Building, Securing and Deploying smart industrial solutions

Rob Dobson, Technology & Pre Sales Director

DEVICE AUTHORITY
Trust for every Thing

Business security challenges for Industrial IoT?

Operator injury/fatality

Sensitive data theft – IP, Process etc

OT Meeting IT challenges

Disruption for manufacturing operations

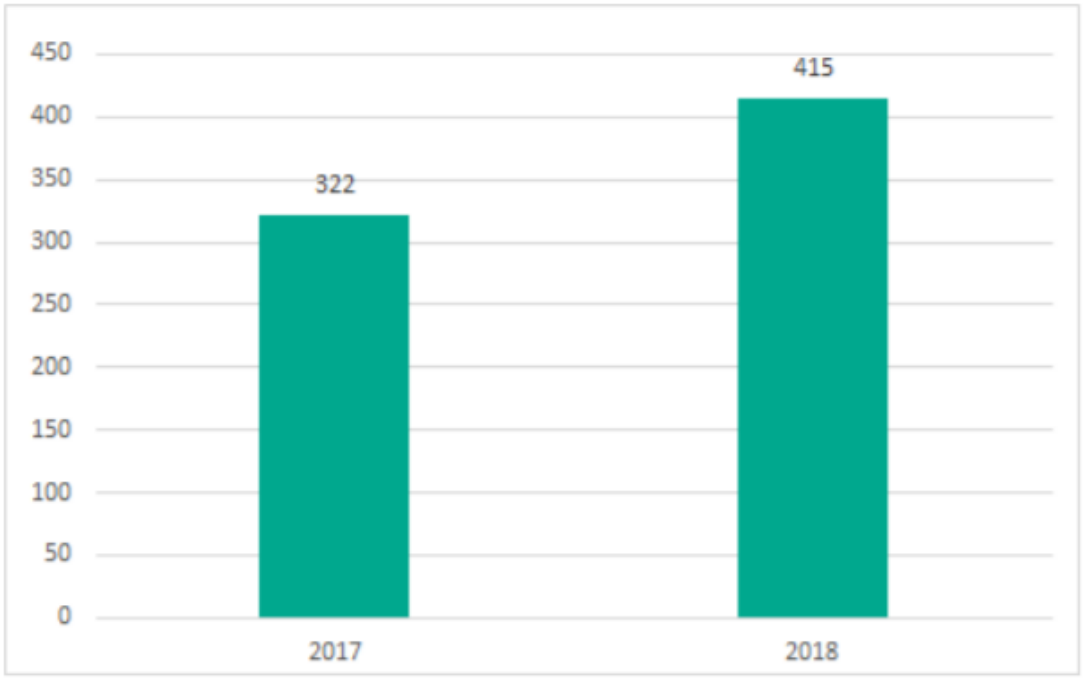
Brand damage and reputation

Compliance and Financial liability

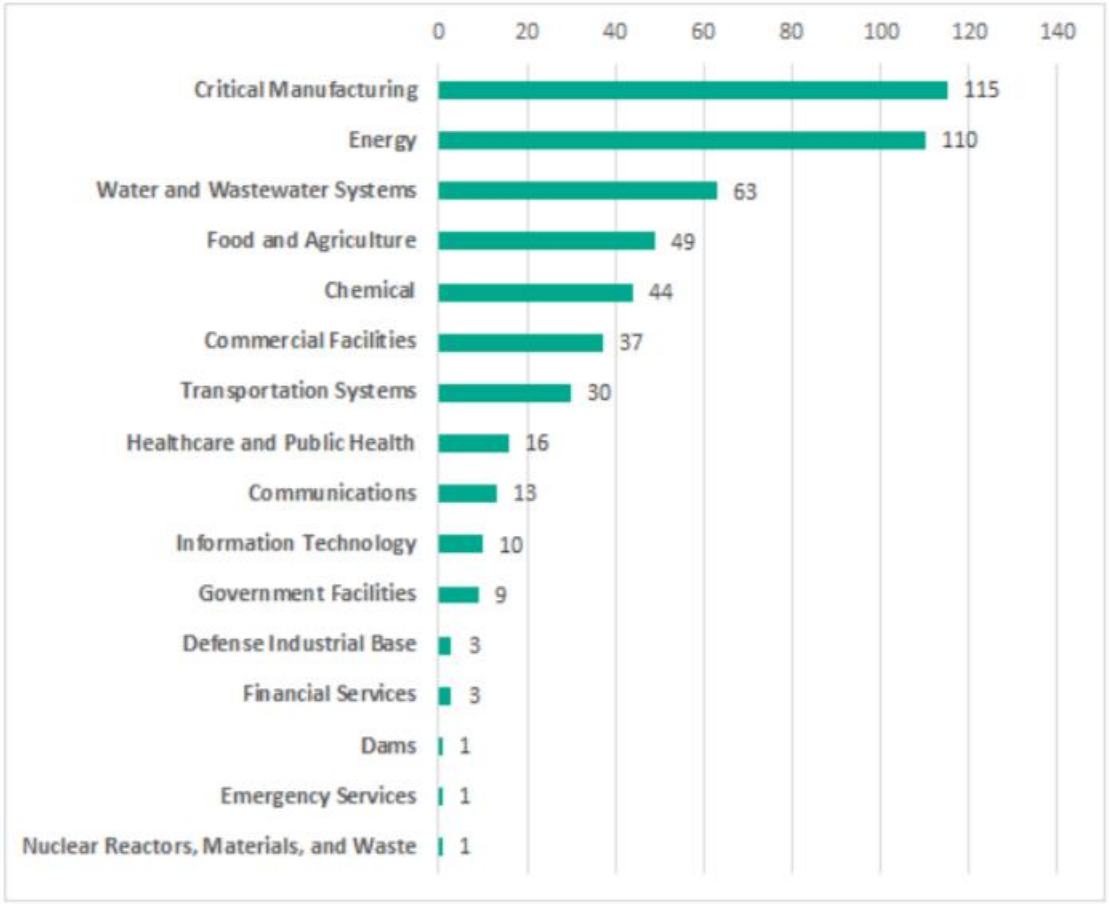
- GDPR the higher of **€20 million or 4% of annual global turnover**

DEVICE AUTHORITY
Trust for every Thing

Security trends in industrial automation



Number of vulnerabilities in different ICS components, as published on the US ICS-CERT website



Number of vulnerable products used in different industries (according to US ICS-CERT classification). Vulnerabilities published in 2018

Ref: Kapersky Lab ICS-CERT

4.4.1 Trust and Integrity Management Security measures that can help ensure the integrity and trustfulness of data and devices.

TM-01: Verify the integrity of the software before starting to run it ensuring that it comes from a reliable source (signed by the vendor) and that it is obtained in a secure manner.

TM-02: Authorise all IIoT devices within the OT network utilising appropriate methods, e.g. digital certificates/PKI.

TM-03: Define data exchange channels between IIoT devices in the form of a whitelist and choose only secure channels whenever possible.

TM-04: Implement application whitelists and review the list at least annually and in case of a change to the system. Good practices for Security of Internet of Things in the context of Smart Manufacturing November 2018 41

TM-05: Ensure production data integrity through utilisation of appropriate cryptographic mechanisms and key storage tailored to processing capabilities of the implemented solutions.

TM-06: Monitor the production data at rest and in transit to identify potential unauthorised data modification.

