Technical Insight Guide:

Security Suite for Microsoft Azure IoT

To accelerate and build trusted IoT solutions

IoT creates new security and operational challenges introduced by the scale, variety of devices with different characteristics connecting to IoT Platforms and applications. Without trusted and automated security operational management, the envisioned benefits and adoption of IoT will not be realized.

For Microsoft, their customers and partners, Device Authority brings to market a complimentary set of solutions that enable their end to end service offerings with enhanced security. This helps to accelerate, optimize and leverage their investments in their Internet of Things (IoT) deployments.

The Security Suite benefits customers, partners and IoT service providers that integrate Microsoft Azure IoT services, including:

- IoT Central
- IoT Edge
- Device Provisioning Service (DPS)
- Azure IoT Hub
- Azure Key Vault enabling private CA Services.
- Microsoft Sphere implementations for secure Microcontroller (MCU) device
- Microsoft Active Directory (AD) for Authorization for their IoT end points

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 Azure, DPS and Sphere alone cannot deliver all the essential security functionalities without undertaking custom development. Device Authority's KeyScaler platform helps customers to quickly implement this functionality and leverage their existing investments in Microsoft infrastructure.

Based on customer demand and real use case requirements, KeyScaler delivers eleven significant solution components that are included in the Security Suite for Microsoft:

• **IoT Central** – For building high security enterprise-grade IoT applications rapidly

• **IoT Edge Gateway** – To provide a gateway proxy which will forward on authorized requests to KeyScaler from leaf nodes connecting to it, to provision IoT leaf devices with certificates, and enabling mutual TLS between it and IoT Hub

• **Device Attestation and Automation for DPS** – Source of truth for automated IoT device onboarding

• **Azure IoT Hub Certificate Provisioning Connector** – For provisioning x.509 Certificates to Azure IoT Hub

• **Azure Event Hub -** Enables IoT Edge devices to securely transfer real-time encrypted data into Azure Events Hub for consumption and to get the data decrypted by back-end applications

• **Azure IoT Hub SAS Token** – Used to authorize and provision Shared Access Signature (SAS) tokens to devices where PKI is not used

• **Microsoft (AD) Connector** - To provide integration into Enterprise networks to provide authorization to IoT end points

• **Microsoft AD CS Connector** – To provide integration into Enterprise networks for Certificate Services

• **Microsoft Key Vault Connector** – Enables the use of Key Vault for Private Certificate Authority services, including the use of customer BYOK.

• **Azure Kubernetes Services (AKS) -** Allows for a swifter deployment of KeyScaler Platform and its services

• **Windows Credential Management Agent** – For onboarding and certificate provisioning to Windows based IoT devices

KeyScaler platform can manage and provision both the devices at the edge and the IoT Platform, Azure IoT Hub, with x.509 certificates, which enables them to securely communicate and ultimately transfer sensitive data from device to Azure IoT Hub over a mutual Transport Layer Security (TLS) connection.

Azure IoT Central Connector

• Enables access to Microsoft's fully managed, highly scalable IoT SaaS solution to build enterprise-grade IoT applications rapidly.

• Provide real-time updates regarding device certificate management events within the KeyScaler platform to any Azure IoT Central application

• Leverages KeyScaler Enhanced Platform Integration Connector (EPIC) to receive updates on device certificates that have been issued, to automatically provision new devices to a specific IoT Central application instance as well as removing the device when the certificate is revoked.

