KEYFACTOR

Strengthening PKI and IEC 62443

Originally, industrial automation and control systems (IACS) were not designed with cybersecurity in mind. Their security largely hinged on physical isolation from a network, however, that strategy is becoming impossible in today's interconnected world. With the world's reliance on IACS, IEC 62443 has been put forward to provide a framework to ensure security with their use.

This includes industries such as manufacturing, energy (including oil and gas), utilities, transportation, and infrastructure.

Compliance with IEC 62443 is crucial for all entities involved in the design, deployment, operation, and maintenance of industrial control systems to mitigate cybersecurity risks and protect critical infrastructure from cyber threats. This list includes but is not limited to:

1. **Industrial Control System (ICS) Operators:** These organisations own, operate, or manage industrial control systems within their facilities. This could include manufacturing plants, power generation facilities, or critical infrastructure facilities.

2. **System Integrators:** Companies or individuals that design, implement, or maintain industrial control systems for clients to ensure the security of the systems they deliver.

3. **Original Equipment Manufacturers (OEMs):** Manufacturers of industrial control devices, sensors, controllers, and other components used in IACS must ensure that their products meet the security requirements to provide secure solutions to their customers.

4. **Service Providers:** Companies that provide services to organisations operating IACS may also need to comply to ensure the effectiveness of their services.

5. **Regulatory Authorities and Standards Bodies:** IEC 62443, in similar fashion to ISO 27001, has evolved into the default baseline requirement in the industrial domain, regardless of vertical. For organisations operating in industrial domains, IEC 62443 is fast becoming the most requested and expected cybersecurity compliance amongst regulatory authorities and standards bodies.

6. **Suppliers and Vendors:** Suppliers of software, hardware, and other technologies used in industrial control systems are expected to comply with IEC 62443 to meet the security requirements specified by their customers or regulatory authorities. Customers are expecting to achieve "Compliance by Design", by utilising compliant components.

Public key infrastructure (PKI) and digital certificate management and automation play a crucial role in supporting compliance with IEC 62443, from Security Level 2 and onwards:

1. **Identity and Access Management (IAM):** PKI enables strong authentication of users, devices, and applications within industrial control systems. Digital certificates are used to verify the identities of entities and enforce access control policies, ensuring that only authorised individuals and devices can access critical systems and data.

2. **Secure Communication:** PKI facilitates secure communication channels between components of industrial control systems. Digital certificates are used to authenticate the endpoints of communication and establish encrypted connections, protecting sensitive information from unauthorised access or tampering.

3. **Key Management:** PKI provides a framework for managing cryptographic keys used for encryption, digital signatures, and authentication within industrial control systems. Proper key management practices, including key generation, distribution, storage, and revocation, are essential for ensuring the security of communications.

4. **Non-Repudiation:** Digital certificates enable non-repudiation, which is the ability to prove that a particular action or transaction was performed by a specific entity. By using digital signatures generated with private keys associated with digital certificates, organisations can ensure accountability and deter malicious actors from denying their actions.

5. **Device Authentication and Integrity:** PKI supports the authentication and integrity verification of devices connected to industrial control systems. Digital certificates can be used to authenticate the firmware and configuration of devices, ensuring that only trusted and unaltered components are allowed to participate in critical processes.

6. **Compliance Auditing and Reporting:** Digital certificate management and automation solutions often include features for auditing and reporting on certificate usage, lifecycle events, and compliance with security policies. These capabilities help organisations demonstrate compliance with IEC 62443 requirements and facilitate the preparation of audit trails and reports for regulatory purposes.

PKI and digital certificate management and automation are essential components of cybersecurity strategies for industrial control systems, helping organisations achieve compliance with IEC 62443 by enabling strong authentication, secure communication, key management, non-repudiation, device authentication, integrity verification, and compliance auditing. Implementing robust PKI and certificate management practices with tools like EJBCA and Keyfactor Command is critical for mitigating cybersecurity risks and protecting critical infrastructure from cyber threats in accordance with IEC 62443 standards.

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.