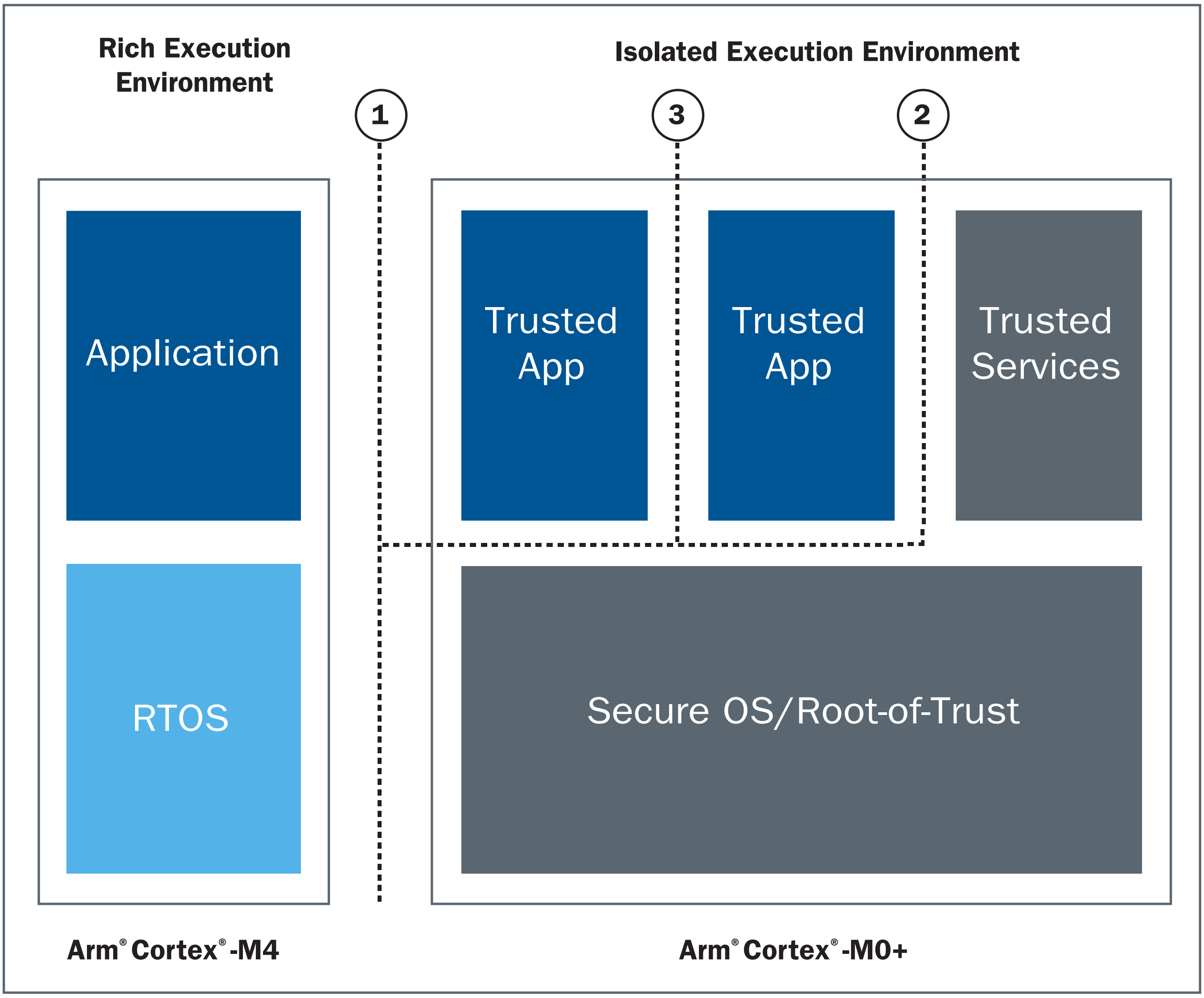

Figure 2: PSoC 6 Three-Layer, Hardware-Based Security Isolation

A cumulative advantage of using a secure MCU like Cypress' PSoC 6 as a pair to the LoRaWAN radio for security instead of a common secure element is the consolidation of important features into one chip. Security, BLE, and programmable digital and analog interfaces for sensor hub capabilities, plus a Cortex-M4 core to run a myriad user applications, are all available in a single chip. Simply add the radio and a sensor, and you have your solution.

Security Best Practices

Security best practices refers to 1) the roles and responsibilities of the actors in the LoRaWAN ecosystem, and 2) the security controls that are in place through the lifecycle of sensors that attempt to join LoRaWAN networks.

Roles and Responsibilities in the Ecosystem

- The KMS role is responsible for issuing and securely storing all root LoRaWAN keys. The KMS also makes root keys available to the Join Server for session key derivation.
- The device provisioning role is responsible for initial device key programming via the KMS. Device keys are programmed so that no one has access to root keys.
- The service provider role only has access to the network session key (NwkSKey) for device authentication.
- The owner role has access to the application session key (AppSKey) and ultimately sensor data that resides on an application server. The owner has ultimate control over the sensor.

Security Controls for Key Lifecycle Management

The KMS, being aware of the roles and responsibilities, must have an authentication model in place for each role. The roles tend to differ due to operational circumstances. For example, the device provisioning role might be a factory where the tester must be authenticated to the KMS using two-factor authentication. For network service providers the LoRa-Alliance defines a back-end specification to access the KMS/Join Server. Finally, the owner has access control over their data that resides on an application server, usually via a dashboard.

Implementation

A practical implementation of these concepts has been demonstrated using the ESCRYPT KMS for LoRaWAN and the Onethinx LoRaWAN module that pairs Cypress' PSoC 6 MCU with the new longer-range and lower-power Semtech radio.

Conclusion

In this paper we present a security model that addresses security from factory provisioning to operations. It relies on the use of a KMS and secure MCU so that sensors cannot be tampered with or replicated. Security best practices are employed so that no one has access to root keys, the service provider only has access to network session keys for device authentication, and the owner only has access to the application session key to retrieve sensor data.

To learn more about secure LoRaWAN, please contact Erik Wood at erik.wood@cypress.com or Tony Rosati at tony.rosati@escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.

Cypress Semiconductor Corporation
198 Champion Court, San Jose CA 95134
phone +1 408.943.2600 fax +1 408.943.6848
toll free +1 800.858.1810 (U.S. only) Press “1” to reach your local sales representative

CYPRESS®
EMBEDDED IN TOMORROW™