A GUIDE TO PKI

Strengthening Security for Energy & Power Generation Organisations in the UKI

The energy sector is a cornerstone of modern society in the United Kingdom and Ireland (UKI), delivering electricity and fuel to power households, businesses, and key infrastructure. However, the threats facing this sector are rapidly evolving and increasingly complex. As threat actors set their sights on critical infrastructure, including gas, water, and power utilities, the risk of supply chain attacks is ever present.

Connectivity brings new advancements – and risks.

In November 2023, the UK NCSC published its seventh annual review to raise awareness about an increasingly unpredictable threat landscape. The UK's critical national infrastructure sectors, such as utilities, energy, communications and internet, transport, and financial networks are experiencing a swathe of increased threat vectors and attacks, including malware and ransomware.

Many UK energy and power generation organisations have adopted a secure-by-design approach, to augment security and reduce risk across their respective value chains. Some have started with an identity-first security posture, while others have embarked upon a zero trust journey, though what is prevailing as a common theme, is that these organisations have started to view PKI as a critical foundation to each of these security strategies.

Throughout this document, we highlight the areas where PKI augmentation serves to enhance existing and future security strategies, with best practices knowledge and information related to the energy and power generation sector in the UKI.

RISKS AND CHALLENGES

Why do manufacturing, energy, and power generation organisations need to consider revamping their security posture?

The dynamic landscape of the UKI's manufacturing, energy, and power generation sectors demands heightened attention to security. With the proliferation of connected devices, the adoption of cloud, and the ever-present threat of cyberattacks, traditional security measures are no longer sufficient. The consequences of a security breach can be catastrophic, including operational disruptions, financial losses, reputational damage, and compromise of sensitive data. To mitigate these risks and safeguard the integrity, confidentiality, and availability of critical systems and infrastructure, organisations must revamp their security posture.

- **Increasing Frequency of Attacks:** Attacks on critical energy and power systems are escalating in both sophistication and frequency. Energy and power generation companies, particularly those operating within national infrastructures, have become prime targets for threat actors.
- **Varied Attack Targets:** Attackers employ diverse strategies, targeting enterprise IT infrastructure, industrial control systems, smart meters, and both modern and legacy operational technology (OT) environments. Manufacturing facilities have also witnessed a surge in attacks. Notable examples include Industroyer, Stuxnet, and the high-profile Colonial Pipeline attack.
- **Motivations for Targeting:** Attackers aim to exploit vulnerabilities in these industries to cause infrastructure failures, disrupt critical operations, compromise essential services, induce factory downtime, inflict financial losses, exfiltrate sensitive data, and even impact national economies on a wide scale.
- **Emerging Threat Vectors:** The convergence of operational technology (OT) and information technology (IT) environments, the proliferation of Industrial Internet of Things (IIoT) devices such as smart meters, sensors, and wireless modules, the interconnectivity of devices and systems in connected manufacturing and vehicles, as well as technology modernisation efforts to meet business goals, introduce new avenues for potential attacks.
- **Third-Party Attacks:** Attackers have extended their focus to include third-party providers associated with these organisations. Securing communication channels between organisations and their third-party partners has become crucial to prevent potential breaches and protect critical infrastructure.

PKI FOR IOT & OT

Why PKI is critical to mitigate risks facing the manufacturing, energy, and power generation sector.

In this era of digital transformation, PKI emerges as the cornerstone of robust security for the manufacturing, energy, and power generation sectors. PKI delivers end-to-end protection, including mutual authentication to secure connections, encryption to protect sensitive data, and signing to ensure the integrity of systems and the software that runs on them.

Device Authentication
Certificates validate the identity of devices, ensuring that only authorised systems, applications, and servers have access to the device.

Data Protection
Certificates establish an encrypted connection between machines, ensuring that any data transmitted is private and protected.

System & Software Integrity
Certificates and digital signatures ensure the integrity of systems and software running within industrial and manufacturing environments.

How are others doing it?

"With Keyfactor, our security teams will be able to shift their focus from reactive PKI management and certificate outage prevention to a more proactive, scalable model that will streamline business enablement and operational efficiencies."

Chris Barnicott

CTO, SSE

Learn more ↗

- **Gain asset visibility:** Digital certificates provisioned from a proper PKI provide unique identities for connected machines, gateways, and industrial systems, providing transparency and visibility into every asset.
- **Protect sensitive data:** Securing data in transit using digital certificates is critical as manufacturing and industrial environments become more interconnected, and data passes over networks.
- **Reduce attack surface:** Every machine, workload, and software component running in critical industrial environments must be authenticated and verified with a trusted identity, or risk compromise from threat actors.
- **Enhance existing controls:** Oftentimes there are drawbacks associated to existing security controls, such as default or universal credentials. Private keys are never shared, making systems inherently more secure than password-based solutions.
- **Rapidly secure existing and future investments:** PKI touches all assets: Business Applications; Cloud; DevOps; Enterprise IT; IAM; PAM; Security Controls. A regimented and secure PKI will greatly secure these assets and investments.

What is the demonstrable ROI of working with Keyfactor?

By implementing PKI, your organisation can stay one step ahead of adversaries, instilling confidence in stakeholders and demonstrating a commitment to safeguarding critical operations.

Asset Discovery

Leveraging PKI to find all assets within the organisation allows you to more efficiently prioritise your team's efforts and initiatives, with up to 20% of a security team's time being saved.

Asset Reduction

Discovery exercises enable you to retire assets, controls, and systems which are no longer fit for purpose, reduce Shadow IT, and reduce licenses fees, providing monetary savings by including decommissioning multiple physical servers.

Automation

PKI's inherent automation capabilities allow your organisation to enhance security controls quickly for the areas of most concern, reducing the need to spend resources and time investing in new people by 2-3 FTEs.

Improve Customer & Employee Experience

Speed up employee onboarding with rapid authentication to applications and systems, via digital identities issued to users. Leverage PKI as a critical asset for identity with issuance of secure identities to customers, allowing them to access data quickly.

Risk reduction for the future

Scalable PKI enables organisations to push their technologies forward. Secure your assets now and into the future to reduce operational downtime from outages. Customers have experienced savings of more than $9.6m per annum by reducing outages.

Risk reduction by Post-Quantum Cryptography

Organisations can apply for budget from regulators to facilitate this work, as it is aligned to securing post-quantum cryptography.

Secure Software Updates

Secure systems and assets by way of secure code signing, to assure no rogue code or malware that could move laterally, cause downtime, and cost the business major resources.

Time-to-value

PKI is on every system. Rapidity of discovery and security enables a far quicker time to value comparative to purchasing and implementing point solutions. With multiple deployment options you can issue certificates in as little as 20 minutes.

Explore our solutions

See how to modernise your PKI and move up the maturity model with flexible, scalable, and agile solutions.

PKI your way

Simplify and scale PKI with the only platform that deploys fast, runs anywhere you need it, and scales on demand without limits.

Learn more ↗

PKI as a service

Offload the cost and complexity of PKI with a fully-managed, cloud-hosted PKI service operated by experts.

Learn more ↗

Certificate lifecycle automation

Gain complete visibility of all certificates, centralise control, and enable automation to reduce downtime and risk.

Learn more ↗

IoT identity management

Centrally manage and automate the lifecycle of identities across your fleet of connected IoT products and devices.

Learn more ↗

KEYFACTOR

Contact us

Email
sales@keyfactor.com

Phone
+46 8 735 61 01

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organisations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.