IOT SECURITY LIFECYCLE MANAGEMENT

WITH DEVICE AUTHORITY KEYSCALER AND MICROSOFT AZURE

This eBook has been created for customers considering or currently deploying IoT projects in Azure, and for Microsoft to support their customers.

Introduction

The Internet of Things (IoT) presents a massive business opportunity across almost every industry. But to realize that opportunity, enterprise IoT security must become a primary focus. IoT brings new security challenges introduced by the scale and pace of adoption, as well as the legal and safety consequences of compromised security.

Until now, security has been treated as an afterthought; by adding layers of security after devices are delivered, with infrastructure and applications already in place. But security for IoT is too important to be treated as an afterthought. IoT's unique characteristics are also forcing a fundamental rethink about how Enterprises need to implement security management for devices and data.

IoT use cases are all about the data. IoT applications can't trust the data unless the device is trusted. If the device and data it collects can't be trusted, there is no point collecting it, analyzing it, and making an incorrect decision or policy change. Imagine if a doctor or clinician adjusts the wrong dose of medication for a connected medical device based on untrusted data; this is a patient safety and healthcare issue. To address this challenge effectively there needs to be a device-bound data security model.

Microsoft has conducted a large amount of research to create the features and flexible interfaces for a Secure by Design approach and simplify how to build IoT solutions as part of the Azure IoT platform. The rich set of components in Azure enable customers to adopt the right integration and policies as per their application requirements.

Identity and Access Management (IAM) for IoT is an important capability to provide trust and automation as an integral part of IoT platforms. IoT IAM is the security glue across core constituents of IoT solutions, to extend the proven PKI trust and automation, including IoT platforms, edge devices, HSMs, CAs and data security platforms.

Device Authority's KeyScaler, the industry's first device centric IoT IAM platform, is a perfect companion to Azure IoT components. KeyScaler acts as the glue to build end-to-end service offerings with enhanced security, to help organizations accelerate deployments, and also leverage their existing enterprise resources.

Microsoft and Device Authority have been actively working together to provide robust and simplified Enterprise IoT solutions. The following Insight Guide outlines the considerations for Enterprise IoT Security Solutions including Microsoft Azure and Device Authority KeyScaler.

Enterprise IoT Security Requirements

Key Requirements for any Enterprise IoT Security Solution

- Device and Data Security
- Implementing and running security operations at IoT scale
- Meeting Compliance requirements and requests

- Meeting performance requirements as per the use case

IoT is not the same as traditional Enterprise IT

- Devices are often constrained with no User Interface (UI)
- Devices may be in areas that are not easily accessible
- Devices are expected to be running for a long time, operational downtime will have service impacts
- Devices may or may not be network connected, and may not have IP connectivity
- Legacy OT devices exist with proprietary protocols and no connection

Secure by Design and Security Lifecycle Management

In recent years there has been the Mirai DDoS ("Distributed Denial of Service"), and WannaCry ransomware attacks that are forcing us to think about security differently; responding with defense in depth and with a Secure by Design approach.

The compelling economic and social benefits envisioned with the IoT ecosystem (convergence of Digital + Physical) are at risk because we do not have a way to manage the scale and complexity of device-centric relationships and the data collected and consumed. Existing IT security solutions evolved as an afterthought and fail to protect IoT solutions. The traditional detect and respond methods for security management, and human identity-centric IAM solutions do not work for IoT devices. The manual processes are fraught with security holes and operational challenges and cannot scale for IoT.

In March 2018, the UK government published a report titled "Secure by Design: Improving the cyber security of consumer Internet of Things Report" which aims to shift the burden of IoT security from the consumer or end user to other parties including device manufacturers, IoT service providers and application developers in an effort to improve security and ultimately safety. The report outlines a proposed code of practice, which includes 13 items that focus on the need for security, privacy and safety for individuals and personal data, while also recognizing the threat of cyberattacks launched from IoT devices. Even more recently, in May 2019, the UK Department for Digital, Culture, Media and Sport (DCMS) announced it is launching a consultation on how it can regulate the industry to better secure IoT devices.

In September 2018 California stepped into the forefront of this issue by enacting Senate Bill 327, the Internet of Things Cybersecurity bill (which will become law on January 1, 2020) that requires manufacturers to equip connected devices with reasonable security features protecting both the device and its data. The law's main focus is to utilize secure authentication to create trust in IoT devices and protect data privacy by preventing unauthorized access.

In 2019, members of US Congress introduced the IoT Cybersecurity Improvement Act of 2019, to help improve cybersecurity for IoT Devices. It requires NIST to issue recommendations addressing the Secure

Development, Identity Management, Software Patching/Updates and configuration management of IoT devices.

IoT's unique characteristics and government regulations are forcing a fundamental rethink about how IoT devices need to be designed and programmed with trusted root keys and automation for ownership transfer when devices are deployed in the Enterprise.

There is an opportunity to redefine Security by Design, from the beginning, by adopting the right security model and technologies. An IoT security breach goes beyond simple data loss, it's also a safety issue, with potentially disastrous impact. Enterprises must get IoT security right from the start to realize its full potential. Everyone, including Governments, regulatory bodies and standards groups are being forced to rethink this issue.

IoT use cases present new security challenges:

- Devices need to have proper resources to protect the secrets and prevent IP theft and data breaches
- Root of Trust and device bound Identity are the core foundational components for trust and automation.
- Implementations need to look at device bound data security.
- Data centric security, independent of network or human is required for any critical use case.
- Use cases span across disparate entities including IoT Platforms. Often a security automation layer becomes an important.
- Majority of the IIoT use cases are expected to be edge centric. The level of security required at the edge is higher since data isn't sent to the cloud over the network. Also, the devices at the edge are prone to attacks and hacks. Along with delivering edge trust, cloud managed and leveraged are part of typical use cases.
- Include the standards driven and proven trust infrastructure like PKI as trust fabric

Microsoft Azure needs secure lifecycle management at scale to accelerate IoT solutions and deployments

Microsoft Azure provides several capabilities and features to build and deploy IoT applications, solutions, services in a better, faster, more cost-efficient and integrated way. Microsoft talk about a shared responsibility, providing support with relevant tools but it is ultimately the customer's responsibility to build the right security model that works for their requirements and integrates with Azure. Another key requirement for IoT use cases is the binding and protecting of the secrets (private keys, crypto keys, authentication credentials) to the devices.

