Industrial IoT Case Study:

Aachen Secure Smart Factory Demonstrator

Overview

The European 4 Transformation Center (E4TC) is located in Aachen University Industry Campus and is also known as the Aachen Demonstration Factory. It provides visitors an experience to Digital, Physical Business Transformation and Industry Practices around Product Lifecycle Management (PLM), Service Lifecycle Management (SLM), ERP Application Integration, Systems Engineering and Industrial Internet of Things (IIoT).

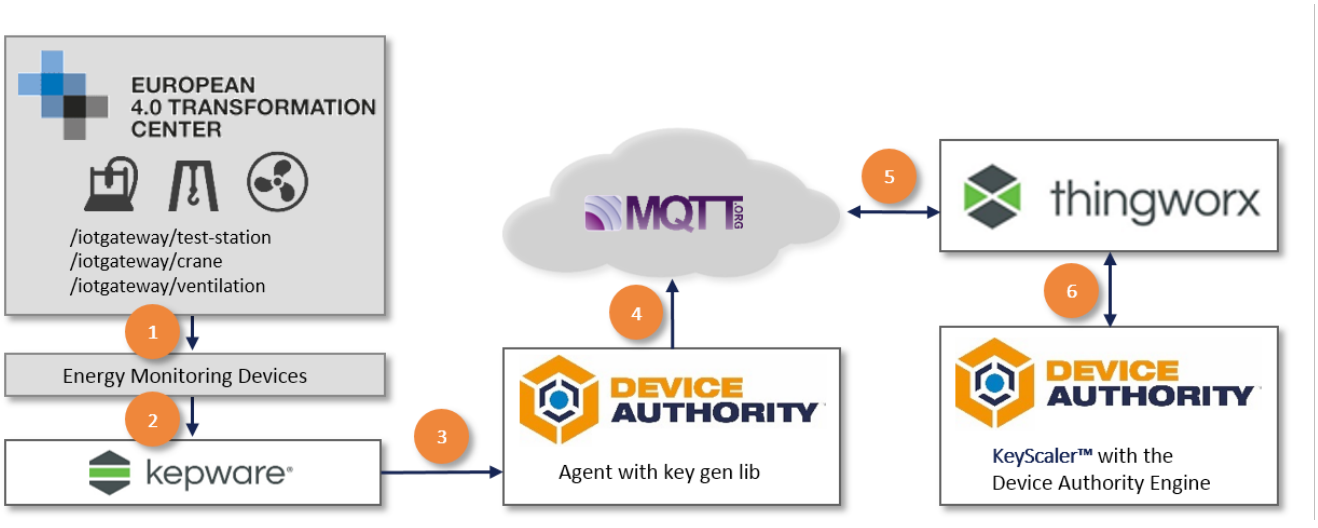
At the Aachen Demonstration Factory, PTC's Energy Monitoring IoT Devices from different machinery on the shop floor transfer data (Details of Power, Voltage & Current) to the analytics platform over Internet.

The Problem

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

Our Solution

Device Authority's KeyScaler™ platform uses unique patented Dynamic Device Key Generation (DDKG) technology to address these problems. It provides policy-driven registration controls to enable secure, automated onboarding and provisioning of devices at IoT scale. KeyScaler™ securely authenticates the devices, transfers data to the target applications maintaining privacy as follows:



DEVICE AUTHORITY
The IoT Security Automation Company

1. Energy monitoring devices collect parametric data such as power, voltage and current. The collected information is shared to Kepware platform.
2. The Kepware platform (KEPS-EX) translates data into JSON format and publishes the same to the Device Authority Gateway Agent.
3. The Device Authority Gateway Agent authenticates to KeyScaler™. During the authentication handshake process, the KeyScaler server shares Crypto-Policy with the Gateway Agent on the client. The Device Authority platform makes sure that only authenticated devices get connected.
4. The Gateway Agent encrypts data and publishes encrypted data to Message Queuing Telemetry Transport (MQTT) Broker. Even though the data remains with MQTT broker, it is encrypted and securely protected.
5. ThingWorx subscribes MQTT Broker for encrypted data. It also gets authenticated by KeyScaler™.
6. KeyScaler™ generates and transports a decryption key securely to ThingWorx platform, which then applied on the encrypted data.

What Makes This Unique

- Device Authentication Keys are dynamically generated and unique to each device for each authentication session, eliminating problems with spoofed credentials
- Device-derived Crypto Keys are generated from the dynamic device authentication process, which eliminates the need to share or store symmetric keys on devices
- Dynamic Device Keys are not stored on devices or servers and are never passed over the network, which eliminates theft, copying credentials and secrets
- Control device authentication and data encryption policies from 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.

Device Authority fulfills industry practice O9 of Closed Loop Lifecycle Management - End to End Security for connected services.