IoT / Things – Devices, Characteristics, Scale

IT

Human Identity
MFA for Trust
User Centric

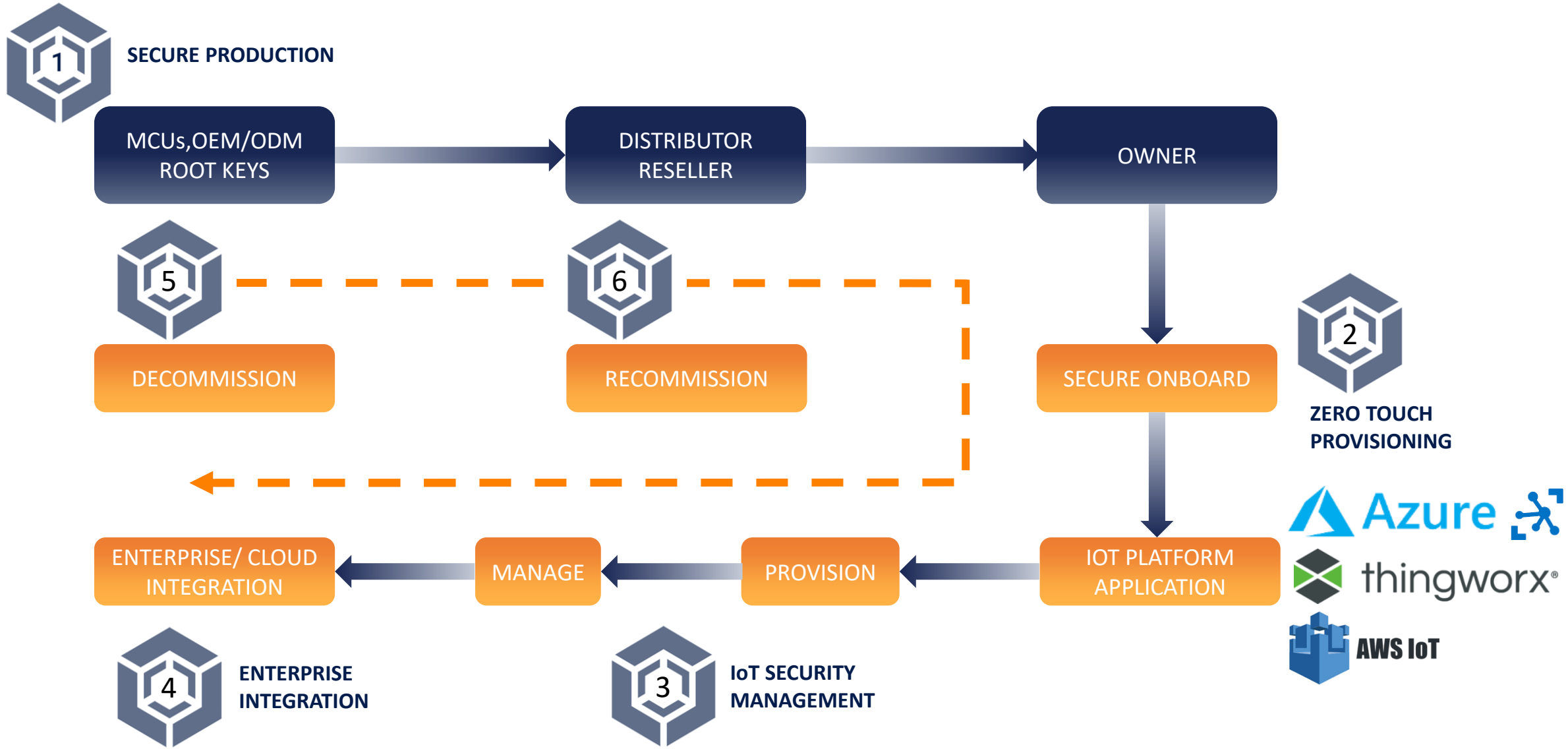
Vs

IOT

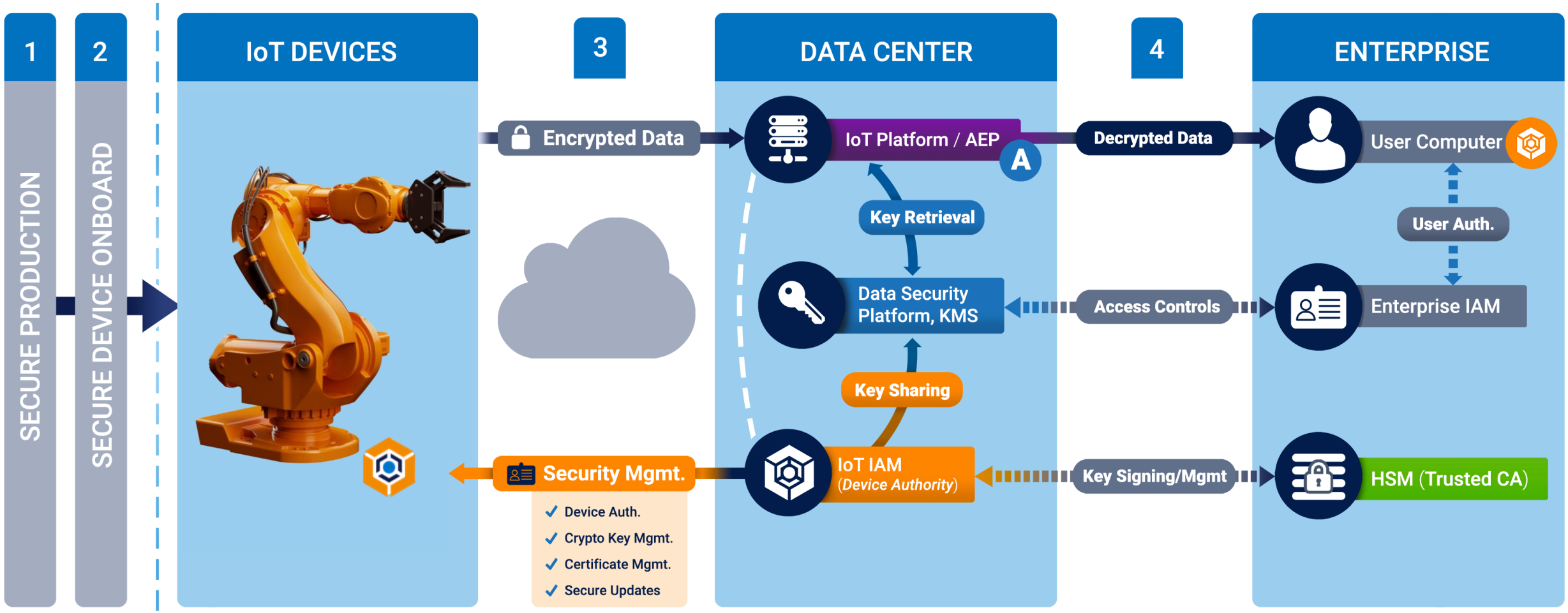
Device Identity
Trust?