IoT Security Model, Components, Guidelines

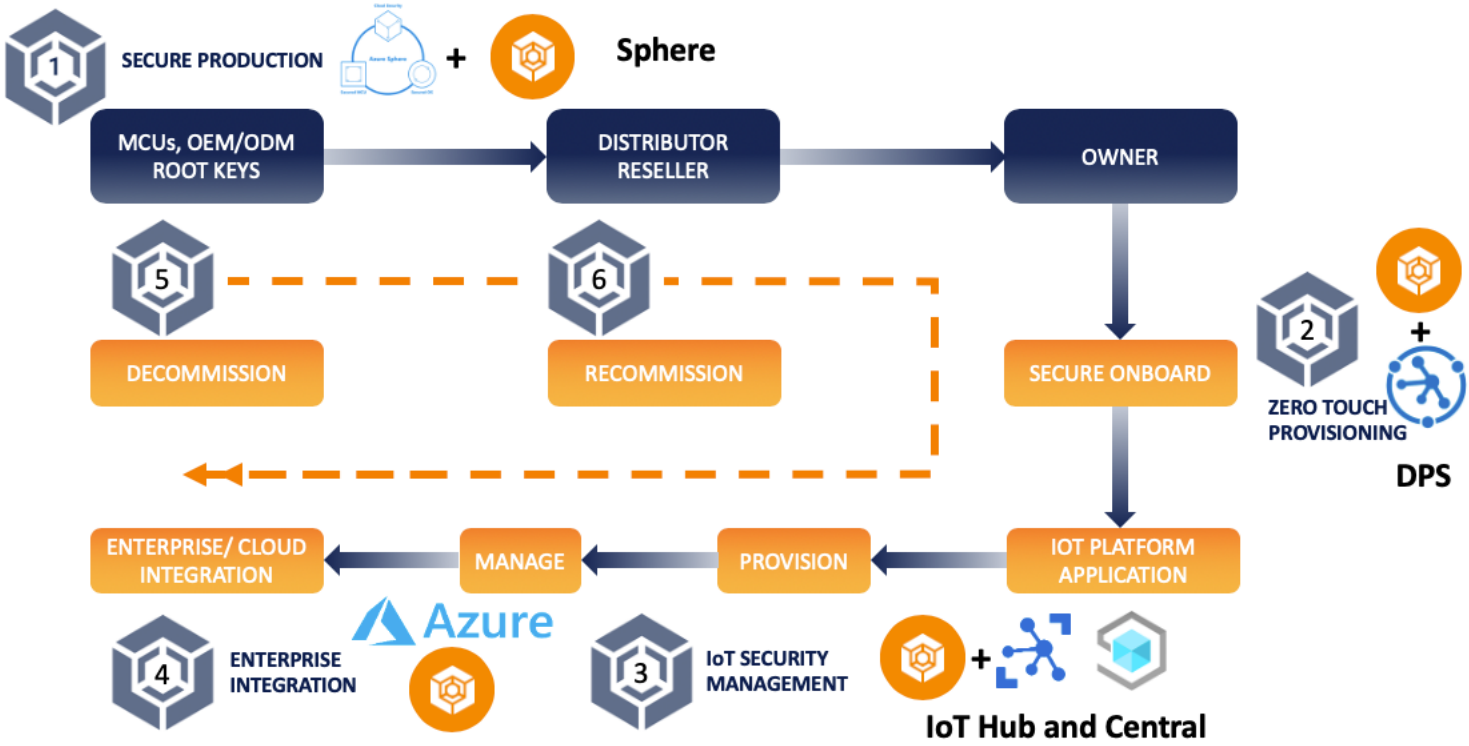
Key Functional Blocks

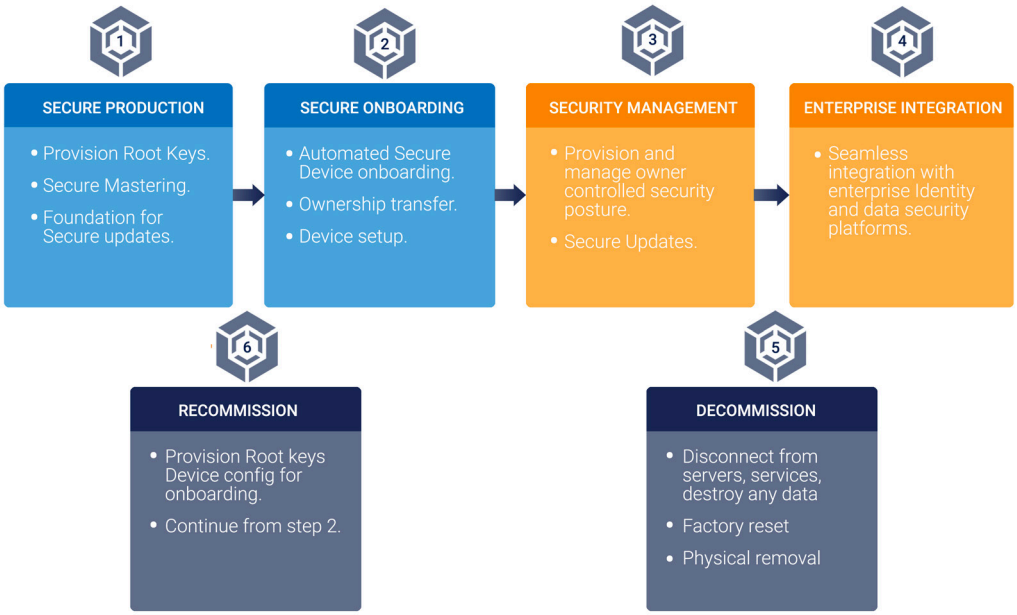
- **Device Trust**: Establishing and managing device identity and integrity
- **Data Trust:** Policy-driven end-to-end data security, integrity, privacy from creation to consumption
- **Operationalizing the Trust:** Automating at IoT scale and interfacing to the standards based, proven technologies/products. E.g. Enterprise PKI products

Note: The Enterprise IoT security solutions need to implement the above functional blocks as interconnected modules, not in isolation, in order to meet the IoT scale, data security, and compliance requirements.

