Healthcare IoT Case Study:

Portable Oxygen Concentrator

Overview

The GCE Group has designed and manufactured a portable oxygen concentrator Zen-O, which allows patients with respiratory disorders to manage their oxygen treatment better remotely. InVMA has worked closely with GCE to build a custom IoT application using PTC's ThingWorx platform, to allow patients, doctors and service providers to carefully monitor data, whenever and wherever they are, dependent on the patient's needs.

The device can monitor the patients' blood oxygen levels and automatically adjust the amount of oxygen delivered (as set by a clinician). To ensure patient safety, it is critical that devices cannot be spoofed and that the two-way communication is secure and the data protected.

The Problem

Maintaining the privacy of patient records and data is paramount to healthcare. If a healthcare facility or device collects patient data and exchanges this data over the internet, then data privacy and security is a real problem. Strong IoT security is critical to prevent hacking and data breaches.

The first challenge here is to have strong mutual trust and authentication between the Zen-O device and ThingWorx servers/applications. The second challenge is sensitive information flows all the way from the device to the ThingWorx platform and ultimately the end user application. This causes huge uncertainty in data being transferred to a trusted destination, thus raising concerns on Data Privacy and Data Security.

DEVICE AUTHORITY
Trust for every Thing

Our Solution

Device Authority's KeyScaler™ platform provides a strong root of trust, securing the medical devices' identity and offers an automated approach for registering and authenticating devices to KeyScaler at IoT scale. Data is encrypted from the medical device, in transit and persists encrypted at rest in the ThingWorx IoT platform, all defined and controlled by policy and the customer. All medical data is transferred, agnostic to any network architecture or communications used, maintaining the privacy of medical data as follows:

1. The Zen-O connects to KeyScaler for registration and PKI key provisioning (Assigned Device ID and Authentication Key, Crypto Key ID and Key).
2. The Zen-O encrypts data using the Crypto keys and sends the encrypted data to the ThingWorx platform.
3. ThingWorx authenticates to KeyScaler to request the decryption key and decrypts the patient data residing at rest in the ThingWorx platform.

What Makes This Unique

- Crypto Keys are generated as per policy, and are never shared over the network.
- Device authentication and data encryption policies are managed continously from the server side security engine.
- Data is encrypted end to end from the source, in transit and persisted at rest, agnostic to any network architecture.

Conclusion

The Gateway Agent and KeyScaler platform from Device Authority addresses all the security concerns that any industry vertical would have by providing the most appropriate Identity and Access Management for Internet of Things (IoT) devices. Device Authority remains the most secure Trust and Privacy platform for Internet of Things (IoT) devices.