

BACnet Europe Journal

Issue / Ausgabe 44

March / März 2026



BACnet
30 YEARS
BUILDING A SMARTER FUTURE



BACnet 30 years

The Development of
"Open Communication"

Der Werdegang zur
„Offenen Kommunikation“

6

Light + Building

BACnet at
Light + Building 2026

BACnet auf der
Light + Building 2026

30

Solutions

The One – Cutting-Edge
Building Automation

„The One“ – Zukunftsweisende
Gebäudeautomation

35

BIG-EU News

Successful CES Certificate
Exchange Summit Plugfest

Erfolgreiches CES Certificate
Exchange Summit Plugfest

83

The Practice-Oriented Life Cycle of BACnet/SC

Der praxisorientierte Lebenszyklus von BACnet/SC

The rapidly growing interconnectivity of building technology opens up new opportunities for attackers to manipulate and sabotage, for example, cooling systems for IT and OT rooms. BACnet Secure Connect (BACnet/SC) is a building brick for securing the associated complex automation systems and should be considered from an operational perspective throughout the entire building life cycle.

Die rasant wachsende Vernetzung von Gebäudetechnik eröffnet Angreifern neue Einfallstore zur Manipulation und Sabotage von bspw. Kälteanlagen für IT & OT-Räume. BACnet Secure Connect (BACnet/SC) ist ein Baustein für die Absicherung der damit verbundenen, komplexen Automatisierungssysteme und sollte vom Betrieb her, über den kompletten Gebäudelebenszyklus, mitgedacht werden.

Encrypted communication in building technology

The digital transformation of building technology (OT-Building) faces organisations and infrastructure operators with complex challenges in the area of cyber security (OT-Security). BACnet Secure Connect is developing into a crucial technology that systematically closes security gaps in building automation and enables encrypted communication for sensitive building technology.

The regulatory landscape is increasingly tightening the requirements for the protection of building technology. The NIS2 Directive and the BSIG require operators of critical infrastructures to implement risk management and comply with comprehensive security measures, while the Cyber Resilience Act (CRA) forces manufacturers of components that can communicate via networks to comply with technological security standards, such as encryption.

The technical implementation of encrypted communication is associated with challenges. Companies need a public key infrastructure for this or must expand the existing IT PKI for building OT. This requires professional certificate management to ensure compatibility with existing systems. Certificate management requires a precise strategy for the initial generation, distribution, revocation and regular renewal of cryptographic keys.

Life cycle of BACnet/SC – from requirement to certificate

BACnet/SC requires more than just a simple change-over from unencrypted to encrypted communication. The process starts with the future operator and user, who first define the basic security requirements. What are our specific security objectives (protection needs assessment)? Which protection mechanisms need to be implemented? These strategic considerations form the foundation for all further steps regarding organisational and technical protective measures.

Building automation specialists translate these conceptual requirements into a concrete system or network architecture. They develop a comprehensive certificate strategy that takes into account not only technical implementation but also long-term security aspects. How often are certificates exchanged? How are they managed? These questions are answered iteratively with the operator.

Device manufacturers play an important role in the life cycle, as they already integrate initial security certificates into their BACnet/SC-enabled devices at the factory. These pre-installed certificates create an initial basic level of trust and enable secure transfer and integrity checks during commissioning.

On site, the contractors/integrators take over further security measures. They integrate the devices into the PKI infrastructure and, in consultation with the operator, replace the initial certificates with organisation-specific certificates. This enables the consistent and traceable integration of network-compatible building technology into a secure building automation system.

