Microsoft IoT Central Connector

Introduction

Device Authority provides solutions to accelerate the deployments by providing trusted automation solutions to make security the foundation to a connected IoT experience. For any service provider who plans to use Microsoft IoT Central for their IoT Application, Device Authority's KeyScaler IoT Central Connector helps customers operationalize device enrolment, identity/Certificate management at scale.

What is it?

Microsoft's IoT Central is an IoT application platform that reduces the burden and cost of developing, managing, and maintaining enterprise-grade IoT solutions. The application delivers the following benefits to customers:

- Simplified PaaS only model for customers who don't want to manage or host an IoT application
- Simplify setting up your IoT solution
- Connect and manage your things with ease
- Rest easy with world-class security and privacy

Azure IoT Central is powered by a number of core components, including Microsoft's Device Provisioning Service (DPS) and IoT Hub. Device Authority has pre-built service connectors to these services which effectively enable customers to enroll devices at scale in a headless way, and provision identities/ certificates without the need for human intervention.

What are the benefits?

- Automates device lifecycle management for IoT – including initial device registration / onboarding, enrolment to chosen IoT application, certificate provisioning, certificate revocation and renewal.

- KeyScaler automatically creates and manages new device enrolments in the configured IoT Central application instance.

- Device Authority's patented Dynamic Device Key Generation (DDKG) provides attestation for devices that do not have an initial trust anchor (keys from the device manufacturing stage)

- Using dynamic keys (i.e. not a single static key) through Azure DPS and Azure IoT Hub, prevents device cloning

- Use KeyScaler as a "security gate" to control automated registration with DPS

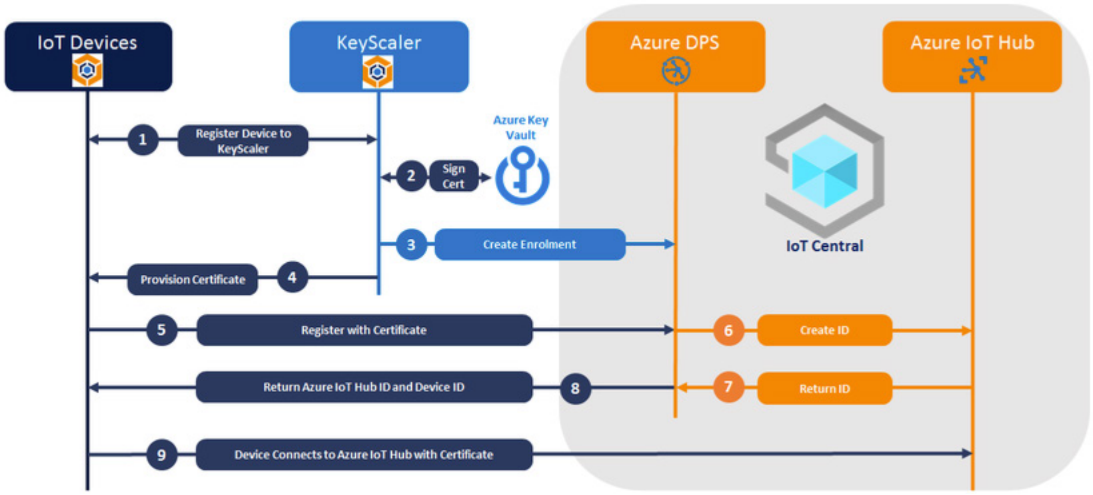
- Combine cost effective private CA certificate Signing Services, optionally backed by Azure Key Vault key storage for securely storing root keys.

- Solves the fundamental challenges of IoT security Automation at scale i.e. How to manage cert expiry, how to manage certificate revocation and renewal

How does it work?

Once the KeyScaler IoT Central connector has been initially setup, IoT devices can then utilize the service for operation. In the diagram above, it is also possible to utilize Key Vault with KeyScaler for certificate signing purposes and key storage.

Prior to devices onboarding to KeyScaler, devices are whitelisted, so that only authorized devices can register and enroll with the platform. Following this initial setup the following flows and processes happen:



Step 1 - When a device powers up, it connects to KeyScaler and registers to the platform (assuming it is an authentic device)

Step 2 - Devices enroll to a group within KeyScaler, where each group has policies assigned to them. In this example each device has to go through a certificate provisioning process and each certificate is signed by a Key in Key Vault.

Step 3 - KeyScaler will then reach out to the IoT Central application and create an enrollment within its Device Provisioning Service.

Step 4 - A signed certificate is then sent to the IoT device securely.

Step 5 - The IoT device then connects to the IoT Central and registers to its DPS.

Step 6 - IoT Central DPS creates the IoT device ID in its IoT Hub

Step 7 - IoT Hub ID is then returned to DPS

Step 8 - IoT Hub ID & Device ID is then returned to the IoT device

Step 9 - IoT device now has a valid certificate and knows which IoT Hub it should connect to, to communicate with the IoT Central application.

Through these steps the whole end-to-end process for certificate provisioning and automation has been achieved without having to touch either the device or IoT application – to provision keys or to create device enrollments. Enabling security lifecycle management at IoT scale and solving the fundamental challenges of how to provision certificates, manage expiry of certificates and get them signed by a trusted entity.

This automation also provides a mechanism to manage the lifecycle of those certificates / identities. Customers can choose through policy to renew certificates at certain intervals and automate the process – required for IoT scale. Also, devices can be quarantined at an individual level, which in turn revokes a device's certificate status – meaning a device is no longer authorized to connect the chosen IoT application. On re-authorization, a device would then go through a process of renewing its credential so it can re-connect.

DEVICE AUTHORITY