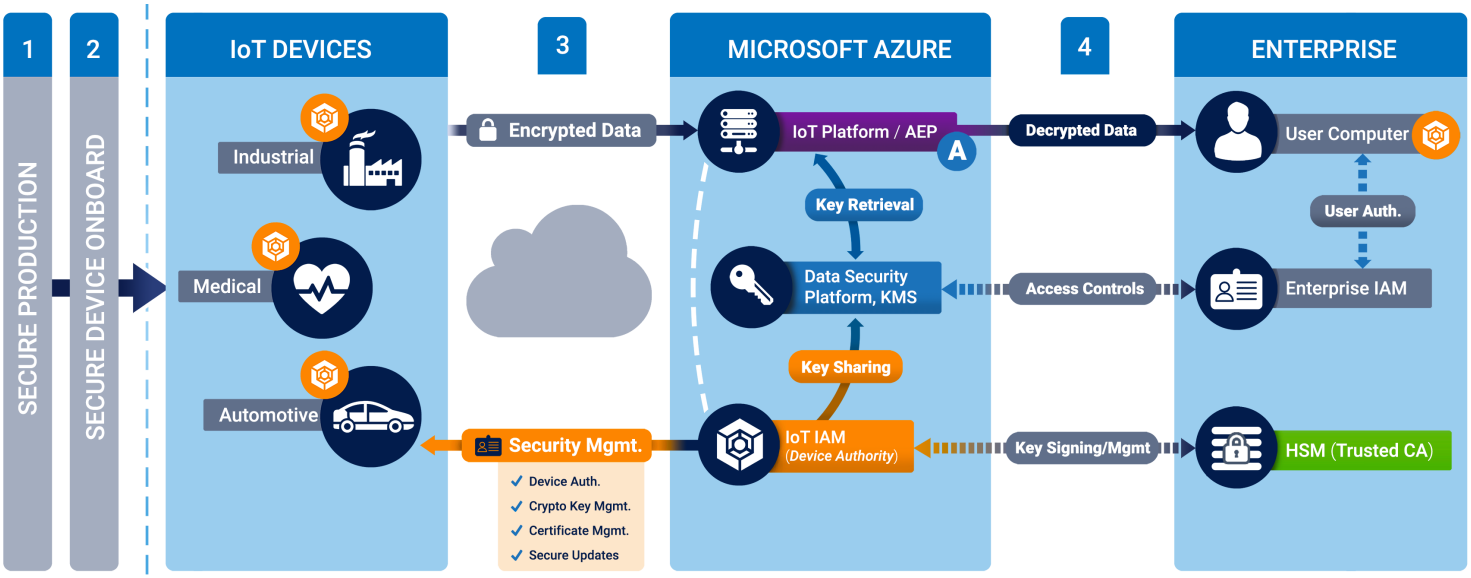
Security Lifecycle Management for the IoT Device Journey with Azure IoT and Device Authority KeyScaler

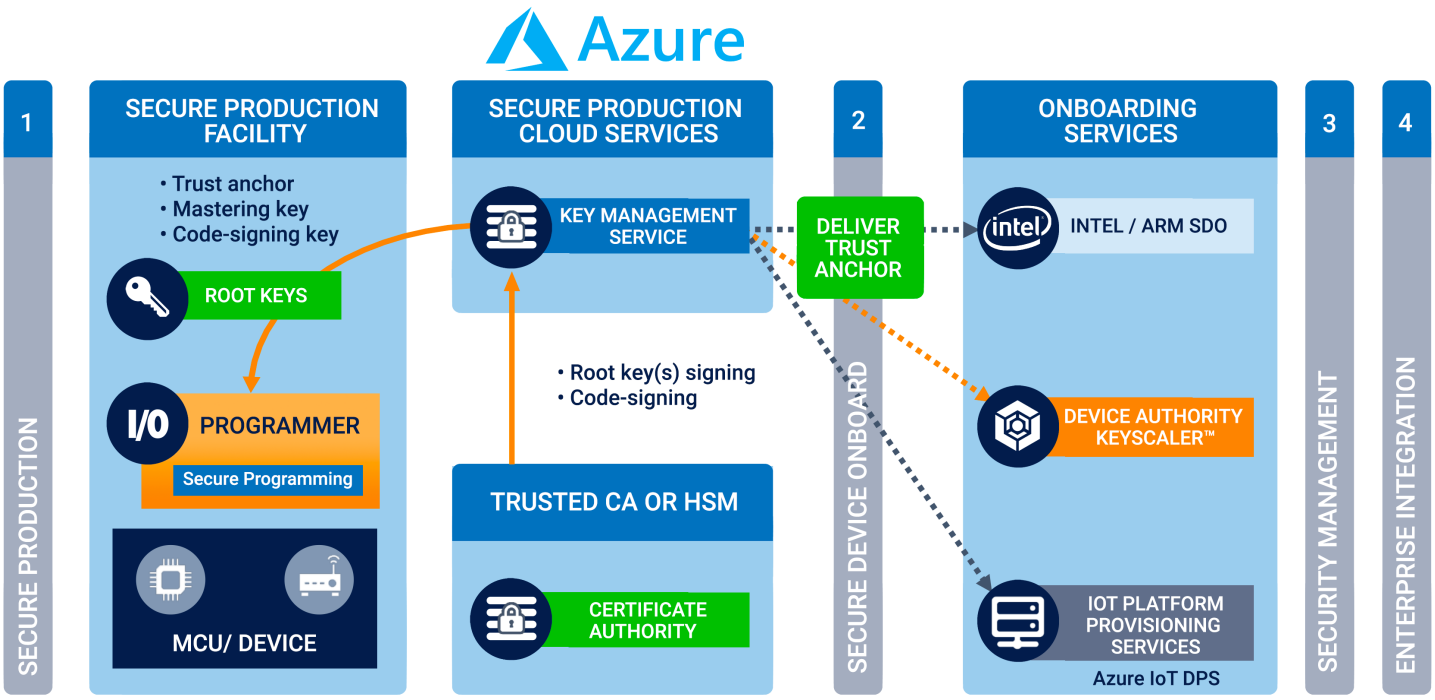
Using the outlined requirements and key functional blocks, a typical IoT device journey requires trust and automation during its lifecycle across the six steps defined in the picture below.





