terra solutions
Industrial IoT

Device Authority

Device Authority Overview

Scaling and Simplifying IoT Security with KeyScaler™

KeyScaler

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.

Proven Platform, Partner Ecosystem, Recognized by Experts

Gartner	**Cool Vendor** - 2016
FORRESTER	**TechRadar™: Internet Of Things Security, Q1 2017** A Mix of New and Existing Technologies Help Secure IoT Deployments
techUK	UK's Most Innovative Small Cyber Security Company
451 Research	**IMPACT REPORT – May 2nd 2017** Device Authority takes a dynamic approach to IAM for IoT devices
SC Media INNOVATORS	**SC Media 2018 Hall of Fame** **Industry Innovator 2016 & 2017**
Quadrant Knowledge Solutions	**Technology Leader in IoT IAM Market 2019** **Emerging Star in Global IoT Security Market 2018**

Business security challenges for Industrial IoT?

Operator injury/fatality

Sensitive data theft – IP, Process etc

OT Meeting IT challenges

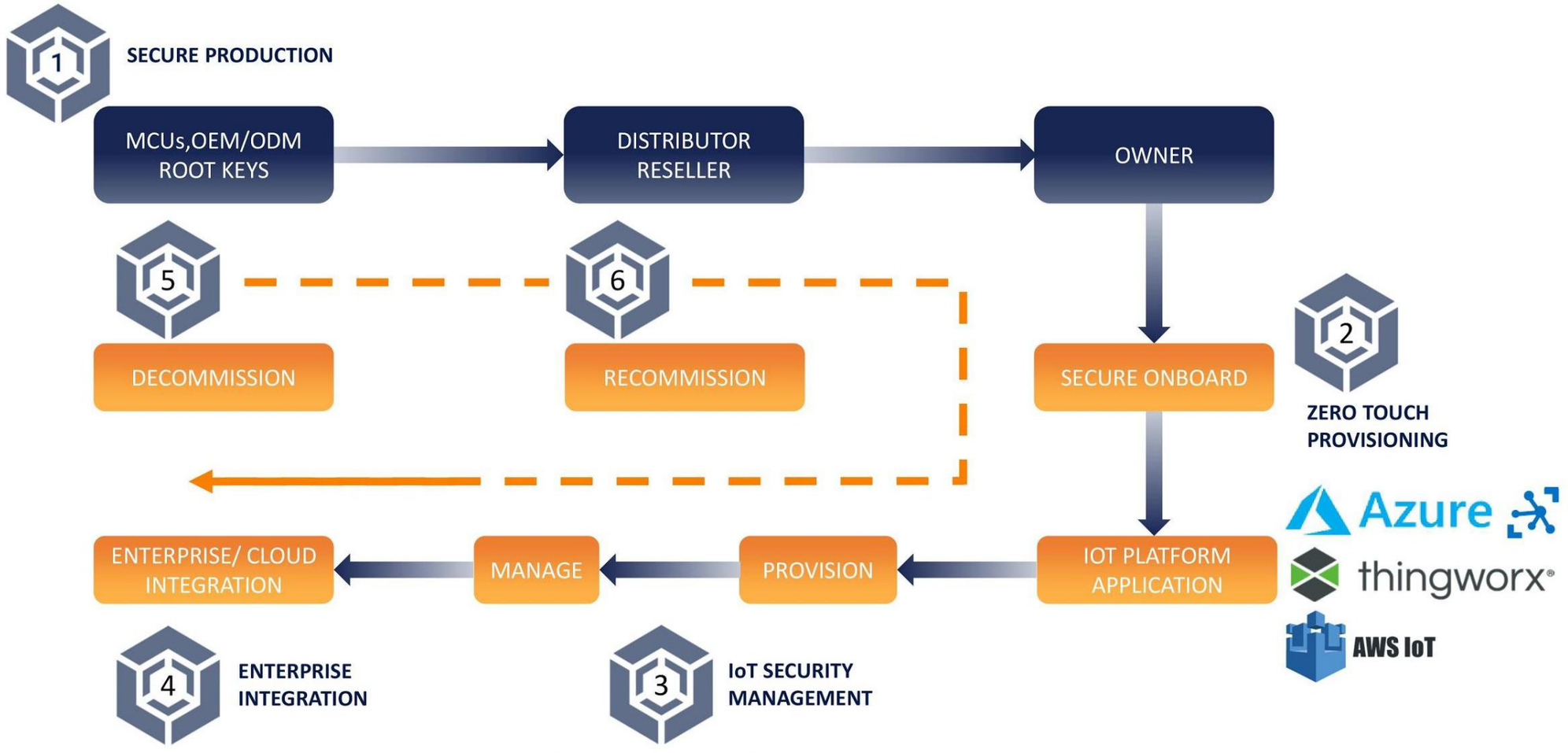
Disruption for manufacturing operations

Brand damage and reputation

Compliance and Financial liability

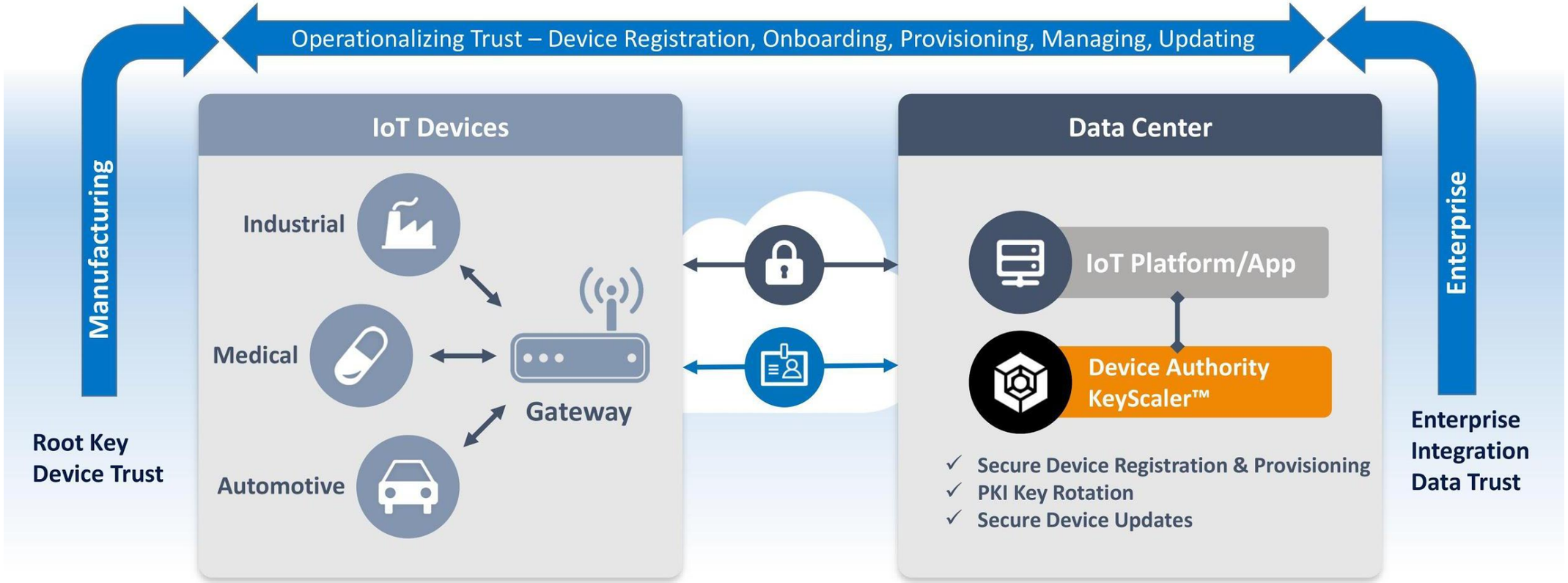
- GDPR the higher of **€20 million or 4% of annual global turnover**

