DEVICE AUTHORITY
Automating Zero Trust for IoT

IoT Technical Market Insight Guide

Automating Zero Trust for IoT Deployments

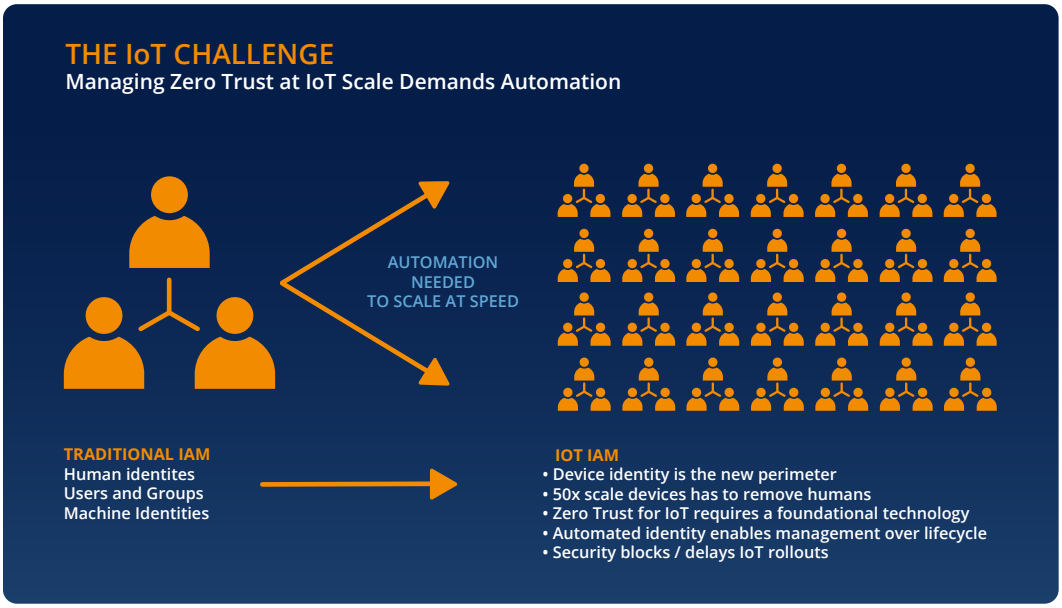
Contents

Trust and Automation of Machine Identities and Zero Trust are Fundamental for IoT Success

Digital Transformation has become a common goal for most enterprises as they look to capitalize on digital technologies and a wealth of data to introduce new product capabilities, gain access to new market segments, and create better, more compelling experiences for their customers. As organizations pursue their own Digital Transformation journey they increasingly rely on the Internet of Things (IoT) - connected devices with ubiquitous presence ranging from consumer technologies to jet engines, logistics to product development, healthcare to municipal planning, industrial settings to automotive platforms. This document provides an overview of the current state of the IoT security landscape, an enterprise blueprint that lays out the 6 discrete steps in an IoT device's lifecycle, and how Device Authority's KeyScaler platform addresses the need for automation throughout that device's journey to meet today's Zero Trust security requirements.

Accompanying the rapid proliferation of devices within the enterprise, and outside the firewall at the Internet "Edge", is a never-ending series of global threats creating a new sense of urgency to secure these connected devices. Zero Trust has become the new standard for security to address this need. Adopted by most enterprise vendors and reinforced by governments to improve Cybersecurity capabilities and protect critical national infrastructure, Zero Trust focuses on securely managing the identities of anything connecting to the network and follows the mantra of "never trust, always verify". In this environment the rise of PKI-based technologies to help secure enterprise assets has led to the existence of three distinct categories of Identity and Access Management: Humans, Machines, and IoT devices.

Human identities rely on usernames and passwords and are the domain of traditional IaM vendors. Machine identities refer to credentials used by servers, applications, containers, and other non-human (digital) entities that rely on keys and certificates, offered by today's leading PKI vendors. IoT device identities also rely on keys and certificates much like machines, but with a few important distinctions: context and scale. IoT devices, unlike digital machines, often interact



with the physical world and can have real physical consequences – surgical robots performing procedures on patients; autonomous construction vehicles performing pre-programmed tasks based on GPS coordinates; flood sensors that help control water pressure and flow. Further, these physical devices have a complex identity lifecycle different than that of a typical corporate asset and can span many years. For example, some IoT devices operate for decades and may have two to three different owners in that timeframe. Combine that with the scale of IoT – analysts predict between 20-40 Billion devices will be online by 2025 – and when you comprehend the threat landscape that growth represents, it is clear: traditional methods of identity management will not work for IoT and a new model is required.

The Role of Data in IoT

IoT use cases are all about the data. To realize the full benefits of IoT, we must be able trust the connected objects and the data they generate, and that data must then be accessible by authorized entities: either humans, machines, or other devices. Why is the concept of "trust" so important here? IoT applications can't trust device-based data unless the device itself is trusted. If the device and data it collects can't be trusted, there is no point collecting it, analyzing it, or making a decision or policy change based on it. Imagine if a doctor or clinician incorrectly adjusted a dose of medication for a connected medical device based on untrusted data; or a pipeline technician adjusted the flow based on faulty pressure data. To effectively address this challenge there needs to exist a device-bound identity and data security model.

Why Automation is Critical for Managing IoT Device Identities

IoT presents new security challenges when dealing with the unique characteristics, scale, and consequences of a breach of a device's machine identity. In today's Cybersecurity environment, time and speed are the main determining factors in the severity of a breach. Consider the following data:

- Analysts predict IoT devices to reach 27 Billion or more by 2025 (IDC, IoT Analytics)
- University of Maryland research indicates hackers attack once every 39 seconds
- 2021 Verizon Data Breach Investigations Report: credential data now factors into 61% of all breaches
- Gartner estimates that "75% of security failures will result from inadequate management of identities, access, and privileges" by 2023
- According to Crowdstrike the world's best hackers can gain access to a target network in as little as 19 minutes to 2 hours
- A Ponemon Institute study found that the average amount of time for organizations to identify a data breach is 197 days; 69 days to fully contain.

Clearly, securely managing identities and quickly reacting to adverse events is of paramount importance. Many enterprises today already rely on Public Key Infrastructure (PKI), a security approach based on certificate issuance that has progressed since the mid-1990's, to solve identity, authentication, integrity, and privacy problems for the Internet and cloud environments. These standards-based PKI technologies have been securing the devices, data, and connections between servers for years, and are a natural fit for today's IoT devices. However, anybody engaged with PKI solutions knows the complexity challenge of adopting PKI at IoT scale, particularly for headless devices with no User Interface (UI) or associated user.

The time required to manually track certificates and associated keys across multiple device types, rotate according to policy, revoke when needed, and maintain integration across platforms is daunting. There simply aren't enough humans to perform these tasks for IoT given that, according to CyberArk, device identities outnumber human identities 45:1. When seconds count, adapting PKI security to fit today's Zero Trust model at IoT scale requires a unique set of capabilities and associated automation.

IoT IAM utilizing machine identities has emerged as the preferred method to support Zero Trust for connected devices

IoT Identity and Access Management has now become a mainstream topic of security professionals and is covered by industry analysts such as Quadrant Knowledge Solutions, ABI Research and others, as its own category. But the IoT security market has undergone significant changes over the past 4-5 years.

As specific examples of how the industry has evolved around the requirements for IoT security, in March 2018 the UK government published a report titled “Secure by Design” which aimed 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 safety.

At that time, California also stepped into the forefront of this issue by enacting Senate Bill 327, the Internet of Things Cybersecurity bill 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.

Most recently, the President of the United States signed a Cybersecurity-focused Executive Order 1408 in May 2021 to improve the nation’s cybersecurity, which directly relates to the trustworthiness and transparency in ALL digital infrastructure - IT, OT, IoT, IIoT. Importantly, this Executive Order calls for transparency in the software supply chain requiring a Software Bill of Materials – (SBOMs), shared threat intelligence for critical infrastructure (Collaboration) and Zero Trust.

Helping to improve cybersecurity with SBOMS

As described above, modern IoT solutions and devices rely on standards-based approaches to authentication, such as PKI certificates, which provide a highly-secure way to verify device identity for network systems and applications.

However, many other systemic issues such as firmware bugs, cloning, or missed maintenance SLAs can mean the device and its data are still not trustworthy. A device with a legitimate certificate can still pose serious security and compliance risks to an organization since rogue software or malfunctioning equipment will have privileged access to the network and enterprise resources.

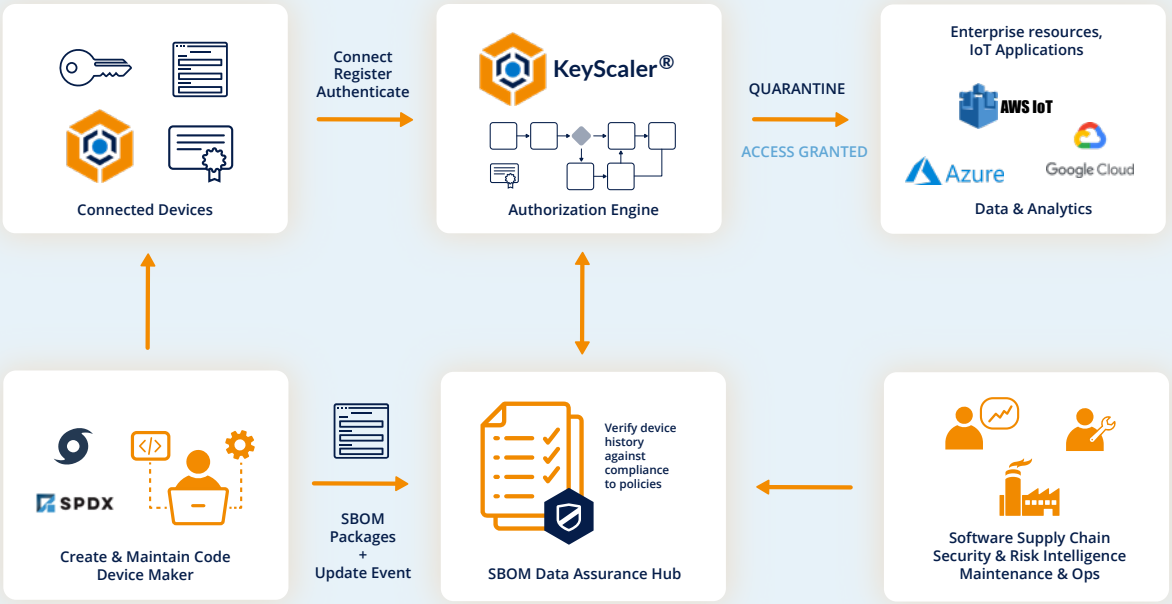
Rogue or malfunctioning software is difficult to spot, and often stems from the lack of transparency in development of commercial software, and through the extensive use of widely available open-source software tools, a common source of exploitation. A one-shot security evaluation or pen test is not enough – proof of security and safety must accompany any software throughout its useful lifespan.

