Use Case: Secure Connected Factory

Situation

A global manufacturer of precision motion control systems was experiencing unpredictable downtime across their geographically distributed factory locations, disrupting production and affecting their end customers' supply chain.

As part of their Digital Transformation strategy, they wanted to improve Overall Equipment Effectiveness (OEE) by digitizing the plant floor and installing smart sensors to automate monitoring of production systems, allowing them to proactively spot errors and pre-determine when equipment needs maintenance.

These sensors and production systems need to be protected from outside threats, as any disruption to the manufacturing process costs up to hundreds of thousands of dollars per day, and if exploited, valuable proprietary data can be lost or compromised.

Solution

The customer deployed Device Authority KeyScaler utilizing the following capabilities:

- Dynamic Device Key Generation (DDKG) technology to establish device root-of-trust and enable automated crypto key generation at each authentication session.
- Zero Touch device provisioning and registration with Microsoft Azure IoT Hub.
- Automated Device Identity Lifecycle Management for all production assets and monitoring devices on the factory floor, using x.509 Certificates from their existing PKI platform.
- KeyScaler Edge, allowing for management of offline devices connecting via secure Edge gateways.

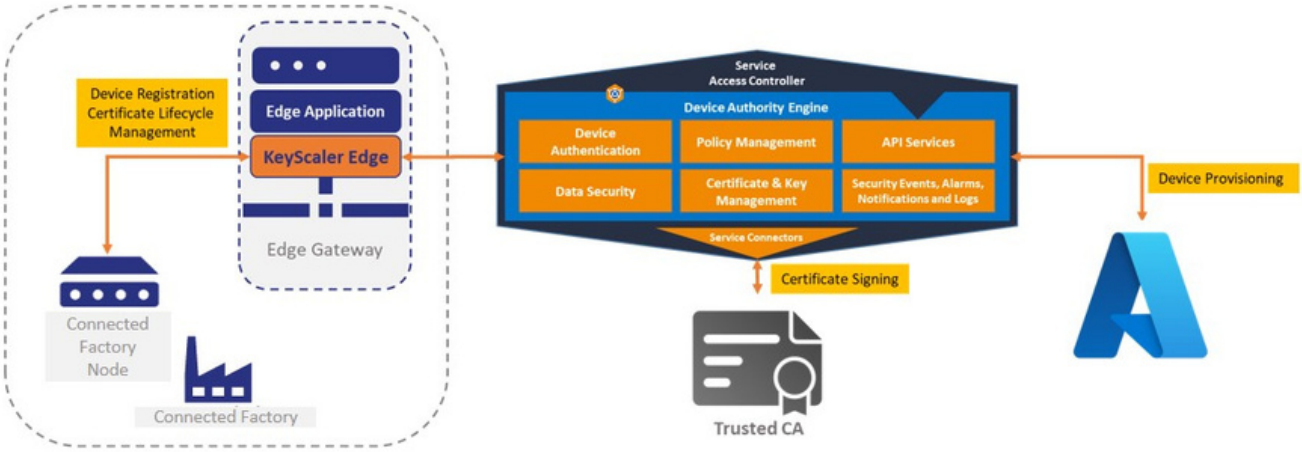
www.deviceauthority.com
contact@deviceauthority.com

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

Industrial IoT: Secure Connected Factory

Customer Requirements:
- Client Authentication - DDKG
- Offline Capability – KeyScaler Edge
- Automated Certificate Provisioning/Rotation
- IoT Hub Provisioning



Conclusion

The implementation of KeyScaler with patented Dynamic Device Key Generation (DDKG) trust anchor technology establishes a unique device-specific identity making each device extremely difficult to exploit. As a result, device-based data is inherently trustworthy and reliable, and production operations are less likely to be disrupted due to the enhanced supply chain visibility and control.

Further, automation throughout the device identity lifecycle eliminates many error-prone manual processes, speeds incident response, preserves brand reputation, and reduces potential liability.

The end result: the customer's overall downtime from device quarantines is minimized, and the increased availability of the production equipment will improve OEE by an estimated 5-8%.

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