KeyScaler for Trust and Automation in IoT Device Journey

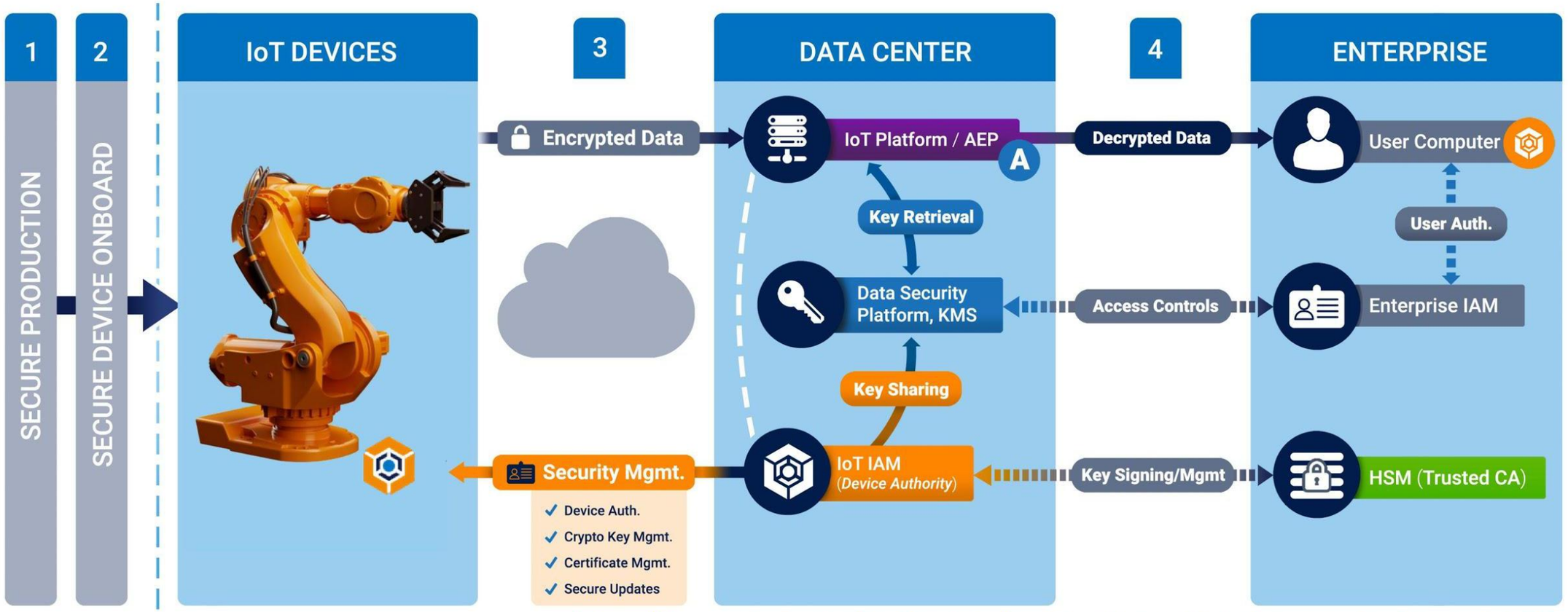


Our Solution

IoT Trust and Scale problems solved with Device Centric IAM Platform

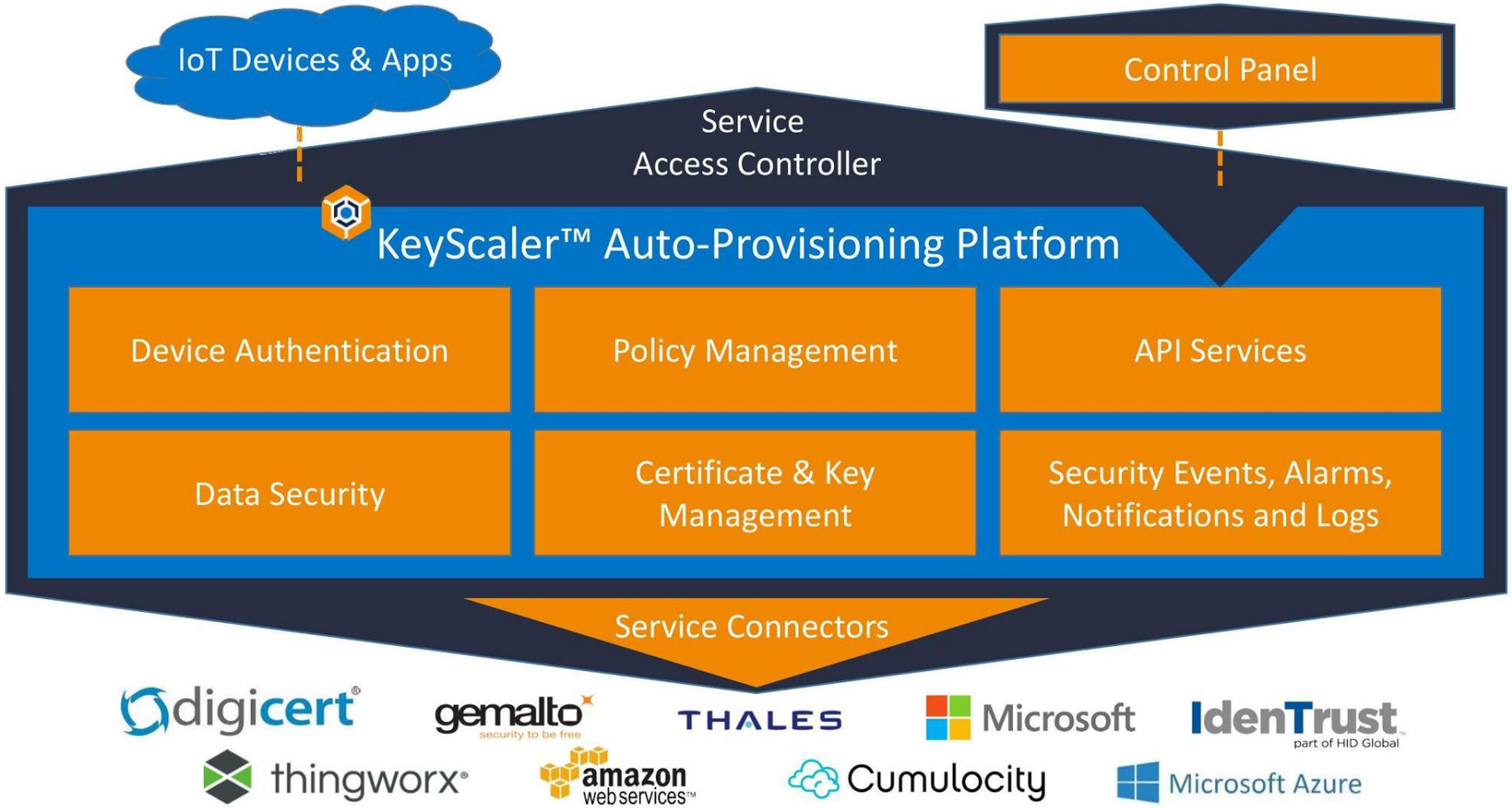


Smart Industrial, OT meets IT – Managing Security…



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

KeyScaler™ Platform



Product Delivery: On-Premise / VPC or SaaS

ON-PREMISE / VPC

- Download, Install, and manage KeyScaler system
- Deploy into own data center or VPC
- Services architecture allows for n-Scale deployment

MANAGED SERVICE - KSaaS

- Subscribe to hosted KeyScaler service
- No infrastructure deployment or running costs

KeyScaler™ Features

- Registration Controls, Onboarding
- Automated Certificate Management
- Automated Password Management
- Device Group Management
- End-to-End Data Security
- Secure Soft Storage
- PKI Signature+
- Delegated Security Management
- DDKG Trust anchor, protocol
- Drop-in agents
- Client SDK and Development tools

