Security Suite for Microsoft Azure IoT

Delivered by Device Authority KeyScaler

Introduction

IoT presents opportunities across every industry, including healthcare / medical devices, industrial / manufacturing, automotive, utilities, oil and gas. However, it is also creating attack surfaces, introduced by the scale and pace of adoption, as well as the consequences of compromised security.

While many IoT platform vendors claim their functionality enables easy device enrollments and security management, most platforms provide open and flexible interfaces and shift the responsibility to customers to adopt the right integration and policies as per their application requirements. While there are some home-grown implementations by platform vendors, many industry experts and analysts have talked about the need for IoT IAM functionality, substantially different from traditional IAM.

For Microsoft, their customers and partners, Device Authority presents to the market a Security Suite that enables their end to end service offerings with enhanced security, and to accelerate, optimize and leverage their investments in their Internet of Things (IoT) deployments.

What is included in the Security Suite?

Azure IoT Central Connector

- Automatically enrolls devices to Azure IoT Central application instances
- Utilizes x.509 Group Enrollment feature for enhanced certificate-based authentication to Azure IoT Central
- Supports assigning appropriate IoT Central Device Template to enrolled device instances
- Device Authority's patented Dynamic Device Key Generation (DDKG) provides attestation for devices that do not have initial trust anchor (keys from the manufacturing)

Azure DPS Connector

- Automatically enrolls devices to Azure DPS
- Leverages KeyScaler Enhanced Platform Integration Connector (EPIC)
- Automatically provisions KeyScaler device certificates to Azure DPS
- Device Authority's patented Dynamic Device Key Generation (DDKG) provides attestation for devices that do not have initial trust anchor (keys from the manufacturing)

Azure IoT Hub Connector

- Automates and secures enrolment process; registering and provisioning devices to Azure IoT Hub
- Leverages KeyScaler Enhanced Platform Integration Connector (EPIC) to deliver real-time x.509 certificates to Azure IoT Hub
- KeyScaler works with Azure IoT Hub to help ensure seamless delivery of SAS tokens

Azure IoT Edge Gateway

- 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 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 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 Key Vault and KeyScaler for trust and automation in IoT
- Accelerate deployments with end to end Certificate Signing and Certificate Provisioning to devices

Microsoft Active Directory (AD) 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 connector service, a new connector enables integration with Microsoft AD CS Services
- Allow 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

Azure Event Hub Data Privacy

- Secure transfer of real-time encrypted data from edge device, leverages Azure Data Services to provide data insights faster
- Enhanced data privacy features, providing end-to-end data privacy using dynamic encryption keys and policy provisioning to device ensuring compliance to regulations such as HIPAA and GDPR

Windows Credential Manager

- Drop-in Windows Credential manager for Windows end-points
- Credential Management Agent supports Windows-based IoT devices. This includes support for Windows 8, 10, 2012 Server and 2016 Server

What are the benefits?

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
- KeyScaler supports both Shared Access Signatures (SAS) tokens and certificate credentials for devices connecting to Azure IoT services
- Key Vault integration provides a secure mechanism to store Private Keys as a cost-effective alternative to using a dedicated HSM
- 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 also available for installation for on-premise or on Azure Kubernetes Cloud
- Reduces complexity and timelines to deployment
- Microsoft AD connector integrates to Enterprise IT and manage IoT Endpoint security access
- Rapidly onboard large number of devices to Azure IoT Hub, DPS, and IoT Central applications
- KeyVault integration accelerates deployments with end to end Certificate Signing and Certificate Provisioning to devices within Azure IoT ecosystem

Flexible Integration and Extended Support

- Flexible Certificate Authority (CA), Hardware Security Module (HSM) integrations for certificate signing and issuance
- Expanded support for IoT projects using Windows (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
- More flexible registration controls provide device attestation and automation for DPS and IoT Central
- 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 and IoT Central

Azure IoT customers are using the Security Suite for:

Device-bound Data Security, Operations and Automation: Companies are using the Security Suite to protect their IoT devices, applications and data through automation without human intervention for Identity, Authentication and Data Security

End-to-End Data-Centric Security and Device Authentication – Companies evaluating Azure IoT have engaged with us to provide robust, scalable and easy to integrate end-to-end encryption and identity solutions for their devices.

GDPR and HIPAA Compliance - Companies are using the Azure Event Hub Connector for policy-based encryption of personal data.

How do I trial, evaluate or buy the Security Suite?

Contact us!

Our team will be happy to speak with you to understand your IoT use cases and security challenges in more detail. We can provide a demonstration of exactly how the connectors work, and you can gain value and knowledge instantly.

About Device Authority

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, Wipro and more.

Keep updated by visiting www.deviceauthority.com, following @DeviceAuthority on Twitter and subscribing to our BrightTALK channel.