

## Use Case: Digital Transformation in Oil and Gas with KeyScaler platform and Azure IoT Edge

As part of its digital transformation strategy, a leading oil and gas company seeks to enhance operational efficiency, data visibility, and security in its oil fields. The organization aims to implement a robust data collection and transmission system using Azure IoT Edge gateways, leveraging the Purdue model for Industrial Control Systems (ICS) to ensure secure and efficient data exchange across its operational technology (OT) and information technology (IT) environments. By utilizing the Azure IoT Hub, the company plans to create a reliable, scalable, secure infrastructure that connects field devices to the cloud for real-time analytics and decision-making. The initial IoT devices will be Variable Speed Drives used for ESP control as well as various chemical injection equipment.

### Challenges Faced

- 1. Manual Device Enrollment:** Devices are not enrolled automatically, requiring manual intervention that delays deployment and increases the risk of errors.
- 2. Certificate Management:** Certificates need to be provisioned manually, complicating the management process and leading to potential security risks.
- 3. No Automated Certificate Rotation:** Certificates are not rotated automatically, exposing the organization to the risk of having an expired certificated that could cause service disruptions or compromised certificates.
- 4. High Maintenance Costs:** The manual maintenance of device identities and credentials incurs high operational costs and resource demands.

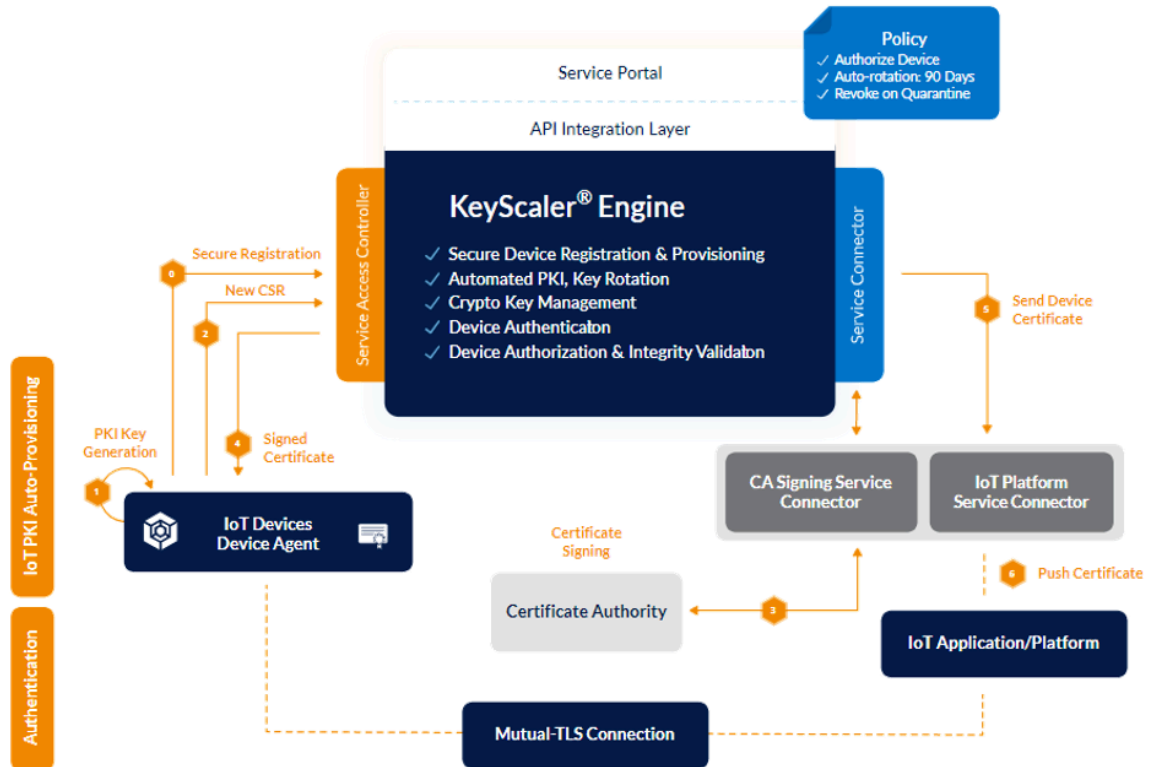
### Solution

To address these challenges, the company will implement Device Authority's KeyScaler Platform to automate the device identity and lifecycle management:

- 1. Automated Device Registration:** Utilizing the EST (Enrollment over Secure Transport) protocol, KeyScaler automates the device registration process, significantly reducing manual workload and associated errors.
- 2. Policy-Based Certificate Lifecycle Management:** KeyScaler enables policy-based certificate lifecycle management, including automated provisioning, rotation, and revocation. This ensures that all devices maintain up-to-date and secure certificates throughout their lifecycle.
- 3. Automated Device Provisioning:** The provisioning of devices into the Azure IoT Hub is automated, eliminating manual steps and minimizing the risk of human error.
- 4. Automatic Transfer of Parent – Child Relationships:** KeyScaler automatically transfers the parent-child relationships of gateways to Azure IoT Hub, ensuring accurate hierarchy management and streamlined data flow.
- 5. Secure Key Transfer Mechanism:** A secure mechanism for provisioning and transferring keys to the gateways will be established, enhancing overall security and reducing the risk of unauthorized access.

# PKI Certificate Management for IoT Devices

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



## Conclusion

- Enhanced Security:** The use of TPMs, KeyScaler automated certificate management, and secure key provisioning ensures that all communications are encrypted and authenticated, significantly reducing the risk of cyber threats.
- Simplified Device Onboarding:** Automating the EST protocol enrollment and device registration process facilitates a straightforward and secure onboarding experience, minimizing operational downtime, accelerating deployment and saving money by not having to send technicians in the field.
- Scalability:** KeyScaler capabilities provide the organization with a scalable solution that can adapt to changing operational needs, supporting the addition of new devices without compromising security.
- Cost Reduction:** Automating the management of device identities and credentials lowers operational costs, freeing resources for more strategic activities.
- Compliance and Governance:** Implementing a structured approach based on the Purdue model for ICS aligns with industry standards for cybersecurity, ensuring regulatory compliance and governance throughout the data exchange processes.

**DEVICE  
AUTHORITY**

UK Head Office  
Level 2, Thames Tower  
Station Road,  
Reading,  
RG1 1LX

Device Authority, Inc.  
c/o Workbar  
399 Boylston St fl. 6  
Boston  
MA 02116