- Azure IoT Security Suite (PKI, Token, Crypto)
- AWS IoT Security Suite (PKI, Crypto)
- PTC ThingWorx Security Suite (Token, Crypto, Management)
- Internal Private PKI
- Public CA connectors
- Thales and Gemalto HSMs support
- Intel Secure Device Onboard partner
- Multi-tenant
- Partner tenant model, branding
- AWS SaaS Contracts option
- Server side REST APIs

KeyScaler Supports Two Authentication Methods

Dynamic Device Key Generation (DDKG)

- Patented technology to authenticate devices based on hardware attributes
- Provided to customers as a development library
- Level-1 DDKG includes support for common attributes available via OS
- Level-2 DDKG includes support for device-specific components

PKI Signature+

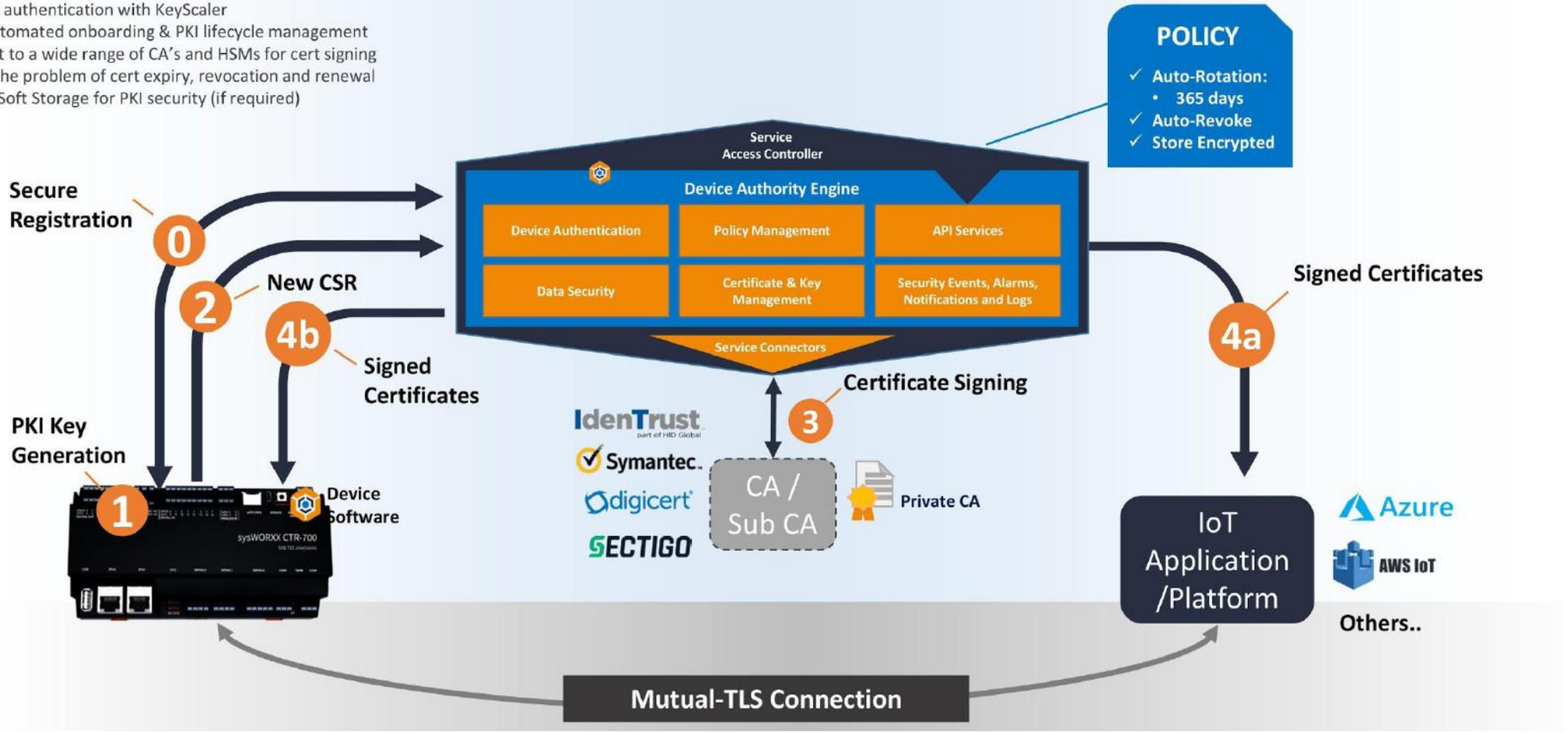
- Authenticate devices based on public key signatures
- Provided as an integration reference guide (no library required)
- Developer-independent implementation enabling broader device support
- Extremely lightweight solution for low-power devices

