Industrial IoT Case Study:

AMRC Secure Smart Factory Demonstrator

Overview

The AMRC Factory 2050 is the UK's first fully reconfigurable assembly and component manufacturing facility for collaborative research. AMRC provides an environment in which real physical manufacturing and machines can be used to demonstrate operations and service models based on new technologies and methods. PTC leverages AMRC to build demonstrators to showcase industrial IoT applications, with a view to shorten sales cycles. Through partnership between Device Authority and PTC, a continuous collaborative effort is being made to integrate Device Authority's KeyScaler platform into new and existing demonstrators.

The primary use case is to encrypt data sourced from a MAZAK Milling Machine Center located at the AMRC facility, in motion and at rest, to eliminate the risk of industrial espionage attacks for commercial and economic purposes. Authentication also plays an important role in this use case, to ensure only authenticated and authorized devices can encrypt and decrypt data.

The Problem

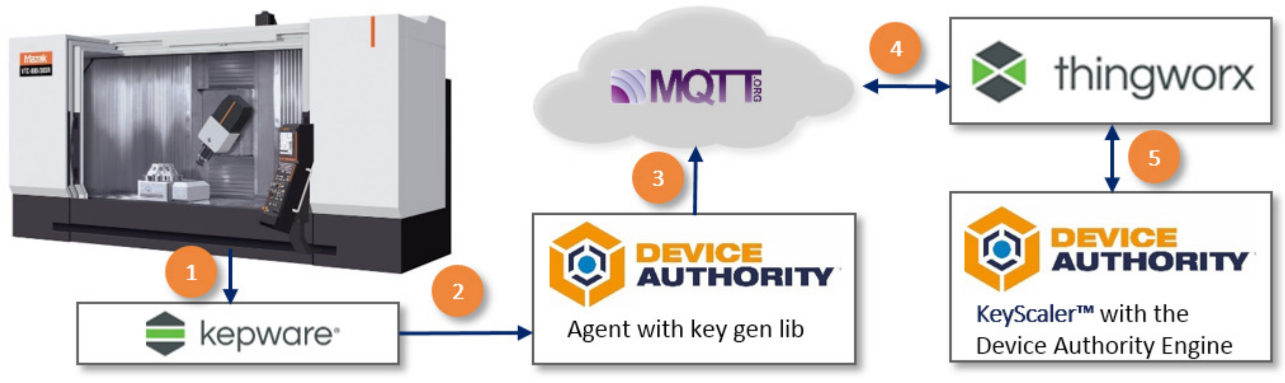
Sensitive data from the industrial Mazak milling machine in the AMRC Smart Factory needs to be protected. The MAZAK milling machine resides within the AMRC facility and will generate data, such as rotary speed, degrees, hydraulic pressure, linear axis values etc. This data will be transported from the MAZAK Machine to the ThingWorx platform, where it will be processed, monitored, and analyzed to enable operational efficiency.

Sensitive information flows all the way from the source to the destination. Protecting the data at rest, in motion and in use is a huge challenge. 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 a strong root of trust, securing the milling machine's identity and offers an automated approach for registering and authenticating machine to KeyScaler. Data is encrypted from the machine, in transit and persists encrypted at rest, defined and controlled by customer policy.

All machine data is transmitted agnostic to any network architecture or communications used, maintaining the privacy of machine data as follows:



1. Sensor data from the MAZAK Milling Machine Center is passed to Kepware which translates machine data into JSON format
2. The Device Authority Agent authenticates to KeyScaler™, applies crypto policy to the payload and encrypts the payload.
3. The encrypted data is published to the MQTT Broker
4. ThingWorx subscribes to data via MQTT topics
5. ThingWorx authenticates to the KeyScaler™ platform to decrypt the at rest encrypted data from the ThingWorx database

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 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 devices. Device Authority remains the most secure Trust and Privacy platform for Internet of Things devices.

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