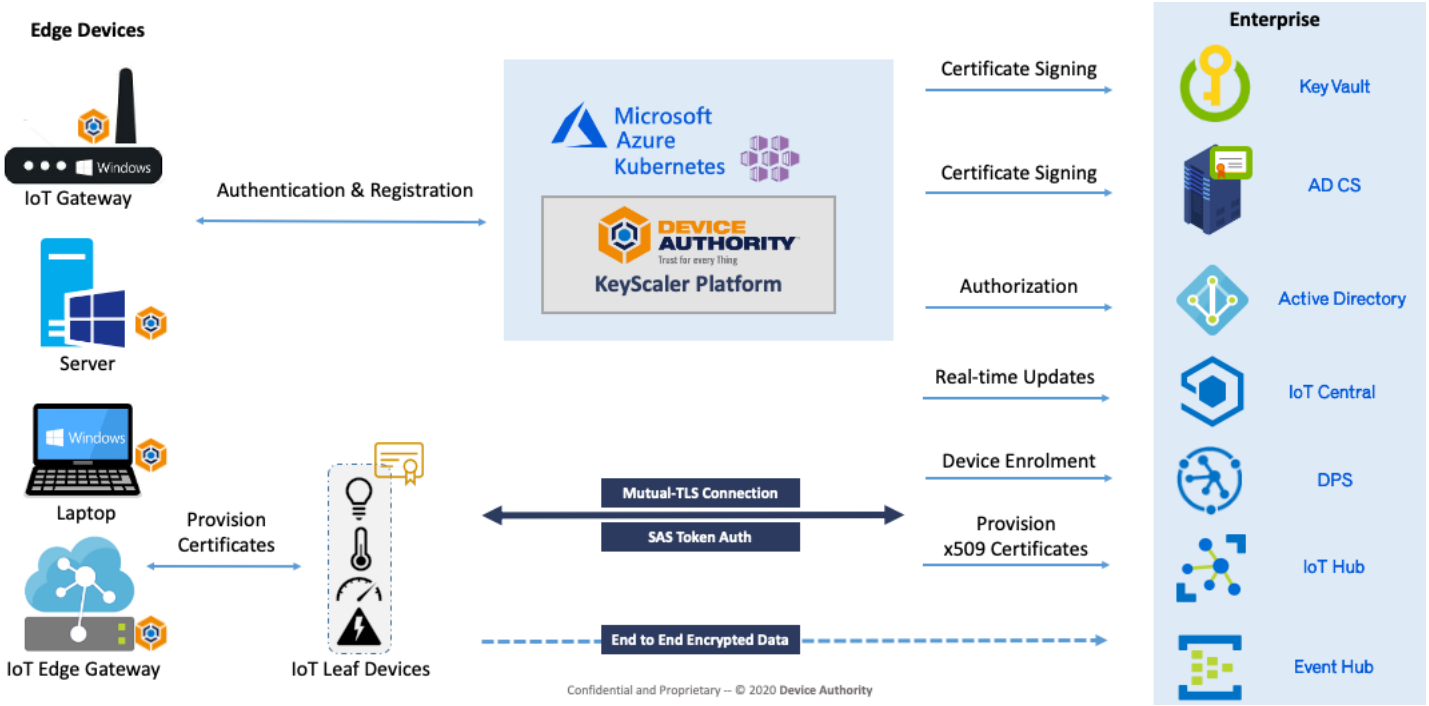


Figure 1 - Microsoft based IoT Ecosystem enabled with Device Authority

Azure DPS Connector

• Leverages KeyScaler Enhanced Platform Integration Connector (EPIC)

• Automatically provisions device registration ID to Azure DPS

• 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

Azure IoT Hub Connector

• KeyScaler automatically creates a 'Thing' on Azure IoT Hub and provisions it with a certificate

• Leverages KeyScaler Enhanced Platform Integration Connector (EPIC) service to build the connector to deliver real-time x.509 certificates to Azure IoT Hub

• Azure management API credentials are stored securely in KeyScaler as a connection configuration i.e. Not written to disk in a configuration file

• Azure management API credentials are stored securely in KeyScaler as connection configuration i.e. not written to disk in a configuration file

• Ability to automate and manage ongoing certificate lifecycle through policy i.e. solving certificate expiry issues and removing the need for long life certificates

Azure IoT Edge

• With Device Authority Gateway Service Module deployed in a dockerized container, it enables Azure IoT Edge gateways to register with KeyScaler and act as a proxy to manage and deliver certificates to local ecosystem devices. Certificates are made available to the IoT Edge Security Daemon via a workload API

• By moving certain workloads to the edge of the network, IoT devices spend less time communicating with the cloud, react more quickly to local changes and operate reliably even in extended offline periods

Azure Key Vault

• Combined with KeyScaler, enables cost effective private CA certificate Signing Services backed by Azure Key Vault key storage for securely storing root keys.

