DEVICE AUTHORITY™
Edge to Enterprise IoT Security

KeyScaler™ IoT Security Platform

KeyScaler™ delivers comprehensive IoT security lifecycle management at scale. Secure device registration and provisioning, digital identity management (PKI, Tokens), automated password management, policy-driven crypto and credential management, secure updates along all with devices without human intervention.

- **KeyScaler Edge -** A lightweight version of KeyScaler that is created specifically for Edge nodes, with the ability to register, authenticate, and provision certificates & tokens to devices in the local network, independent of an available internet connection.

- **Secure Asset Delivery** - Real-time delivery of assets to IoT devices, that can be executed by the device, with the results provided back to KeyScaler e.g. Access Credentials (SSH), device scripts etc. With flexible REST API framework to integrate with Enterprise Applications, such as Privileged Access Management (PAM) services.

- **FIDO FDO –** Integrating FIDO Device Onboarding (FDO) standard (Spec 1.0) with KeyScaler, to offer an industry standardized approach to Zero Touch device onboarding for IoT.

- **Security Suite for Microsoft Azure IoT -** Enhanced security for Microsoft customers and partners to accelerate, optimize and leverage their investments in IoT deployments with connectors for Azure Sphere, Azure IoT Central, Azure IoT Hub, Azure Key Vault, Azure IoT Edge, Azure DPS, Microsoft Active Directory, Azure Event Hub data privacy, Active Directory Certificate Services and Windows credential manager.

- **Security Suite for PTC ThingWorx** - Simplified integration between ThingWorx and KeyScaler offering data security, device authentication, management interface and device authorization.

- **Amazon Web Services (AWS) IoT PKI Connector** - A service connector, utilizing the AWS SDK, supports certificate provisioning, revocation as well as 'thing' creation and certificate assignment.

- **Enhanced Platform Integration Connector -** Flexible interface to integrate with ANY external platforms and services. Provides real-time notification of events that occur in KeyScaler.

- **Automated Certificate Management** – Automated certificate provisioning and management for IoT devices and gateways.

- **Internal Private PKI** - Customers can generate their own internal private root certificate authority and key, to enable provisioning of self-signed certificates to devices and the Azure and AWS IoT service.

- **Secure Soft Storage -** To prevent theft of certificates and unauthorized usage, the agent stores the certificate and associated key pair in an encrypted state. Decryption is available only to authorized applications as defined in the policy on the KeyScaler server.

- **End-to-End Data Security** – Granular, efficient policy-driven crypto that provides secure, end-to-end delivery and storage when using third party networks and cloud services.

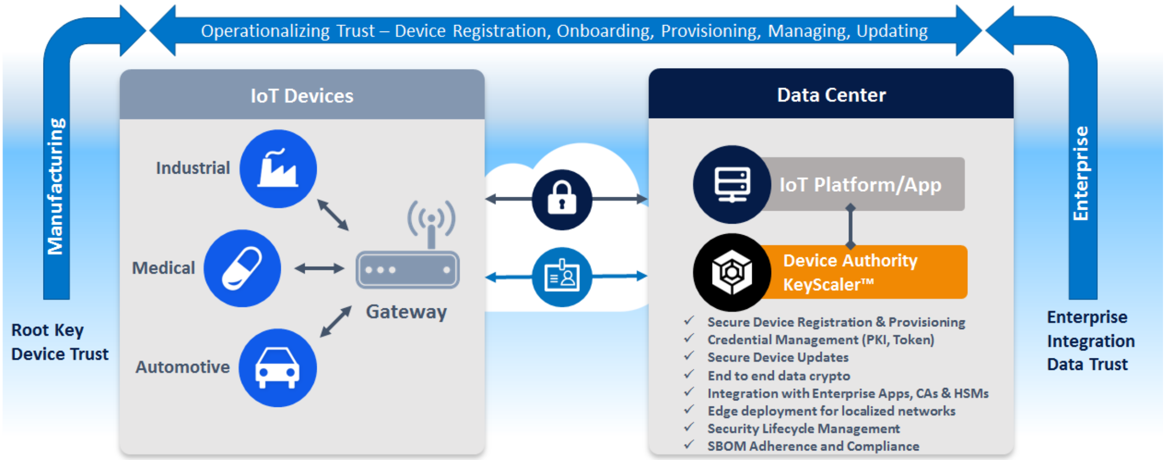
- **Hardware Security Module (HSM) Support** - KeyScaler supports nCipher Security and Thales/Gemalto Hardware Security Modules (HSM) as a Root of Trust (ROT) to provide secure storage for KeyScaler system keys, secure execution and private PKI root CA key.

- **HSM Access Controller** - Ability to manage a connected HSM using KeyScaler API's for the purpose of key generation, data signing, data crypto, and general public key storage. Secure Data Repositories provide centralized encrypted data stores used to securely store data that can be transmitted to authorized entities.

- **PKI Signature+** - Designed for low-power devices, where Dynamic Device Key Generation (DDKG) is not suitable. Utilizing asymmetric key signatures with automated authentication key rotation policies to deliver strong device identity.

- **Automated Password Management** - Automatically set and manage passwords on devices and rotate as per policy, with the ability to restrict access to privileged individuals only.

- **Development Tools** - Client-side SDK and development libraries provide an easy integration method into new and existing applications. Server-side REST APIs make it simple to consume KeyScaler services.


Operationalizing Trust – Device Registration, Onboarding, Provisioning, Managing, Updating
Manufacturing
Root Key
Device Trust
IoT Devices
Industrial
Medical
Automotive
Gateway
Data Center
IoT Platform/App
Device Authority
KeyScaler™
✓ Secure Device Registration & Provisioning
✓ Credential Management (PKI, Token)
✓ Secure Device Updates
✓ End to end data crypto
✓ Integration with Enterprise Apps, CAs & HSMs
✓ Edge deployment for localized networks
✓ Security Lifecycle Management
✓ SBOM Adherence and Compliance
Enterprise
Enterprise
Integration
Data Trust

Delivery Models

Device Authority offers two flexible options for integrating KeyScaler platform features. Customers and partners can choose the right model for their use case requirement.

1. On Premise / Cloud: Download, install and manage KeyScaler platform in own data center, or on cloud infrastructure.

2. Managed Service - KSaaS: 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 are:

- Multi-tenant model for customer enrolment and management
- Branding support
- Integrated billing and customer support
- Quick to integrate with KeyScaler through APIs

Seamless end-to-end Security for every IoT Ecosystem

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

sales@deviceauthority.com

www.deviceauthority.com

DEVICE AUTHORITY™
Edge to Enterprise IoT Security