Device Centric
Scale 20X

Establishing and Managing **Trust at Scale**

Trust and Automation in an IoT Device Journey



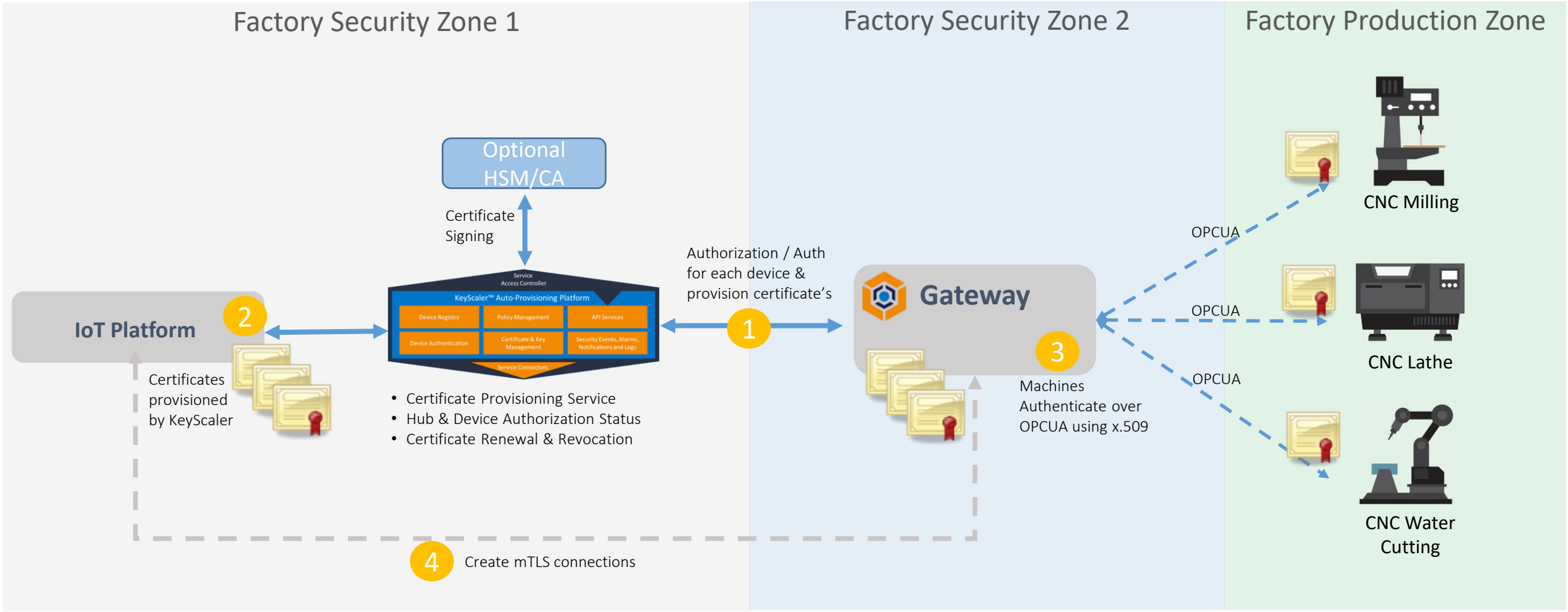
Smart Industrial, OT meets IT – Managing Security…