The operational phase requires dynamic certificate management. This is not just a one-off issue, but a continuous process: certificates are regularly checked, replaced if necessary and compromised certificates

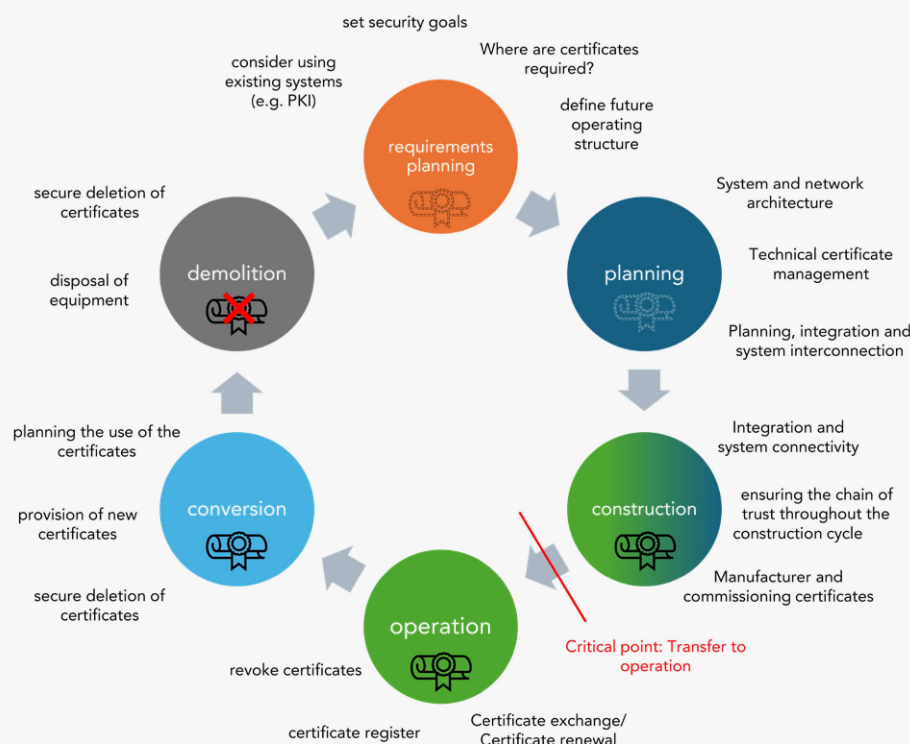


Figure 1 Certificates in the building life cycle

Abbildung 1 Zertifikate im Gebäudelebenszyklus © M&P Braunschweig



Figure 2 Proof of Concept: Hands-on OT security from M&P Braunschweig
Abbildung 2 Proof of Concept: OT-Security zum Anfassen der M&P Braunschweig © M&P Braunschweig

are immediately withdrawn. To achieve this, existing structures must be broken down and expanded in order to ensure continuous cyber security.

Practical implementation of BACnet/SC in M&P proof of concept

The theoretical feasibility of BACnet/SC has been promised by the BACnet standard and various manufacturers who have BACnet/SC-compatible devices in their portfolios. However, there are still very few projects, buildings or facilities in which BACnet/SC has been fundamentally implemented, let alone thought through and implemented across the entire life cycle.

True to the motto 'OT security: just do it', M&P's life cycle-oriented planning and consulting concepts were implemented in the form of a proof of concept for secure building automation systems in accordance with the 'state of the art'. From the management to the field level, everything has been thoroughly thought through, built to be hands-on and tested ('security by design').

This also includes encrypted communication using BACnet/SC, regardless of whether it is a new system, integration or migration in existing systems (BACnet/IP to BACnet/SC). The system architecture consisting of BACnet/SC hubs and failover hubs, both physical and virtual, as well as specific BACnet/IP/SC routers, enables all scenarios and demonstrates

the functionality of BACnet/SC across manufacturers.

A particular highlight is the implementation of a multi-level public key infrastructure (PKI) from a German manufacturer as a critical component for the various protection areas of a GA system. The PKI enables dynamic certificate management throughout the entire life cycle. This also includes automated certificate exchange via BACnet, possible from protocol revision 24, which is currently in the PoC pilot phase. The results currently emerging are promising.

The success of BACnet/SC as a protective measure for HVAC systems depends on a holistic concept. OT security must be considered from the outset – from initial requirements planning to daily system monitoring. This requires clear responsibilities, well-thought-out system architectures, continuous training and a high degree of adaptability on the part of all those involved.