The US Executive Order calls to equip federal users with a new defense that will deliver trust through transparency: the Software Bill of Materials (SBOM).

What is an SBoM?

- A Software Bill of Materials (SBOM) is a list of components in a piece of software.
- SBOMs allow the **manufacturer** of a product to make sure those components are up to date and to respond quickly to new vulnerabilities.
- **Buyers** can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product.

Using SBOMs for device authorisation and remedition



The following is an example of how KeyScaler supports SBOMs, providing a Zero Trust capability for IoT deployments, in order to:

- Ensure visibility and SBOM status across all assets, with continuous tracking, and automated reporting against policy
- Deliver real-time Zero Trust defence with assured SBOMs
- Provide operational efficiency and automation at scale, with remediation controls into IoT/Cloud Apps
- Reduce risk, mitigating compromised device data from entering critical enterprise infrastructure
- Improve trust and security in the supply chain by ensuring integrity, provenance, and transparency
- Lower administration fees and mitigate fines by providing compliance

Enterprise IoT Security Blueprint 2.0: Support for Zero Trust

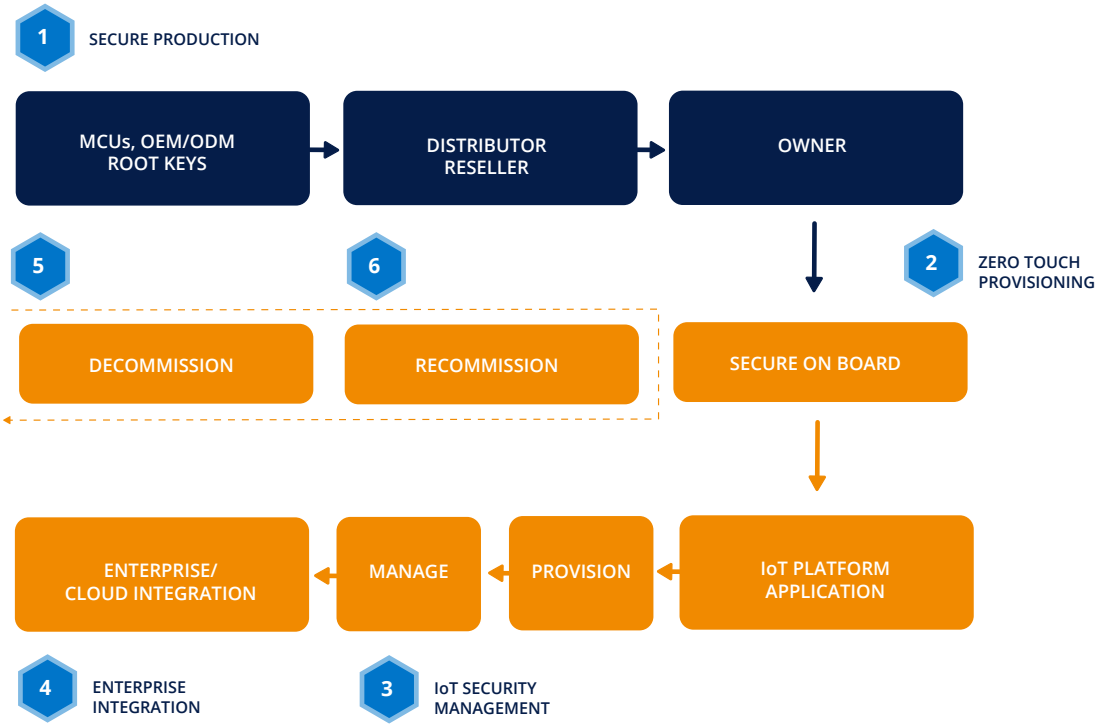
The Enterprise IoT Security Blueprint was first introduced by Device Authority in April 2018 and has since evolved to incorporate further steps within the rapidly growing Enterprise IoT industry. This evolution is a result of continued innovation based on emerging technologies, and through the benefit of working with customers across multiple industries to explore real world use cases. Two of the biggest developments in Enterprise IoT are the importance of Zero Trust as a security framework, and reinforced by the NIST Cybersecurity Framework; and the growth of machine identities using keys and certificates for identity and access of connected devices.

ENTERPRISE IOT SECURITY BLUEPRINT 2.0

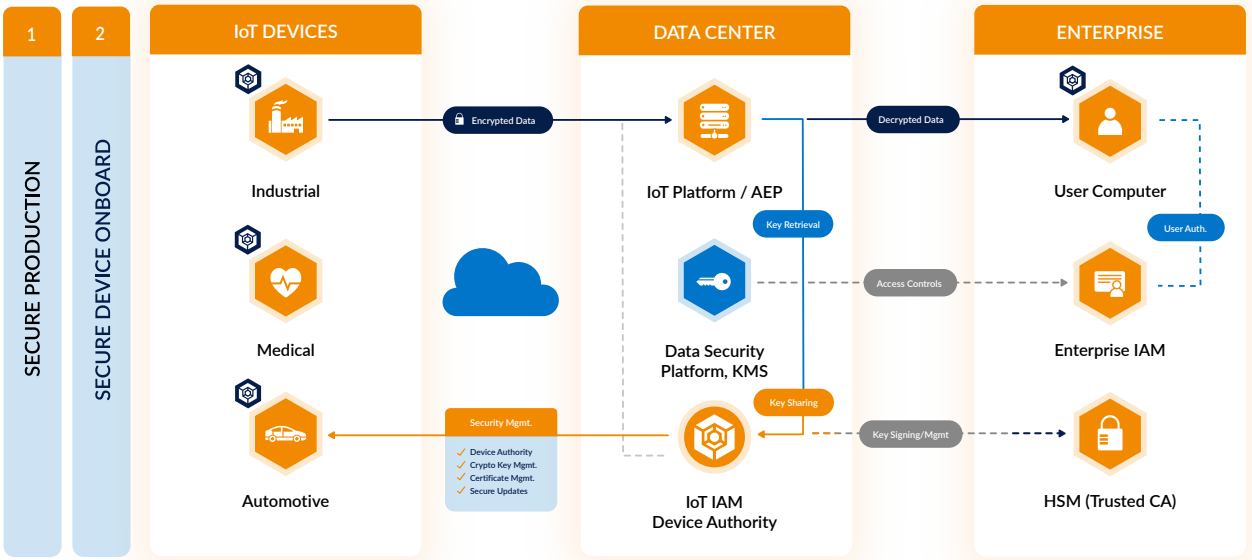
Our updated blueprint further underscores the need for Enterprise IoT security solutions to implement the following functional blocks as interconnected modules, not in isolation, to meet the scale, data security, and compliance requirements of IoT and achieve Zero Trust:

1. Device Trust: Establishing and managing device identity and integrity throughout its lifecycle
2. Data Trust: Policy-driven end-to-end data security, integrity, and privacy from creation to consumption
3. Operationalizing the Trust: Automating and interfacing to the standards-based, proven technologies and products such as Enterprise PKI and Cloud platforms

Using these outlined requirements and key functional blocks, a typical IoT device journey requires continuous trust and automation of its machine identity during its lifecycle throughout the six phases outlined in the picture below, to satisfy Zero Trust policy.



Enterprise IoT Blueprint



KeyScaler addresses PKI operational complexity with a comprehensive architecture that supports a Zero Trust approach. The platform has been repeatedly proven in high security and compliance- conscious use cases.

1. Secure Production

Provisioning of Root Keys and Certificates at the Time of Manu-facturing.

Existing security solutions evolved as an afterthought. Now, 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 Onboarding
Zero Touch Provisioning.

Manual processes do not work for IoT devices due to their scale and unique security requirements. This step is required to transfer the device ownership from the manufacturer, and connect to an owner-controlled environment - without human intervention. Prominent vendors like Intel and Microsoft have initiated this type of implementation to help bolster IoT security and adoption.

- Automated onboarding and ownership transfer which leverages 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. Security Management
Automated enforcement of Security Policies

This functionality is delivered by device identity-centric IAM platforms like Device Authority 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, and leverages machine identities at scale.

- 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
Connect to existing enterprise platforms

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

Automatically revoke a device's credentials

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 like surgical robots 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
- Securely remove data
- Perform 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 and additional keys required are established/programmed.

Real World Use Cases

The following section captures the key use case examples that highlight the need for technology capabilities mentioned in this Insight Guide.

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

The KeyScaler Security Solution

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

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 be suitably trained to deploy and connect IT/network equipment.

Requirements

- Secure headless device enrolment 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

The KeyScaler Security Solution

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

Automotive

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).

Requirements

- Support offline/disconnected use case
- Secure vehicle registration and onboarding to manufacturer cloud services
- 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

The KeyScaler Security Solution

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

What makes KeyScaler unique?

- KeyScaler automates critical PKI-based machine identity management processes, through a proven, out-of-box solution with pre-built integrations to the leading Certificate Authorities and Cloud Platforms. In doing so, KeyScaler uniquely addresses the challenges of device trust, data trust, and operational efficiency at IoT scale while supporting Zero Trust policy – something which no other vendor can provide.
- KeyScaler can be deployed quickly and offers ultimate flexibility in deployment – Enterprise SaaS, on-prem or private cloud via Docker images – and procurement via direct engagement, resellers and OEM partners, or transactable in the Azure and AWS Marketplaces.
- The KeyScaler platform architecture is supported by 13 issued patents, including Dynamic Device Key Generation (DDKG), which provides a software-only root of trust for both greenfield and brownfield devices, and for some deployments can eliminate the need for additional costly PKI infrastructure.

KeyScaler Features Supporting IoT Deployments:

- Root of Trust, Secure Production, Supply Chain Integrity – A foundation for Secure by Design and Zero Trust
- Device-bound Identity/Authentication – Securing device secrets
- Device-bound Data Security
- Data-Centric Security
- Support for Offline Devices and other Edge scenarios including nested gateways
- Code Signing and Secure Updates
- SBoM Validation and Remediation for devices
  Out-of-the-box integration with leading PKI and Cloud platforms

KeyScaler Capabilities Overview

Leveraging Device Authority's patented Dynamic Device Key Generation (DDKG) technology, the KeyScaler platform is designed to deliver the Nine Core Security Capabilities essential to the success and scalability of Zero Trust IoT applications:

1. Automated Device Provisioning
2. PKI Services for IoT
3. Identity Lifecycle Management (including Edge)
4. Automated Password Management
5. Data Privacy/Policy-driven Encryption
6. Code-Signing and Secure Updates
7. HSM Access Controller
8. Secure Asset Delivery
9. Network Access Control (NAC) for Enterprise IoT

1. Automated Device Provisioning

The initial onboarding and provisioning of IoT devices must be secured and controlled to protect the integrity of IoT applications and the data they are processing. Device Authority's DDKG technology allows organizations to create device "whitelists" that lockdown the device registration and provisioning process to known-good hardware, ensuring that only authorized devices can register with the system. Traditionally, the security surrounding this process has leveraged keys that are injected into devices as part of the manufacturing process. Using KeyScaler PKI Signature+ method, manufacturer-provisioned public keys can be used to define the whitelists that lock down the device registration process. Following successful registration, the key is rotated to increase the security of the device and help detect and prevent device cloning.