• Leverages KeyScaler Enhanced Platform Integration Connector (EPIC) to send device CSR to get signed by the Private Key stored in Azure Key Vault

• Enables a BYOK model for customers to setup their own CAs utilizing KeyVault and KeyScaler for trust and automation in IoT

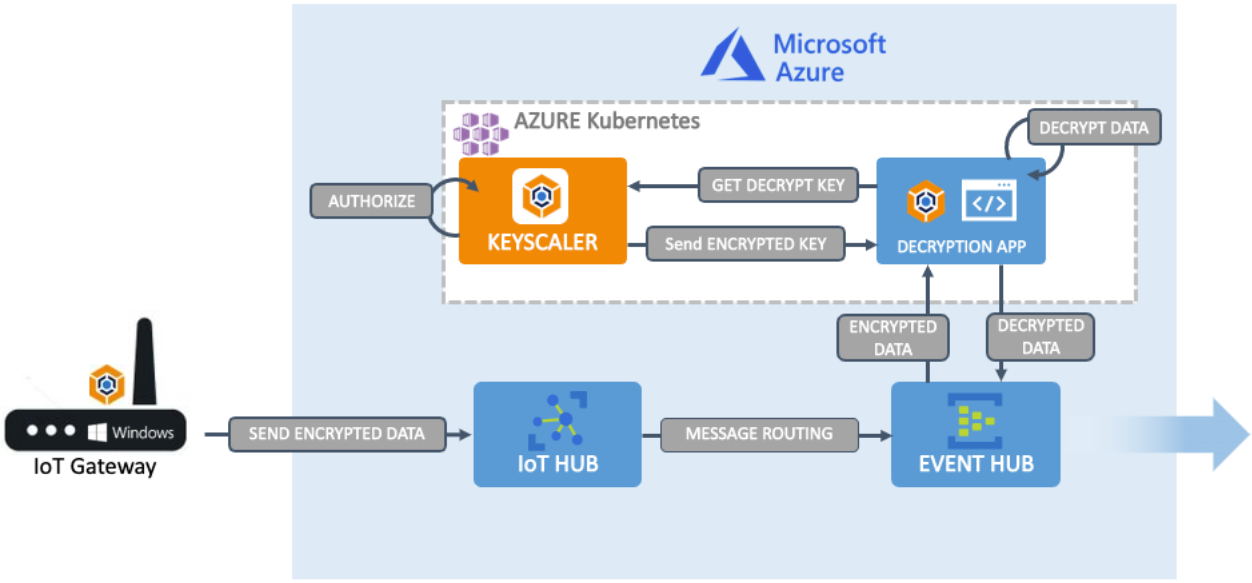
• Accelerate deployments with end-to-end Certificate Signing and Certificate Provisioning to devices

Azure Event Hub Data Privacy

• Integration with Azure Event Hub enables the secure transfer of real-time encrypted data from edge device and leverages Azure Data Services to provide data insights faster

• Allows customers to focus on building real-time big data pipelines and respond to the immediate business challenges instead of managing data security infrastructure

• Enhanced data privacy features, providing end-to-end data privacy using dynamic encryption keys and policy provisioning to the device ensuring compliance with regulations such as HIPAA and GDPR



Azure IoT Hub SAS Tokens

• KeyScaler works with Azure IoT Hub to help ensure seamless delivery of Shared Access Signature (SAS) tokens providing authentication of the device to IoT Hub