Enterprise IoT Security Solution Reference Architecture with Azure and KeyScaler





There are six main areas in this Enterprise IoT security solution

1. **Provision Root Keys and Certificates at the Time of Manufacturing**: Existing security solutions evolved as an afterthought. The potential impact of an IoT security breach is forcing the right security model from the design and manufacturing phase.

- Provision strong Root of Trust and keys/certificates as required.
- The root key along with other device parameters like serial number would act as registration information (whitelisting). In an ideal scenario the registration keys will be rotated with a new key at the time of onboarding the device.
- Secure mastering, production and foundation for secure updates need to be included in this step.

2. **Secure Device Onboard/Zero Touch Provisioning**: Today's manual processes do not work well for IoT devices, scale and security. This new step is required to transfer the device ownership and connect to an owner-controlled environment without human intervention. Prominent vendors like Intel and Microsoft have initiated this type of implementation to help IoT security and adoption.

- Automated onboarding and ownership transfer which is leveraging the Trust anchor and registration information from step 1.
- Initial device configuration for interaction with the right IoT Identity and Access Management (IAM) or Security Management system.

3. **Provision and Manage Owner-Controlled Security for the Devices**: This functionality is delivered by device identity-centric IAM platforms like Device Authority's KeyScaler. However, this step is also new for IoT. While there are some home-grown implementations by platform vendors, many industry experts and analysts have spoken about the functionality as IoT IAM, which is substantially different from traditional IAM.

- Provision and manage owner/application required keys and/or credentials.
- Provision and manage application required identity/authentication.
- Policy-based automation for identity, authentication, and data security keys.

4. **Enterprise Integration**: The majority of Enterprise IoT security implementations need to take existing IT security controls into account and seamlessly interoperate with IoT devices. The challenge is integrating IoT IAM with the traditional Enterprise IAM, Hardware Security Modules (HSMs), and Data Security Platforms.

- Enterprises use HSMs for Root of Trust, secure storage of keys, and secure crypto operations. HSMs are used for IoT identity provisioning and data security operations.
- Enterprises already use data security platforms for key management and policy-based data access authorization. Integration with these systems is essential for end-to-end data security and compliance. This is required for secure data exchange between IoT devices and other Enterprise resources including enterprise users.
- IoT IAM and Enterprise traditional IAM need to interoperate to authorize and share data between the IoT devices, Enterprise systems, and users.

5. **Device Decommission**: The lifecycle of an IoT device refers to the operational phases of a thing in the context of a given application or use case. The phases mentioned above assume a new device is going into operation. For devices with a lifespan of several years, occasional maintenance cycles may be required. During each maintenance phase, the software and operational data may be upgraded. Depending on the operational changes to the device, it may be repurposed at the end of the maintenance cycle. However, the end-of-life of a device doesn't necessarily mean that it is defective, but rather decommissioned with the existing service and current owner. It can be moved to a new owner and start the device lifecycle from the beginning. Some medical devices are moved to new countries for re-use. During the decommissioning of the device, the security management must remove all sensitive data and proprietary applications and revert the device to a factory-fresh state. The typical steps involved are:

- Delete the device connections/relationships with all the entities
- Secure data removal
- Factory reset

6. **Device Recommission**: The device recommission can follow the same steps from step 2, provided the old trust anchor is preserved. If not, a new Root of Trust needs to be established.

Microsoft Azure IoT and Device Authority KeyScaler address the Trust, Automation and Lifecycle Management throughout the Device Journey

Microsoft Azure IoT Platform

As outlined above, Microsoft Azure IoT provides several capabilities and features to build and deploy IoT applications, solutions, services in a better, faster, more cost-efficient and integrated way. Azure IoT brings together a bundle of services such as IoT Hub, DPS, Event Hub, Machine Learning, Stream Analytics, Notifications Hubs, Power BI, Web apps, and Logic apps. It also enables quick interconnection of assets and supports a wide variety of operating systems and devices. Azure IoT Suite helps give organizations a quick start to end-to-end Enterprise class IoT implementations by orchestrating the required Azure services. Recently Microsoft enhanced the core services with additional offerings, Azure Sphere, Key Vault, Azure IoT Edge, Plug and Play, etc.

Microsoft's latest announcement, Azure Sphere, addresses an important Secure by Design foundation in IoT for devices, takes a step forward to help monitor security, and also provides a secure software update mechanism for these devices. This approach is solving a foundational challenge that we articulated in step 1 of our security Solutions Reference Architecture model.

Azure IoT has been attracting large Enterprise customers interest, including Kroger, Starbucks, Shell, and many more. Microsoft is further expanding their toolset to make it more appealing for SIs, ISV and Technology partners.

While IoT products and services continue to evolve, security is still the #1 concern for IoT adoption, introduced by the scale, unique characteristics as well as the consequences of compromised security. The IoT continues to grow rapidly but concerns about security remain a significant barrier and are hindering the adoption.

Device Authority KeyScaler – First Device Identity centric IoT IAM Platform

Device Authority's KeyScaler platform closes the gap for security, trust and automation, and addresses the requirements, delivers flexibility and security, without compromise along with a growing partner ecosystem.

KeyScaler uniquely combines the device trust, data trust and automation in a single platform. The policy based end-to-end data security is unique and manages the crypto keys at IoT scale. The service connector architecture extends these core capabilities to Enterprise IT Security infrastructure. This helps customers to accelerate and build trusted Enterprise IoT solutions.