KeyScaler provides policy-driven registration controls to enable secure, automated onboarding and provisioning of devices at IoT scale. Registration control records can be pre-established in the system to support headless onboarding of devices in the field without requiring administrative access to manually register, authorize and provision devices with data security policies, keys and credentials, e.g. PKI certificates.

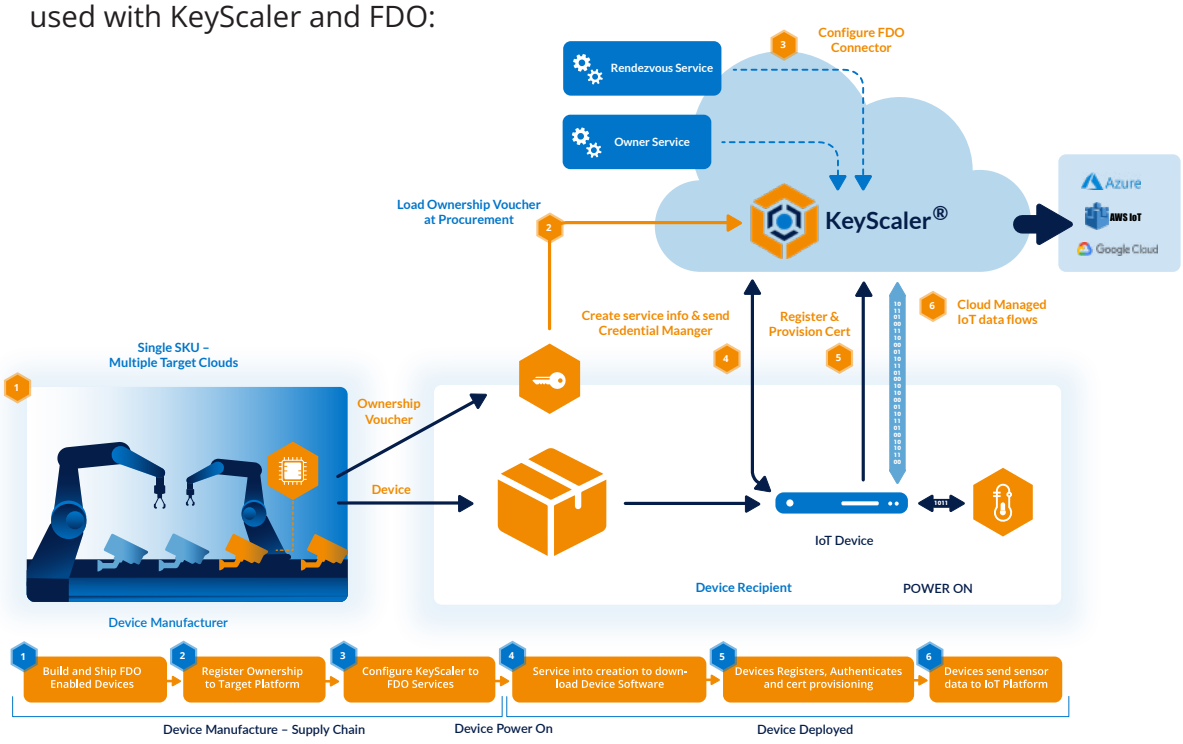
Registration control records can be specifically tailored for individual customer environments and device deployments and can be managed and monitored through the KeyScaler Control Panel or established through

KeyScaler API services. Registration control provides the initial trust anchor for authorizing the device with the IoT application.

KeyScaler supports a number of approaches for zero touch device onboarding and provisioning, providing flexibility for customer choice to fit within their operating environments and use cases. Another example of this is with KeyScaler implementing Fido Device Onboarding (FDO) Protocols. The FIDO Device Onboard (FDO) protocol which is an automatic onboarding mechanism, meaning that it is invoked autonomously and performs only limited, specific, interactions with its environment to complete. A unique feature of FIDO Device Onboard is the ability for the device owner to select the IoT platform at a late stage in the device life cycle. The secrets or configuration data may also be created or chosen at this late stage. This feature is called “late binding”.

FIDO Device Onboard works by establishing the ownership of a device during manufacturing, then tracking the transfers of ownership of the device until it is finally provisioned and put into service. In this way, the device onboarding problem can be thought of as a device “transfer of ownership” or delegation problem. In a common situation for FIDO Device Onboard that uses the “untrusted installer” model, an initial set of credentials and configuration data is configured during manufacturing. Between when the device is manufactured and when it is first powered on and given access to the Internet, the device may transfer ownership multiple times. A structured digital document, called an Ownership Voucher, is used to transfer digital ownership credentials from owner to owner without the need to power on the device.

The diagram below shows the various components and service interconnects used with KeyScaler and FDO:



2. PKI Services for IoT

Automated PKI is the foundation for IoT Security

PKI (Public Key Infrastructure) is set of proven technologies that have solved identity, authentication, integrity, and privacy problems for the Internet and Cloud for many years. Standards-based PKI certificates, or alternatively tokens, provide trust for devices, data, and the connections between machines. Today there is a strong ecosystem of PKI vendors like Venafi, Entrust among others that offer PKI solutions designed for delivering certificates to enterprise assets. However, anybody engaged with PKI knows the complexity of adopting and managing PKI at the scale present in IoT (where according to CyberArk machine identities outnumber humans 45:1) particularly for headless devices with no User Interface. In this world of connected devices, certificates alone cannot address the multiple levels of authorization, role-based policies, and complex, sensitive information flow across platforms. Automated PKI services are essential and are the only option available to deliver device and data trust required for IoT.

Device Authority KeyScaler® brings PKI automation to IoT deployments by streamlining initial attestation and authorization of devices, delivering standards-based x.509 Certificates to those devices eliminating weak credentials, and enforcing Zero Trust policies throughout the device identity lifecycle, all without human intervention.

KeyScaler provides several methods for connecting with IoT devices that traditional PKI platforms do not possess:

1. Dynamic Device Key Generation (DDKG)

- Patented technology to authenticate devices based on hardware attributes
- Provided to customers as a development library
- Requires no unique credentials (keys or certificates) on the device

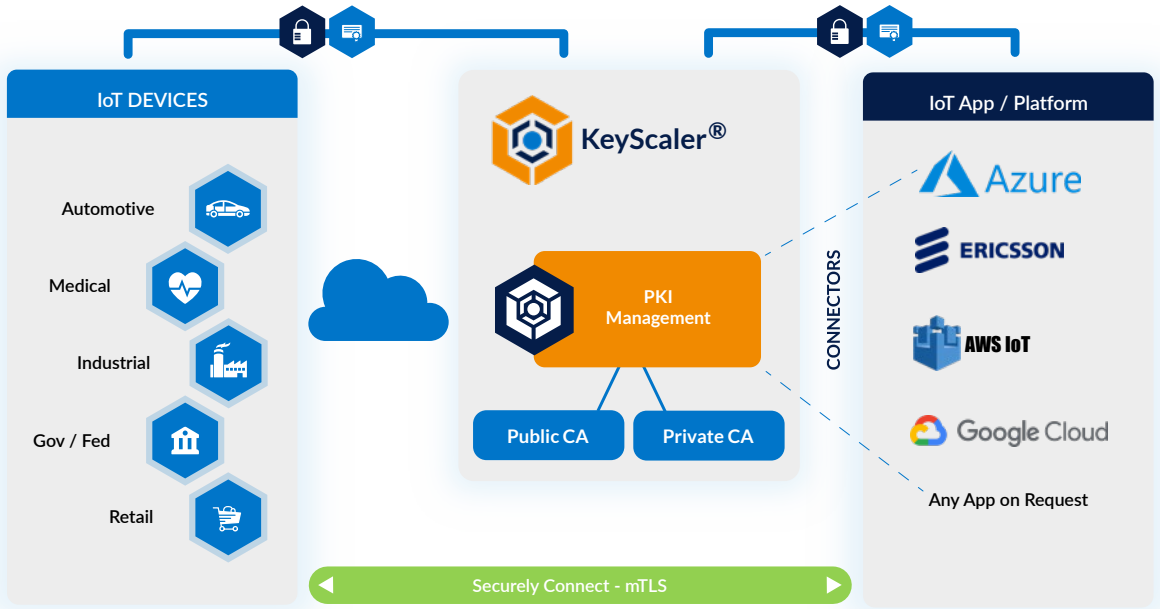
2. Mutual TLS (Certificates)

- Standards-based implementation suitable for almost any device
- Easy-to-use REST APIs utilizing device X.509 certificates
- Requires bootstrap certificate, issuing CA imported to KeyScaler

3. PKI Signature+

- Authenticate devices based on public key signatures
- WebSocket API to enable multiple operations over single connection
- Requires a unique key pair on the device, device public key imported to KeyScaler

While some PKI providers or Public Certificate Authorities primarily offer development kits or API's to integrate IoT devices to their platforms, KeyScaler is the only platform that provides a proven, out-of-box solution for connecting the entire IoT ecosystem - any device, any CA, and any IoT management platform.