Verschlüsselte Kommunikation in der Gebäudetechnik

Die digitale Transformation der Gebäudetechnik (OT-Building) stellt Organisationen und Infrastrukturbetreiber vor komplexe Herausforderungen im Bereich der Cybersicherheit (OT-Security). BACnet Secure Connect entwickelt sich dabei zu einer entscheidenden Technologie, die Sicherheitslücken in der Gebäudeautomation systematisch schließt und eine verschlüsselte Kommunikation für sensible Gebäudetechnik ermöglicht.

Die regulatorische Landschaft verschärft zusehends die Anforderungen an den Schutz der Gebäudetechnik. Die NIS2-Richtlinie und das BSI-Gesetz verpflichtet Betreiber kritischer Infrastrukturen zur Durchführung eines Risikomanagements und Erfüllung umfassender Sicherheitsmaßnahmen, während der Cyber Resilience Act (CRA) Hersteller von Komponenten, welche über Netzwerke kommunizieren können, zur Einhaltung technologischer Sicherheitsstandards, wie z.B. Verschlüsselung, zwingt.

Die technische Umsetzung verschlüsselter Kommunikation ist mit Herausforderungen verbunden. Unternehmen benötigen dafür eine Public-Key-Infrastruktur oder müssen die bestehende IT-PKI für die Building-OT erweitern. Dazu bedarf es eines professionellen Zertifikatsmanagements, um die Kompatibilität mit bestehenden Systemen zu gewährleisten. Das Zertifikatsmanagement erfordert eine präzise Strategie für die initiale Generierung, Verteilung, Revokation und regelmäßige Erneuerung kryptografischer Schlüssel.

Lebenszyklus von BACnet/SC – von der Anforderung bis zum Zertifikat

BACnet/SC fordert mehr als nur das einfache „Umschalten“ von unverschlüsselter auf verschlüsselte Kommunikation. Der Prozess startet beim zukünftigen Betreiber und Nutzer, die zunächst die grundlegenden Sicherheitsanforderungen definieren. Was sind unsere spezifischen Sicherheitsziele (Schutzbedarfsfeststellung)? Welche Schutzmechanismen müssen implementiert werden? Diese strategischen Überlegungen bilden das Fundament für alle weiteren Schritte hinsichtlich der organisatorischen und technischen Schutzmaßnahmen.

Die Fachplanung Gebäudeautomation übersetzt diese konzeptionellen Anforderungen in eine konkrete System- bzw. Netzwerkarchitektur. Sie entwickelt eine umfassende Zertifikatsstrategie, die nicht nur die technische Umsetzung, sondern auch langfristige Sicherheitsaspekte berücksichtigt. Wie häufig werden Zertifikate ausgetauscht? Wie werden sie verwaltet? Diese Fragen werden iterativ mit dem Betreiber beantwortet.

Die Gerätehersteller spielen eine wichtige Rolle im Lebenszyklus, da sie bereits werkseitig initiale Sicherheitszertifikate in ihre BACnet/SC-fähigen Geräte integrieren. Diese vorinstallierten Zertifikate schaffen eine erste grundlegende Vertrauensebene und ermöglichen eine sichere Übernahme und Integritätsprüfung bei der Inbetriebnahme.

Auf der Baustelle übernehmen die Ausführenden/Integratoren die weitere Absicherung. Sie binden die Geräte in die PKI-Infrastruktur ein und tauschen, in Abstimmung mit dem Betreiber, die initialen Zertifikate mit organisationsspezifischen Zertifikaten aus. Dies ermöglicht eine durchgängig nachvollziehbare

Integration von netzwerkfähiger Gebäudetechnik in ein sicheres Gebäudeautomationssystem.

Die Betriebsphase erfordert ein dynamisches Zertifikatsmanagement. Es geht nicht nur um die einmalige Ausgabe, sondern um einen kontinuierlichen Prozess: Zertifikate werden regelmäßig überprüft, bei Bedarf ausgetauscht und kompromittierte Zertifikate umgehend zurückgezogen. Hierfür müssen bestehende Strukturen aufgebrochen und erweitert werden, um die Cybersicherheit kontinuierlich gewährleisten zu können.