KeyScaler delivers simplified device registration and onboarding, provisioning and management of credentials for IoT devices that connect to Azure IoT Hub. KeyScaler automates many tasks for Azure IoT Hub Device Provisioning Service (DPS), provides device attestation, and also acts as the source of truth

for devices that do not have keys from manufacturing.

KeyScaler can be deployed quickly (within hours, compared to multiple days for similar systems, which often require teams of bespoke developers), used on-premise, SaaS, using traditional VM based servers, or deployment using Docker which makes it truly scalable. KeyScaler is already available in the Azure Marketplace.

The Security Suite for Microsoft Azure includes connectors for Device Provisioning Services (DPS), Azure IoT Hub, Event Hub, IoT Central, Key Vault, Active Directory Certificate Services and IoT Edge. Often Enterprise customers need a security framework that encompasses multi-platform, multi-cloud environment and integration with their existing IT security infrastructure to successfully deliver secure and compliant IoT solutions. In order to make it simple and easy for Microsoft customers and partners to adopt the Azure IoT platform, the KeyScaler core security automation components are offered as a suite. Find out more details here: https://www.deviceauthority.com/microsoft

Microsoft Azure IoT + Device Authority KeyScaler = Secure Lifecycle management for IoT

The following tables provides detailed view of different components from both platforms to deliver trusted and automated IoT solutions.

Implementation level functional details, value to the solution and role of each platform component:

Function	**Description, what for**	**Core value**	**Platform Components**
Provision root keys and trust anchor early in the device lifecycle (e.g. at the time of manufacturing)	Provision immutable trust for devices at the time of manufacturing or before registering for secure device on boarding at IoT scale without human intervention	• Device Trust • Zero touch provisioning • Operational Certs • Secure updates	• Sphere • KeyScaler
Registering and onboarding the devices into IoT platform and applications	The trust anchor and whitelisting based approach to register, provision, and update devices through active, policy-based security controls that do not require human intervention	• Device Identity/ Authentication • Eliminate rogue devices (cloned and counterfeit devices) • Policy based • IoT Scale	• DPS • IoT Hub • IoT Central • KeyScaler

Establish owner/app required security and manage as per the policy	Provision and manage identity, authentication, and crypto keys as per the application requirements. This might involve interfacing to third party products and services. E.g. private or public Certificate Authority for device certificate issuance.	• PKI management • Credential management • Token policy management • Protect IoT application and data • Operational management / efficiency	• IoT Hub • Azure AD • Key Vault • KeyScaler
Policy-driven end-to-end data encryption	Secure data exchange between IoT devices, IoT applications and Enterprise resources including enterprise users	• Data security and privacy • Network independent • Compliance	• Event Hub • KeyScaler
Policy-driven authorization for applications and users	Only authorized applications access secrets on the device and authorized users access the data. Data at rest is stored encrypted and unreadable to unauthorized entities	• Data security and privacy • Entity bound, identity and data security • Compliance	• Event Hub • KeyScaler
Decommission devices	Remove all the current owner information, configuration and data. Device is back to same state as if the device is new from production	• Disconnect from the service and remove all the configuration and information • Factory reset	• Sphere • KeyScaler
Recommission devices	Back to onboarding and provisioning (step 2) to new service	• Establish new Root of Trust if required • Follow the steps from onboarding	• Sphere • DPS • KeyScaler

IoT requires a more practical approach to security than traditional IT: Protect and Prevent vs. Legacy Detect and Respond is an important and different approach required for IoT deployments.

The following section goes into the practical details and specific requirements of IoT use cases that traditional IT security models have so far struggled to address.

Root of Trust, Secure Production, Supply Chain Integrity – A foundation for Secure by Design

IoT security needs to be architected into the devices from the moment of inception, and there needs to be foundation in the devices to deliver the secure updates throughout its lifecycle. Devices need a strong Root of Trust (RoT) in the MCUs/processors/systems and a mechanism to deliver signed and encrypted images either for production and/or for ongoing updates. This will enable secure production, protect against IP theft and detect cloning, and help mitigate security breaches.

Microsoft Azure Sphere identified and addressed this with the seven properties of highly secure, network connected devices: a hardware-based root of trust, a small trusted computing base, defense in depth, compartmentalization, certificate-based authentication, security renewal, and failure reporting. For any network-connected device to be secure, we assert it must possess all seven of these properties. To implement these seven properties, the hardware and software (firmware) of the device must work together, with device security rooted in hardware, but guarded with secure, evolving software.

Device-bound Identity/Authentication – Securing device secrets

Strong IoT device authentication is required to ensure online (or offline, in some use cases) devices can be trusted. Each IoT device needs a unique identity that can be authenticated and bound to that device only when that device attempts to connect to other resources. Device keys/secrets need to be protected by purpose-built secure hardware, where the hardware implements physical countermeasures against side-channel attacks. In cases where devices don't have hardware protection available, an equivalent secure software storage solution can be utilized as a best endeavor. In some use cases the devices can leverage gateway resources with the correct binding and authorization models. An entity that is interacting with the device needs to have strong device authentication that can't be spoofed.

Device-bound Data Security

As mentioned earlier, IoT use cases are about data - you can't trust the data if you can't trust the device. Device Trust and Data Trust must be coupled for a successful IoT solution. The first challenge is to have strong mutual trust and authentication between entities and the device and data that is propagated, i.e. IoT platforms, applications, and users. The second challenge is that sensitive information flows all the way from the device to different constituents where only the authorized entities should use the relevant data. The data security and privacy need to be maintained independent of the network i.e. in motion and at rest. When accessing the data, the original device association is important. The applications that use the data need to have the device coupled to the data. For example, when a doctor receives medical data from the patient's healthcare device, the data must be securely delivered and the association of the data to the device must be guaranteed.

