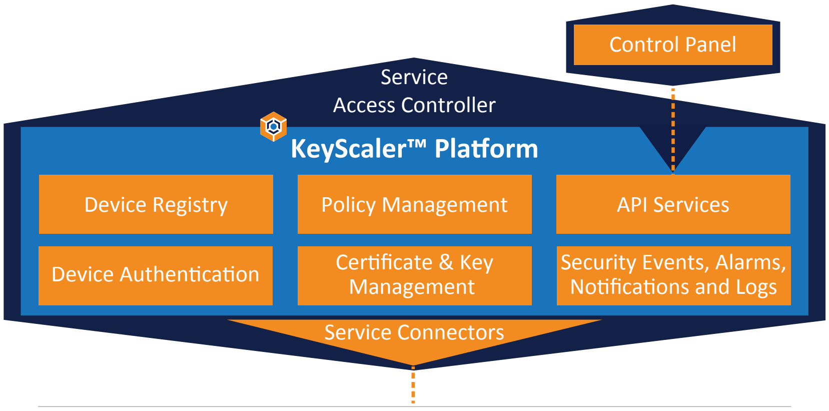
DEVICE AUTHORITY™
Trust for every Thing

KeyScaler™ IoT Security Platform

KeyScaler™ delivers comprehensive IoT security automation at scale. Secure device registration and provisioning, automated password management, policy-driven crypto and credential management, along with the delivery of Public Key Infrastructure (PKI) certificates to devices without human intervention.

- **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 DPS, Azure IoT Hub, Microsoft Active Directory, Azure Event Hub data privacy and Windows credential manager.
- **Registration Controls -** Automated device registration and authorization policies for headless onboarding of IoT devices.
- **Device Group Management** – The ability to assign devices to groups and assign crypto and certificate provisioning policies at a group-level.
- **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.
- **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.
- **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.
- **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.
- **Delegated Security Management (DSM) -** Providing high assurance device authentication for IoT platforms, network and power efficiency, and simplified integration with KeyScaler.
- **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.
- **Docker Support -** Support for deploying KeyScaler services inside Docker Containers.
- **Enhanced Platform Integration Connector -** Flexible interface to integrate with ANY external platforms and services. Provides real-time notification of events that occur in KeyScaler.
- **IdenTrust CA Connector -** Automated certificate provisioning and management for IoT devices with IdenTrust (part of HID Global) as Trusted CA.
- **Security Suite for PTC ThingWorx -** Simplified integration between ThingWorx and KeyScaler offering data security, device authentication, management interface and device authorization
- **Automated Certificate Management** – Automated certificate provisioning and management for IoT devices.
- **Azure IoT Hub connector -** A service connector that provides Shared Access Signature (SAS) tokens. KeyScaler authenticates to devices and delivers SAS tokens. Devices use SAS tokens to authenticate to Azure IoT Hub.
- **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.
- **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 AWS IoT service.
- **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.



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 enrollment 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 Blockchain. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/encryption.

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

DEVICE AUTHORITY™
Trust for every Thing

sales@deviceauthority.com

www.deviceauthority.com