ASHRAE BACnet ACADEMY EUROPE

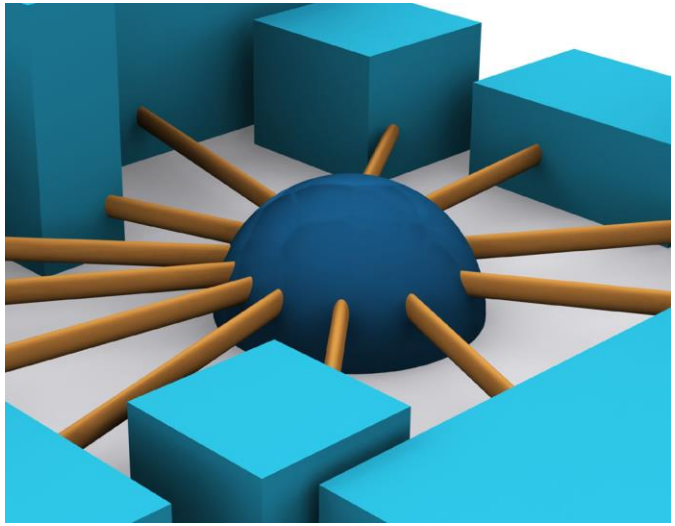
ASHRAE BACnet INTEREST GROUP EUROPE

Building Automation via BACnet

Willkommen

BACnet/SC Secure Connect

Eine neue BACnet-Option für sichere Gebäudeautomation



Rüdiger Schröder - Zentrales Infrastruktur Management - Fraport AG
Stefan Thomanek - Integriertes Facility Management - Fraport AG

Mit Unterstützung von Hans Symanczik, BIG EU Office

Warum BACnet/SC?

- **IT-Anforderungen**
  - Zertifikate
- **Sicherheitsanforderungen**
  - TLS
- **Kommunikationsanforderungen**
  - Cloud
  - VPN Abhängigkeit

Warum BACnet/SC?

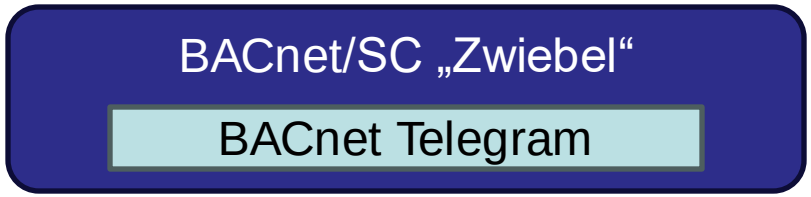
Ein BACnet/IP Netz ist nur so sicher, wie die am ***wenigsten*** *geschützte Netzwerkdose...*

BACnet/SC?

- **BACnet/SC bietet eine hochentwickelte Netzwerksicherheitslösung, die von der IT-Gemeinschaft weitgehend akzeptierte Standards verwendet.**

BACnet/SC?

- **BACnet/SC bietet eine hochentwickelte Netzwerksicherheitslösung, die von der IT-Gemeinschaft weitgehend akzeptierte Standards verwendet.**



BACnet/SC?

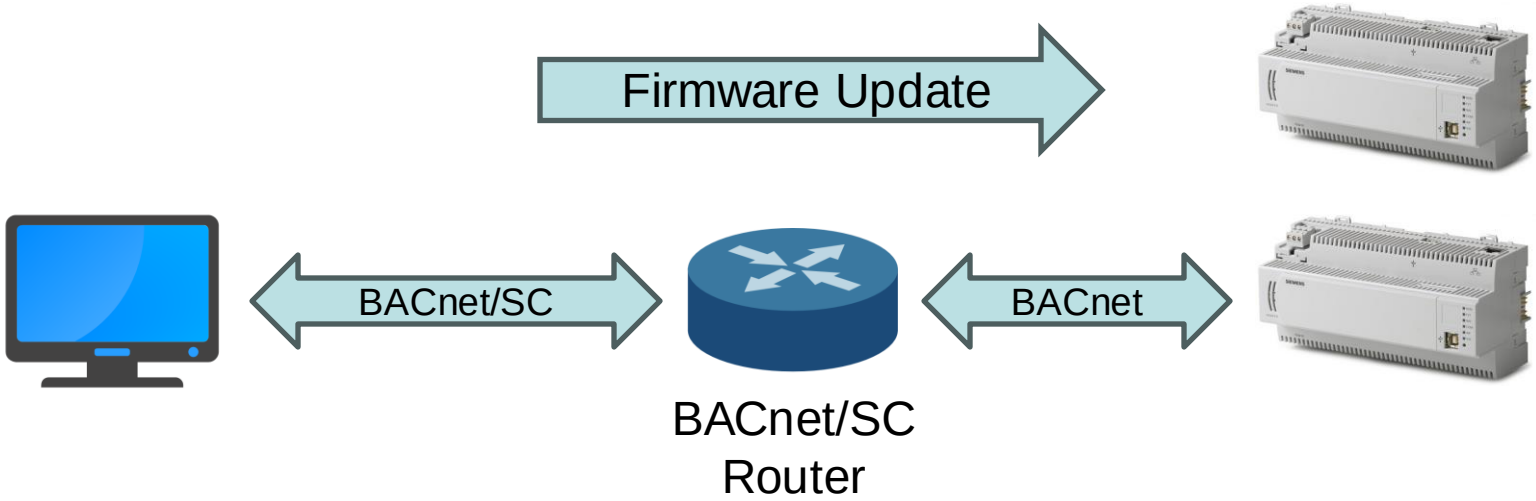
- BACnet/SC bietet eine hochentwickelte Netzwerksicherheitslösung, die von der IT-Gemeinschaft weitgehend akzeptierte Standards verwendet.
- BACnet/SC macht statische IP-Adressen überflüssig.
- BACnet/SC ist nicht abhängig von Network Broadcast Messaging.
- **BACnet/SC eliminiert BACnet/IP Broadcast Management Devices (BBMDs) und deren Konfiguration und ist tolerant gegenüber Änderungen der Netztopologie.**
- **BACnet/SC funktioniert problemlos mit Firewall-Geräten, die in der IT-Infrastruktur üblich sind.**

BACnet/SC?

- BACnet/SC bietet eine hochentwickelte Netzwerksicherheitslösung, die von der IT-Gemeinschaft weitgehend akzeptierte Standards verwendet.
- **BACnet/SC macht statische IP-Adressen überflüssig.**
- **BACnet/SC ist nicht abhängig von Network Broadcast Messaging.**
- BACnet/SC eliminiert BACnet/IP Broadcast Management Devices (BBMDs) und deren Konfiguration und ist tolerant gegenüber Änderungen der Netztopologie.
- BACnet/SC funktioniert problemlos mit Firewall-Geräten, die in der IT-Infrastruktur üblich sind.

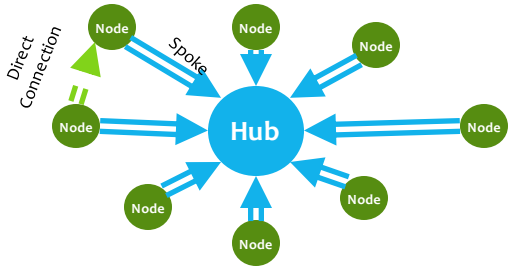
BACnet/SC!

