Microsoft IoT Edge Gateway Service Module

Introduction

Edge computing has become an essential component of the overall IoT infrastructure. Azure IoT Edge offers a managed serviced built on Azure IoT Hub to deploy customer cloud workloads, Azure/third party services or user specific business logic at the edge.

Device Authority has developed a custom module for Azure IoT Edge to increase the security posture of your IoT Edge Gateways and Leaf Devices. KeyScaler IoT Edge Gateway Service automates the life cycle management of certificates for both Edge Gateways and connected Leaf Devices. Furthermore, the KeyScaler platform operationalizes the onboarding of Leaf Devices into IoT hub using X.509 certificates.

The KeyScaler platform brings IoT IAM to the edge enabling policy driven credential delivery and management, secure registration and provisioning into Azure services (e.g. IoT Hub and DPS) and end-to-end data crypto.

What is it?

The KeyScaler IoT Edge Gateway Service is an IoT Edge Custom Module that enables automated certificate lifecycle management for gateways and Leaf Devices. The core capabilities of the Edge Gateway Service Module include: policy driven key (X.509 certificates) provisioning, revocation and renewal. The service module also provisions and manages intermediate (Sub CA) certificates used by the IoT Edge Gateway to generate and sign Workload and EdgeHub certs locally on the Gateway itself.

What are the benefits?

- Complete automated life cycle management for IoT Edge Gateways and Leaf Devices.
- Streamline IoT Gateway deployment process with KeyScaler Gateway Service Module.
- Easy to deploy using native Azure Edge Module management functions
- Increase operational efficiencies by leveraging existing enterprise PKI .
- Issue certificates for IoT Edge Gateways and Leaf Devices
- KeyScaler ADCS, Public CA connectors, Key Vault and Private CA
- Support for both DDKG and PKI Signature+ devices.

How does it work?

- Automated Certificate management for IoT Edge Gateway – Policy based certificate life cycle management. Provision intermediate certificates (Sub CA) on IoT Edge Gateway for certificate signing.
- Automated Certificate management for Leaf Devices – Policy based certificate life cycle management

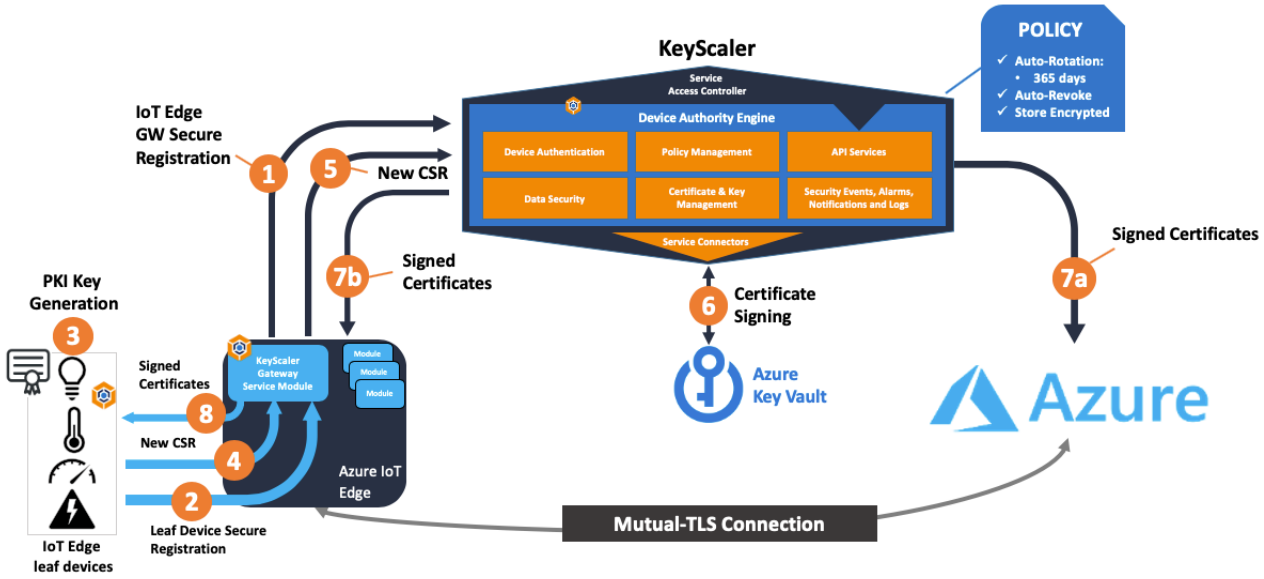
for IoT Leaf Devices connected to IoT Edge Gateway.

• Support for both DDKG and PKI Signature+ authentication methods.

• Leaf Device provisioning into IoT Hub using X.509 certificates. Zero-touch provisioning using X.509 certificates. KeyScaler provision Leaf Devices as children of a parent IoT Edge Gateway to enable Leaf Device offline operation.

• KeyScaler Gateway Service Custom Module – Easy to deploy using IoT Hub's Edge Module management.

• Streamline IoT Edge deployments at scale – KeyScaler enables automation of trust and credential management for IoT Edge Gateways and Leaf Devices



Step 1 - Edge Gateway registers and authenticates to KeyScaler.

Step 2 - Leaf Device registers and authenticate via Edge Gateway Service Module to KeyScaler.

Step 3 - KeyScaler sends down a certificate generation instruction, providing certificate generation details, such as Common Name (CN), and key size. Device generates key pair and PKCS#10 (Certificate Signing Request).

Step 4 - Leaf Device submits CSR to Edge Gateway.

Step 5 - Edge Gateway authenticates request and forwards CSR to KeyScaler.

Step 6 - KeyScaler validates the CSR against the certificate management policy and submits it to the configured Certificate Authority for signing (in this example, a private CA created in Key Vault).

Step 7 - KeyScaler performs two actions:

- KeyScaler delivers the signed certificate to Azure IoT Hub/DPS and configures the device instance in that service.
- KeyScaler delivers the signed certificate to Edge Gateway.

Step 8 - Edge Gateway delivers signed certificate to the Leaf Device.

DEVICE AUTHORITY