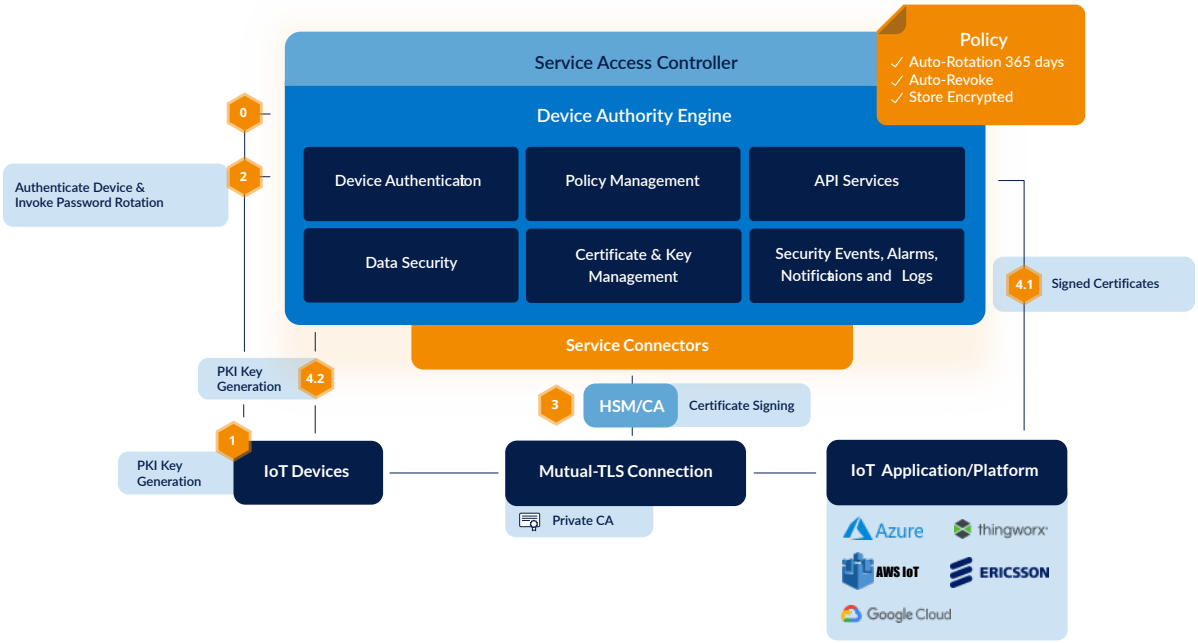


3. Identity Lifecycle Management

Managing PKI for enterprise services is already a challenging and time-consuming operation. For IoT deployments, the complexities are even greater. With KeyScaler, IoT device certificates and keys are securely generated, provisioned, managed, and signed through policy-driven automation. Large-scale IoT projects can be efficiently deployed and managed while avoiding the manual provisioning procedures that inhibit efficiency, scalability, security, consistency and reliability.

Automated Certificate Management offers an optional feature known as Secure Soft Storage which gives devices the ability to store certificates and their associated private keys encrypted at rest, to help protect against unauthorized use, theft, and cloning. Authorized applications are defined in the certificate management policy (e.g. to authenticate to an IoT platform).

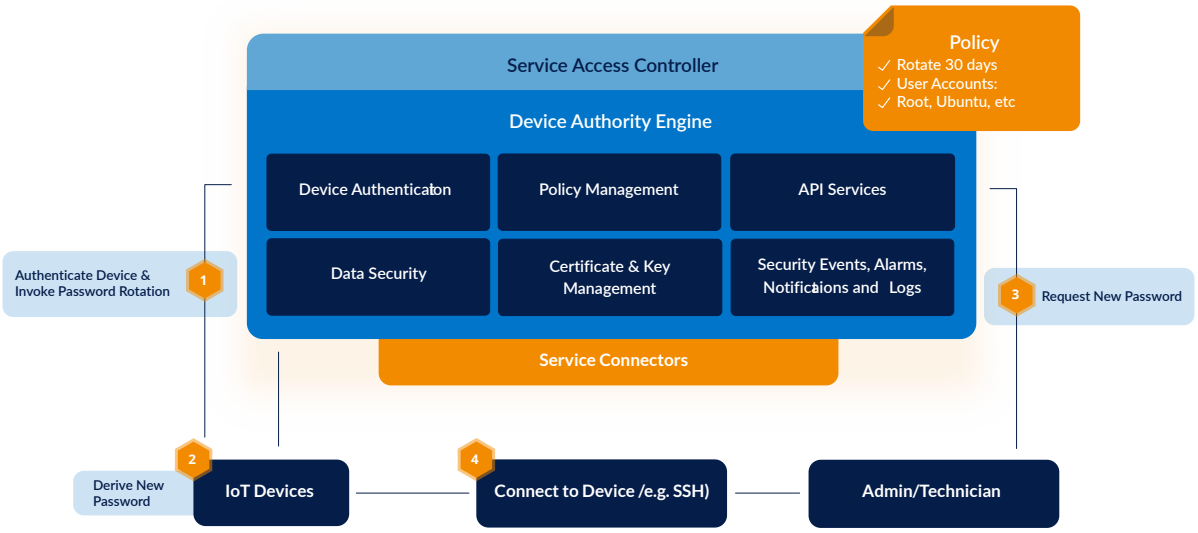
Typically, before a device can use a certificate to connect to an IoT platform (i.e. using mutual TLS), the certificate has to be imported to the platform, and a device entry must be created, often representing the "digital twin" of the device. KeyScaler provides a number of service connectors to automate the enrollment of new device certificates to third-party IoT platforms.



4. Automated Password Management

Weak, default, and stale passwords are the low-hanging fruit for hackers looking to attack and deploy large-scale botnets, and other malware. Managing device passwords at scale is a daunting responsibility, especially since IoT devices do not typically have human operators to instigate the password change.

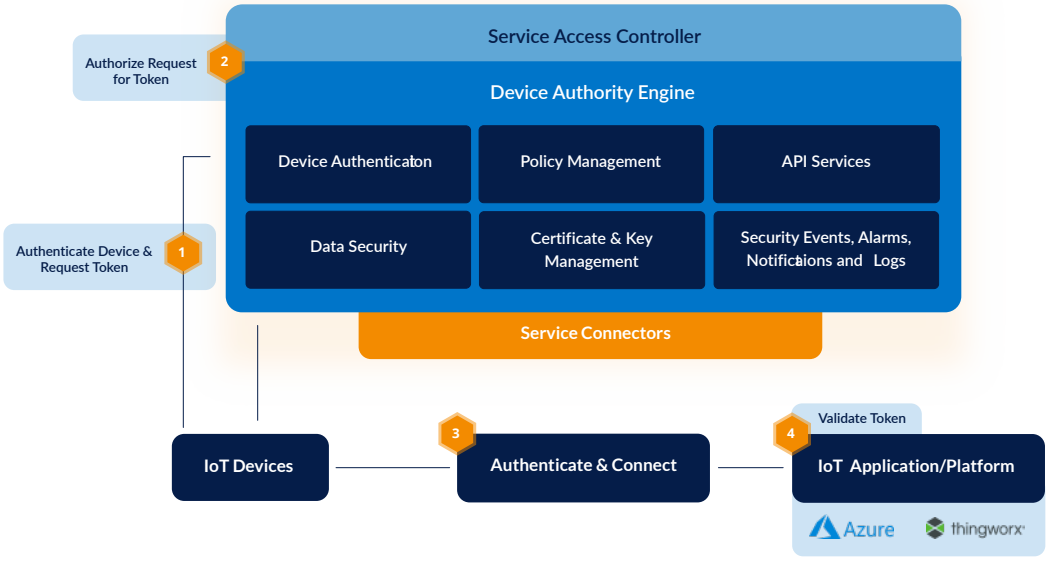
Device Authority's KeyScaler platform provides an Automated Password Management (APM) solution that helps organizations deal with the complexities of setting and managing local account passwords on IoT devices. Centralized policies ensure that the passwords are rotated frequently and securely. The policies allow the rotation to target specific local accounts to ensure that high-value credentials (such as 'root') remain secured.



Device passwords may also be rotated easily on demand, and all administrator actions, such as revealing a password, are logged for auditing purposes.

5. Data Privacy/Policy-driven Encryption

The protection of IoT data is paramount to the integrity of IoT applications. The data feeding IoT applications result in automated actions and controls that can have dangerous physical consequences. It is critical that both the source and the content of data generated by IoT devices are protected and verifiable. However, data must be encrypted from creation to consumption, and requires a higher level of crypto versatility and intelligence than traditional one-way Transport Layer Security (TLS) encryption can provide.



Device Authority's policy-driven encryption, see diagram below, utilizes our patented dynamic key generation, device-derived key technology and crypto-policy agents to provide "drop-in" application-level crypto that is configurable for specific data payloads and transmissions.

The drop-in agents support transparent crypto processing of data sent over HTTP, MQTT, and custom protocols such as ThingWorx AlwaysOn™, which means there is no requirement to change existing applications on devices – simply install the agent and set the policy on KeyScaler to begin securing the data.

Dynamic keys ensure that each data payload can be encrypted with one-time-use keys that are not shared over the network or stored on the device. Individual data elements can be encrypted for dynamic audiences, independently from data transport protocol security. Using KeyScaler "set and deploy" policies to determine precisely which data needs to be encrypted, our smart agent technology processes and encrypts the vast quantities of data generated at the device or network edge. This ensures regulatory compliance (e.g. EU GDPR and HIPAA) and the mitigation of risk and data loss.

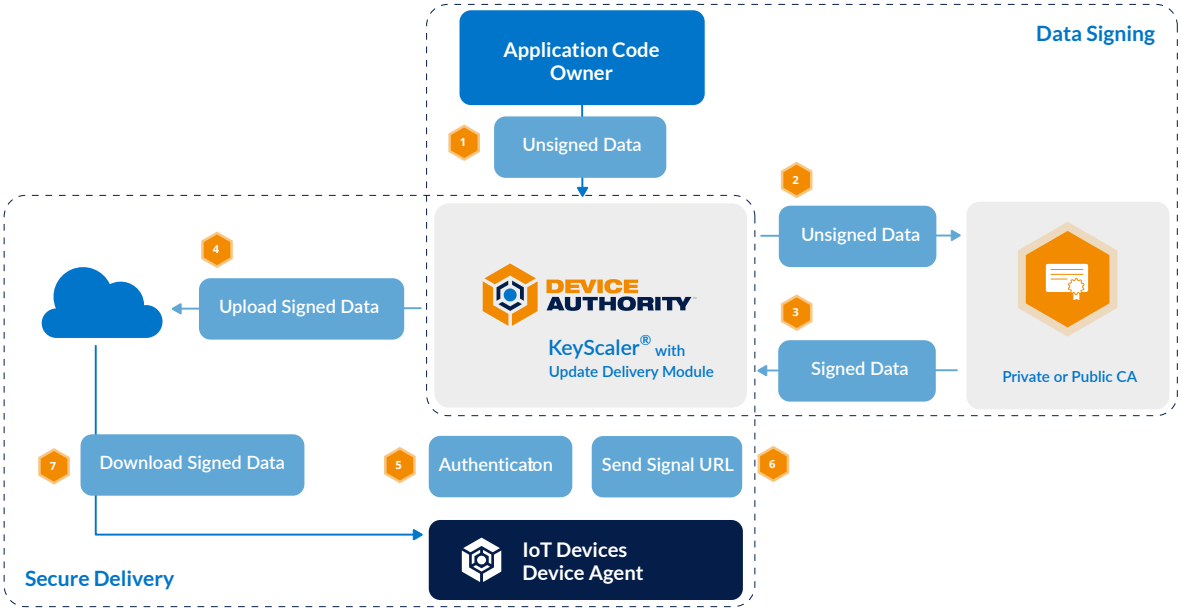
6. Code-Signing and Secure Updates

Unauthorized software and firmware updates are a major threat vector for IoT cyber-attacks. IoT breaches can have physical consequences that result in loss and can introduce substantial legal liability and erode brand reputation.