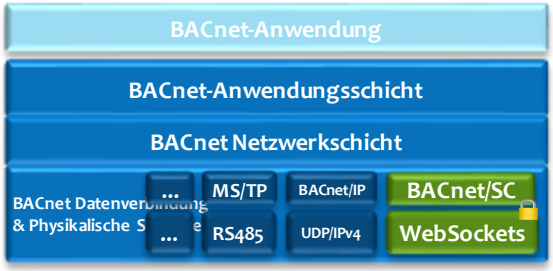
Alles Umstellen; Oder?



BACnet/SC Secure Connect

Überblick und Einführung

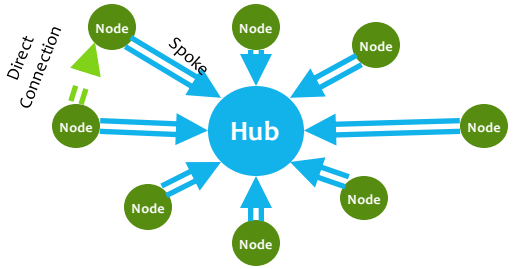


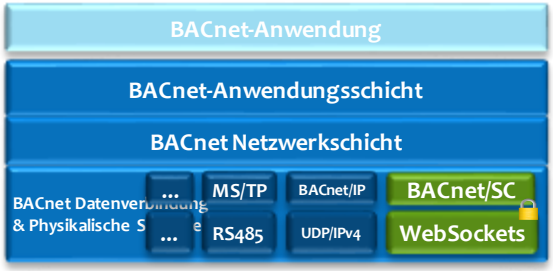


- **Neue Virtual Datalink Option für BACnet**
- **Virtuelles Hub-and-Spoke-Modell**
- **Failover Hub Konzept**
- **Direktkommunikation optional**
- **Gesicherte Verbindungen durch WebSockets über TLS V1.3**
- **Volle Kompatibilität mit allen anderen BACnet Datalink Optionen (BACnet/IP, BACnet/IPv6, BACnet/MSTP, ...)**
- **Anwendungen und Integrationen sind nicht betroffen.**
- **Unterstützung für jede BACnet-Protokollversion**

BACnet/SC Secure Connect

Überblick und Einführung

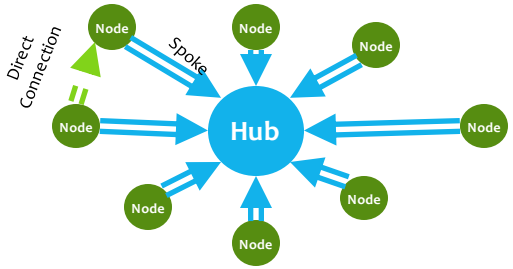


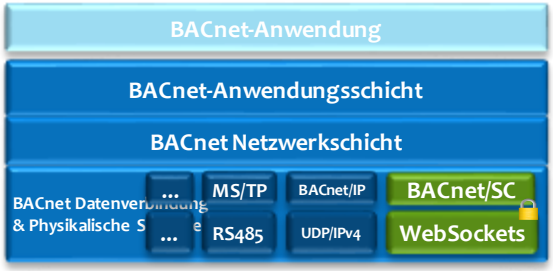


- **Neue Virtual Datalink Option für BACnet**
- Virtuelles Hub-and-Spoke-Modell
- Failover Hub Konzept
- Direktkommunikation optional
- Gesicherte Verbindungen durch WebSockets über TLS V1.3
- Volle Kompatibilität mit allen anderen BACnet Datalink Optionen (BACnet/IP, BACnet/IPv6, BACnet/MSTP, ...)
- Anwendungen und Integrationen sind nicht betroffen.
- Unterstützung für jede BACnet-Protokollversion

