KeyScaler Support for Microsoft Azure Sphere

Introduction

IoT security needs to be architected into devices from the moment of inception, and there needs to be a foundation in the devices to deliver secure updates throughout its lifecycle. Devices must have a strong Root of Trust (RoT) in the MCUs/processors/systems and a mechanism to deliver signed and encrypted images either for production and/or for ongoing updates.

This will enable secure production, protect against IP theft, detect device cloning, and help mitigate security breaches. These devices need to connect to different constituents including Microsoft and non-Microsoft assets in operations. KeyScaler is a key component in this ecosystem to extend the trust and automation needed in operations.

What is it?

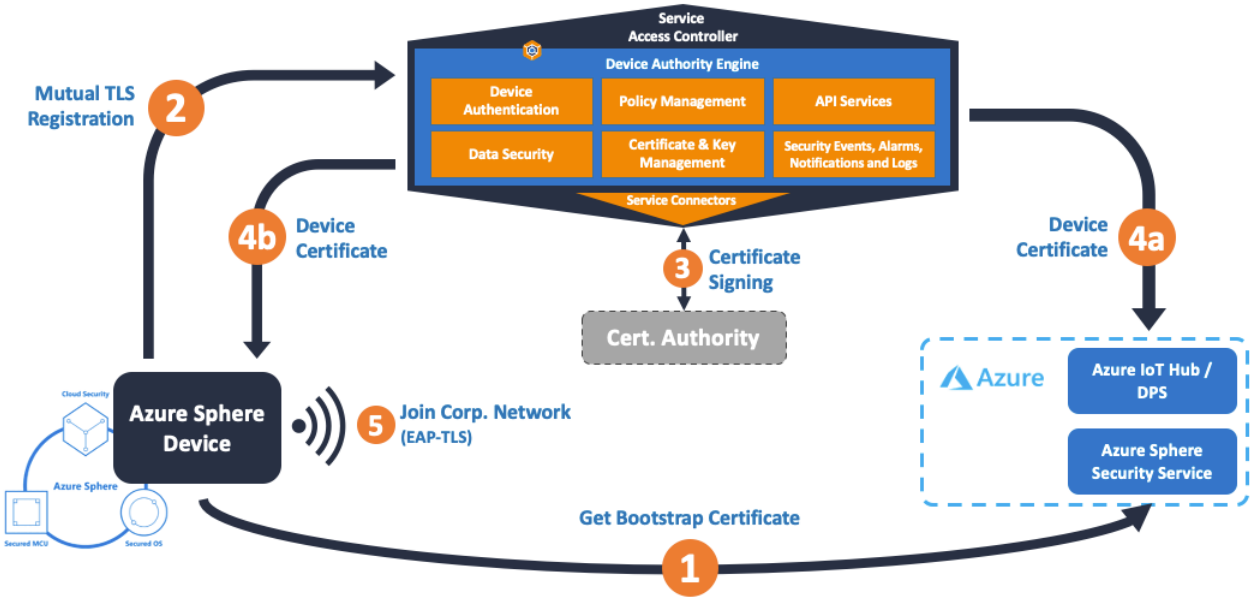
Microsoft Azure Sphere identified and addressed the highly secure devices with the seven properties for network connected devices: a hardware-based root of trust, a small trusted computing base, defense in depth, compartmentalization, certificate-based authentication, security renewal, and failure reporting. Azure Sphere brings together the best of Microsoft's expertise in cloud, software and silicon to provide security foundation and connectivity to create intelligent secure products and accelerate the IoT adoption at scale.

Device Authority KeyScaler platform has the ability to leverage this initial security foundation by enabling Azure Sphere devices to connect to it and provide them with operational certificates to automate and secure device enrolment to any IoT platform. The extended family of security suite to Azure and connectors to HSMs, CAs and IoT platforms will greatly help to accelerate Sphere devices adoption for secure trusted IoT solutions.

What are the benefits?

- Automated PKI certificate solution for Azure Sphere devices – Accelerate time to deployment
- Reduce development time through easily consumable standard APIs
- Increased security of device identities through policy driven credential rotation
- Automation – Support Any IoT Platform, Any HSM, Any CA, including Azure Key Vault for Root of Trust
- Ecosystem of supported partners to accelerate time to revenue
- Completeness of offering in line with evolving standards and legislation (FIDO SDO)
- Increases network security posture by removing use of hardcoded Pre-Shared Keys (PSK) for connecting to enterprise networks

How does it work?



1. On first boot, the Azure Sphere device connects to the Azure Sphere Security Service and receives a short-life bootstrap certificate.

2. The Azure Sphere device then uses that bootstrap certificate to register with the KeyScaler platform, using standard client authentication (mutual) TLS.

3. KeyScaler generates a unique key pair and certificate for the device and submits this to the Certificate Authority configured in the device policy for signing.

4. KeyScaler is now ready to provision the certificate:

   a. KeyScaler delivers the device public certificate to the configured IoT platform, (Azure IoT Hub, Azure DPS, Azure IoT Central, etc...) so that it can be used by the Azure Sphere device to authenticate and connect.

   b. The unique certificate and keypair are delivered to the device, and stored securely in the onboard Azure Sphere certificate store.

5. The device can now use that certificate to join the corporate/enterprise network, utilizing standard EAP-TLS, instead of using hardcoded pre-shared keys (PSK).

Additionally, the device is now ready to connect to cloud services, such as the Azure IoT suite.

DEVICE AUTHORITY