Microsoft Key Vault 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. Device Authority's Key Vault Connector helps customers operationalize Key Vault for IoT applications and CA signing purposes, to quickly implement this functionality and leverage existing investments in Microsoft Key Vault.

What is it?

The KeyScaler Key Vault connector has been implemented to connect to Key Vault to automate IoT certificate services. Azure Key Vault is a tool for securely storing and accessing secrets and helps solve the following problems:

- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets

- **Key Management** - Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.

- **Certificate Management** - Azure Key Vault is also a service that lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.

- **Store secrets backed by Hardware Security Modules** - The secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs

Combining Key Vault with KeyScaler platform enables a fully functional private CA model for IoT certificate automation. Enabling management of IoT device attestation, device registration, certificate provisioning, certificate lifecycle management (including revocation & renewal) all with the private keys stored in a robust key store – Key Vault. Additionally, this solution enables customer to utilize a Bring Your Own Key (BYOK) model which can be used to setup the CA with the appropriately but with the customer maintaining and owning their root keys.

What are the benefits?

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

- Cost effective private CA certificate signing services backed by Azure Key Vault key storage for securely storing root keys.

- Enables a BYOK model for customers to setup their own CAs utilizing Key Vault and KeyScaler for trust and automation in IoT

- Accelerate deployments with end-to-end certificate signing and certificate provisioning to devices

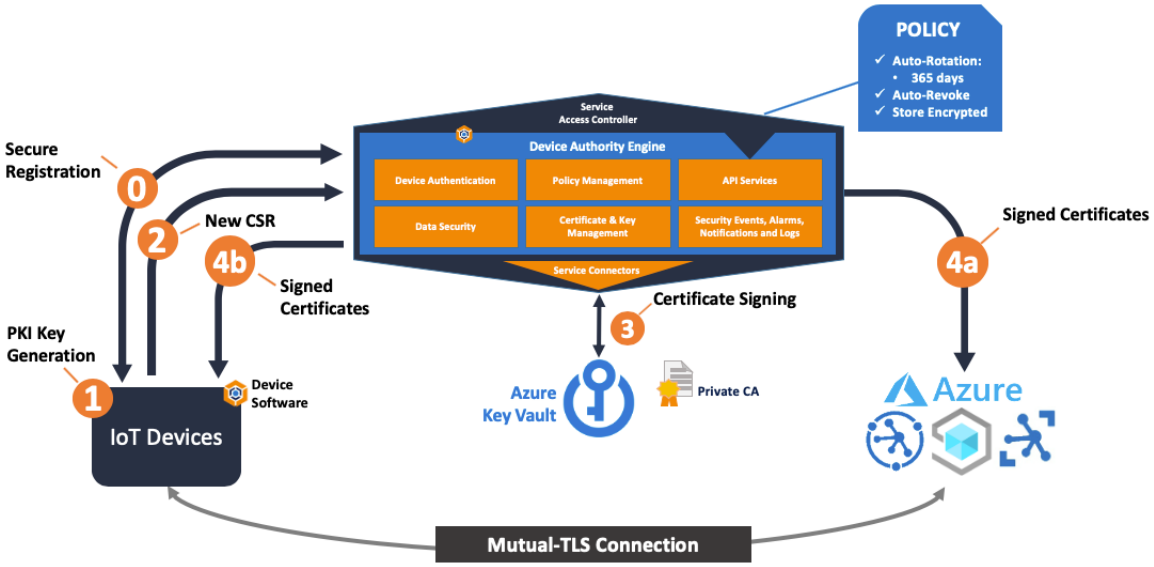
- Flexibility to integrate with HSM Backed key storage – for FIPS 140-2 Level 2 compliance

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

How does it work?

Once KeyScaler and Key Vault have been initially setup, IoT devices can then utilize the service for operation. In the diagram above KeyScaler has been configured with Key Vault (for certificate signing purposes) and can also be configured to enroll devices to Azure Device Provisioning Service (DPS), IoT Hub or IoT Central, using KeyScaler prebuilt connectors for full IoT security onboarding and lifecycle management automation.

Prior to devices onboarding to KeyScaler, they 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 0 - When a device powers up, it connects to KeyScaler and registers to the platform (assuming it is an authentic device)

Step 1 - 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. Thus, the device will receive instructions that it needs to generate a key pair on the device.

Step 2 - The output of step 1 will be a Certificate Signing Request which is then sent to KeyScaler for signing through the appropriate signing authority

Step 3 - KeyScaler has been configured to sign certificates utilizing the keys inside Key Vault. Thus with this step, KeyScaler reaches out to Key Vault and gets the Certificate Signed.

Step 4a - KeyScaler now pushes the signed identity into the chosen IoT application – This could be through and enrollment process with DPS or directly into a chosen IoT Hub.

Step 4b - KeyScaler now pushes the signed identity to the IoT device.

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 devices certificate status – meaning a device is no longer authorized to connect the chosen IoT application. On re-authorization, a device would go through a process of renewing its credential so it can re-connect.

DEVICE AUTHORITY