BACnet/SC Secure Connect

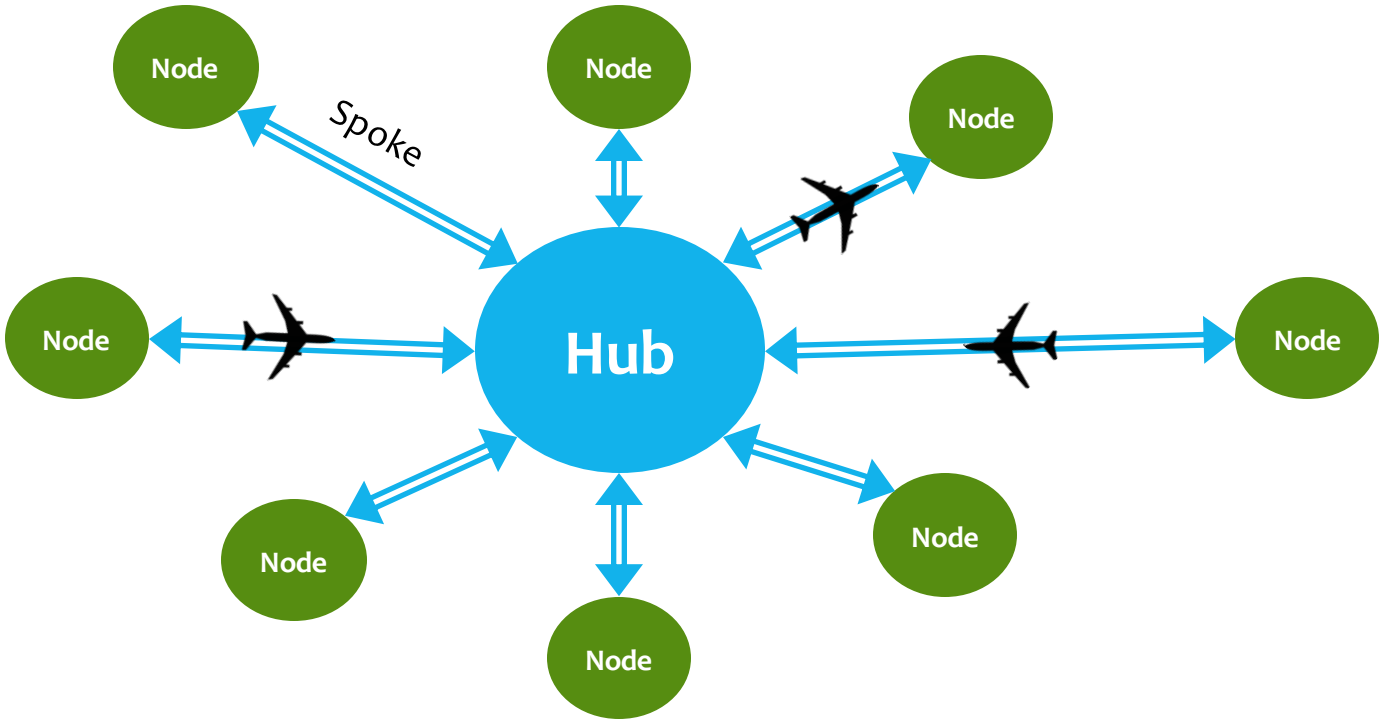
Überblick und Einführung





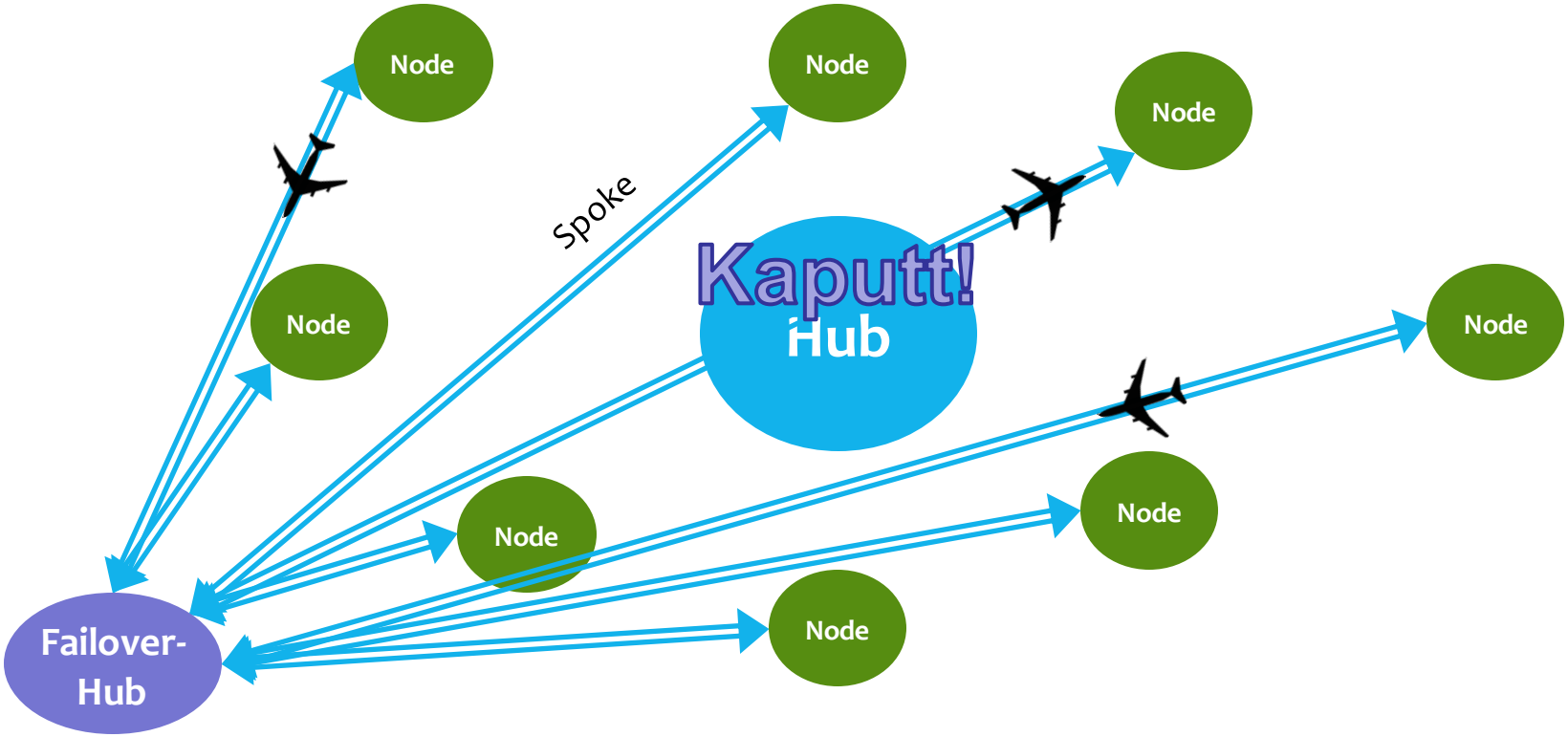
- Neue Virtual Datalink Option für BACnet
- **Virtuelles Hub-and-Spoke-Modell**
- Failover Hub Konzept
- Direktkommunikation optional
- Gesicherte Verbindungen durch WebSockets über TLS V1.3
- Volle Kompatibilität mit allen anderen BACnet Datalink Optionen (BACnet/IP, BACnet/IPv6, BACnet/MSTP, ...)
- Anwendungen und Integrationen sind nicht betroffen.
- Unterstützung für jede BACnet-Protokollversion

