Secure Cloud Integration with EmSPARK™ Security Suite

Device integration with cloud platforms, such as AWS IoT Core or Microsoft Azure IoT, creates a variety of exciting opportunities for any IoT application. Cloud platforms enable management and monitoring of devices at a large scale. Integration with purpose-built analytics applications that can be used to optimize the performance of a fleet of devices, becomes practical. Additionally, today's applications processors can deliver a rich array of data regarding the health and security state of an IoT device. This data can be used to identify and address threats. To take advantage of this capability, it is critical to create a mutually authenticated, secure connection between the device and the cloud platform.

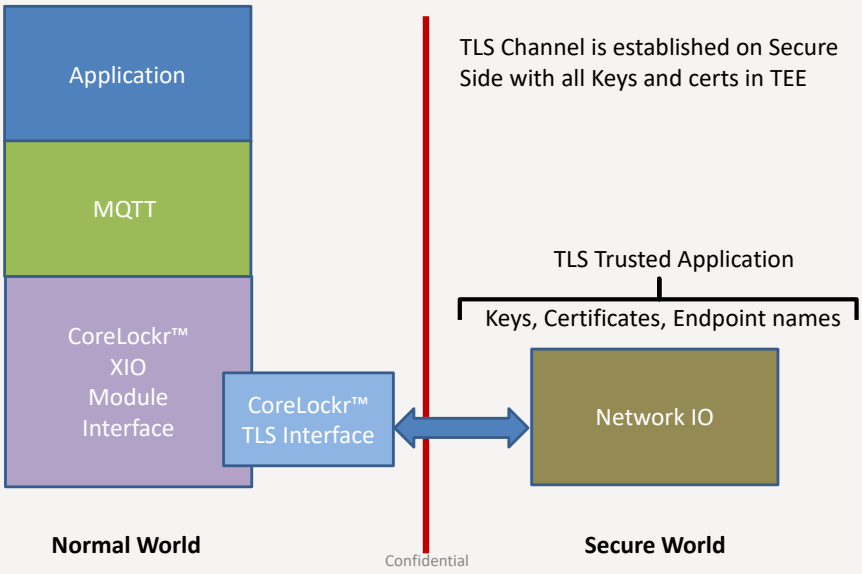
To establish a mutually authenticated connection, the device and the cloud platform employ the following assets:

1. **Device Key Pair.** This key pair—created during device provisioning—consists of a public key used for authentication, and a private key housed in the secure Trusted Execution Environment (TEE). Sequitur Labs' Trusted Execution Environment is called CoreTEE™.
2. **Device Certificate.** During device provisioning, a Certificate Signing Request (CSR) is generated in order to produce a certificate signed by the device vendor's Certificate Authority.
3. **Cloud Certificate.** The Certificate Authority of the cloud platform is loaded to the certificate repository managed in the secure TEE.

Using these assets, mutual authentication can be achieved using the following steps, using Transport Layer Security (TLS):

1. The device validates the cloud's certificate, using its list of Certificate Authorities, which is stored securely in the device's Trusted Execution Environment (TEE).
2. The device certificate is presented to the cloud server.
3. The cloud server authenticates the device certificate by checking it against its list of registered device certificates.
4. The cloud server issues a challenge to the device.
5. The device responds by signing the challenge with its private key. This challenge can then be verified by the cloud server.

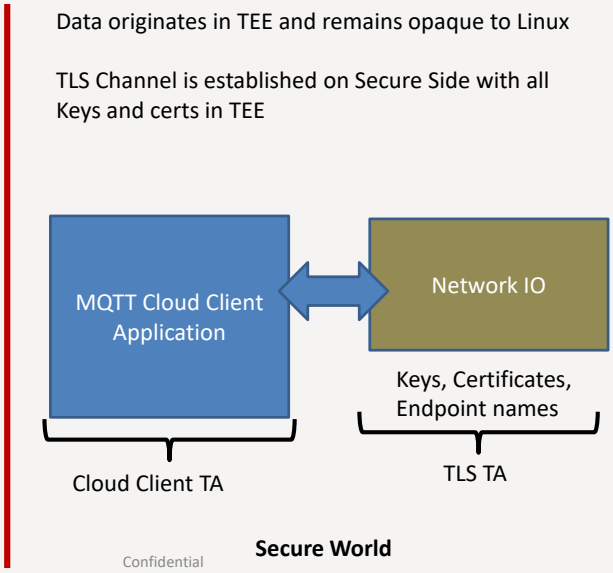
The EmSPARK™ Security Suite provides a Transport-Level Security (TLS) API—part of the CoreLockr™ API suite—and a TLS Trusted Application to perform the steps listed above. In the following example, the TLS Trusted Application, along with Sequitur Labs' supporting Trusted Applications (Certificate Management, Crypto, and Storage) are housed in the Secure Environment memory partition.



For fully encrypted data transmission to the cloud, the local application can also be housed in the Trusted Execution Environment (TEE).

EmSPARK™ supports the following functions for secure cloud integration:

1. Secure Software Provisioning during manufacturing, which provides credentials. (For more information, see the Secure Software Provisioning Solutions Brief.)
2. Support for a secure memory enclave which houses a Trusted Execution Environment (i.e., Sequitur's CoreTEE™).



3. Trusted Applications for Certificate Management, Encryption, and Secure Storage.
4. A dedicated API and Trusted Application for Transport Layer Security, used for device-to-cloud mutual authentication.
5. A Software Developer's Kit (SDK) which can be used to develop a Trusted Cloud Client Application.

Learn More

EVAL KIT Download the free evaluation kits and user's guide for more details and code examples

Download "Surviving The IoT Wave: EmSPARK™ Security Suite" Whitepaper

MSBEm-0006-Rev A. Printed in the U.S.A.