Praktische Umsetzung von BACnet/SC im M&P-Proof-of-Concept

Eine theoretische Machbarkeit von BACnet/SC wird durch den BACnet-Standard sowie diverse Hersteller, welche BACnet/SC fähige Geräte im Portfolio haben versprochen. Bisher gibt es allerdings noch wenige Projekte bzw. Gebäude oder Anlagen, in welchen BACnet/SC grundlegend umgesetzt, geschweige denn über den kompletten Lebenszyklus durchdacht und implementiert wurden.

Getreu dem Motto „OT-Security: Einfach machen“ wurden die lebenszyklusorientierten Planungs- und Beratungskonzepte der M&P in Form eines Proof of Con-

cept für sichere Gebäudeautomationssysteme nach dem „Stand der Technik“ umgesetzt. Von der Management- bis zur Feldebene, alles sicher durchdacht, zum Anfahren und Testen errichtet („security by design“).

Dies beinhaltet auch die verschlüsselte Kommunikation mittels BACnet/SC, egal ob als neu zu errichtendes System, Integration oder Migration im Bestand (BACnet/IP zu BACnet/SC). Die Systemarchitektur aus BACnet/SC Hubs und Failover-Hubs, physikalisch und virtuell sowie spezifische BACnet/IP – /SC-Router ermöglicht hierbei alle Szenarien und zeigt die Funktionsfähigkeit von BACnet/SC herstellerübergreifend auf.

Besonderes Highlight ist die Umsetzung einer mehrstufigen Public Key Infrastructure (PKI) von einem deutschen Hersteller, als kritische Komponente, für die unter-

schiedlichen Schutzbereiche eines GA-Systems. Die PKI ermöglicht ein dynamisches Zertifikatsmanagement über den kompletten Lebenszyklus. Dies beinhaltet auch den automatisierten Zertifikatsaustausch über BACnet, möglich ab Protokollrevision 24, welcher sich aktuell im PoC in der Pilotphase befindet. Die sich aktuell abzeichnenden Ergebnisse sind vielversprechend.

Der Erfolg mit BACnet/SC, als Schutzmaßnahme für GA-Systeme hängt von einem ganzheitlichen Konzept ab. Die OT-Security muss von Anfang an mitgedacht werden – von der initialen Bedarfsplanung bis zur täglichen Systemüberwachung. Dies erfordert klare Verantwortlichkeiten, durchdachte Systemarchitekturen, kontinuierliche Schulungen und eine hohe Anpassungsfähigkeit aller Beteiligten.



Nicolas Fouquet-Braun

Expert OT-Security Building Automation
M&P Braunschweig GmbH

nicolas.fouquetbraun@mp-gruppe.de | www.mp-gruppe.de



IHR QUALIFIZIERTER NIAGARA 4 TRAININGSPARTNER



GET CERTIFIED!

Individuelle Trainings sowie das Niagara 4 TCP Zertifikat

Lassen Sie sich jetzt bei OAS zertifizieren und starten Sie Ihre Niagara Karriere. Wir bieten Schulungen zum Niagara 4 Technical Certification Program und individuelle Kundentrainings in Deutsch und Englisch an. Das offizielle fünftägige Niagara 4 Training deckt alle Aspekte des Niagara Framework® ab. Die Teilnehmer nehmen an Übungen, Demonstrationen und einer Reihe praktischer Schritt-für-Schritt-Workshops teil.

Get certified with OAS now and start your Niagara career. We offer trainings for the Niagara 4 Technical Certification Program and individual customer trainings in English and German. The official five-day Niagara 4 training covers all aspects of the Niagara Framework®. Participants take part in exercises, demonstrations and a series of practical step-by-step workshops.



04.05. - 08.05.2026



TRIDIUM authorised distributor

OAS Open Automation Systems
www.openautomationsystems.store