Virtuelles Hub-and-Spoke-Modell

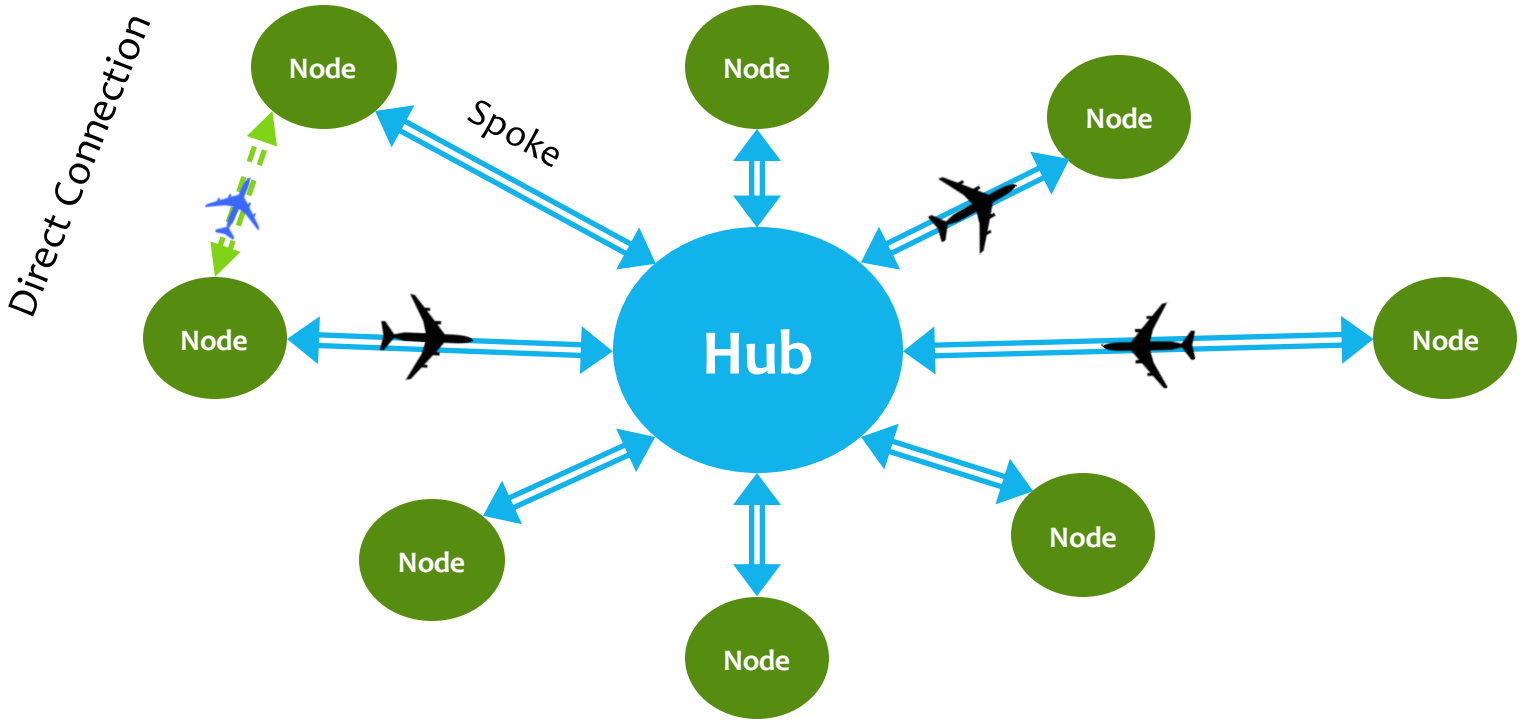


Virtuelles Hub-and-Spoke-Modell

Failover-Hub

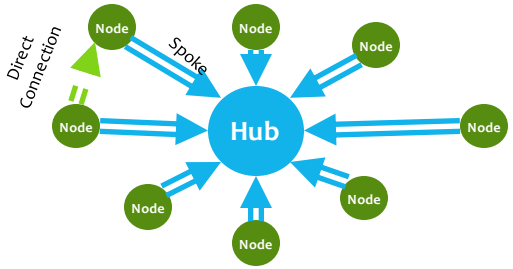


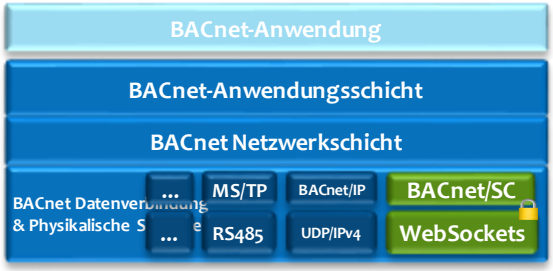
Virtuelles Hub-and-Spoke-Modell
optionale Direktkommunikation (Charter Flüge)



BACnet/SC Secure Connect

Überblick und Einführung

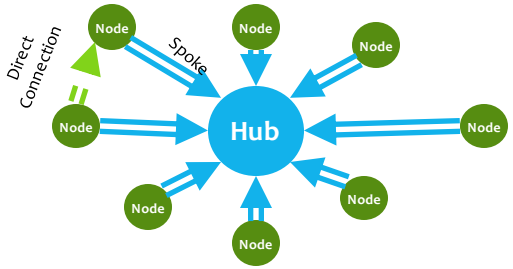


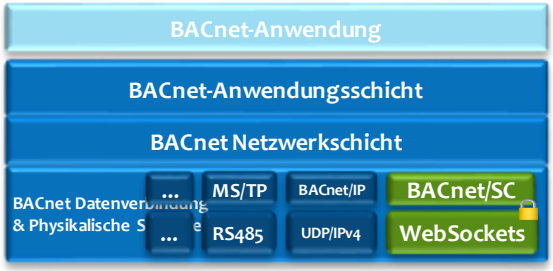


- Neue Virtual Datalink Option für BACnet
- Virtuelles Hub-and-Spoke-Modell
- Failover Hub Konzept
- Direktkommunikation optional
- **Gesicherte Verbindungen durch WebSockets über TLS V1.3**
- Volle Kompatibilität mit allen anderen BACnet Datalink Optionen (BACnet/IP, BACnet/IPv6, BACnet/MSTP, ...)
- Anwendungen und Integrationen sind nicht betroffen.
- Unterstützung für jede BACnet-Protokollversion

BACnet/SC Secure Connect

Überblick und Einführung

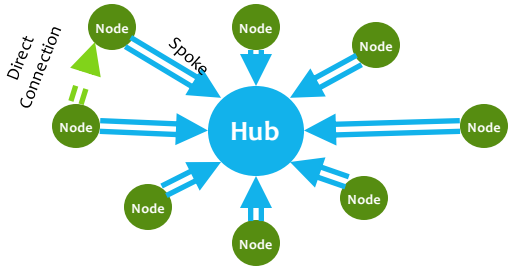


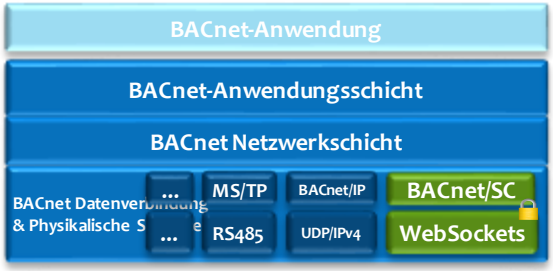


- Neue Virtual Datalink Option für BACnet
- Virtuelles Hub-and-Spoke-Modell
- Failover Hub Konzept
- Direktkommunikation optional
- Gesicherte Verbindungen durch WebSockets über TLS V1.3
- **Volle Kompatibilität mit allen anderen BACnet Datalink Optionen (BACnet/IP, BACnet/IPv6, BACnet/MSTP, ...)**
- Anwendungen und Integrationen sind nicht betroffen.
- Unterstützung für jede BACnet-Protokollversion

BACnet/SC Secure Connect

Überblick und Einführung

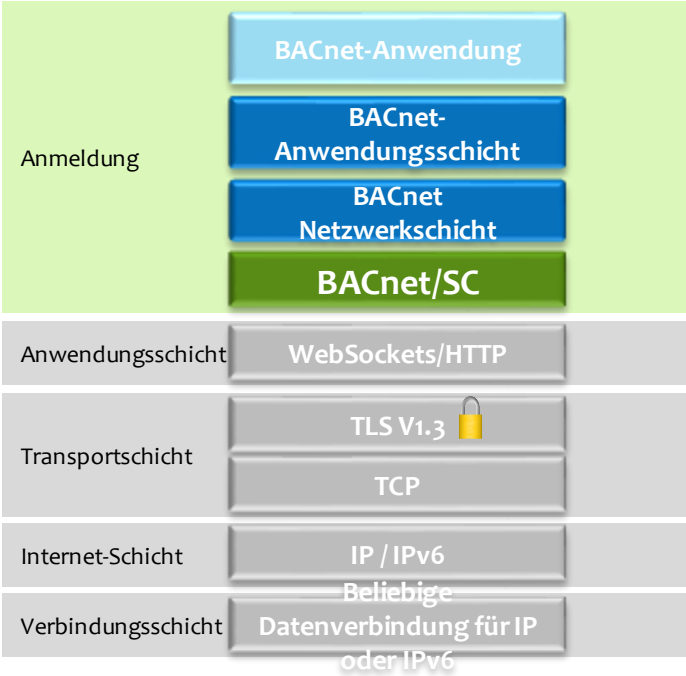




- Neue Virtual Datalink Option für BACnet
- Virtuelles Hub-and-Spoke-Modell
- Failover Hub Konzept
- Direktkommunikation optional
- Gesicherte Verbindungen durch WebSockets über TLS V1.3
- Volle Kompatibilität mit allen anderen BACnet Datalink Optionen (BACnet/IP, BACnet/IPv6, BACnet/MSTP, ...)
- **Anwendungen und Integrationen sind nicht betroffen.**
- **Unterstützung für jede BACnet-Protokollversion**