PKI Certificate Management for IoT Devices

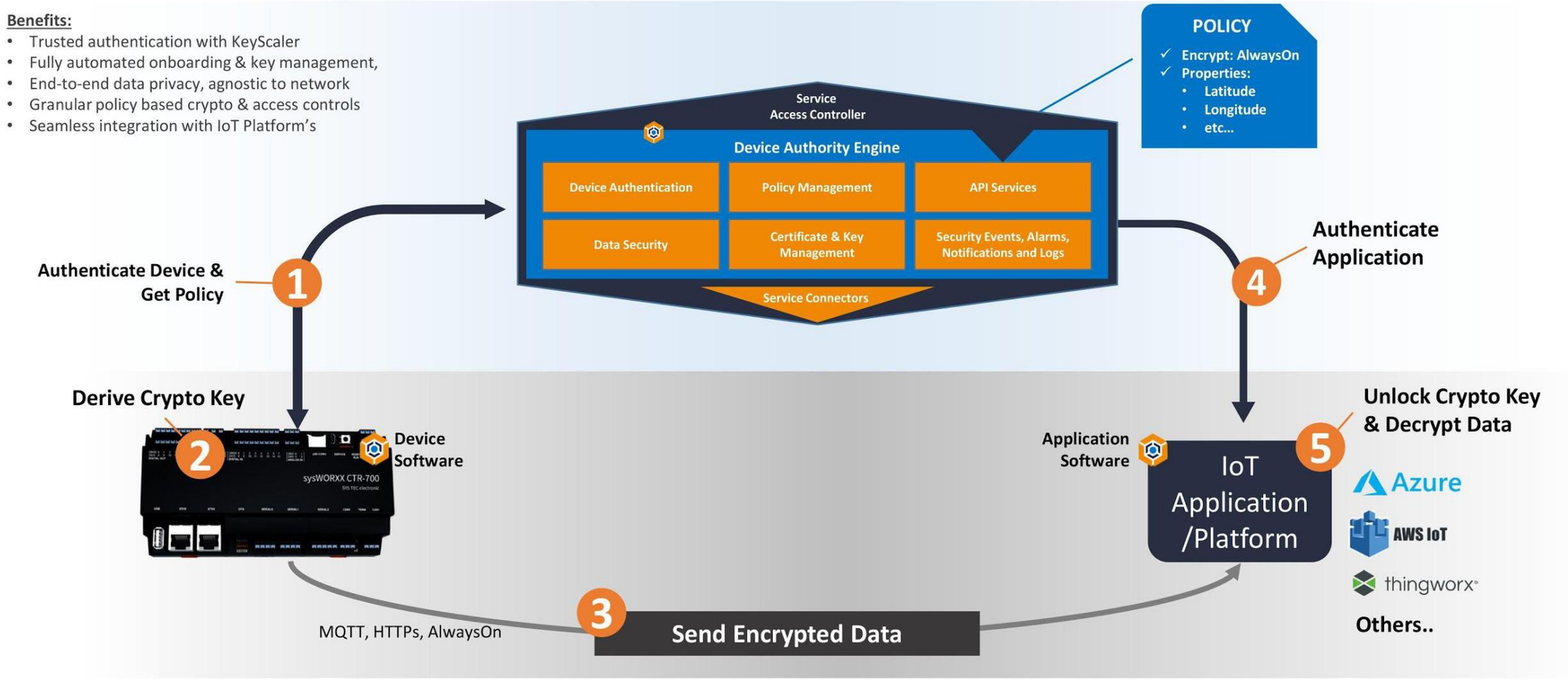
Device-bound, Policy-driven Key Provisioning, Revocation, and Renewal solution for certificates

Benefits:

- Trusted authentication with KeyScaler
- Fully automated onboarding & PKI lifecycle management
- Connect to a wide range of CA's and HSMs for cert signing
- Solves the problem of cert expiry, revocation and renewal
- Secure Soft Storage for PKI security (if required)



