AWS IoT Technical Supplement

MQTT, Device Authentication, mTLS, AWS Security Overview, and JSON

AWS IoT Brief Technical Supplement

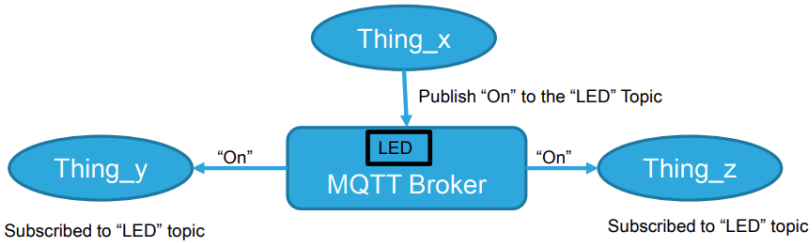
- What is MQTT and how does it work?
- AWS IoT Device Authentication basic overview
- What is TLS Mutual Authentication?
- AWS Security Overview (device certificates & keys)
- AWS IoT Policies
- JSON

More About MQTT

- MQTT
  - MQTT stands for MQ Telemetry Transport.
  - It is a simple and lightweight messaging protocol, designed for resource constrained devices and low-bandwidth, high-latency or unreliable networks.
- MQTT for IoT
  - MQTT is used because it requires minimal resources, and network bandwidth, while ensuring reliability and some degree of delivery assurance.
  - This makes MQTT ideal in “machine-to-machine” (M2M) or “Internet of Things” connected devices, where bandwidth and battery power are at a premium.

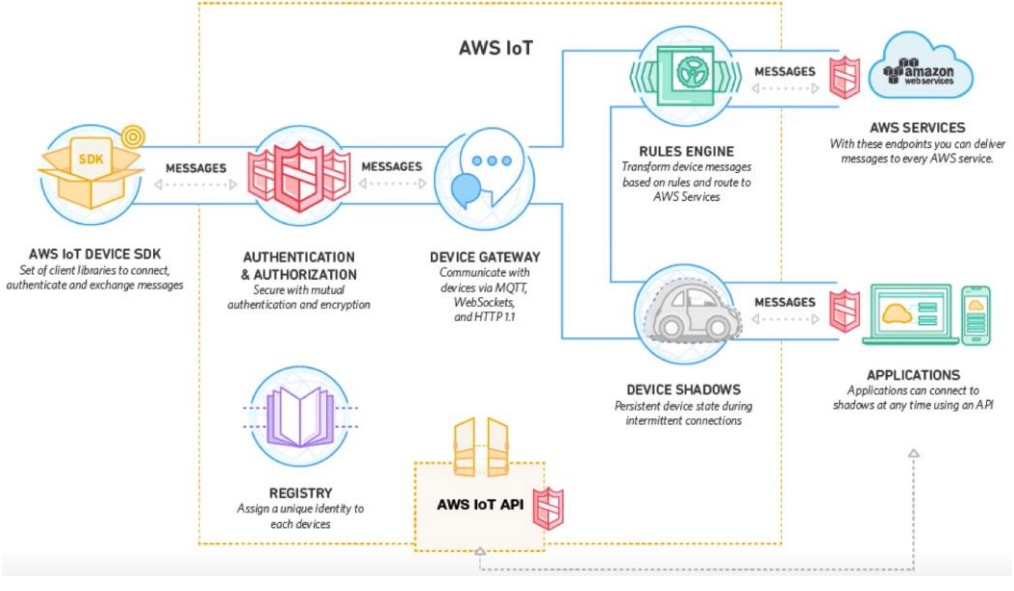
How MQTT Works

- MQTT uses a client/server model where every IoT device is a client and is connected to a server, called an MQTT broker (AWS IoT).
- The clients send messages to an address, called a topic. The MQTT broker will forward that message to all the clients subscribed to that topic.



AWS IoT Device Authentication

- AWS IoT devices are authenticated using mutual TLS (mTLS) authentication with X.509 certificates.
- Once a certificate is provisioned and activated it can be installed on a device. The device will then use that certificate for all requests to AWS IoT.

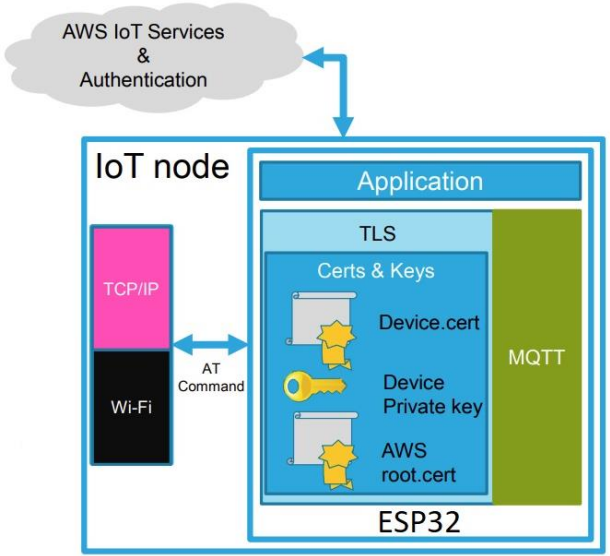


What is Mutual TLS Authentication?

- In Brief
  - mTLS is used to establish trust between two parties.
  - Each party verifies the certificate provided by the other.
  - Certificate Authorities (CA) like Verisign are an important part of the mutual authentication.

AWS Security Overview

- AWS provides the device certificate and keys (AWS is the CA).
- The certificates and keys are installed on the device. The device will then use that certificate and key to authenticate itself and send all requests to AWS IoT.
- To perform AWS IoT operations with your device, you must create an AWS IoT policy and attach it to your device certificate.



AWS IoT Policies

- In Brief
  - AWS IoT policies are JSON documents that authorize your device for performing AWS IoT operations.
  - AWS IoT defines a set of policy actions describing the operations and resources for which you can grant or deny access. For example:

iot:Connect represents permission to connect to the AWS IoT message broker.
iot:Subscribe represents permission to subscribe to an MQTT topic or topic filter.

What is JSON?

- In Brief
  - JSON (JavaScript Object Notation) is an open standard lightweight data-interchange format.
  - As a text document, it is easy for users to read and write, and for machines to parse and generate.

Let’s get started!