There are three critical security requirements for delivering updates securely to IoT devices:

1. Securing access to the updates
2. Verifying the source of the updates
3. Verifying the integrity of the updates

Device Authority's Secure Updates and Data Signing solution delivers each of these critical requirements for IoT environments. Access to secure updates is restricted to authorized devices. Updates are also specifically encrypted for target devices and are not exposed as unprotected software or firmware downloads. Lastly, secure updates ensure that both the update source and the integrity of the updates themselves are verified, delivering end-to-end protection for device updates.



KeyScaler manages the signing and/or delivery of software updates to ensure that both the update source and the integrity of the updates themselves are verified, delivering an end-to-end protection for device updates. The diagram above illustrates this two-stage process:

1. Application Signing Process:
- KeyScaler receives the 'unsigned data/code' from the application code owner
- The hash is calculated and is then forwarded on to the signing authority to be signed
- The signing authority then sends back the 'signed hash' to KeyScaler

2. Secure Delivery process:
- KeyScaler uploads the signed data to a third-party Cloud Storage (e.g. Azure Storage)
- When the IoT device authenticates and checks-in with KeyScaler, it will receive a notification of a pending update
- KeyScaler then sends a signed URL to the authenticated device, along with the data signature

The device then downloads the signed data from the cloud repository The solution does not rely on network transport security for update protection and is transport-agnostic to support both Over-the-Air (OTA) and Over-the-Network (OTN) updates utilizing various transport protocols.

7. HSM Access Controller

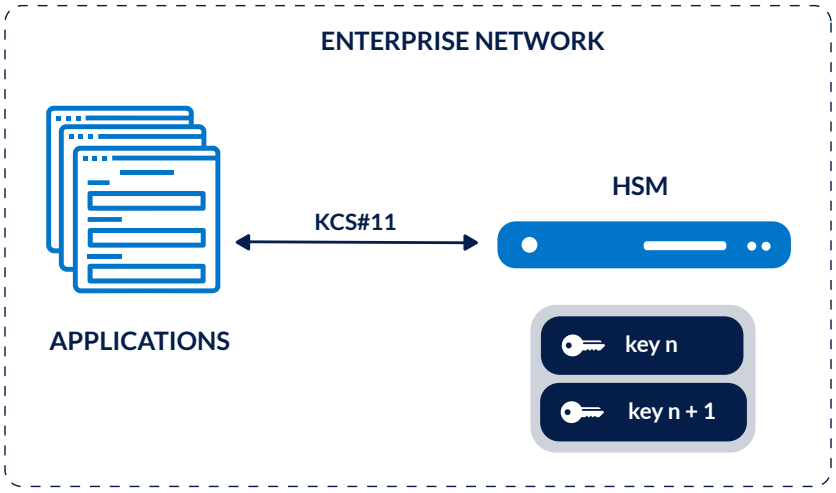
Hardware Security Modules ('HSM') provide secure key storage and crypto processing capabilities and are often utilized in use cases where the highest level of security is required, for example FIPS 140-2 Level 3. HSMs are designed to provide a secure storage point for secret keys – which means that the secret keys can often never be exported or made available outside of the secure operating environment of the HSM.

When an application needs to use secrets stored in the HSM (e.g. private key) it will send a request to the HSM, typically using an SDK or development library, that contains the data to be processed, the function (e.g. decrypt, sign, etc.), and the name/alias of the secret key to use. Upon receiving the request, the HSM will process the data using the requested key and returns the output.

When deploying and integrating an HSM, there are three main security points to consider:

1. Authentication – How do I trust the client making the request to use a key?
2. Authorization – Is the requestor allowed to use this key for this HSM function?
3. Network Security – Is my HSM in a secure location in my network?

The diagram below shows a typical deployment model for HSMs:



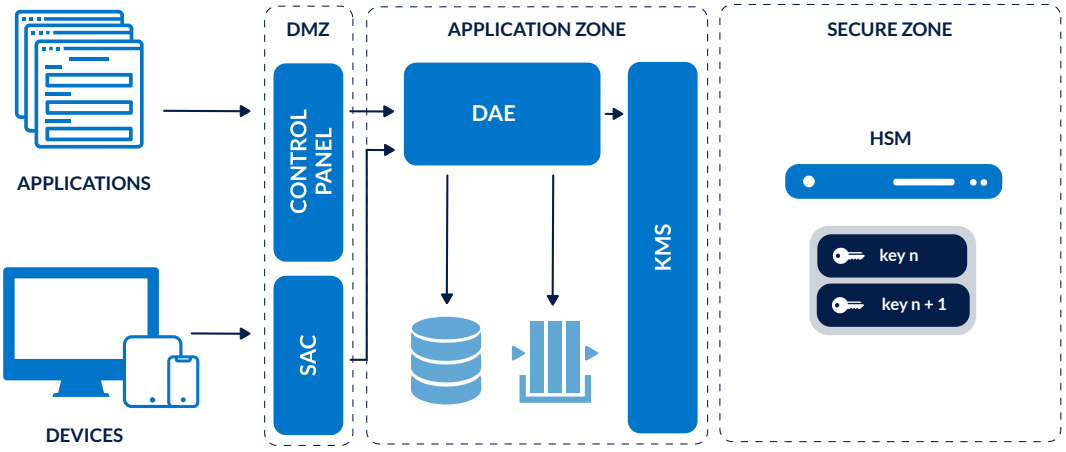
The KeyScaler HSM Access Controller solution provides a secure and simple approach to integrating applications, services, and devices with off-the-shelf HSMs, via a standard set of RESTful APIs.

By utilizing the DDKG authentication process, KeyScaler HSM Access Controller solution is able to strongly authenticate and validate clients requesting use of the HSM, and the keys that are stored within it.

Once the identity of the requesting client has been authenticated and verified, the KeyScaler then assesses the client request against the authorization policies. This ensures that the requesting client is authorized to use the function (e.g. decrypt, sign, etc.), and specifically whether the client is authorized to use the requested key. This means that organizations can use central policy to define narrow key usage scopes for certain applications.

These authorization policies are designed to help define the role of an application instance. For example, if the application provides code-signing capabilities, then I would create a policy that limits the scope of usage to only the “Data Signing” function and specify that only the corporate signing key can be used.

The following diagram provides an overview of the KeyScaler HSM Access Controller solution, deployed between requesting clients and the HSM itself, provides enhanced security and protection through strong authentication, granular authorization policies, and logical network separation.



8. Secure Asset Delivery

Secure Asset Delivery is a crucial element of a trusted IoT device lifecycle. Without strong authentication and data encryption between machines connecting over an open network, remote administration, automated operations, and secure transfer of files between devices is impossible, and the ability to securely operate an IoT environment at scale is limited.

KeyScaler enables real-time delivery of actional assets that can be executed by the IoT device, including Access Credentials (SSH), device scripts, device configuration, and is sent via real-time communication protocol for instant 'synchronous' response. Script secrecy and integrity is maintained using Dynamic Device Key Generation (DDKG) derived crypto keys.

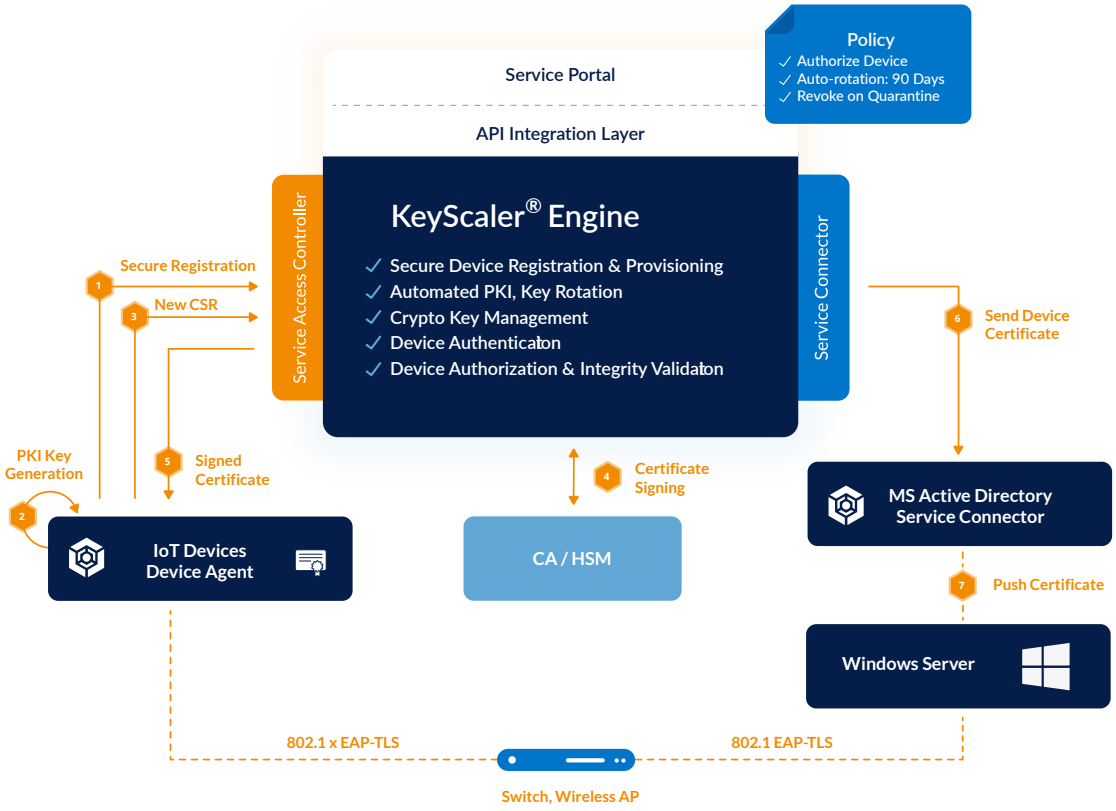
KeyScaler also enables the binding of unique access credentials to individual devices, supported by a flexible policy engine to enable time-bound access credentials. KeyScaler's flexible REST API framework also integrates with Enterprise Applications such as VPN, Privileged Access Management (PAM), and Privilege Identity Management (PIM) services for extended security controls. These capabilities provide a "least privilege" access model for IoT, enabling a Zero Trust environment.

9. Network Access Control for Enterprise IoT

Within traditional enterprise networks there are a wide range of devices, computers, access points and switches that all connect into a network and are typically managed through Microsoft's Active Directory (AD) Domain services. Managing authorization and network access control is not easy for the number and variety of devices. Adding IoT devices to a corporate network raises more complex challenges as these devices can be very different to traditional user devices and switches. One of the most obvious challenges being the sheer scale/number of IoT devices that will connect to the network. Another major challenge for the enterprise CIOs and system administrators is security. How would they trust these devices connecting to their networks? Typical IoT devices are "headless" which means they have no user input or GUI. This means it's difficult to apply the traditional enterprise Network Access Control (NAC) mechanisms on such devices.