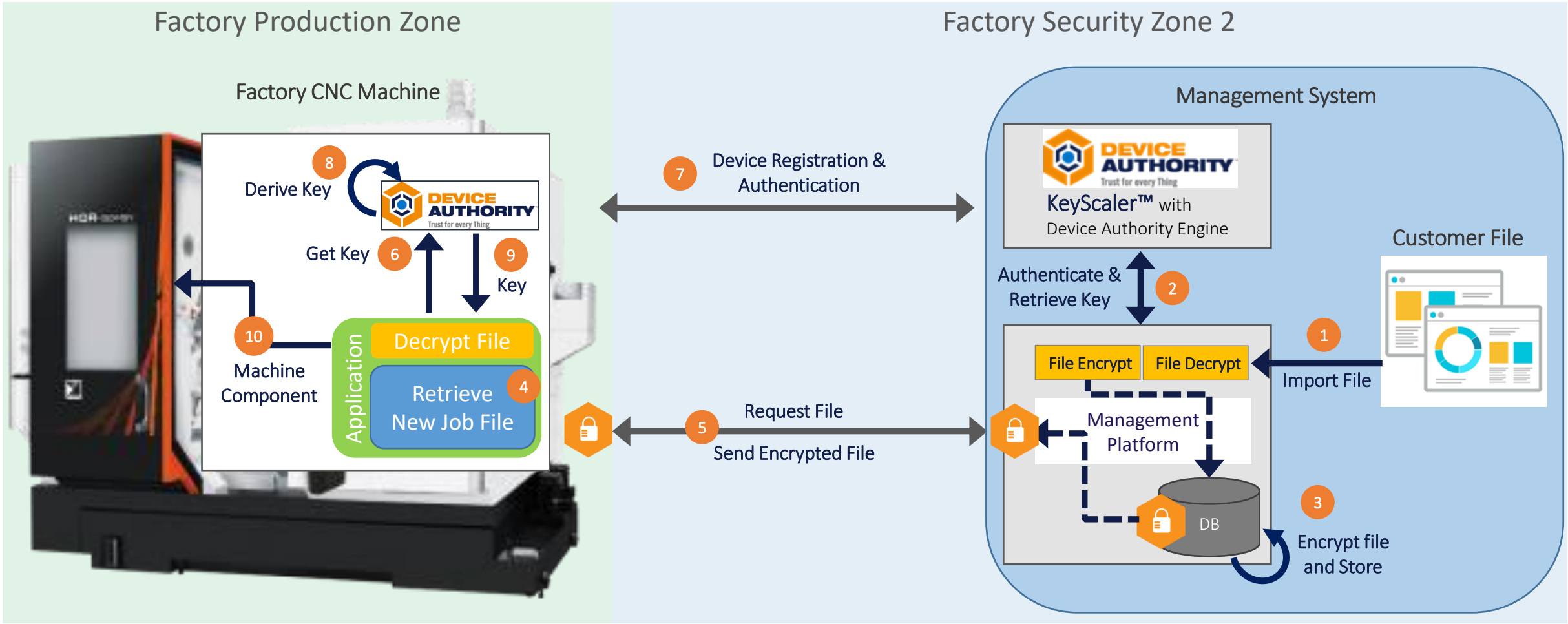
https://www.deviceauthority.com/insights/enterprise-iot-security-blueprint-20

