DEVICE AUTHORITY

# Use Case: Smart Connected Hospitals

## Situation

A global medical technology company operating across multiple hospital networks needed a secure, automated method to manage device identity and X.509 certificate lifecycles across a range of connected medical devices and edge gateways. These environments included both Linux- and Windows-based systems, many of which operate in offline or intermittently connected modes, such as in surgical suites, imaging labs, and intensive care units.

To meet internal compliance standards and healthcare data protection regulations, the customer required a zero-touch solution that would ensure device trust and secure communication even in offline states. They also needed the ability to sign files and configurations securely, integrate with AWS cloud services, and utilize hardware-based trust (TPM) across a diverse ecosystem of medical technologies.

## Solution

Device Authority KeyScaler was used to deliver:

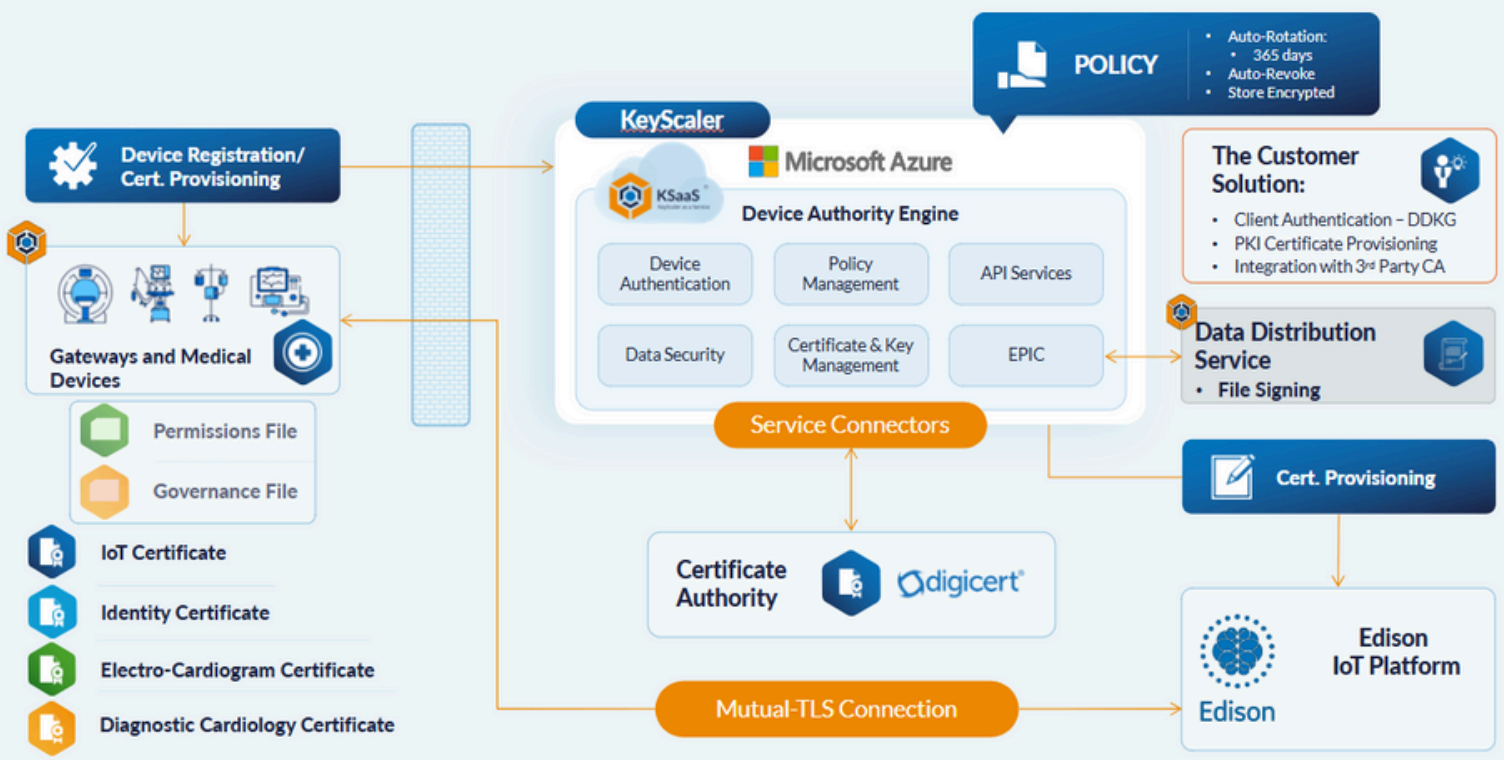
- Dynamic Device Key Generation (DDKG) for establishing root of trust at the device level.
- PKI Services for IoT, using X.509 certificates integrated with enterprise identity and access systems.
- Automated Device Provisioning and zero-touch registration to AWS cloud services.
- Automated Identity Lifecycle Management for both edge gateways and leaf devices.
- Secure file signing capabilities to verify the integrity of critical configuration and update files.
- Support for Trusted Platform Module (TPM) hardware to further harden device identity and protection.

DEVICE AUTHORITY
www.deviceauthority.com
contact@deviceauthority.com

**UK Head Office**
**Level 2, Thames Tower**
**Station Road,**
**Reading,**
**RG1 1LX**

**North America Office**
**12677 Alcosta Blvd**
**Suite 250**
**San Ramon, CA 94583**
**USA**

# IoMT: Smart Connected Hospitals




## Conclusion

The deployment of KeyScaler enabled the customer to automate security operations across a complex and highly regulated hospital environment. By managing certificates and device identity through a zero-touch workflow, they reduced manual intervention and minimized security risks — even for offline devices that play a role in life-critical patient care. Integration with AWS and TPM hardware strengthened their Zero Trust posture while ensuring that only trusted devices and software operated within the hospital network. As a result, the company improved its compliance readiness, enhanced patient safety, and freed up internal resources to focus on delivering innovative healthcare solutions.

DEVICE AUTHORITY
www.deviceauthority.com
contact@deviceauthority.com

**UK Head Office**
**Level 2, Thames Tower**
**Station Road,**
**Reading,**
**RG1 1LX**

**North America Office**
**12677 Alcosta Blvd**
**Suite 250**
**San Ramon, CA 94583**
**USA**