BACnet sicher verbinden

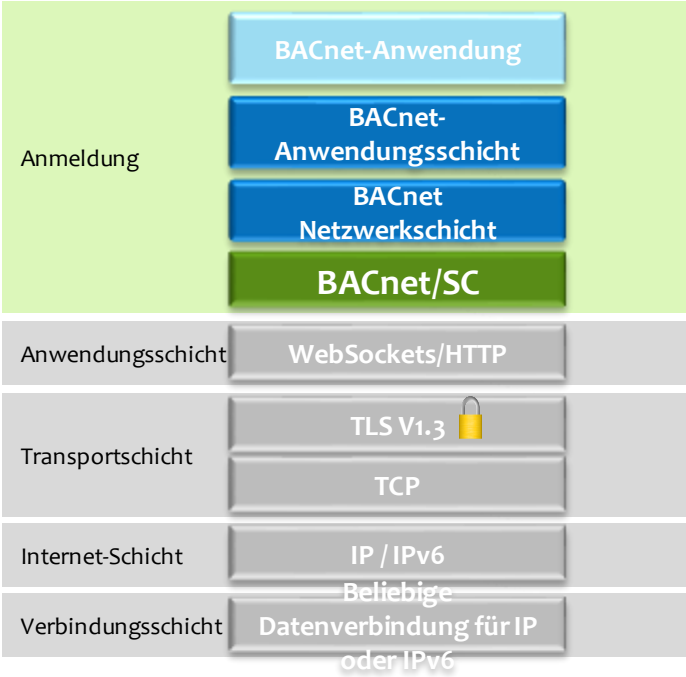
IT-Konvergenz



- **WebSockets werden durch HTTP-Upgrades eingerichtet**
- **Verwendung von bekannten HTTP(S)-Ports**
- **Nutzung der HTTP-bezogenen Konfiguration von IT-Umgebungen**
- **Gesichert durch Verwendung von TLS und X.509-Zertifikaten**
- **Die Verwendung von TCP verbessert die Unterstützung von IT-konfigurierten Firewalls, NAT-Boxen und anderen Middlebox-Geräten.**
- **Host-Identifizierung durch DNS-Namen ermöglicht dynamische IP-Adressierung und Unabhängigkeit von der IP-Netzstruktur**
- **Agnostisch gegenüber IP-Version. Kann über IPv4 und IPv6 laufen**
- **Andere TLS-Versionen als V1.3 ermöglichten die Kompatibilität mit rückständigen IT-Sicherheitsanwendungen und -Richtlinien**

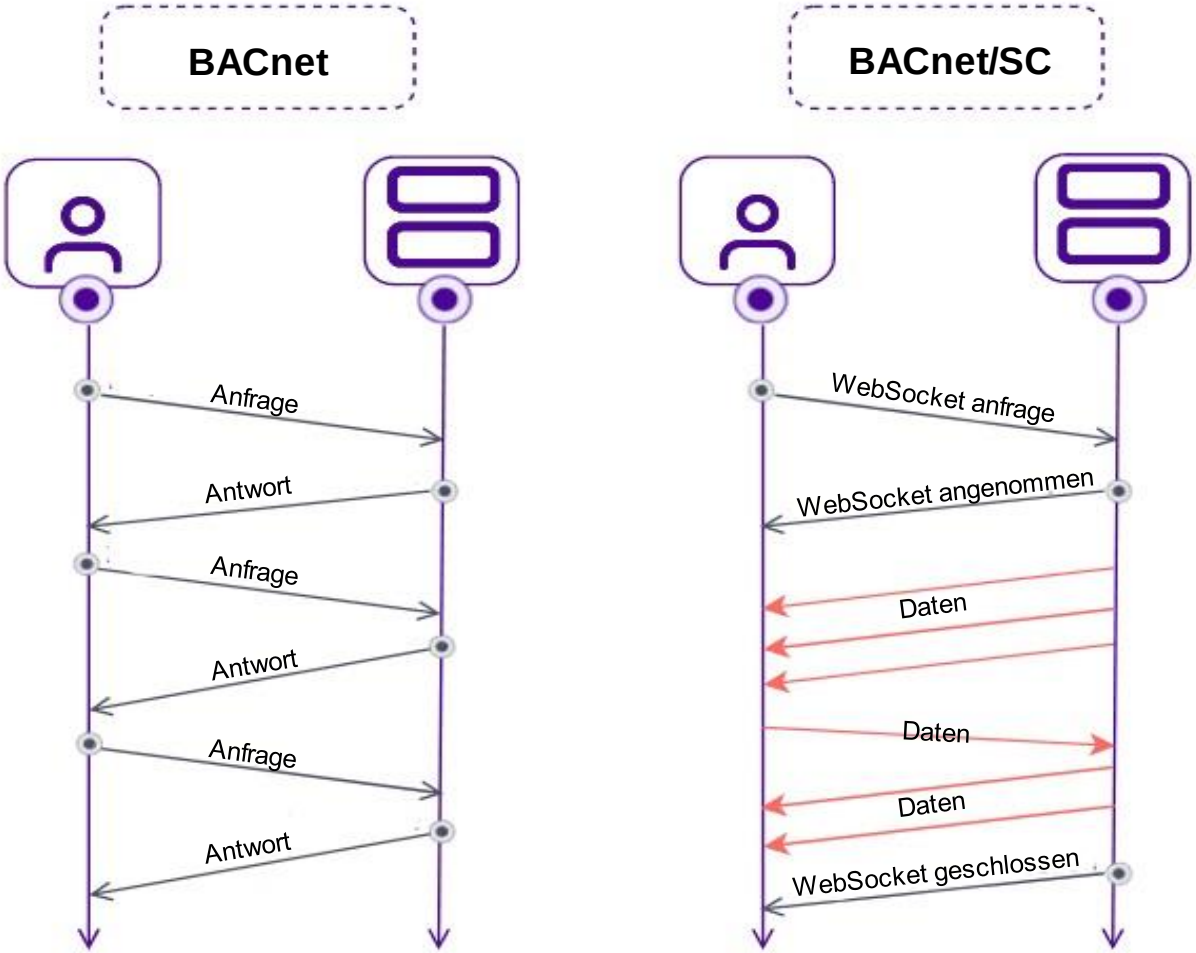
BACnet sicher verbinden

IT-Konvergenz



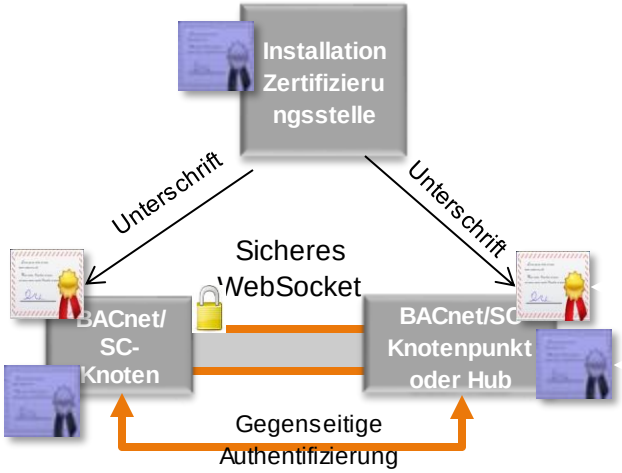
- **WebSockets werden durch HTTP-Upgrades eingerichtet**
- **Verwendung von bekannten HTTP(S)-Ports**
- **Nutzung der HTTP-bezogenen Konfiguration von IT-Umgebungen**
- Gesichert durch Verwendung von TLS und X.509-Zertifikaten
- Die Verwendung von TCP verbessert die Unterstützung von IT-konfigurierten Firewalls, NAT-Boxen und anderen Middlebox-Geräten.
- Host-Identifizierung durch DNS-Namen ermöglicht dynamische IP-Adressierung und Unabhängigkeit von der IP-Netzstruktur
- Agnostisch gegenüber IP-Version. Kann über IPv4 und IPv6 laufen
- Andere TLS-Versionen als V1.3 ermöglichten die Kompatibilität mit rückständigen IT-Sicherheitsanwendungen und -Richtlinien

