DEVICE AUTHORITY

KeyScaler™ Edge

What is KeyScaler Edge?

Many IoT use cases are demanding the use of localized Edge deployment models and require Edge security solutions to support this, where today there is no complete solution. Edge deployments typically operate by having an Edge Gateway with leaf devices connecting to these gateways, all functioning in a private local network.

Security automation is still paramount here for security lifecycle management, device bound identity, leaf device authentication/authorization, zero touch onboarding to ensure customers meet regulation, compliance, data theft/privacy concern, prevent harm and enable business to protect revenue. KeyScaler Edge is a lightweight version of KeyScaler that is created specifically for Edge nodes, with the ability to register, authenticate, and provision certificates and tokens to devices in the local network, independent of an available internet connection.

Challenges organizations are facing with IoT Edge gateway deployments, which KeyScaler Edge can solve

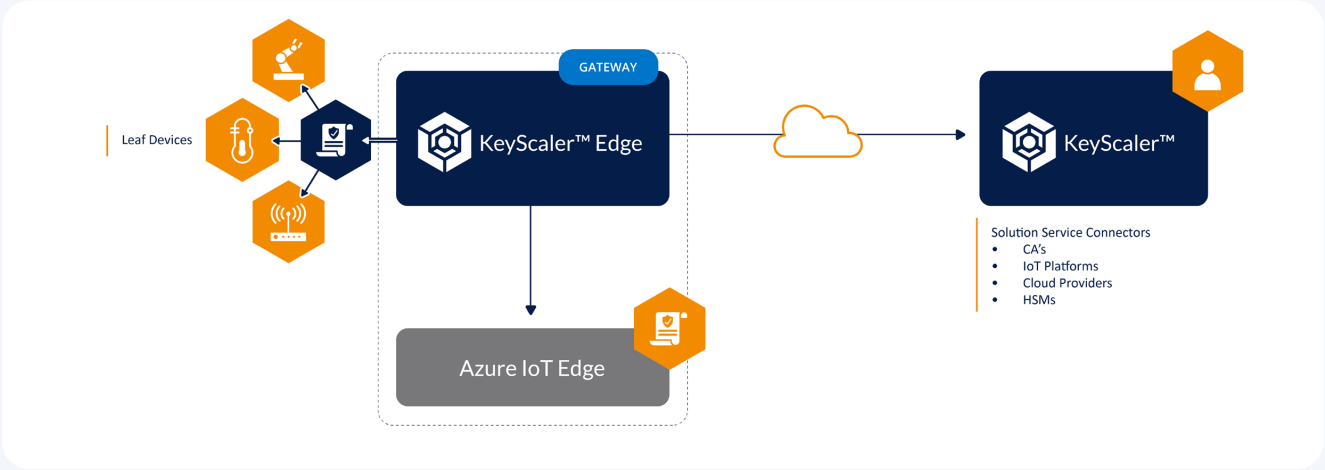
- **Typical IoT applications rely on single-key usage with the possible of device clones**
- **No device-bound certificate capabilities**
- **Lack of ongoing devices authentication key rotation and management for edge gateway and leaf devices**
- **No devices attestation prior to registration-integrity validation, hardware validation, etc.**
- **No data encryption key or encryption policy provisioning to device**
- **Manual generation and configuration of Edge Gateway Device and Root Certificates**

Human error could expose sensitive information like private keys!

KeyScaler Edge for ONLINE environments

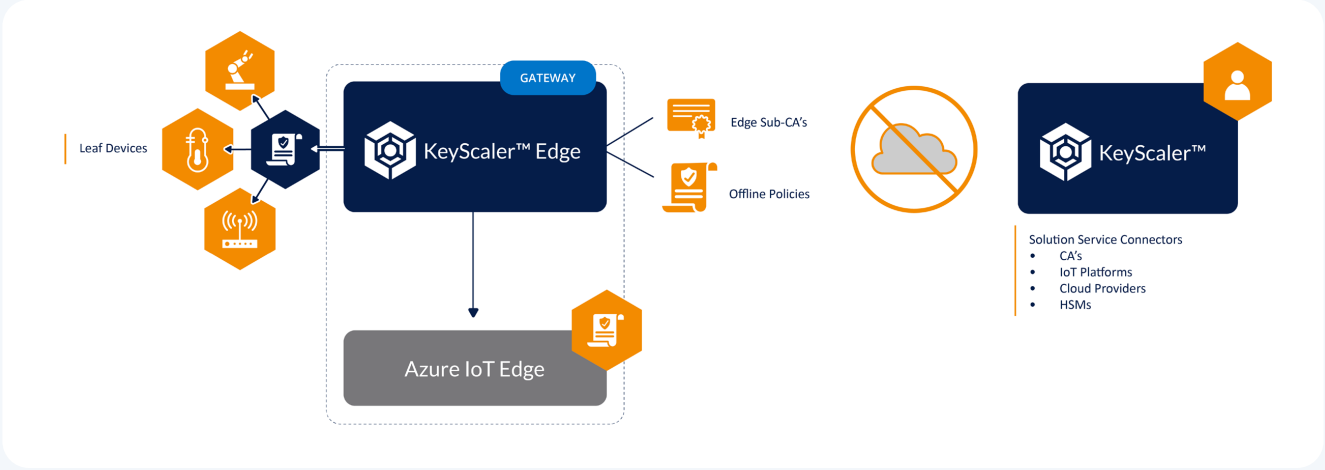
Device Authorityand Titan Automotive Solutions have worked together to solve some of these fundamental challenges in Automotive. KeyScaler has been enabled on Titan automotive cellular modules to “enable out of the box” Vehicle to Cloud trust, identity management and data privacy solutions solving several fundamental security challenges, specifically:

- KeyScaler Edge acts as a localized service – for devices that do not have direct internet connection.
- Can leverage central KeyScaler CA (Cert Authority) and IoT Platform service connectors.
- Stores operational policies from central KeyScaler in event of loss of internet connection.