Network access control of IoT devices requires:

- Device Identity – Scalable and proven identity model that doesn't require human intervention, e.g. PKI certificates
- Integration – Ensuring seamless integration with AD and existing administrator workflows, Certificate Authorities (CA) and enterprise
- Hardware Security Modules (HSM)
- Automation – Secure onboarding and authorization of devices to the network without human intervention



There are several techniques used in the market today to manage network access and authorization control which broadly fall into two main solution areas. The first is a solution which can defend and protect network infrastructure by characterizing each device and actively monitoring them, detecting rogue behavior and revoking access from the enterprise.

Another approach is to use proven networking concepts and existing standards such as 802.1x to authorize and authenticate devices. 802.1x is an IEEE Standard for Port-based Network Access Control (PNAC) and is part of the IEEE 802.1 group of networking protocols and can be used to identify users and devices by controlling their access to the network. NAC controls access to enterprise resources using authorization and policy enforcement.

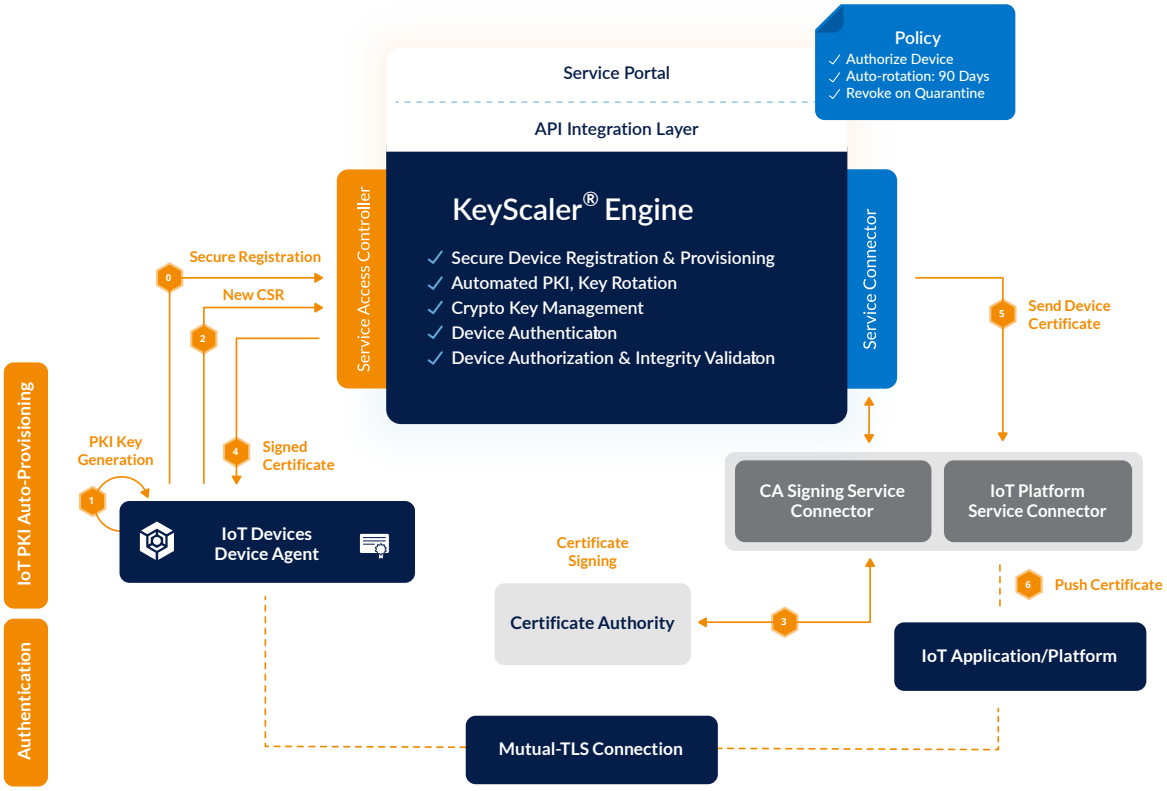
Device Authority's KeyScaler platform can be utilized to authorize and deauthorize devices connecting to a network utilizing PKI certificates. KeyScaler can automate the process for managing device identity, automating secure registration and onboarding, lifecycle management of PKI certificates to devices, which in turn are automatically pushed to Microsoft AD to be used for validation during the network authentication process. Each associated device will be given a PKI certificate to enable it to authenticate over 802.1x using EAP-TLS to a RADIUS server connected inside the network. Devices can be denied access to the network by revoking their associated certificate. The customer needs to ensure their network gear supports 802.1x and an appropriate RADIUS server if available to support this approach.

Integrations and Connectors

KeyScaler Enhanced Platform Integration Connector ('EPIC')

Device Authority's KeyScaler Platform provides a flexible interface to integrate with ANY external platforms and services which enables the building of custom service connectors by partners and System Integrators. It leverages MQTT, a light weight, standards-based interface protocol which is supported by many IoT platforms including ThingWorx. These service connectors enable the Real-time notification of events that occur in KeyScaler such as:

1. Certificate provisioning and revocation events - to integrate into a Certificate Authority platform
2. Device authorization status events – e.g. device registered, device quarantined, device blacklisted, etc.
3. Code-signing and secure update delivery – to integrate the core secure update solution into existing code-signing, or cloud storage platforms for update delivery.
4. Device update events – device received update, device successfully applied update, etc.



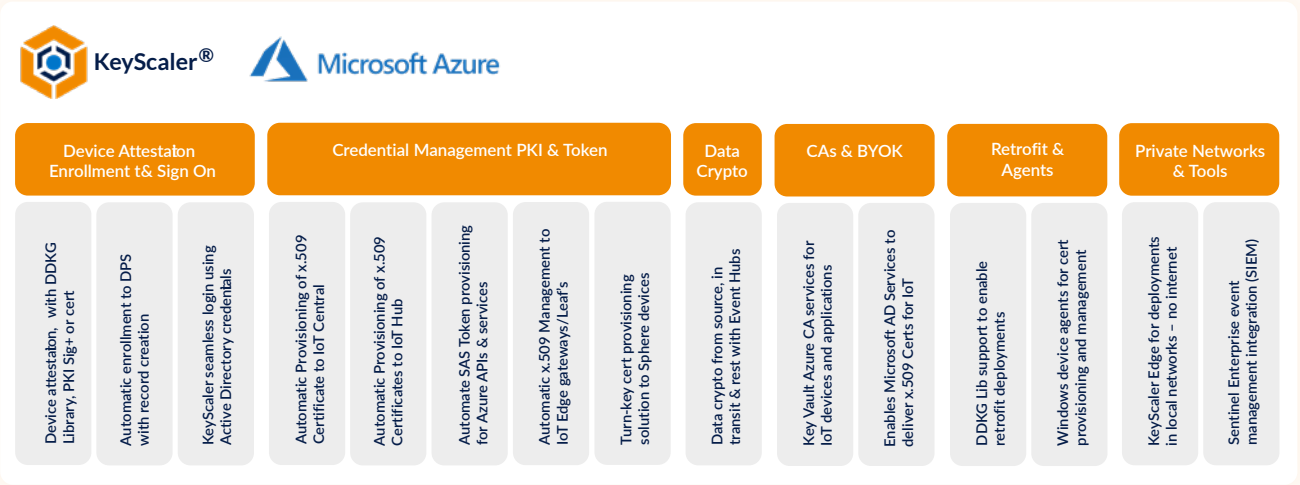
KeyScaler Integration Capability to ANY IoT Platform or Service.

KeyScaler Security Suite for Microsoft Azure IoT

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 management policies.

Device Authority provides a Security Suite for Microsoft Azure, offering enhanced security and automation fully integrated across core Azure IoT services,helping customers accelerate, optimize and leverage their investments in their Azure IoT deployments.

This includes:



Connector for Azure IoT Central

- Automatically enrolls devices to Azure IoT Central application instances
- Utilizes x.509 Group Enrolment 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)

Connector for Azure DPS

- Automatically enrols 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)
- Supports Custom Allocation Policy via webhook url and api version

Connector for Azure IoT Hub

- Automates and secures enrollment 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

Connector for Microsoft Azure Active Directory

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

Data Privacy for Azure Event Hubs

- 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

Credential Manager for Windows

- Drop-in Windows Credential manager for Windows endpoints
- Credential Management Agent supports Windows-based IoT devices. This includes support for Windows 7, 8, 10, 2012 Server and 2016 Server

CA Key Storage for Azure Key Vault

- Enables secure generation and storage of KeyScaler Private PKI signing keys on Azure Key Vault
- Utilize Azure Key Vault secure key storage to issue certificates to devices and other entities.

HSM Access Controller for Azure Key Vault

- Integrates KeyScaler HSM Access Controller solution with Azure Key Vault
- Generate and store keys in Azure Key Vault, and limit access using HSM Access Controller policies

PTC ThingWorx Security Suite

IoT devices produce sensitive data which needs to be protected. This data will be transported from the devices to the ThingWorx platform, where it will be processed, monitored, and analyzed to enable operational efficiency. Sensitive information flows all the way from the source to the destination.

Protecting the data at rest, in motion, and in use is a huge challenge. This causes uncertainty in data being transferred from a trusted source to a trusted destination, thus raising concerns on Data Privacy and Data Security. In addition, IoT devices connecting into ThingWorx applications require validation, to ensure unauthorized devices aren't providing invalid data.

What is included in the Security Suite?

Data Security (Crypto) Extension

- Supports encrypting and decrypting data directly within ThingWorx platform
- Dynamic, session-based key derivation eliminates the need to share or store crypto keys on devices
- Policy-based, end-to-end data encryption for data privacy
- Support for the AlwaysOn protocol and ThingWorx 8

Device Authentication Extension

- Introduces ephemeral token-based authentication for ThingWorx
- Prevents unauthorized device-to-Thing Bind
- Re-authentication without having to disconnect device
- Replaces use of "AppKey" for connecting devices to ThingWorx

Management Interface Extension

- Simplified integration to manage device identities, policies and groups within KeyScaler, directly from the ThingWorx management console
- Provides ThingWorx customers and partners with a "single pane of glass" for device management

Device Authorization Extension

- Flexible integration with KeyScaler for real time device authorization status updates
- KeyScaler automatically creates, manages and synchronizes the device identities of Things in ThingWorx

KeyScaler Connector for AWS IoT

Traditionally, manual provisioning of certificates was time-consuming and cumbersome, and almost impossible at IoT scale. Automating the PKI process is an essential step to help organizations continue to benefit from the agility and flexibility of AWS IoT, without sacrificing security.