Building Automation via BACnet



BACnet sicher verbinden

Absicherung von BACnet mit TLS V1.3

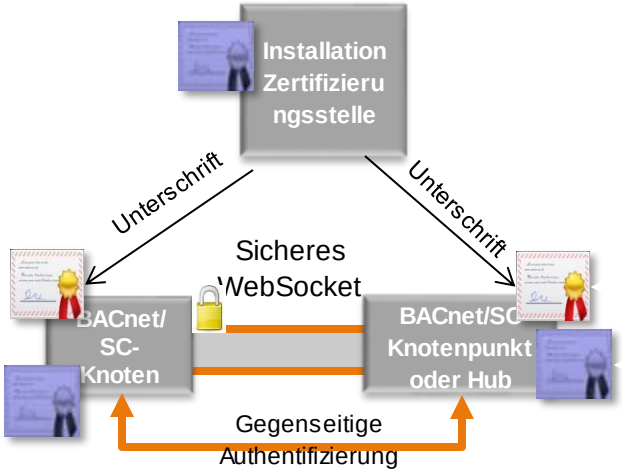


Knoten legen ein von einer vertrauenswürdigen CA signiertes Betriebszertifikat vor

- **TLS V1.3 bietet starke Cybersicherheit für die BACnet-Kommunikation**
- **X.509-Zertifikate und PKI**
- **Vertrauensbildung auf der Grundlage der für die Installation akzeptierten Zertifizierungsstellen (CA) für die Installation**
- **Gerätebetriebszertifikate, die von einer dieser CAs signiert sind**
- **Die gegenseitige Authentifizierung authentifiziert den WebSocket-Peer unabhängig von seiner Funktion.**
  Z.B. Hub authentifiziert auch das Gerät
- **Die Zertifikatsparameter werden durch die Installation bestimmt, nicht durch einen Produktanbieter.**
- **Andere TLS-Versionen, die für bestimmte IT-Umgebungen und Richtlinien zulässig sind**

BACnet sicher verbinden

Absicherung von BACnet mit TLS V1.3

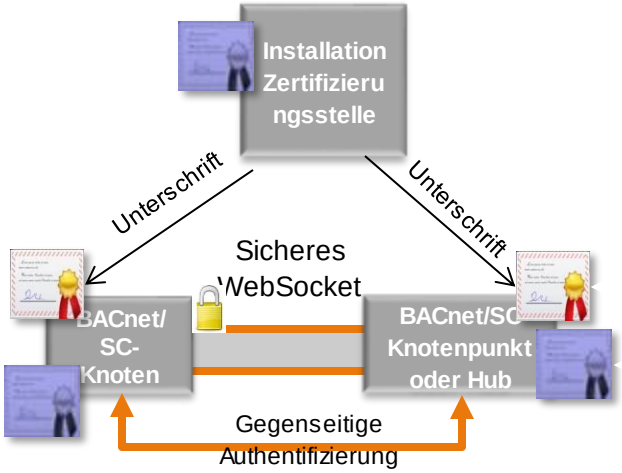


Knoten legen ein von einer vertrauenswürdigen CA signiertes Betriebszertifikat vor

- **TLS V1.3 bietet starke Cybersicherheit für die BACnet-Kommunikation**
- X.509-Zertifikate und PKI
- Vertrauensbildung auf der Grundlage der für die Installation akzeptierten Zertifizierungsstellen (CA) für die Installation
- Gerätebetriebszertifikate, die von einer dieser CAs signiert sind
- Die gegenseitige Authentifizierung authentifiziert den WebSocket-Peer unabhängig von seiner Funktion.
  Z.B. Hub authentifiziert auch das Gerät
- Die Zertifikatsparameter werden durch die Installation bestimmt, nicht durch einen Produktanbieter.
- Andere TLS-Versionen, die für bestimmte IT-Umgebungen und Richtlinien zulässig sind

BACnet sicher verbinden

Absicherung von BACnet mit TLS V1.3

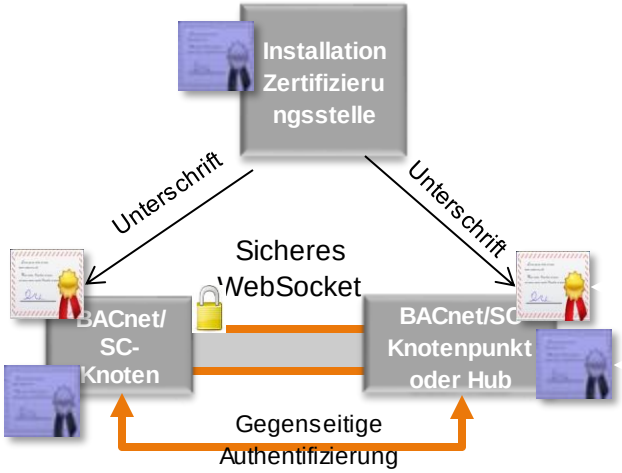


Knoten legen ein von einer vertrauenswürdigen CA signiertes Betriebszertifikat vor

- TLS V1.3 bietet starke Cybersicherheit für die BACnet-Kommunikation
- **X.509-Zertifikate und PKI**
- Vertrauensbildung auf der Grundlage der für die Installation akzeptierten Zertifizierungsstellen (CA) für die Installation
- Gerätebetriebszertifikate, die von einer dieser CAs signiert sind
- Die gegenseitige Authentifizierung authentifiziert den WebSocket-Peer unabhängig von seiner Funktion.
  Z.B. Hub authentifiziert auch das Gerät
- Die Zertifikatsparameter werden durch die Installation bestimmt, nicht durch einen Produktanbieter.
- Andere TLS-Versionen, die für bestimmte IT-Umgebungen und Richtlinien zulässig sind

BACnet sicher verbinden

Absicherung von BACnet mit TLS V1.3

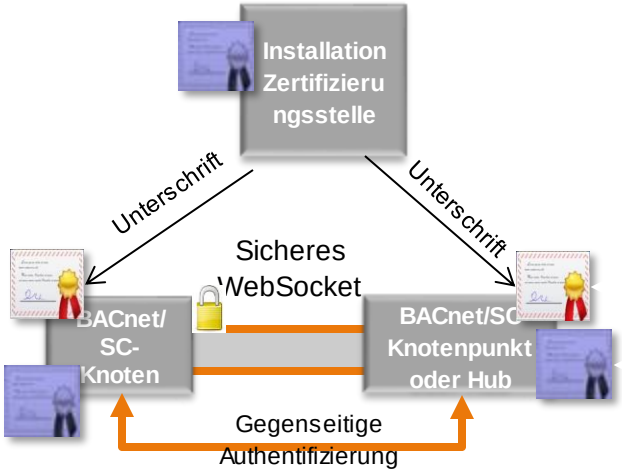


Knoten legen ein von einer vertrauenswürdigen CA signiertes Betriebszertifikat vor