DEVICE AUTHORITY
Trust for every Thing

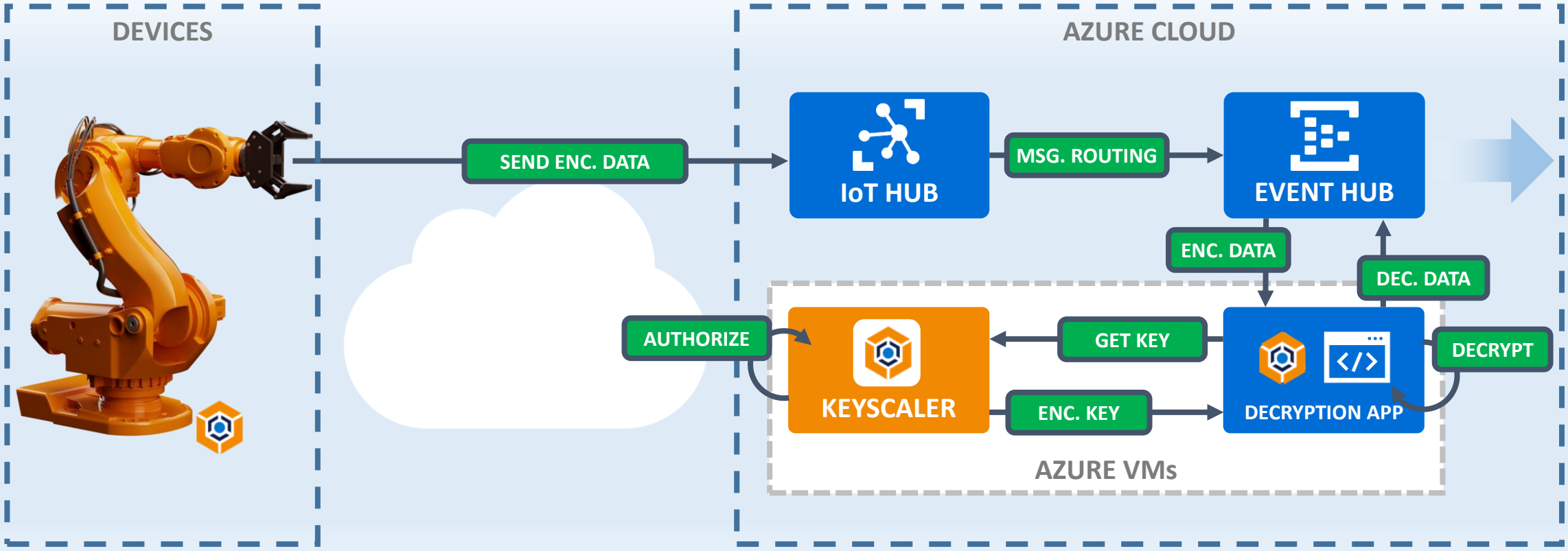
Example Use Case: Industrial, PKI Certificate Management for OPCUA