• KeyScaler provides the capability to manage SAS token expiration and renewal

• Devices can authenticate to KeyScaler and receive SAS tokens that authorize them to connect to Azure IoT Hub. This provides automated centralized IoT credential management, reduced risk and improved efficiencies for customers

• Customers can take advantage of granular authorization policies, to restrict access to certain Azure IoT services or end points

Deploying KeyScaler in Azure Kubernetes (AKS)

• Using a managed container orchestration service, such as AKS, provides a quick and easy framework for deploying KeyScaler and its services without complications with application details such as versions and configurations

• Enables rapid scaling and management of KeyScaler as a containerized Docker application

• Flexibility, automation and reduced management overhead are benefits for our customers' administrators and developers

• Developers can use KeyScaler API's and EPIC systems while remaining free to choose the best toolsets, dramatically reducing IT costs, both CAPEX and OPEX, while improving productivity

Windows Credential Manager

• Credential Management Agent supports Windows-based IoT devices. This includes support for Windows 8, 10, 2012 Server and 2016 Server.

• Can be installed as a Windows service

- Enables Windows devices to securely register and authenticate to KeyScaler
- Supports certificate provisioning and management
- Supports Secure Soft Storage for device-bound certificates

Microsoft Active Directory Connector

- Pre-built integrated connector allows Enterprise IT to manage IoT Endpoint security access
- Leverage AD group access controls to IoT devices / Device group

Microsoft Active Directory Certificate Services (AD CS)

- Leveraging KeyScaler EPIC service, a new connector enables integration with Microsoft AD CS Services
- Enabling customers to leverage the existing public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities for their organization to provide certificate-based authentication for any IoT devices registered with KeyScaler

Example Use Case

Healthcare providers and institutions require secure communications between gateways used in a patient monitoring solutions. Ensuring strong data security, privacy and compliance is important for this use case. The solution shown in Figure 2 details the use of Windows-based Gateways installed in various locations in a healthcare deployment, with Azure IoT Hub as the data aggregation point.

Security needs to be maintained for medical devices connecting to Gateway 1, and patient data security and privacy needs to be assured from gateway to gateway. The solution required a third party Certificate Authority (CA) for additional trust and PKI certificate signing. KeyScaler provides extensive operations and security management; automating security from Gateway-to-Gateway, managing device identity, data integrity, security, and privacy along with automating the certificate-based authentication into Microsoft Azure IoT Hub. Device Authority's patented Dynamic Device Key Generation technology solves the problem of managing crypto keys at scale without sharing over the network, and authorization between Gateways.