With the KeyScaler Conenctor for AWS IoT, Amazon Web Services customers benefit from the KeyScaler platform which:

- Delivers operational efficiency and support at IoT scale
- Mitigates security breaches related to human error
- Provides a highly secure, cost-effective security framework for
- Amazon Web Services customers

Key features of the AWS IoT Connector include:

- Zero touch provisioning
- Automated process for provisioning, revocation and assignment of signed certificates to the AWS IoT service
- Support for both device-side PKI generation and KeyScaler private certificate signing
- Choice of Certificate Authority

KeyScaler Architectural Overview

KeyScaler is built on a robust services-oriented architecture that can be implemented on premise for single customer installations, or as a multi-tenant service platform for cloud and service providers. KeyScaler is also offered as a managed service (SaaS) which allows partners to deliver KeyScaler based solutions without the overhead of infrastructure, dev ops and ongoing management costs of a typical hosted environment. Additional features for partners include:

1. Multi-tenant model for customer enrollment and management
2. Branding support
3. Integrated billing and customer support
4. Quick to integrate with KeyScaler through APIs

The modular architecture allows for lateral scaling of security services which include the device registry, authentication engine, policy engine, Key Management Service (KMS) key store and derived key manager. KeyScaler provides a suite of HTTP RESTful API's to enable organizations to automate device identity management and security functions and allow traditional manual security operations to be rapidly integrated to any existing enterprise processes.

To support a wide array of devices and use cases, KeyScaler is designed to leverage flexible client-side interaction protocol implementation to facilitate "drop-in" device registration, authentication, certificate provisioning and management, and policy-driven data encryption. The protocol can be implemented by customers in their applications or use the agent SDK or pre-built agents provided by Device Authority.

Agents include support for transparent data encryption over HTTP, MQTT, and the ThingWorx AlwaysOn™. With this approach, customers get flexibility, independent of Device Authority client-side agent for KeyScaler security operations functionality.

Flexible Authentication Methods

KeyScaler supports three flexible methods for device authentication, outlined below:

- Dynamic Device Key Generation (DDKG)
- **Mutual TLS** (Client Certificate Authentication)
- **PKI Signature+**

Dynamic Device Key Generation (DDKG) authentication model

leverages a patented challenge and response mechanism that interrogates the hardware of a device to ensure that the KeyScaler platform is communicating with the same physical device that was originally registered to the system. DDKG is provided as a development library, with documentation and source code samples, which can be easily added to new or existing applications. There are two deployment levels for DDKG:

1. Level 1: Supporting common attributes from the device OS, (e.g. MAC address, IP address, Serial Number etc.)
2. Level 2: For a higher security posture, and includes support for device specific attributes, such as pre- shared keys, Vehicle Identification Number, IMEI etc.

Mutual TLS

is a method of device authentication based on open standards and will work with any device that supports client certificate authentication. This method is ideal for smaller devices that have a TPM, or Secure Element available to store private keys securely. The main requirements to use these API's are:

- Any off-the-shelf HTTP and TLS libraries (OpenSSL, WolfSSL, etc)
- Initial bootstrap certificate on the device
- Trusted Certificate Authority imported into KeyScaler

The initial trust is established by importing the bootstrap Certificate Authority ('CA') in to the KeyScaler platform as a trusted identity provider for registration. Once registered, the KeyScaler then provisions an 'operational' certificate to the device that can be used to connect to KeyScaler, and the configured IoT platform, such as Azure DPS, IoT Hub, etc.

PKI Signature+ is a purpose-built lightweight authentication model that leverages existing public key signature standards to authenticate devices to the KeyScaler platform. PKI Signature+ does not require a Device Authority library, and is simply provided with reference documentation and samples, leaving organizations free to design their own implementations around the KeyScaler

Deployment Architecture

KeyScaler deployment architecture is designed with 3 key principles in mind:

- Highly Available

To maintain the integrity and security of the device population, the KeyScaler solution is available 24/7/365 – Device data doesn't sleep.

- Highly Scalable

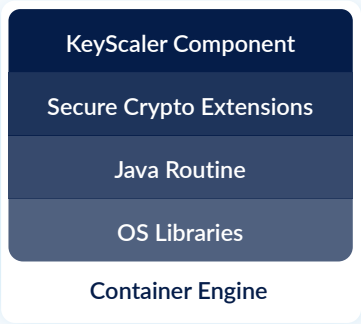
To cater for the dynamic nature of IoT Device ecosystems, the KeyScaler platform maximises efficiency through intelligent monitoring and automatic scaling.

- Highly Robust

Trust is key – for the devices, and the platform that secures them. To achieve these core principles, the KeyScaler technology stack is componentised and allows for the easy deployment of multiple instances as required for the project at hand.

Device Authority Engine (DAE)	The core of the KeyScaler platform
Admin Control Panel (CP)	A flexible and dynamic GUI that allows the configuration and manual management of devices
Enhance Platform Integration Connector (EPIC)	Our extensible queue-based integration framework. EPIC allows full bidirectional integration with almost any 3rd party platform – from device management to Dashboards and reporting
Key Management Service (KMS)	The engine that performs cryptographic functions within KeyScaler – including key generation, certificate signing, and encryption / decryption
Service Access Controller (SAC)	The secure API for devices under KeyScaler management

These components comprise the KeyScaler platform, and are released as container images to allow for easy management and scaling.



KeyScaler-as-a-Service (KSaaS)

Our KSaaS platform offers the quickest and safest route to IoT Device Trust. As a fully managed and hosted platform, it removes the burden of infrastructure and in-house expertise, and allows a near-immediate deployment of the full KeyScaler solution.

Utilizing a secure multi-tenant data model, each tenant built on the KSaaS platform is given a dedicated silo of environments, dedicated secure repositories, and cryptographically isolated databases to ensure the highest level of security.

We host the component containers listed above on the Microsoft Azure Managed Application platform which dynamically scales the components required as the global load varies, ensuring a consistent and robust service. We also employ several IaaS services from the Azure platform to maximize efficiency and scalability.

The KSaaS platform provides several benefits:

1. Transparent managed updates

   The KSaaS platform is upgraded as part of the Device Authority software release cycle, and is the first to receive new features, functionality, and security updates.

2. Industry standard approach

   Bespoke deployments create bespoke dependencies – the KSaaS platform encourages industry standard approaches to IoT device security and makes it easy to work with the biggest players in the market.

3. Time to Production

   Without the burden of infrastructure deployment and in-house training, the full power of KeyScaler is available from day 1 of the project.

4. Scale with your Business

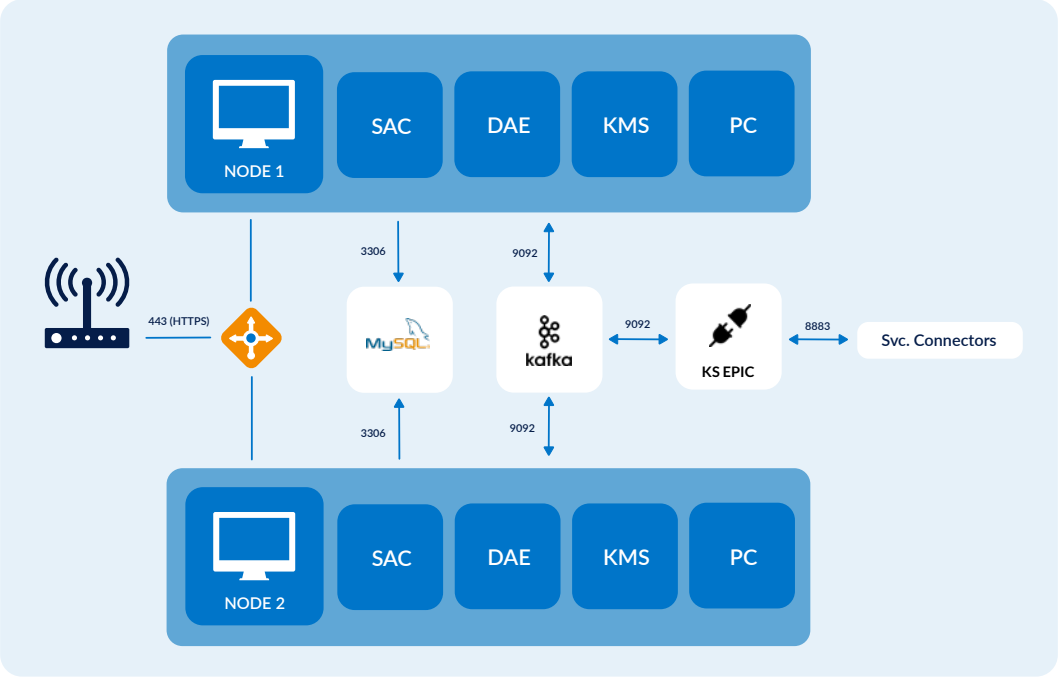
   IoT Device projects often start small, and scale quickly. KSaaS offers a predictable Opex model that scales with the load required.

Self-hosted / On-premise

Often there are situations where security policies or device connectivity mandates that a self-hosted solution is employed. This could be because of an established policy that dictates all critical infrastructure is internal, or because the devices being secured simply do not have access to the internet. In these cases, Device Authority offer support and consultancy services to assist in the deployment and maintenance of the KeyScaler platform on whatever hosting environment is required.

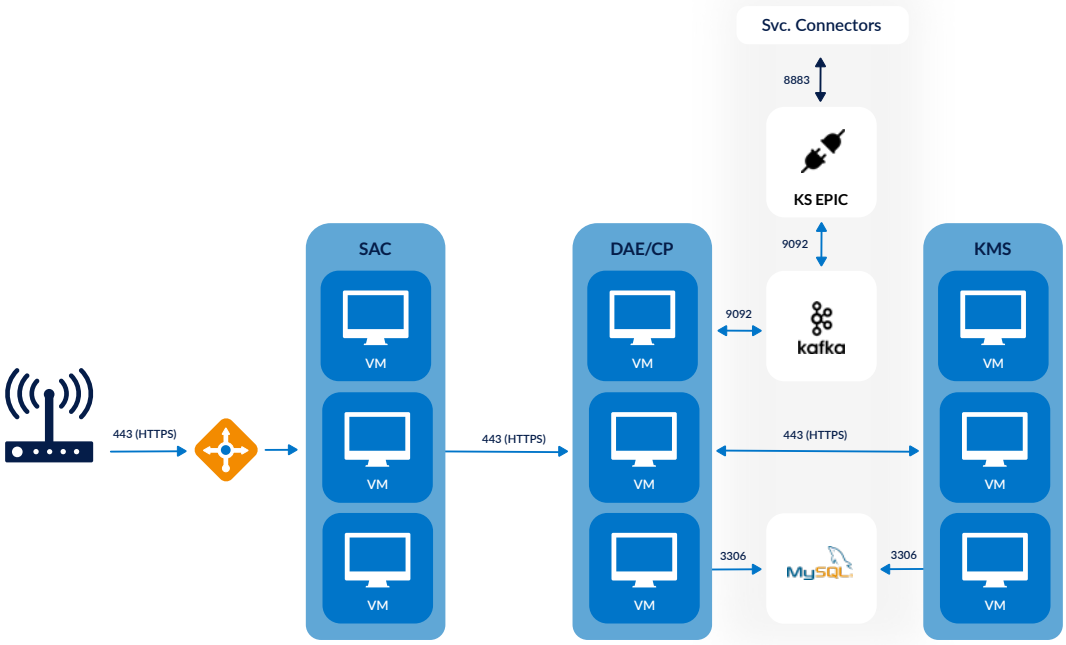
Using the same container-based approach as the KSaaS platform, KeyScaler can be deployed within private client cloud platforms, or on physical servers in datacenters or industrial use-cases.