Data-Centric Security

Data security from creation-to-consumption (i.e. at rest, in motion, and in use) needs to be addressed for any critical IoT use case. In an ideal scenario, data security needs to be implemented independent of network and human intervention. Proven encryption/decryption-based approaches already exist, but they need to be adapted for IoT and scale (hundreds of thousands of devices). Another important requirement is the authorization policies that allow different constituents to consume the data without violating the security and privacy, which is very important for many vertical sectors in medical, insurance, automotive, smart city programs and others. Many assume that TLS is good enough for IoT data security, but in reality this is a fundamental issue that is currently not addressed well. It is extremely complex (or not even practical) to extend the enterprise data security platforms for IoT use cases.

Supporting Devices Offline

Increasingly IoT needs to accommodate both online and offline devices for registration, authentication, and security provisioning without compromising the trust. A gateway or another designated device can act as a security broker to perform the tasks on behalf of the offline devices. From the security point of view, while the security broker can perform the tasks, it should only act as an agent without compromising the security. The security management layer needs to accommodate these scenarios and provide methods to achieve the functionality as though the offline devices are connected online.

Code Signing and Secure Updates

One of the main problems in security is addressing the known vulnerabilities before the hackers exploit them. Almost 99.9% of vulnerabilities exploited are already well-known. So far in cybersecurity this problem is not addressed with a trust model that can work throughout the lifecycle of devices. An Enterprise IoT security strategy should include software and firmware upgrades while ensuring only trusted software is installed. The security management must be able to facilitate and control access to devices for updates, verify the source of updates, and validate the integrity of the updates. In addition, having the correct mastering keys injected at the time of device inception helps elevate the security posture.

Typical code signing solutions use the software originator's public/private key pair and digital certificate, which includes the software originator's public key, and is signed by a suitable CA. It is best practice to protect the private key used for signing software/firmware, and a typical solution is to store the private key in an HSM. There will be many other steps for defining the process, work flows, and code-signing authorization associated with the software build and update process – these will often vary, and are typically specific to use cases, and device characteristics.

Protecting Critical Resources Across the Solution Components

A typical IoT application leverages IoT platforms and cloud/edge infrastructure and services. Not only protecting the edge devices and data, the need for protecting all the critical components in the solution is very important e.g. databases storing the critical data, sensitive nodes, keys that are being used, etc.

Enterprises need to implement strong key management and access policy procedures to eliminate unauthorized access to their own infrastructure as well as the infrastructure that is being leveraged for its end-to-end solution. It's important to verify the authenticity of nodes for access to any critical infrastructure e.g. storing encrypted secrets/keys. Any unauthorized access to critical infrastructure could have serious impact.

Role of IoT Platforms, Application Enablement Platforms (AEP) and Security Automation

Microsoft Azure IoT provides several capabilities and features to build and deploy IoT applications, solutions and services in a better, faster, more cost-efficient and integrated way. IoT platforms also provide quick interconnection of assets and support a wide variety of operating systems and devices.

Enterprise IoT security solutions typically use owner-controlled security posture and need to integrate with IoT Platforms' device and data management. To meet the Enterprise IoT security operational requirements and handle the unique characteristics and scale of IoT, there is a need for the right security framework, without which IoT adoption would suffer.

IoT IAM has emerged as an important capability to provide trust, automation and lifecycle management as an integral part of IoT Platforms. Industry experts and analysts have been providing guidance on this functionality. IoT IAM is a key ingredient and acts as the security glue across core elements of IoT solutions, i.e. IoT platforms, edge devices, HSMs, CAs, and data security platforms to extend the Trust and Automation. It's important that Enterprises realize IoT IAM is substantially different from Traditional IAM, which is not suitable for IoT.

Many IoT platform vendors claim to have comprehensive IoT device management including a range of security operations. However, they usually ask customers to implement their security manually which uses a lot of resource, connecting the different platform specific interfaces as per their platform requirements. Most platform vendors talk about shared responsibility and provide support with relevant tools, but it is ultimately the customer's responsibility to build the right security model that works for their requirements and integrate with the chosen platform components.

Role of PKI, HSMs, CAs

While PKI can deliver a lot of value in the IoT/Digital world, for identity, code-signing, and data security, the current implementations are limited to certain areas like servers because of operational complexities and often require IT administrators. In the case of IoT, more than the cloud/data center, the edge/device

side is the weak link and cannot rely on manual/human intervention. From the sceptic's angle, complexity of adopting the proven PKI technology and products for IoT at scale is compounded by the headless constrained devices. There needs to be a security management platform that manages this complexity and delivers automated PKI at scale to harness the benefits of PKI for IoT.

The security management platforms need to include the automation for PKI, that can leverage the key product vendors in HSM, CAs for proven trust. We already have the initiatives from vendors to address this market but cohesive strategy to address the device lifecycle and customer solution requirements is important.

Role of Traditional User-Centric IAM

Traditional user-centric IAM was built primarily for the use within Enterprises and recently extended to the cloud. Many Enterprise and Industrial IoT use cases require the combination of device and user-centric IAM to manage end-to-end relationships (authentication and authorization). IoT is a true machine-to-machine ecosystem and device identity will be a first-class citizen. The well-established and proven user-centric IAM needs to interoperate with device-centric IAM (or IoT IAM) for addressing the IoT use cases.

Role of Network-Centric and Reactive IT Security Models – Detect/Respond

IT security evolved as an afterthought. It is a multi-layered approach where the majority of the focus is on the last three layers of NIST Framework's five functions (Identify, Protect, Detect, Respond, Recover). As mentioned earlier, the safety and economic impact with IoT is forcing the Secure by Design (from the beginning) security model, shifting the security model to bring defense in depth as explained above. The new security model is evolving, and we do need the traditional IT security models, but the importance is moved to the protect layers.

Why is Device Authority's KeyScaler platform a perfect companion for Microsoft Azure IoT?