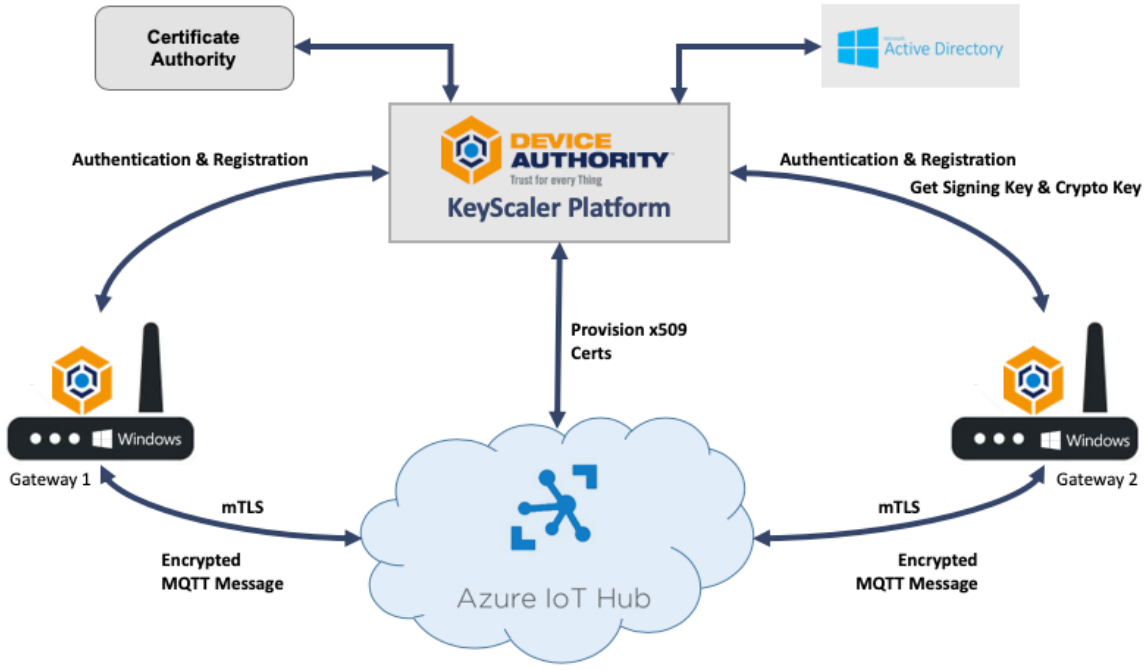


Figure 3 - Remote patient monitoring with multiple Windows based Gateways connected to Azure IoT Hub

Key Benefits and Value for Microsoft Azure Customers and Partners

Enhanced Security

- Increased security through KeyScaler registration and policy driven certificate provisioning and management process
- Lock down and rotate device certificates and tokens – prevent device clones
- Key Vault integration provides a secure mechanism to store Private Keys as a cost-effective alternative to using a dedicated HSM
- KeyScaler supports both Shared Access Signature (SAS) token and Certificate credentials for devices connecting to Azure IoT Hub
- With AD CS integration customers can leverage the existing investment in PKI infrastructure and gain enhanced visibility of their device within enterprise services

Accelerate Deployment

- KeyScaler is offered as a Managed Service for fast, easy and low risk implementation and available for installation for on-premise or on Azure Kubernetes Cloud
- Reduces complexity and timelines to deployment
- Device provisioning for zero-touch secure identity management is the key to minimize operational burden and maximize focus on the experience
- Key Vault integration accelerates deployments with end to end Certificate Signing and Certificate Provisioning to devices within Azure IoT ecosystem
- Microsoft AD connector to integrate to Enterprise IT and manage IoT Endpoint security access

- Rapidly onboard large number of devices to Azure IoT and Azure DPS to scale up IoT deployment

Flexible Integration and Extended Support

- Flexible Certificate Authority (CA), for both Public and Private CA, Hardware Security Module (HSM) integrations for certificate signing and issuance
- Expanded support for IoT projects using Windows based endpoints (in addition to Linux)
- Expanded support for IoT Leaf devices via IoT Edge gateway module
- Provision other security assets such as data encryption keys, manage code signing for secure updates
- Greater support for enterprise opportunities where Windows desktop support is required
- More flexible registration controls provide device attestations and automation for DPS
- Whitelist devices based on hardware attributes, without needing to provision unique keys at factory
- Use KeyScaler as a "security gate" to control automated registration with DPS

Summary

Device Authority provides a set of complimentary Microsoft-compatible security solutions for Microsoft customers and partners, to help optimize and leverage existing investments in Microsoft Azure, Azure Kubernetes, IoT Central, IoT Edge, Device Provisioning Service (DPS), Azure IoT Hub, Azure Key Vault, Azure Event Hub, infrastructure, tools, skills and resources for a connected end-to-end secure IoT experience.

Who We Are

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management, policy based end-to-end data security/ encryption and secure updates.

With offices in Fremont, California and Reading, UK, Device Authority partners with the leading IoT ecosystem providers, including AWS, DigiCert, Gemalto, HID Global, Microsoft, nCipher Security, PTC, Thales, Venafi, Wipro and more. Keep updated by visiting www.deviceauthority.com, following us on Twitter @DeviceAuthority and subscribing to our BrightTALK channel.

sales@deviceauthority.com
www.deviceauthority.com

DEVICE AUTHORITY™