A typical on-premise deployment would be architected for High Availability as follows:



HA Deployment Overview

If deploying in a private cloud environment, an n-scale distributed deployment would be architected as follows:



When self-hosting KeyScaler in a private environment, the Device Authority Enterprise Support Services are available for a range of service levels, from training and consultancy, to always-on 24x7 support services. We will assign a dedicated team to understand your environment and processes, and work with you to shape the KeyScaler platform around your existing estate in the most robust and scalable way as possible. Our in-house support team are well versed in all mainstream cloud platforms, as well as the most common on-premise and industrial deployment topologies.

KeyScaler Edge

Today's market is driving a more mature Edge computing model with localized AI and ML becoming more mainstream. However, no solution exists today to address localized Edge gateway IoT security services. Organizations require automation for Edge deployments to drive efficiency at IoT scale, meet compliance, regulatory requirements at the same time protect confidentiality, prevent data theft, protect brand and so on.
KeyScaler Edge is the first device identity centric IAM to address the complex end-to-end challenges of IoT security lifecycle management at the Edge. It is a lightweight version of KeyScaler that is created specifically for Edge nodes, with the ability to deliver:

- Security lifecycle management
- Device bound identity
- Leaf device authentication and authorization to edge gateways
- Zero touch onboarding and registration
- Automated credential and identity management –
- Certificates, Tokens

All this needs to be done in the local network, independent of an available internet connection.

Simplified Client Integration

In addition to the extensive RESTful management API's, KeyScaler also provides a simple WebSocket interface that allows complex security management operations to be easily added to new and existing applications running on IoT devices. Applications connect to a single WebSocket endpoint and are prompted to register (if a device is new to the system) or authenticate. Once authenticated, KeyScaler delegates any outstanding security operations that must be completed - such as PKI certificate rotation, device firmware updates, changes to data crypto policies, or new authentication tokens for connecting to third party IoT platforms (e.g. PTC's ThingWorx IoT platform).

One important benefit of this model is the significant reduction in development overhead – as there is only one KeyScaler WebSocket interface to connect to. Device applications are prompted with all the steps and actions that need to be taken, so there is no need to assemble multiple API endpoints in the correct order to complete a single security operation.

Device Management

KeyScaler includes an administrative control panel to manage device onboarding, registration, and security policies. The Control Panel is also a window into the functions and configuration of the system and provides a wide range of security and system management functions. Control Panel access is protected by industry standard Time-based One Time Password (TOTP) which can be generated by any application that supports TOTP generation (e.g. Google Authenticator) or delivered out-of-band via email.

KeyScaler Enhanced Platform Integration Connector

In addition to the native service connectors, KeyScaler provides communication channels within the Enhanced Platform Integration Connector ('EPIC') API, to allow organizations to rapidly build new service connectors to extend the core platform solutions and integrate into third-party services – such as Certificate Authorities, or IoT Connectivity platforms.

KeyScaler EPIC consists of a MQTT broker that publishes tasks and notifications in real-time – allowing services with native MQTT capabilities to connect directly and consume the messages. Services without native MQTT capabilities can utilize EPIC clients to convert MQTT messages to appropriate APIs. Existing platforms and services can subscribe to these messages to integrate into KeyScaler solution workflows e.g. sign new certificates for devices.

KeyScaler Client SDK

To help accelerate the client-side integration and development process, Device Authority provides a Software Development Kit (SDK) that implements the client communication process with KeyScaler, and provides a "connected" development library, compared to the core DDKG ("Dynamic Device Key Generator") library.

Since KSClient handles all of the communication with the KeyScaler server - this means that developers can accelerate their timelines for device application integration with KeyScaler through the use of high-level APIs, without needing to understand which KeyScaler REST APIs are appropriate for their use case.

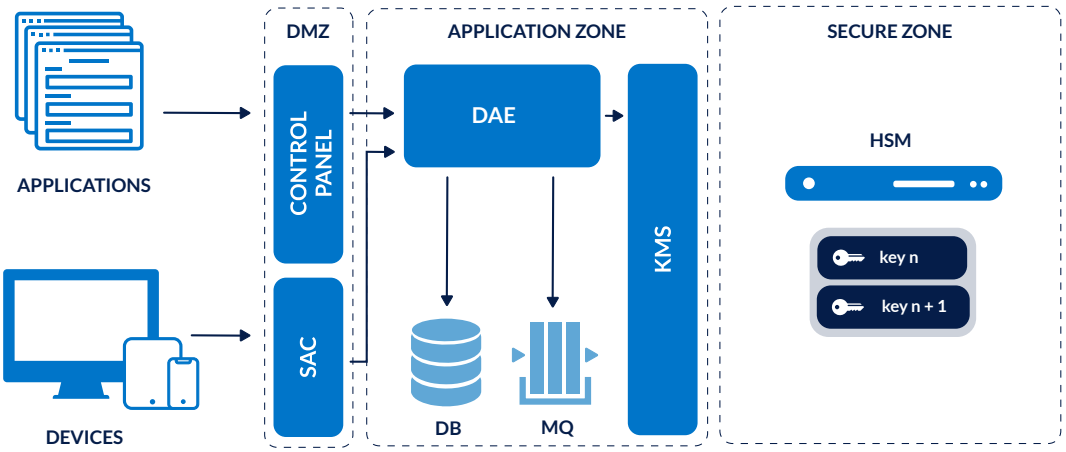
Additionally, a Python wrapper is available for the SDK. The wrapper provides a Python-native class that exposes all of the underlying KSClient functions, for rapid integration in to new and existing Python codebases.

Hardware Security Module (HSM) Support

KeyScaler supports deployments with Hardware Security Modules (HSM). The HSM is used to generate and protect KeyScaler system keys and private Certificate Authority (CA) root keys. The keys protected by the HSM are used for various operations to harden the KeyScaler processes including:

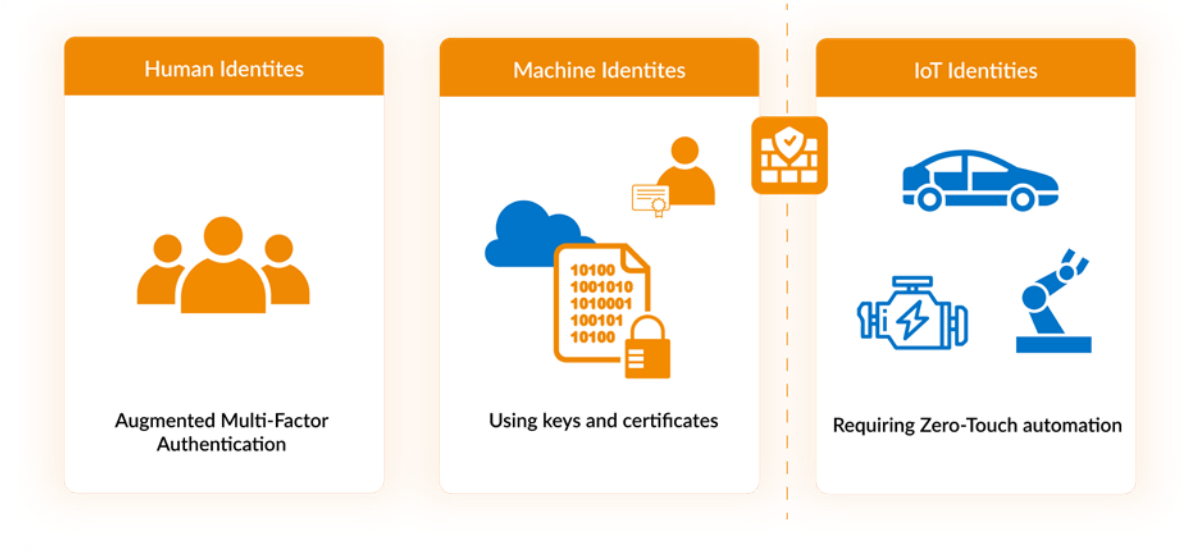
- Encrypting the database
- Encrypting communication with devices
- Signing managed device certificates

The KeyScaler platform Architecture Overview integrated with a hardware security module (HSM) is operationalizing trust and security at IoT scale, providing high-assurance device authentication, managed end-to-end encryption, and certificate provisioning for connected devices.



Conclusion

As the pursuit of Digital Transformation in search of new products and markets leads to an explosion of connected IoT devices globally, a differentiated approach to securely managing device identities – fundamental to a Zero Trust strategy – must be implemented. While the technologies exist to effectively manage enterprise devices, IoT use cases require a coordinated and integrated approach that considers the full identity lifecycle of devices, often outside the firewall and at the Internet Edge.



The rise of machine identities as a category has created three distinct approaches to identity management: human identities managing users and groups, machine identities managing corporate devices and digital assets, and IoT device identities. The updated Device Authority Enterprise IoT Blueprint 2.0 included in this document, provides a comprehensive framework for managing your IoT device identity lifecycle based on Zero Trust, and clearly outlines the Nine Core Security Capabilities essential to the security and scalability of Zero Trust IoT applications in multiple industries.

In today's connected world, where attacks are continuous, breaches take minutes, and damage can be done to your customers, supply chain, or brand in seconds, time and speed are major determinants of successful mitigation. No matter what secure chipset, enterprise security platform, IoT cloud platform, or network security controls you have in place, the complexity of scaled, industry-specific IoT deployments demand automation and integrated trust. Device Authority KeyScaler provides this end-to-end capability with an out-of-box, quick-to-deploy solution that includes proven integrations with leading PKI and Cloud platform vendors, support for any device, and choice of deployment options (on-prem or SaaS) offering ultimate flexibility.

For more information, check out our website or contact us.

DEVICE AUTHORITY™

Automating Zero Trust for IoT