TRUSTONIC

aws partner network

Trustonic secured IoT device auto-enrolment with AWS

In the world of fake news, we all understand that you need to know who is claiming something, not just what they claim; in the world of IoT, the same holds true.

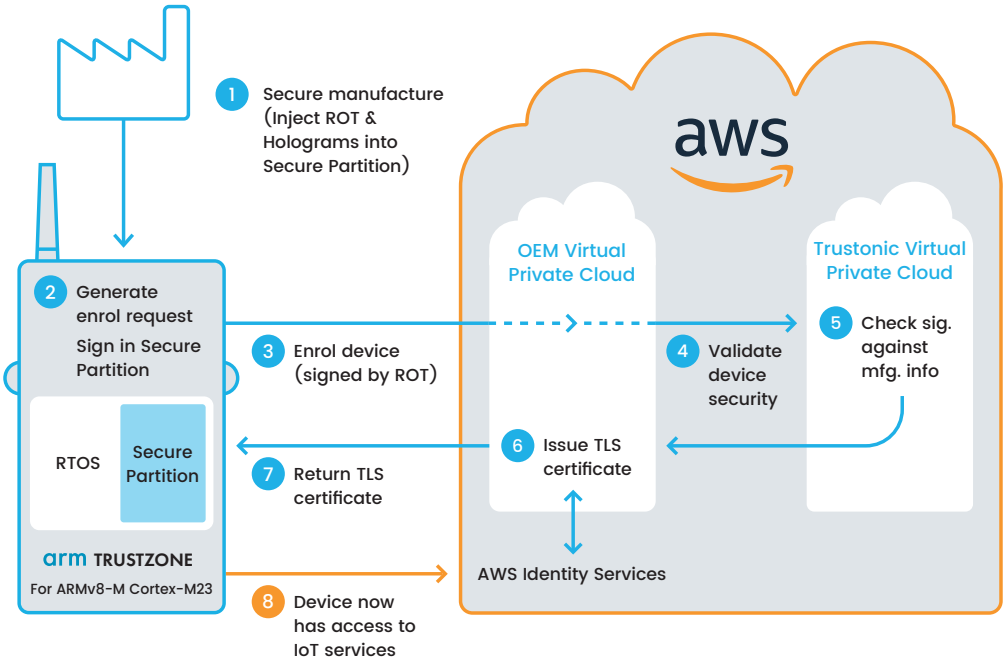
Companies, factories and cities deploying IoT systems need to know that data coming from their sensors and devices really is coming from the actual device, not from a cyber-attack or from a hacker. A good recent example is the hack suffered by Waze.

Customers buying IoT devices need to be sure that the device they have bought is the genuine article – not a fake built from stolen plans or a cheap clone that doesn't meet the functional or safety standards required. Equally, manufacturers of those devices who are supporting large back-end systems need to know that only genuine devices can connect to them. This is to ensure both that the data they generate can be trusted and that their customers don't associate their brand with a sub-optimal experience.

To achieve all of this, you need to be able to trust the device. Trustonic has injected well over 1.2 billion individual device identities and keys into mobile, IoT and other devices to date. The associated keys are only accessible in the most secure part of the device – the Trusted Execution Environment (TEE) on larger, 'A-Class' processors and the Secure Partition on smaller, 'M-Class' processors. Both are protected by ARM TrustZone.

The secure device identity is known as a Root of Trust (think of it like a digital birthmark) providing a unique and provable device identity. TrustZone ensures protected keys and data cannot be accessed by either malware or other software-based attacks. Furthermore, it also enables a Trustonic-secured device to safely identify itself to a back-end service.

Secure provisioning for AWS



- **Device is created with unique identity and key**
- **Device is installed and turned on**
- **Device generates an enrolment request (CSR) for associated cloud IoT services. This is signed in secure world software**

In this demonstration, we are pairing an IoT device using a small/low cost ARMv8-M Cortex-M23 processor with the Amazon Web Service (AWS) IoT Cloud. The AWS IoT cloud leverages x509 client certificates for security and we extend AWS's security model by issuing client certificates automatically. It shows how a freshly-unboxed device can securely enrol with an AWS service, presenting cryptographic proof that it is a valid device from a given manufacturer. In return, it will be issued with an SSL client certificate. Once enrolled, the device can communicate using AWS IoT services, such as MQTT, as shown in the demonstration. Trustonic libraries running in TrustZone and associated strong identify can then be used for further security-sensitive services, such as handling of user data or securing access to peripherals.