Data privacy, Policy-driven Crypto Key Provisioning & Management

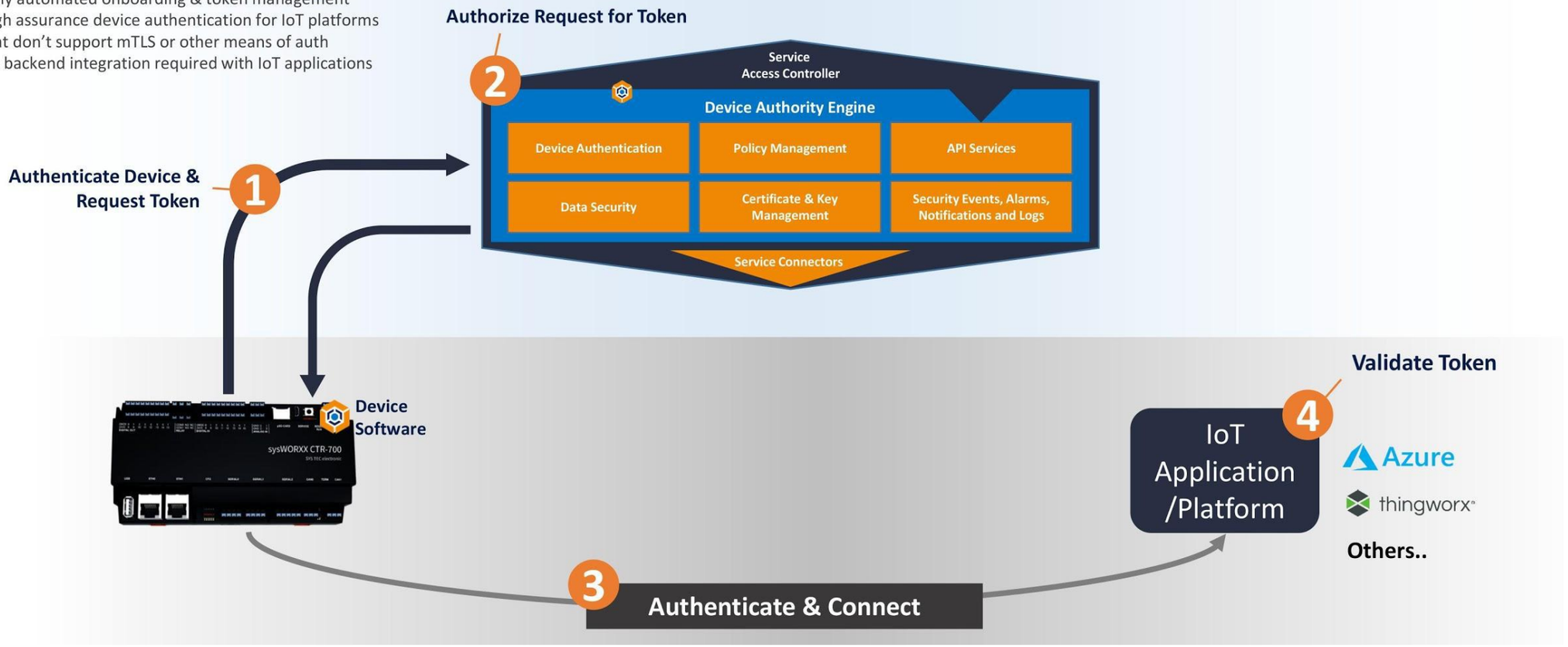


Delegated Security Management (DSM) Solution

Tokenized Authentication Model – Alternative to Certificate Authentication

Benefits:

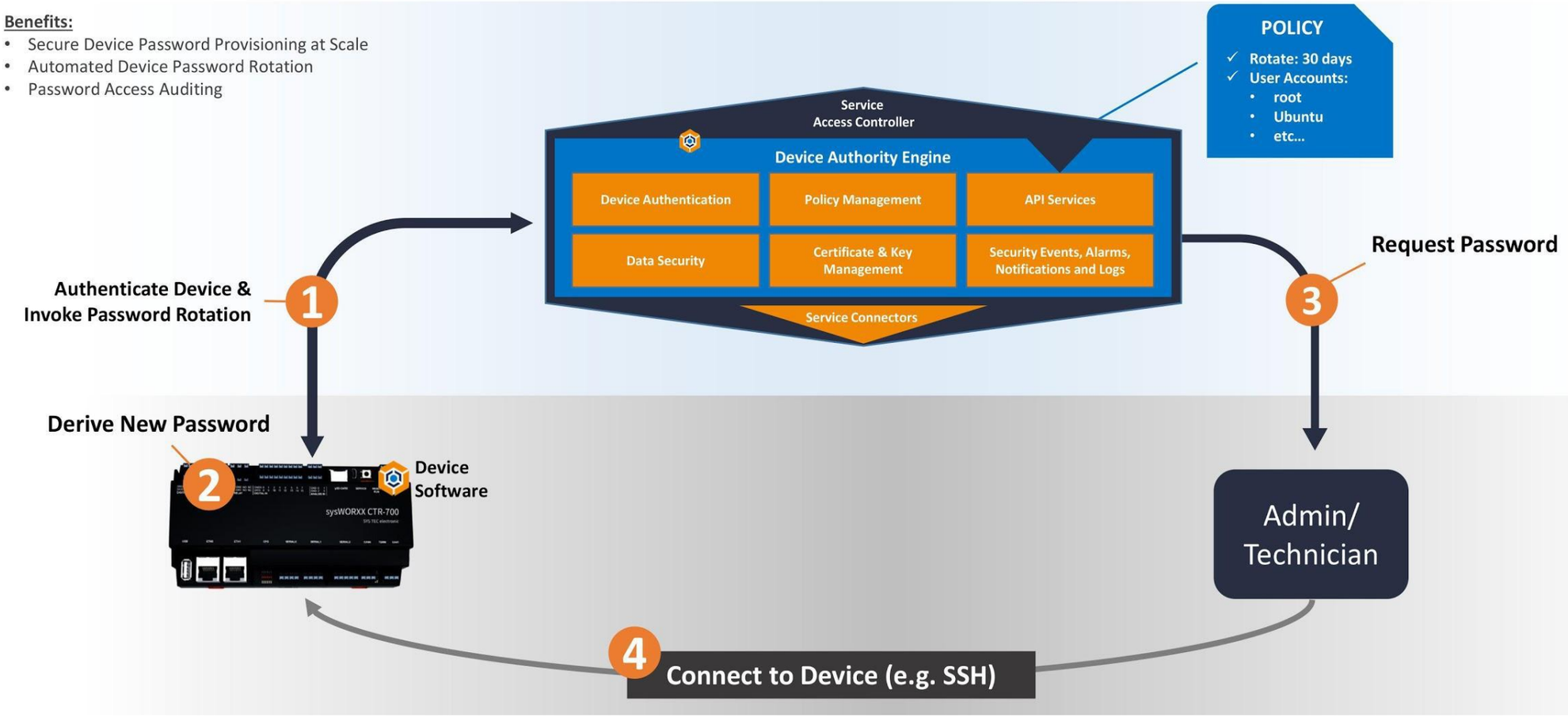
- Fully automated onboarding & token management
- High assurance device authentication for IoT platforms that don't support mTLS or other means of auth
- No backend integration required with IoT applications



