DigiCert-powered PKI for trusted smart building solutions

Building trusted solutions

As smart buildings become more connected, the value of convergence and cloud connectivity increases the need for new solutions, such as OpenBlue. Only when we can confidently validate identity can we place our trust in connected solutions for a wide range of applications from site to cloud.

Public Key Infrastructure

Public Key Infrastructure (PKI) enables trusted identities for users, devices and code on a network and protects communication in the digital world. PKI comprises certificates, encryption, software, hardware, processes and policies. The establishment and deployment of PKI services allow organizations to build trust in their networks and exchange data securely through authentication, confidentiality and data integrity.

- **Trusted communication** – Trust between people and devices is established digitally for encrypted network communications
- **Trusted code** – Software updates are genuine and unaltered, as released by Johnson Controls
- **Trusted devices** – Devices are uniquely identified with confidence for use within solutions and networks
- **Trusted users** – Enhanced authentication is delivered with protection against user impersonation

Certificates for each use case:

Communication certificates

(public and private PKIs) Trust between people and devices

Signing certificates

Stamp/seal on Johnson Controls digital artifacts

Device identity certificates

Stamp/seal on Johnson Controls devices

User identity certificates

Trusted end-users can access IoT

Why is this important?

Building trusted networks is essential in a world of persistent, advanced cyberthreats. Cyber risks heighten as industries and enterprises transform operations through digital channels, technologies and data sharing. Attackers aim to infiltrate and manipulate not just an individual company but the entire ecosystem to which it belongs. You must take preventative steps to ensure your ecosystem remains safe. Be certain your products and solutions have been authenticated and come from a trusted source.

What happens when the certificate is not authenticated or certified?

There can be circumstances where threat actors can impersonate a site, device or even a program using a counterfeit certificate, causing the end-user to have a false sense of trust. Using this technique, cyber attackers can access one device and ultimately take control of operations or pivot to other systems within the building. Furthermore, communications in which the source or destination is not mutually authenticated can result in accepting messages, which could generate false positives/negatives for system alerts, from untrusted sources or delivering content to the wrong destination, causing the disclosure of sensitive information.

Owner perspective

As a building owner or facility manager, you want to ensure the system properly manages the correct devices; if someone adds another camera or controller to the network without authorization, it is excluded by default unless you have it authenticated from a trusted source.

Moving beyond self-signed certificates

Self-signed certificates are typically generated within a system and do not have a trusted organization standing behind their validity. Where they do provide convenience, the expense comes at the cost of a false sense of security. They are not often tightly managed and can have a higher risk for key compromise. This can lead to a potential attack since the self-signed certificates can be generated by a cyber attacker and cannot be revoked to stop the attacker from accessing the system.

Trusted identities

Trusted digital identities are established when a certificate is issued by an organization following PKI industry standards and practices. Similar to a government-issued passport, agencies requiring validated identities work through an official Registration Authority (RA) to validate authenticity so identities can be trusted and confirmed genuine. RAs provide Certificate Authorities (CA) authorization to issue trusted and genuine digital identities. Johnson Controls has selected DigiCert®, a digital identity leader, as our trusted PKI infrastructure provider and Certificate Authority manager.

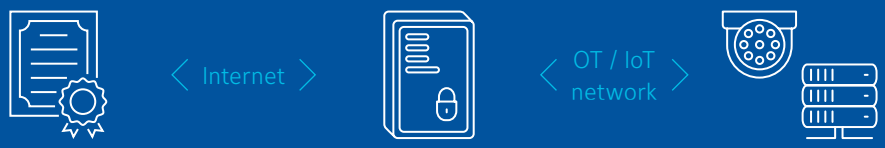
Johnson Controls implementation of DigiCert

Johnson Controls has partnered with DigiCert to enable its OpenBlue digital solutions suite to use the DigiCert ONE PKI platform, providing advanced security and trusted connectivity to intelligent building technology.

Johnson Controls utilizes the IETFX.509 certificate format, providing industry-standard secure authentication and establishing a certificate chain of trust to Johnson Controls with all Certificate Authorities fully managed by DigiCert. This mitigates the risk of costly operational interruptions due to cyberattacks while providing resilient, trusted and smart building solutions that use the most advanced PKI technology.

With modern PKI security and advanced expertise in managing digital certificates, the solution provides authentication and device identity, data encryption and integrity across the environment, protecting smart building solutions throughout their lifecycle.

Our trusted PKI gateway provides CA certificates to devices isolated from the internet:



Certificate Authority (internet)

Trusted Johnson Controls PKI Gateway (on-site)

Trusted OT and IoT devices (on-site)

Benefit of Johnson Controls/DigiCert Solution

Owners of smart buildings can have confidence that system components are safely and securely connected to the network using a robust PKI solution. This solution supports the evolving set of deployment scenarios for the Internet of Things (IoT) and Operational Technologies (OT). Integration of PKI is flexible and simple within the smart building ecosystem. Whether your devices are connected to the internet, on segregated networks, or air-gapped networks, the certificates are managed and updated for continuous trust and risk mitigation. The Johnson Controls partnership with DigiCert ensures that these smart building PKI scenarios are covered.

DigiCert's vigilance in addressing the current and future landscape of digital identities and cryptography, combined with the unmatched experience Johnson Controls delivers across all building systems, allows OpenBlue to provide and maintain trusted smart building solutions within an ever-changing cybersecurity landscape.

Visit www.johnsoncontrols.com for more information and follow @johnsoncontrols on social platforms.

The power behind **your mission**

Johnson Controls