Example Use Case: Smart Machining, IP & Revenue protection

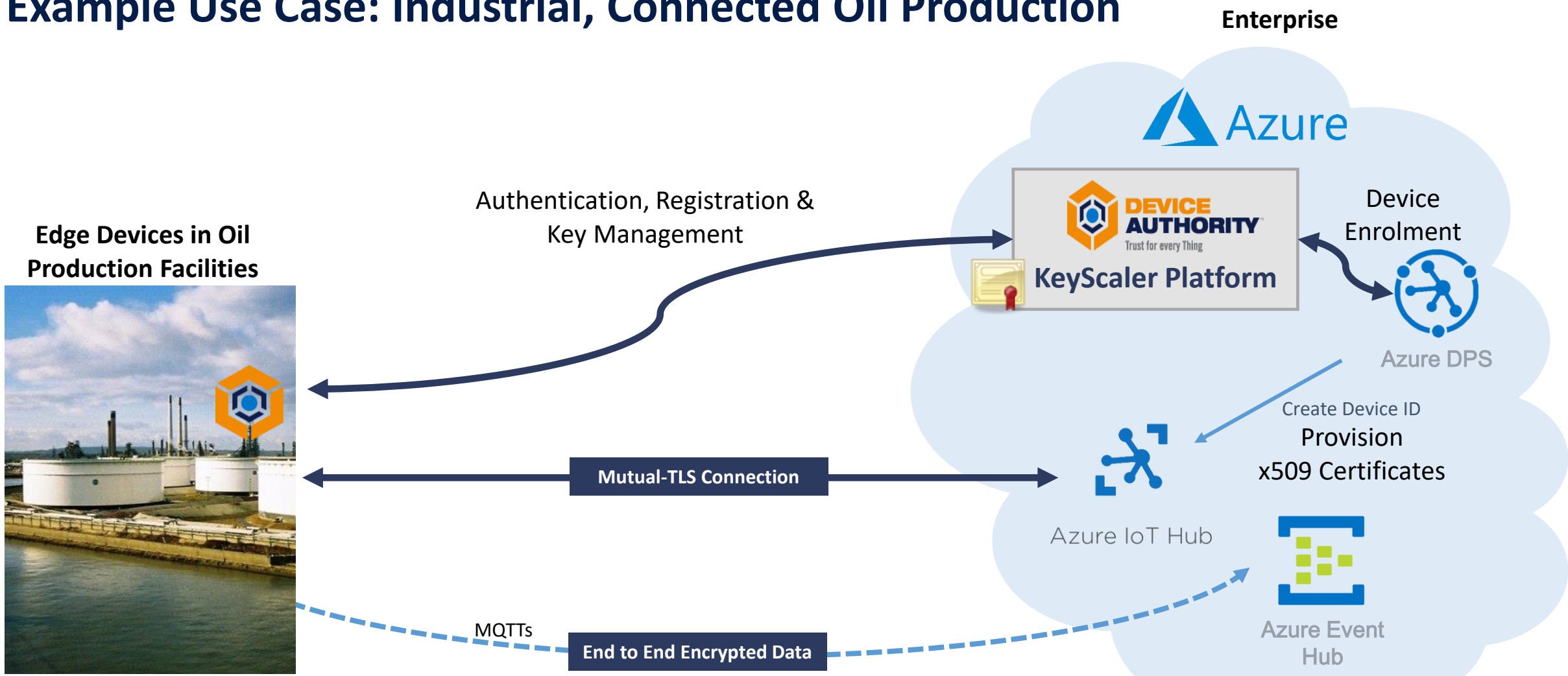


Example Use Cases – Industrial, End to end data privacy



DEVICE AUTHORITY
Trust for every Thing

Example Use Case: Industrial, Connected Oil Production



DEVICE AUTHORITY™

For any organisation building their **IoT strategy**, who require **trust and identity at the edge**, Device Authority is the only company truly able to deliver Identity and Access Management (IAM) for IoT. The KeyScaler platform delivers automation for critical credential management processes, in addition to tokenized access control and policy-based encryption for data, in transit and at rest.

Unlike traditional information security solutions, KeyScaler addresses the core challenges of **device trust, data trust and operational efficiency at IoT scale**, beyond the boundaries of the secure Enterprise.

Thank you!

Contact:

 robert.dobson@deviceauthority.com

 www.deviceauthority.com

 @IoT_Dobson

 http://info.deviceauthority.com/blog-da

DEVICE AUTHORITY
Trust for every Thing