Automated Password Management for Devices

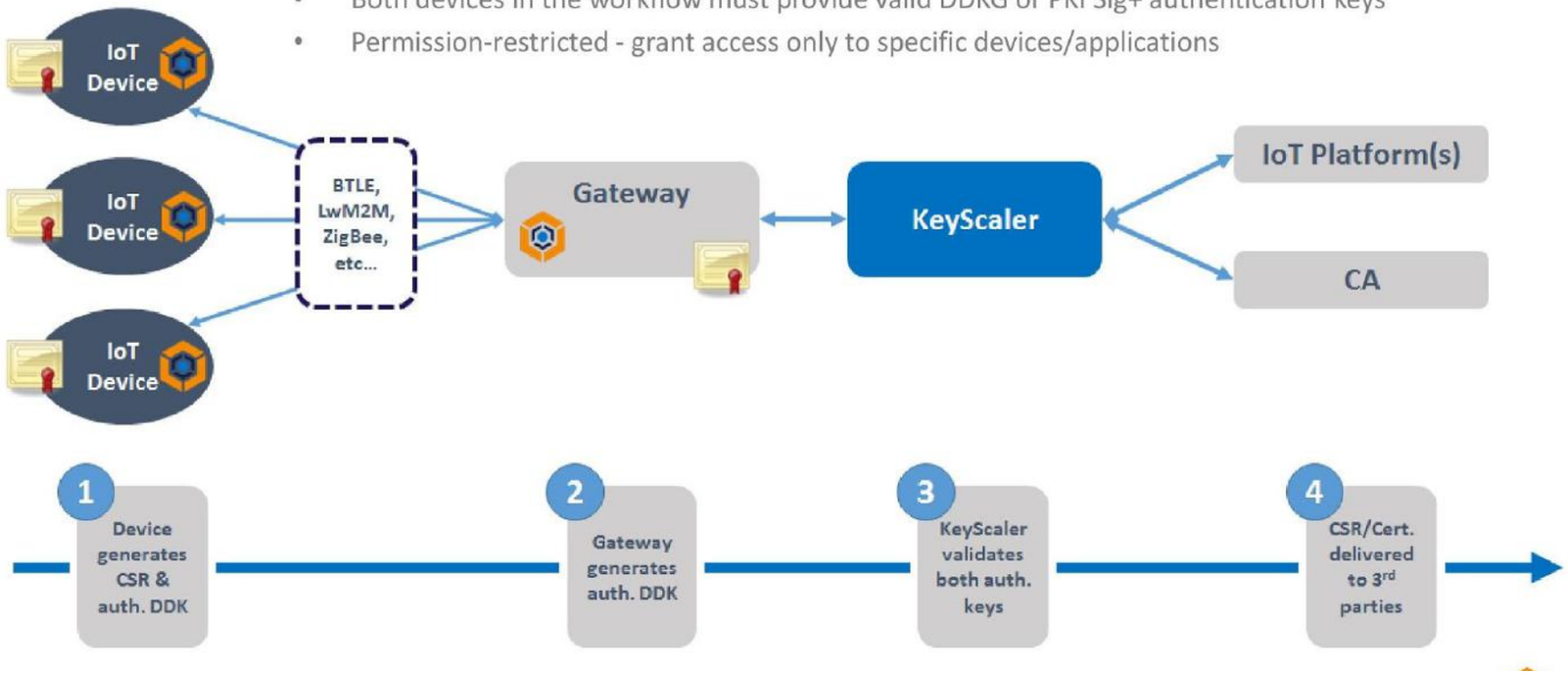
Benefits:

- Secure Device Password Provisioning at Scale
- Automated Device Password Rotation
- Password Access Auditing



PKI Certificate Management for IoT Devices via Hub proxy

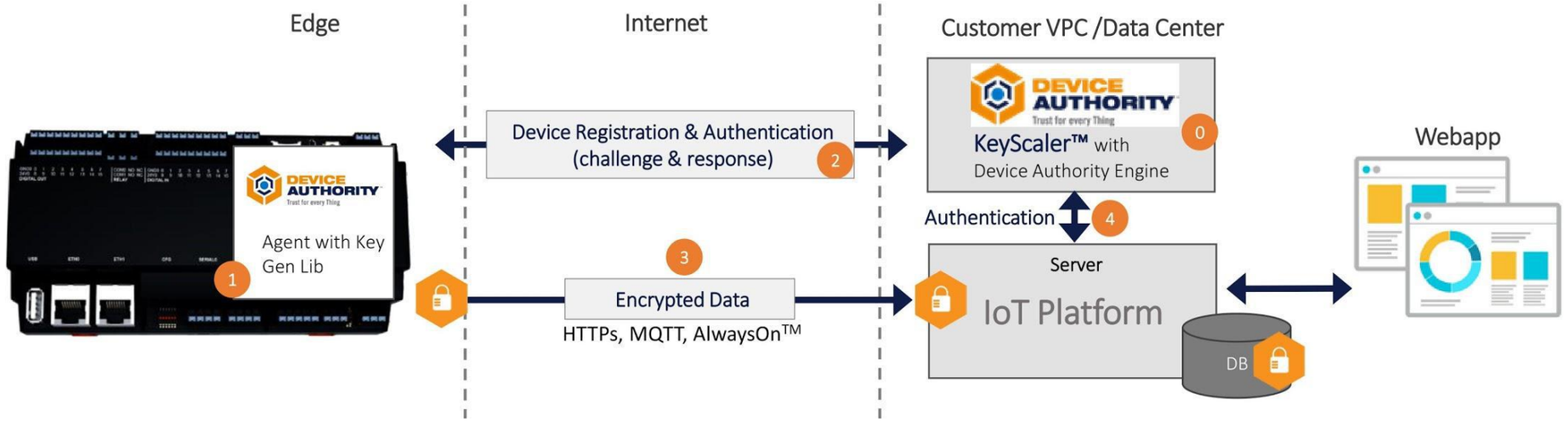
- Authenticated and authorized “brokers” (e.g. gateways) can provision certificates for DDKG and PKI Sig+ enabled devices connected to it (i.e. devices with no direct connection to KeyScaler)
- Both devices in the workflow must provide valid DDKG or PKI Sig+ authentication keys
- Permission-restricted - grant access only to specific devices/applications