- TLS V1.3 bietet starke Cybersicherheit für die BACnet-Kommunikation
- X.509-**Zertifikate** und PKI
- Vertrauensbildung auf der Grundlage der für die Installation akzeptierten Zertifizierungsstellen (CA) für die Installation
- **Gerätebetriebszertifikate**, die von einer dieser CAs signiert sind
- Die gegenseitige Authentifizierung authentifiziert den WebSocket-Peer unabhängig von seiner Funktion.
  Z.B. Hub authentifiziert auch das Gerät
- Die **Zertifikatsparameter** werden durch die Installation bestimmt, nicht durch einen Produktanbieter.
- Andere TLS-Versionen, die für bestimmte IT-Umgebungen und Richtlinien zulässig sind

BACnet sicher verbinden

Absicherung von BACnet mit TLS V1.3

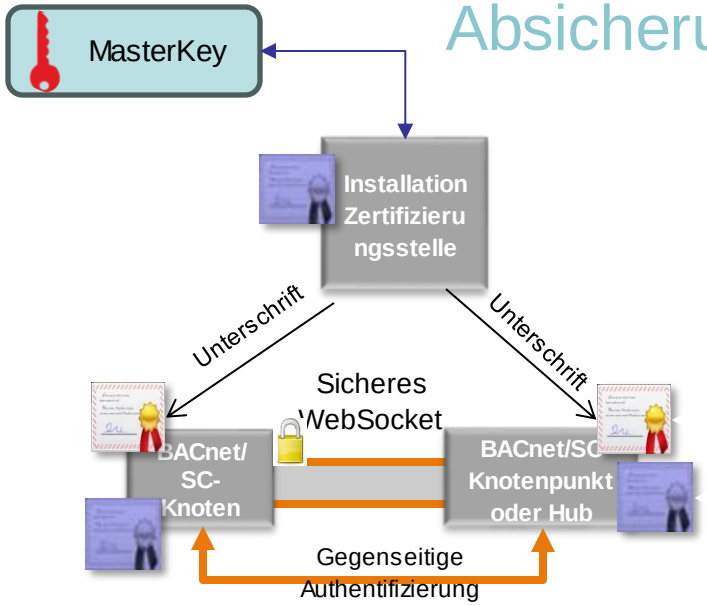


Knoten legen ein von einer vertrauenswürdigen CA signiertes Betriebszertifikat vor

- TLS V1.3 bietet starke Cybersicherheit für die BACnet-Kommunikation
- X.509-Zertifikate und PKI
- **Vertrauensbildung auf der Grundlage der für die Installation akzeptierten Zertifizierungsstellen (CA) für die Installation**
- **Gerätebetriebszertifikate, die von einer dieser CAs signiert sind**
- **Die gegenseitige Authentifizierung authentifiziert den WebSocket-Peer unabhängig von seiner Funktion.**
  Z.B. Hub authentifiziert auch das Gerät
- Die Zertifikatsparameter werden durch die Installation bestimmt, nicht durch einen Produktanbieter.
- Andere TLS-Versionen, die für bestimmte IT-Umgebungen und Richtlinien zulässig sind

BACnet sicher verbinden

Absicherung von BACnet mit TLS V1.3

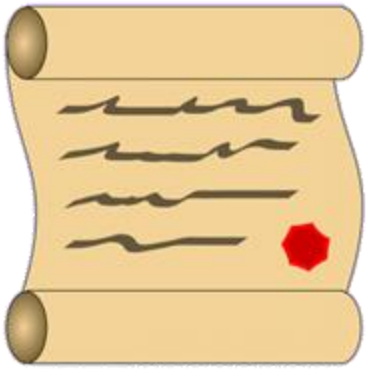


Knoten legen ein von einer vertrauenswürdigen CA signiertes Betriebszertifikat vor

- **Der MasterKey ist der Generalschlüssel für das BACnet/SC Netzwerk.**
- **Geht dieser Verloren, oder gelangt in die Hände dritter, müssen alle Zertifikate der Installation erneuert werden!**