KeyScaler Edge for ONLINE environments

- KeyScaler Edge is disconnected from the central KeyScaler service.
- Synchronised operational policies determine offline behaviour incl. registration, auth, cert. provisioning
- Edge node can continue to operate as if it is a central KeyScaler, for the localized environment.



KeyScaler Edge Use Cases

Edge compute with Edge security management is a big market trend for organizations, where their use case requires localized IoT/OT environments which don't necessarily have persistent internet connections. Although, the Edge compute model has some fundamental differences to a more traditional "connected" model, organizations still require the same level of security, to meet the security posture needed for their use cases, compliance, operational management, and legislation requirements.

Customers recognise that utilizing KeyScaler Edge in their deployments they can realize:

Significant ROI for security management - Saving money through security automation

Being able to provide security operations and management for "online" and "offline" environments – And flexibility to mix the two if required

One comprehensive security solution to meet a wide range of use cases – Secure onboarding, PKI (Provisioning, Renewal, Revocation), To

Remove the need for a costly HW redesign on leaf devices - Retrofit KeyScaler Edge security management to existing IoT infrastructure

Help businesses meet compliance and regulatory adherence, in their private local network deployments

Help businesses meet Safety, confidentiality, Data theft/privacy, Brand Reputation protection, Revenue protection requirements

Future proof designs to help meet evolving regulatory and legislative requirements

KeyScaler Edge has been designed with a Simplicity by Design concept to meet a wide range of security use cases. However, when you look at example use cases across these verticals, they all share the same fundamental security challenges. This is amplified by the number of verticals we operate in such as Medical / Healthcare, Industrial, Transport (Automotive & Marine) and Retail. Whether that's localized Edge compute in hospitals, connecting machines in factories, enabling security on tugboats for marine applications or being able to have localized security for refrigerators, HVACs, and similarly in a retail setting. All these verticals can gain significant business and technical value no matter what your use case is.

KeyScaler Edge Features

Edge compute with Edge security management is a big market trend for organizations, where their use case requires localized IoT/OT environments which don't necessarily have persistent internet connections. Although, the Edge compute model has some fundamental differences to a more traditional "connected" model, organizations still require the same level of security, to meet the security posture needed for their use cases, compliance, operational management, and legislation requirements.

- Suitable for deployment to a single Edge Gateway - Designed to be lightweight.
- Central visibility and control of Azure IoT Edge and Leaf device certificates
- Upcoming EST server support for seamless IoT Edge enrolment
- Manage all certificates centrally, including revocation, and connecting to ANY Certificate Authority

- Edge instances can function in local networks – "Offline" when it is disconnected from central KeyScaler service
- Devices can register/auth to KeyScaler Edge, or KeyScaler Central – Providing flexibility in deployment models
- Devices can be ported from KeyScaler Edge to KeyScaler Central service

- Secure provisioning of IoT Edge workload signing certificate (Identity Cert, Device Cert and Root CA)
- KeyScaler Edge provides policy-driven services to devices:
- Secure device registration and authentication
- Built in Internal Private PKI for Cert. Signing
- Certificate Provisioning & Management (x.509)
- Auth. SAS Token Provisioning & Management

- Standard based mTLS leaf-device enrolment (upcoming support for EST)
  Device clone detection
- Comprehensive policy engine for operational, solutions & Device Enrolment / Authentication
- How often KeyScaler Edge should pull policies from KeyScaler Central, how often KeyScaler Edge should synchronise etc
- Policies allowing registration online and offline, auto quarantining, which CAs to use, Cert validity and Token provisioning

- Edge instance updates & syncs with central KeyScaler to pull new policies, sync devices, upload logs, etc.
- Flexible CA support model to support any private or public CAs, using Internal or External Roots -
  As defined through policy (on-prem or cloud)
- Support for greenfield and brownfield device deployments
- Trusted Platform Module (TPM) support
- Strong ROT generation using the device unique hardware and software attributes – devices do not require a Bootstrap Cert!

KeyScaler Edge Benefits

- Enables customers to deploy Edge IoT infrastructure while still maintaining a high level of security and autonomy in offline private networks - when cloud connectivity is not available
- Significant ROI ($$$ / % TBC) for deployments
- Secure Lifecycle Management
  - Zero touch onboarding & registration
  - Device authentication/authorization to Edge Gateways
  - Automated credential management – Provision, Revoke, Renew for Edge and Leaf devices
- Increases operational efficiencies by using existing enterprise PKI & can support Any
  - KeyScaler ADCS, Public CA connectors, Key Vault and Private CA, Internal/External Roots
- Increases operational efficiencies by using existing enterprise PKI & can support Any
  - KeyScaler ADCS, Public CA connectors, Key Vault and Private CA, Internal/External Roots
- Seamless IoT Gateway deployment process with Azure IoT Hub
  - Service available via IoT Hub, IoT Edge & Module management
  - Strong RoT with a device centric & device bound identity model using DDKG, Mutual TLS, and PKI Signature+
- Retrofit option to legacy leaf devices utilizing DDKG
- Enables businesses to meet compliance and regulatory requirements inside private local networks

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.

With offices in San Ramon, California, and Reading, UK, Device Authority partners with the leading IoT ecosystem providers, including AWS, DigiCert, Entrust, HID Global, Microsoft, 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
Trust for every Thing