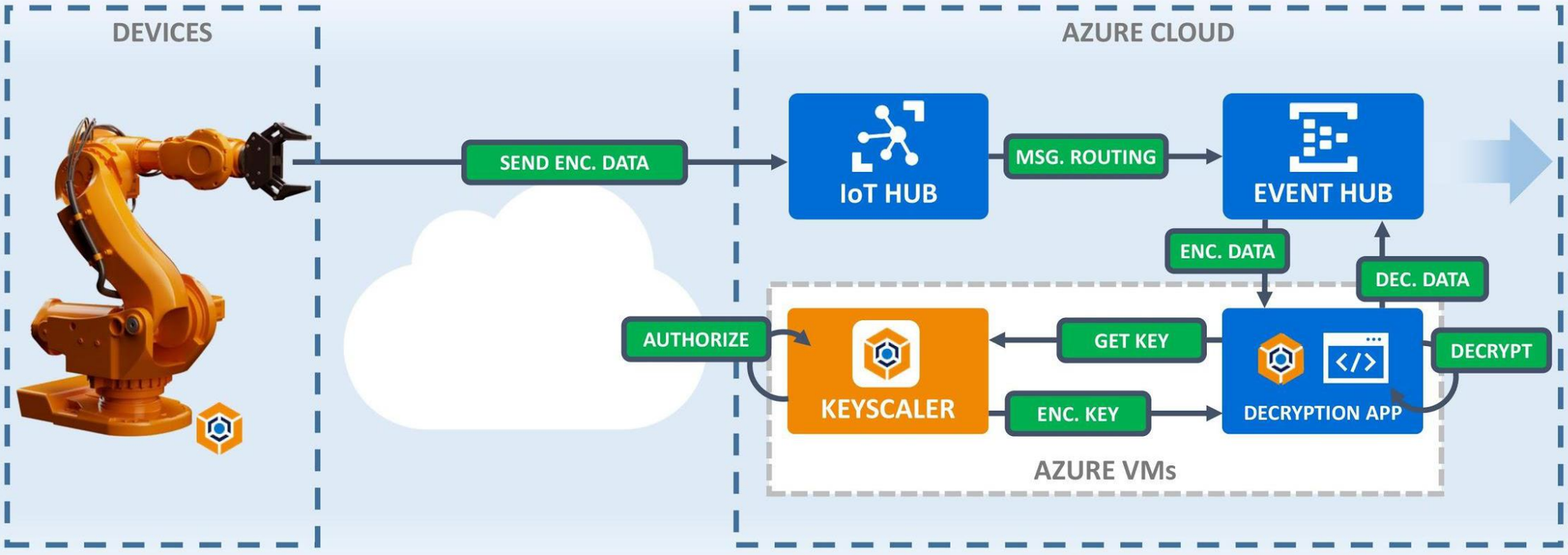
Industrial IoT - End to End data crypto

- Trusted authentication with KeyScaler
- End-to-end data protection, agnostic to network
- Granular policy based crypto
- Zero touch provisioning at IoT Scale

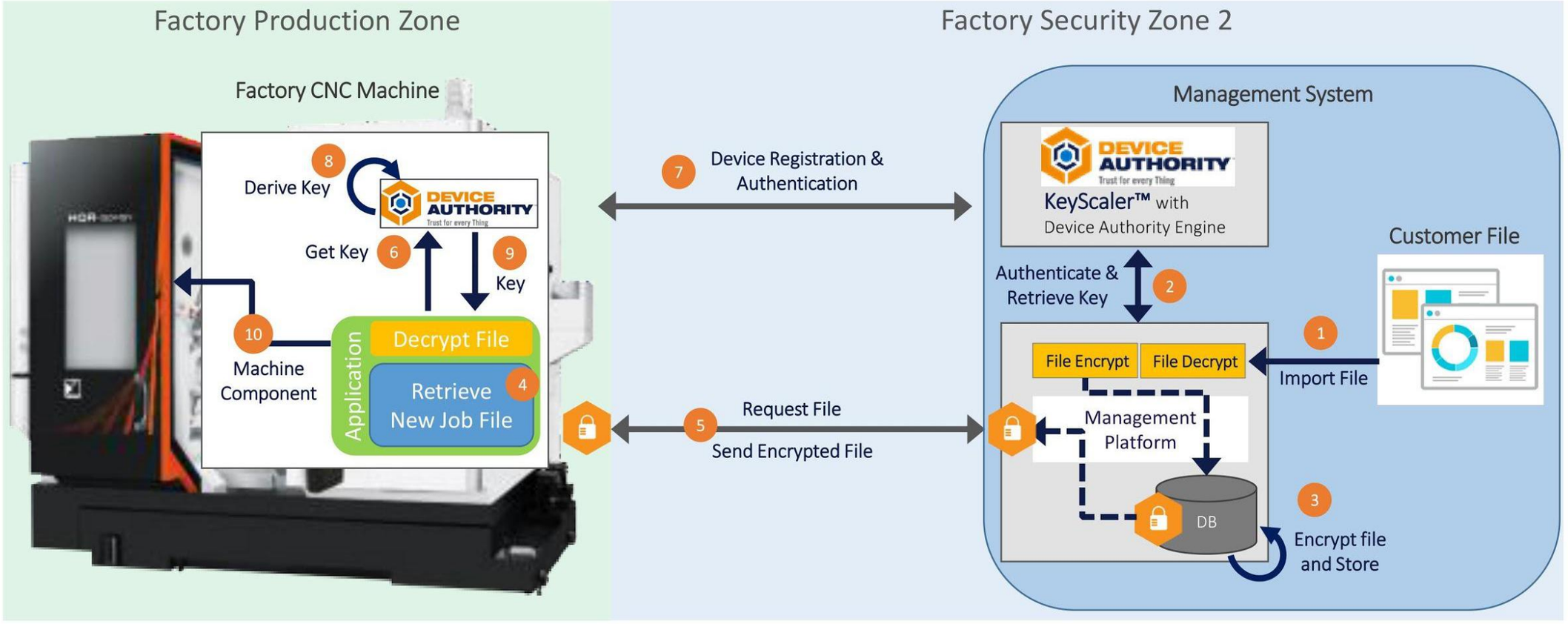
- Policy based data protection
- Policy based access controls / authorization
- Owner controlled security
- Seamless integration with IoT Platform's such as Azure IoT, PTC ThingWorx