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

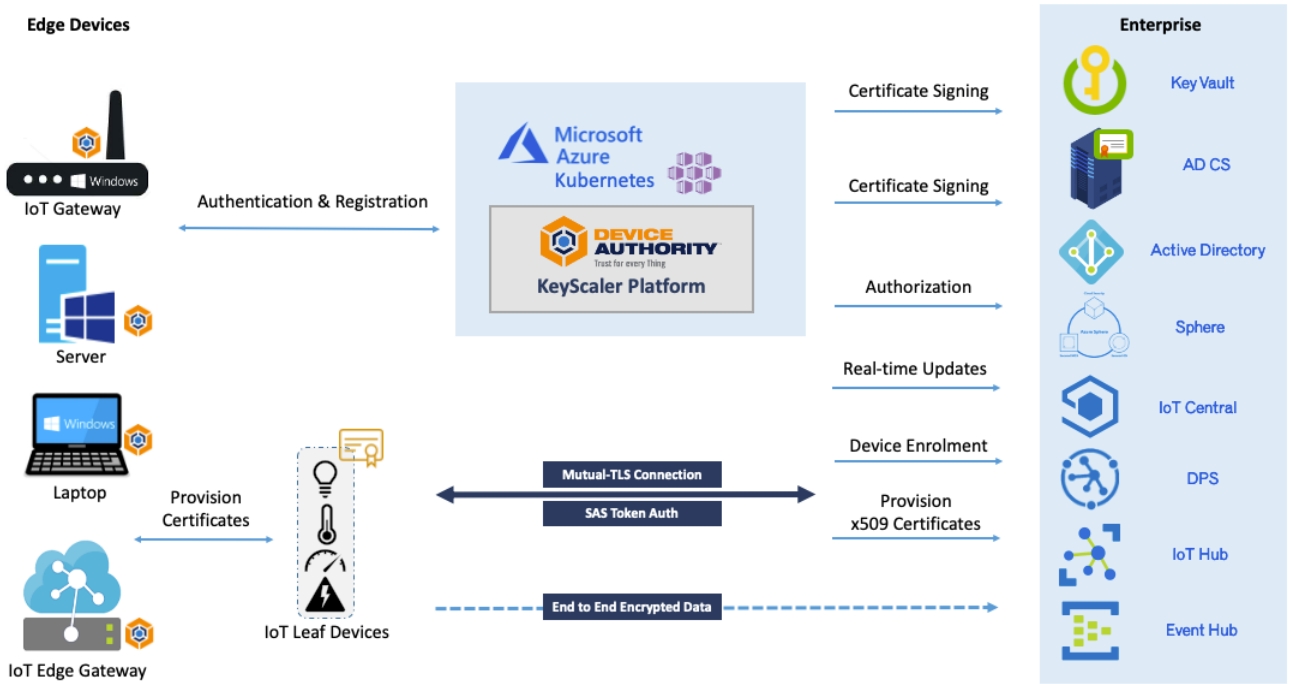
- Device Attestation and Automation for DPS – Source of truth for automated IoT device onboarding
- Azure IoT Hub Certificate Provisioning Connector – For managing the automation and provisioning of x.509 Certificates to Azure IoT Hub
- IoT Central – For building high security enterprise-grade IoT applications 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

- 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 - Provides integration into enterprise networks to deliver authorization for 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

The 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. More importantly, this platform is available in the Azure marketplace for easy to access and deployment for customers and partners.

Figure 1 - Microsoft based IoT Ecosystem enabled with Device Authority



KeyScaler Value Proposition Summary with Azure IoT

Security Lifecycle Management

Seamless integrations with Microsoft Azure accelerate revenue and deployment: Accelerate time-to-market with readily available software and connectors to Azure services including IoT Central, IoT Hub, IoT Edge, Key Vault, DPS, ADCS.

Market differentiation: Device Authority's Security Suite provides Microsoft sales teams with a compelling end-to-end solution (device trust, data trust and security automation) when competing against AWS.

Enhanced security offering for Microsoft Azure: An end-to-end solution, beyond what Azure already provides.

- 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

Increases Microsoft's wallet footprint by expanding traditional Microsoft IT enterprise PKI to IoT deployments.

A solution for brownfield and greenfield deployments: KeyScaler can retrofit and solve the installed base challenges.

Meet regulation and compliance requirements: Companies are using the Azure Event Hub Connector for policy-based encryption of personal data to comply with GDPR, HIPAA, FDA, etc.

Flexible integration and extended support with IoT ecosystem interoperability: Integrating with different devices, Certificate Authority (CA), IoT Platforms and Hardware Secure Modules (HSM).

- 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

Solves the security lifecycle management challenges for customers deploying in Azure, and utilizing the Azure and Edge services.

What makes KeyScaler unique and a perfect companion for Azure IoT?

KeyScaler delivers automation for critical credential management processes, in addition to tokenized access control, and policy-based encryption for data, in transit and at rest. In doing so, KeyScaler is uniquely addressing the challenges of device trust, data trust, and operational efficiency at IoT scale - things that are not currently addressed by any existing solution. It can be deployed quickly (hours, compared to multiple days for similar systems, which often require teams of bespoke developers), used on-premise, SaaS, using traditional VM based servers, or deployed using Docker, and is truly scalable.

Highlights of unique features relevant to IoT use cases:

- Azure Sphere connector – A foundation for Secure by Design
- Device-bound Identity/Authentication
- Device-bound Data Security
- Data-Centric Security
- Supporting Azure IoT Edge and Devices Offline
- Code Signing and Secure Updates
- Protecting Critical Resources Across the Solution Components

KeyScaler is the only platform to deliver additional functionality required for IoT:

- Unified Trust Model - Device and data trust combined
- Security model for safety and data privacy for automotive applications
    - Real-time device authenticity validation
    - Coupled relationship between device identity and data
    - Only trusted entities can participate in the interactions
- User Access Control and Authorization
- Flexible platform for a mix of use cases (token-based access control, PKI management, automation)
- Configurable platform-based solution - highly scalable and flexible
- Automation and support for enterprise security vendor ecosystem
    - HSM integration and support including nCipher Security and Thales/Gemalto
    - Public Certificate Authority and Private PKI options
    - Future proof, flexible options for device manufacturers and their customers
- Device side KeyScaler server interaction footprint can be very small (implementation code <20kb).
- KeyScaler platform architecture is supported by 13 issued patents.

Key Use Case Examples

The following section captures the key use case examples that highlight the points mentioned above.

Connected Medical Devices in Healthcare, also known as the Internet of Medical Things (IoMT)

Connected medical solutions with security that meets GDPR & HIPAA regulatory compliance.

