DEVICE AUTHORITY™
Trust for every Thing

MEDIGATE

Device Visibility, Protection and end-to-end Security Management

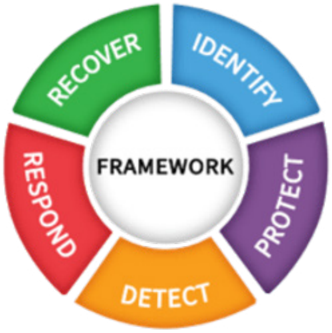
Medigate + Device Authority KeyScaler® = Visibility & Scalable Trusted IoT Solutions Delivered

The Need for Device Visibility, Trust and Automation

The Internet of Medical Things (IoMT) has been disrupting the healthcare industry for a number of years now, not only around patient care/safety but also with regard to cost savings and operational efficiency. Since the COVID pandemic, there has been an almost exponential explosion of telemedicine by healthcare systems. This change happened almost overnight as the virus quickly spread. As a result of quarantines and states closing, health systems stopped seeing many patients in person.

IoMT devices and their ability to connect to Healthcare IT systems have huge benefits but also have increased the number of cyber risks within the healthcare sector, such as telehealth device flaws, insider threats, and the rise of targeted cyberattacks.

In 2014, the National Institute of Standards and Technology (NIST) published a framework which helps organizations mitigate these cyber security risks. The framework describes a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. At the center of this framework are five concurrent and continuous functions; **Identify, Protect, Detect, Respond and Recover.** When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.



When you consider IoMT in these segments, in fact in any IoT segment, you have to consider automation because of the sheer scale of IoT. Operational Technology (OT) requires end to end security operations to be autonomous. That includes device network visibility, detecting devices on the network, automating device integration to IoT applications, security lifecycle management, monitoring devices for anomalies, end to end data trust, secure update management, and credential management to name just a few. Coupling technological requirements with the ever-evolving legislation and compliance rules requires device visibility, trust and automation.

Better together, Medigate & KeyScaler

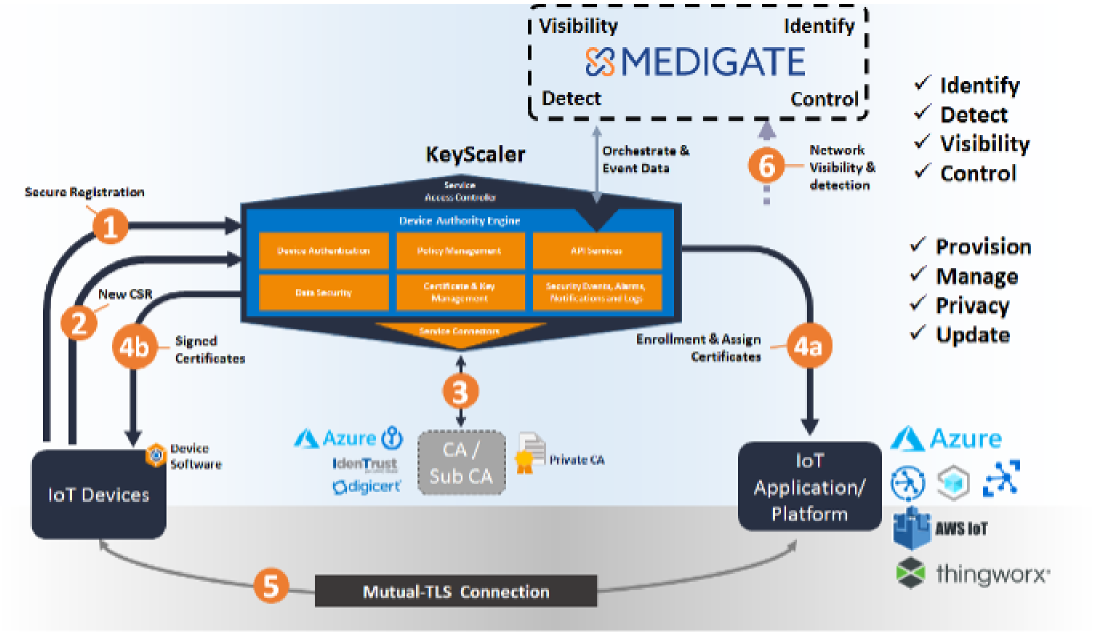
Medigate addresses the **Identify & Detect** functions and gives clear visibility to network administrators, healthcare providers & enterprises on what devices are connecting to their networks, allowing for risk management and mitigating device anomalies and behavior. Integrating KeyScaler with Medigate provides additional Protect function capabilities to address device trust, data trust and automation, along with enhanced device visibility. Benefits include:

- **Gain detailed visibility -** Discover and precisely identify 100% of connected devices on a provider's clinical network.
- **Enhanced device visibility –** Device memory usage, security events, device CPU/process utilization, network connections from devices, user connected, battery info etc.
- **Detect threats in real time -** Accurately detect credible threats.
- **Prevent attacks from succeeding -** Integrates with existing NAC and firewall solutions
- **Security model for patient safety -** Real-time device authenticity validation
- **Unified trust model -** Device and Data trust combined for compliance (HIPAA and GDPR)
- **End to end data protection -** to prevent insider threats
- **Automation for any IoT application -** Available for Azure IoT, PTC ThingWorx, AWS and others
- **Enterprise security integration -** HSM & Public Certificate Authority integration
- **Retrofit capabilities –** Apply Protect functionality to high-risk devices*

*Assumes an update process is in place

User Case Process

A healthcare solution provider deployed a process to identify devices on a network and manage IoMT device authentication into their chosen cloud infrastructure, in this case Microsoft Azure. The diagram and steps below detail their solution:



Through the steps outlined in the diagram each device would:

Step 1:	Authenticate, register and onboard to KeyScaler®
Step 2:	Create key pair and create a Certificate Signing Request (CSR)
Step 3:	Reach out to 3rd party CA or Private CA using prebuilt connectors to sign certificate
Step 4a:	Create enrollment record in chosen IoT Application, such as IoT Hub and assign x.509 certificate to the record.
Step 4b:	Provision signed x.509 Certificate to device
Step 5:	Device and IoT Application now have the credentials to trust each other and can establish a mutual TLS Connection.
Step 6:	Device is passively discovered by Medigate based on its network communication and monitored for data consumption behavior
Step 7:	Additional device data like the device's free memory, CPU load or open sockets, is gathered by Medigate from KeyScaler® to enhance device visibility and its risk assessment.

It is also important to note that Step 6 could be the initial step toward onboarding a device to KeyScaler®. The Medigate platform is used to discover the devices on the hospital's network, assess their risk and act based on this information. For example, for each device in a high-risk category KeyScaler® could be "retrofitted" and be used to provide security lifecycle functionality such as Credential management or Crypto Key management to adjust the device's access in the organization.

About Medigate

Medigate is the industry's first and leading dedicated medical device security and asset management platform, enabling providers to deliver secure, connected care. Medigate fuses the knowledge and understanding of medical workflow and device identity and protocols with the reality of today's cybersecurity threats. With Medigate, hospital networks can safely operate all medical devices on their network, enabling deployment of existing and new devices to patients while ensuring privacy and safety.

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.

sales@deviceauthority.com

www.deviceauthority.com

DEVICE AUTHORITY™
Trust for every Thing