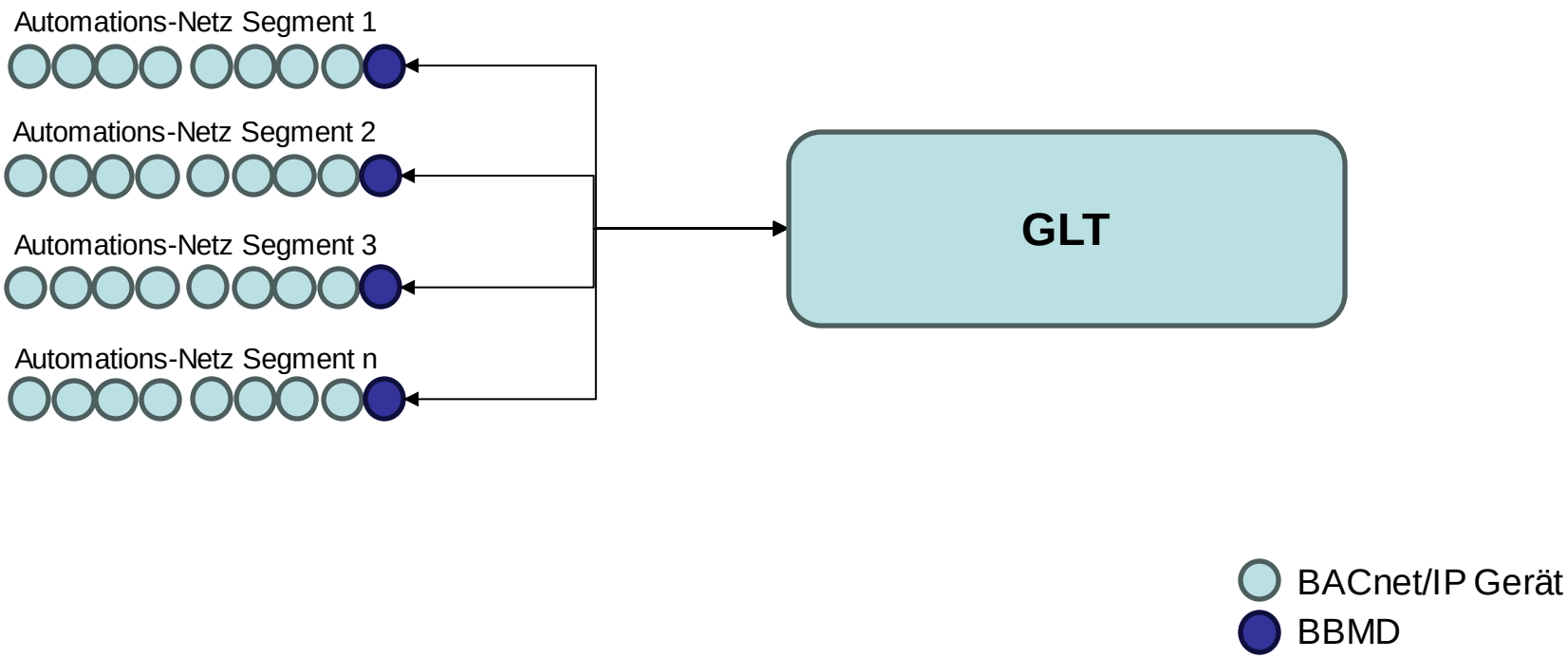
BACnet sicher verbinden

Zertifikatsparameter



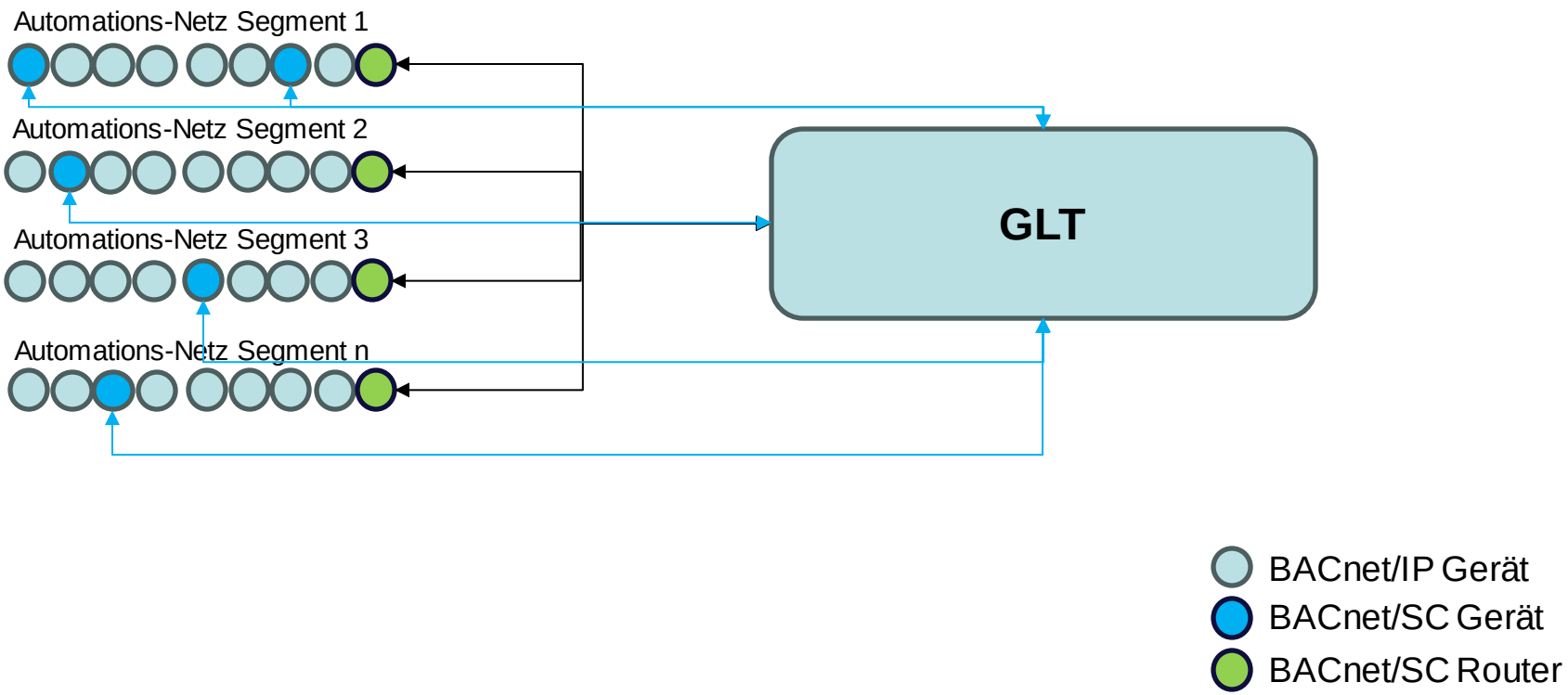
- **Gültigkeitsdauer der Zertifikate**
- **Verschlüsselungssuite(n) und Parameter, die verwendet werden**
- **Zu verwendende Kennzeichnungen und Namen**
- **Zu verwendende Domänennamen**
- **Ggf. weitere X.509-Parameter**

So viele Geräte zu tauschen…

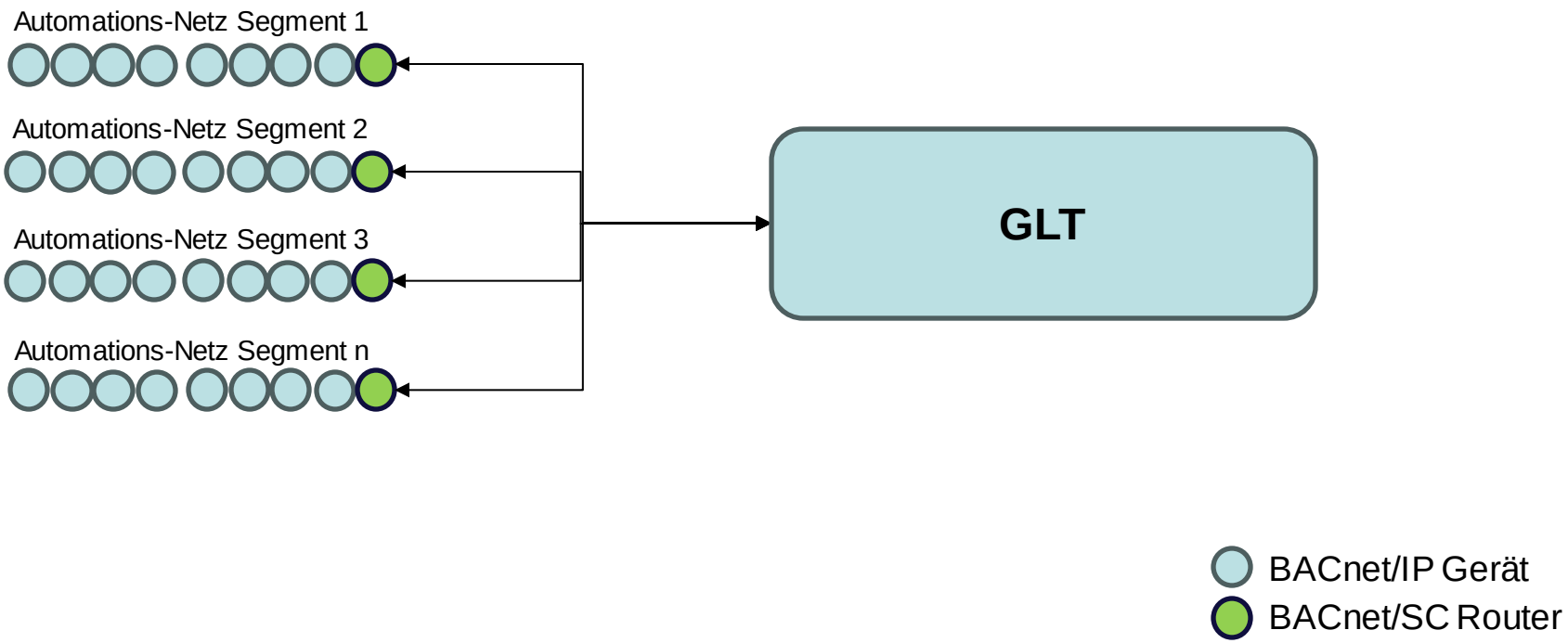


So viele Geräte zu tauschen…Oder?

Auch gemischt!



So viele Geräte zu tauschen…Oder?



Danke für Ihre Aufmerksamkeit!

Rüdiger Schröder r.schroeder@fraport.de
Stefan Thomanek s.thomanek@fraport.de