A healthcare provider has a patient monitoring gateway that provides connectivity to medical devices and instruments that are active within the patient's hospital room – to deliver real-time patient status information to care givers. Gateways collate and provide data to other gateways in the hospital, as patient is transferred between wards/units. All gateways must register and authenticate before they can participate in the ecosystem.

Requirements

- Secure device enrollment and onboarding to the hospital network and services
- Secure decommissioning and deprovisioning at the end of device lifecycle
- Device-bound certificate provisioning for data signing, to communicate with existing sensors/medical equipment
- Device-bound crypto key provisioning for end-to-end data security

Security Solution

Integrate with IoT platforms / applications for secure and zero-touch registration and provisioning, end-to-end data encryption, authorization policies.

Reference solution architecture steps involved

- Onboarding and Provisioning
- Security Management
    - Device authentication
    - Data security
    - Device bound identity
    - Device bound data security
- Enterprise Integration
- Decommission
- Recommission

Industrial IoT (IIoT)

Connected oil production equipment for predictive maintenance and operational efficiencies with analytics.

A large Oil & Gas company assembles and delivers their own remote oil well-monitoring devices that collate large amounts of data to report on the health of the equipment at a drilling site. The company has a requirement to remotely provision the device so that it may seamlessly connect to the cloud-based monitoring application. Equipment installation must be zero-touch, as the remote well engineers may not suitably trained to deploy and connect IT/network equipment.

Requirements

- Secure headless device enrollment and onboarding to multiple cloud services
- Device-bound certificate provisioning
- Device-bound crypto key provisioning for end-to-end data security
- Secure decommissioning and deprovisioning

Solution

Integrate with IoT platforms / applications for secure and zero-touch registration and provisioning, secure OTA software updates, end-to-end data encryption, authorization policies.

Reference solution architecture steps involved

- Secure production
- Onboarding and provisioning
- Security Management
    - Device authentication
    - Data security
    - Device bound identity
    - Device bound data security
- Enterprise Integration

Automotive

Connected Cars – Car dealers and owners leverage the IoT enabled connected cars, value-added services, and applications. Automotive IoT brings in remote auto-companion apps, in-car infotainment apps, automotive ecommerce, usage-based insurance, remote diagnostics, car security services and lot more.

A car manufacturer has a requirement to manage vehicle access using smartphone application and NFC/

BLE. The required solution is to use a smartphone for keyless entry without the need for a fob, where an authorized user and application can simply walk up to their vehicle to gain entry and start the vehicle and drive off. In addition to authorizing owner-access to the vehicle, there is a requirement for the owner to authorize temporary access to the vehicle, for other drivers (e.g. family and friends). The solution must support offline scenarios, in the event that the mobile device, or vehicle, does not have an active connection (e.g. no cell service).

The manufacturer also wishes to provide connected car services to offer additional applications and benefits, potentially via a subscription service, to their customers. To facilitate secure communication between the car and the manufacturer cloud services, a unique certificate needs to be provisioned to each vehicle – supplying the Vehicle Identification Number (VIN) as the certificate common name (CN) – and also provisioned to the cloud services for authentication and authorization.

Requirements:

- Support offline/disconnected use case
- Secure vehicle registration and onboarding to manufacturer cloud services
- Certificate provisioning and management
- IoT platform provisioning
- Secure user registration, and relationship pairing with the vehicle
- Ownership transfer from owner A to owner B upon sale of the car
- Ability to authorize access to another user/mobile device

Reference solution architecture steps involved

- Secure production
- Onboarding and provisioning
- Security Management
    - Device authentication
    - Data security
    - Device bound identity
    - Device bound data security
- Integration (Mobile apps)
- Decommission
- Recommission

Operationalizing the Trust at IoT Scale

Today, a manual process exists where devices are activated in the field, configured on the network by IT, and registered with the device owner in an IoT management platform. This time-intensive process is fraught with security holes, as exemplified by recent large-scale attacks in which device manufacturers have shipped default credentials that were co-opted for botnet-style DNS attacks.

Device Authority's KeyScaler platform plays a major role by allowing organizations to automate and deliver owner-controlled security posture as per the IoT platform/application requirements and also integrate with the Enterprise IT Security infrastructure. KeyScaler makes Enterprises IoT ready, by allowing them to leverage IoT Application Enablement Platforms (AEPs) and use Certificate Authorities (CAs) and Hardware Security Modules (HSMs) for security operations.

Conclusion

Device Identity and Integrity are the new perimeter for IoT. Data security and privacy are extremely important to enterprise IoT use cases. Any enterprise class IoT security solution requires a combination of an IoT Platform (Azure IoT), automated PKI, high assurance PKI key storage and management, along with enterprise data security platform integration. The implementation needs to be device identity-centric. The modules need to work in unison, not as isolated modules, in order to meet various data security and compliance requirements for real Enterprise IoT challenges.

Device Authority has developed this IoT security solution reference architecture for Azure, and it has been implemented for number of mission critical enterprise IoT use cases, including Healthcare / Medical Devices, Industrial IoT and Automotive / Connected Car. Many System Integrators support the requirement for an IoT IAM platform which provides the glue to extend security from the Enterprise to IoT devices. Device Authority delivers IAM 2.0 for IoT that is an integral part of IoT Platforms like Azure IoT.

Contact Us

For further details, please contact Device Authority:

www.deviceauthority.com/contact

Online Resources

Visit the Azure Marketplace:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/deviceauthorityinc.keyscaler?tab=Overview

Learn more about Device Authority and Microsoft, with videos, solution briefs and webinars:

www.deviceauthority.com/Microsoft

About Device Authority

Device Authority is a global leader in identity and access management (IAM) for the Internet of Things (IoT) and focuses on medical/healthcare, industrial, automotive 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 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.

Keep updated by visiting www.deviceauthority.com and following @DeviceAuthority on Twitter. You can also subscribe to our BrightTALK channel.

sales@deviceauthority.com

www.deviceauthority.com

DEVICE AUTHORITY™