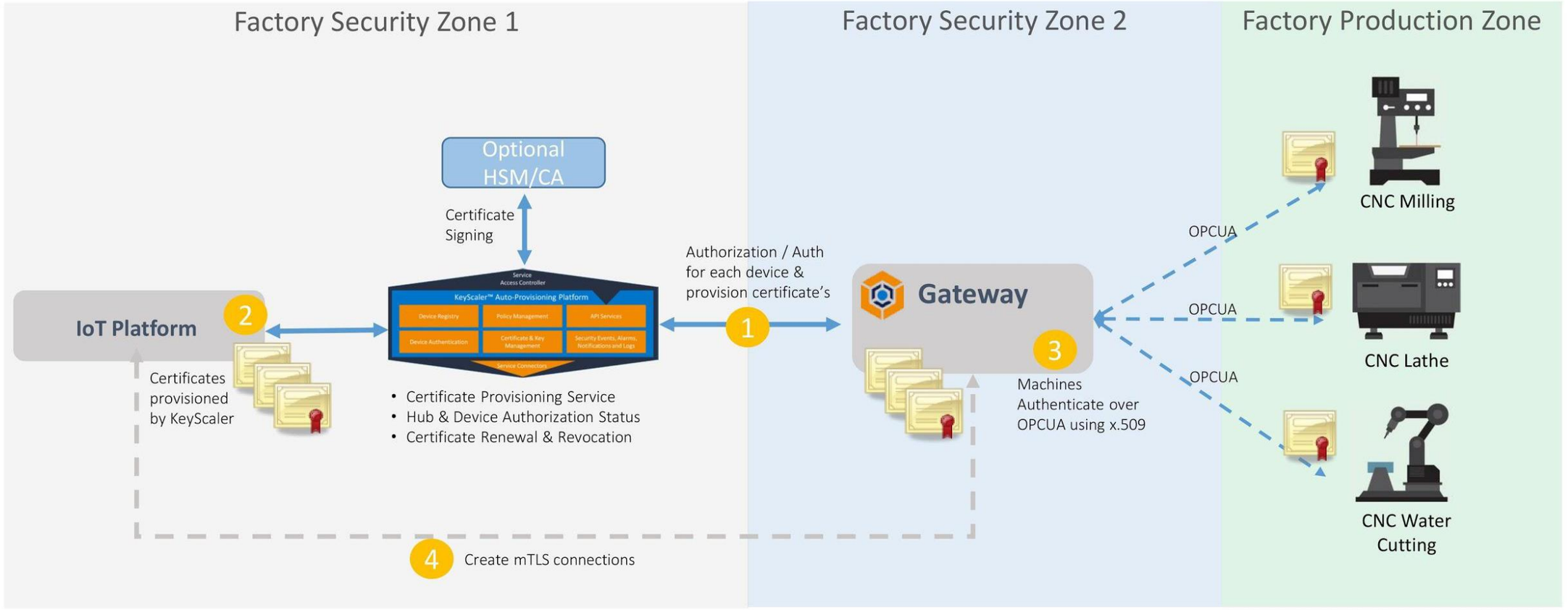
Example Use Cases – Industrial, End to end data privacy



Example Use Case: Smart Machining, IP & Revenue protection



Example Use Case: Industrial, PKI Certificate Management for OPCUA



Industrial IoT: Connected Oil Production Equipment

Connected oil production equipment to realize predictive maintenance and operational efficiencies with analytics.

Business Need

Critical infrastructure requiring a proven secure device identity solution for the equipment to protect against breaches.

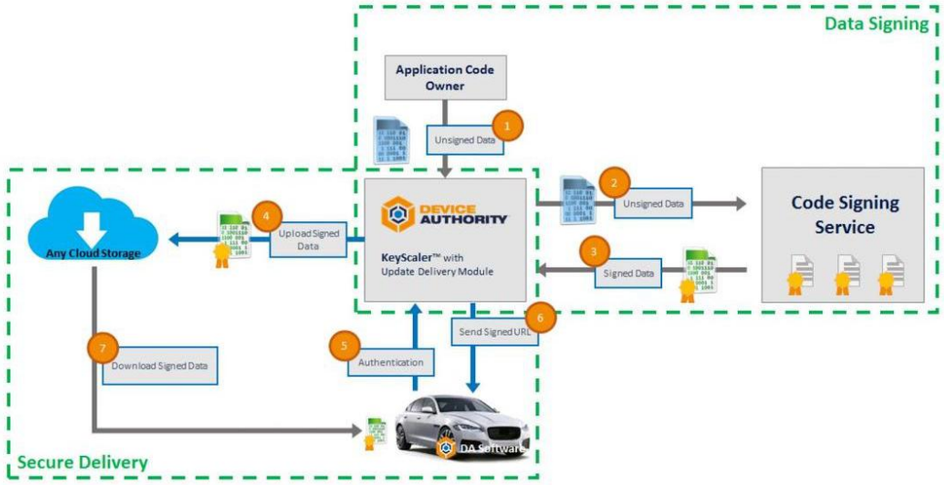
Solution

KeyScaler provides the identity solution needed to deliver device authentication and certificate management solution between devices and Microsoft Azure IoT Hub.

Benefits

- Device authentication/attestation solution
- Seamless integration and support in the device registration with Microsoft Azure IoT Hub
- Automated lifecycle management solution for device certificates with Microsoft Azure IoT Hub including provisioning, renewal, and revoking
- Security product solution meeting all requirements which eliminated customer need for additional development with Azure IoT Hub's Device Provisioning Service (DPS) product.

Automotive: Connected Car, Secure Over The Air (OTA) Updates



Secure OTA updates for vehicle manufacturers to update firmware and software securely to their vehicle systems

Business Need

With the ever increasing demand for Connected Cars, software is an integral part of every vehicle today. Having the ability to update software onboard the Vehicle is a must to mitigate against vulnerabilities found, fixing bugs or just providing feature enhancements. Manufactures need to be able to update their vehicles securely ensuring that the updates each vehicle receives is trustworthy, the update hasn't been tampered with in transit and the update isn't malicious.

Solution

KeyScaler provides the security platform to automate and manage code signing to meet the needs for secure OTA updates. The platform automates data signing, key provisioning and device authentication to ensure end to end that each vehicle is receiving trustworthy and un-tampered with updates. This is achieved utilizing one of KeyScaler client trust anchor(s) to establish trust between KeyScaler and the Vehicle. Coupled to this, each vehicle will have the cryptograph proof to check the validity of each update.

Benefits

- Automates the process for secure data signing
- Enables vehicle manufacturers to verify package updates, to ensure they are trusted, haven't been tampered with and are not malicious
- Turn key solution to manage code and data signing with policy driven update delivery to vehicles
- Flexible solution designed to integrate to new and existing workflows