Seminar 45 – BACnet Secure Connect

What You Need to Know!

Part II

IT Security and Deployment

Bernhard Isler
Member SSPC 135 (BACnet)
Siemens Switzerland Ltd
bernhard.isler@siemens.com

ORLANDO 2020 WINTER CONFERENCE AND AHR EXPO

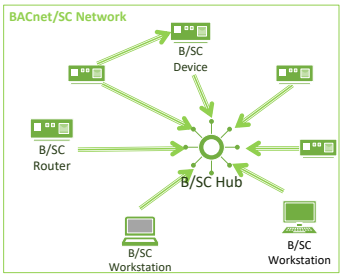
Agenda

- Cyber Security in BACnet/SC
- PKI, CA, Certificates
- Specification of BACnet/SC incl. Security
- Setup and Maintenance of Security
- Security Lifecycle and Roles
- Outlook
- Conclusions

Learning Objectives

- Understand what is BACnet/SC
- Appreciate some of the possible BACnet/SC network topologies
- Understand the requirements to specify, implement and maintain a system using BACnet/SC.
- Appreciate the underlying security inherent in BACnet/SC and what the BAS professional will need to know to successfully maintain the system
- Understand the cyber security concepts in BACnet/SC and what the BAS professional will need to know to successfully keep the system secured.
- Understand that cyber security for a BAS includes a substantial amount of organizational topics that must play with the technical security provided by BACnet/SC.

Cyber Security in BACnet/SC



Each Connection: WebSocket (RFC6455) over TLS V1.3 (RFC 8446)

Device (Client) → Hub (Server)

Hub Connection
Initiated by Device (Client)
Accepted by Hub (Server)

Device (Client) → Device (Server)

Optional **Direct Connection**:
Initiated by Device (Client)
Accepted by Device (Server)

Server and Client both also called a Connection Peer

Acknowledgements

Michael Osborne, Reliable Controls
Dave Robin, BSC Softworks
SSPC 135 BACnet Committee and its IT-WG
Siemens

Cyber Security in BACnet/SC

Client → Server

In BACnet/SC:
Each WebSocket/TLS Connection is Mutually Authenticated

Client "authenticates" Server

Client authenticates Server (as in Web)
- Public Server Operational Certificate signed by one of the accepted Certificate Authorities (CA)
- Server Certificate is valid and not expired
- Server owns Private Key to Server Certificate

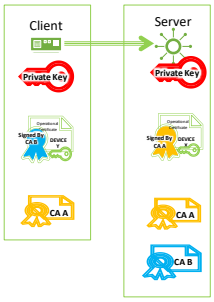
Client "authenticates" Server

Server authenticates Client (For authorization to connect)
- Public Client Operational Certificate signed by one of the accepted Certificate Authorities (CA)
- Client Certificate is valid and not expired
- Client owns Private Key to Client Certificate

= Mutual Authentication

Each Connection Peer authenticates and authorizes the other peer to connect = Mutual Authentication.

Cyber Security in BACnet/SC



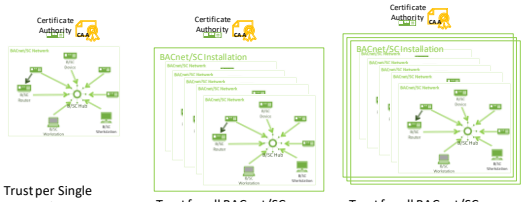
Each Connection Peer (Client and Server) Has:

- 1 Private Key matching the Public Key of the public Device Operational Certificate
- 1 Public Device Operational Certificate with Public Key, signed by a Certificate Authority (CA)

- 1 to multiple Public CA Certificate(s) for authorizing peers to connect

Cyber Security in BACnet/SC

Possible Trust Scopes



Trust per Single BACnet/SC Network

= Device cannot be hooked to any other BACnet/SC network

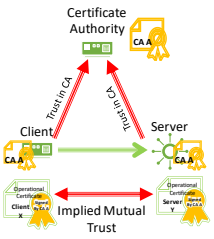
Trust for all BACnet/SC Networks of Installation

= Device can be hooked to any BACnet/SC network of the Installation

Trust for all BACnet/SC Networks of many Installations

= Device can be hooked to any BACnet/SC network of all Installations

Cyber Security in BACnet/SC

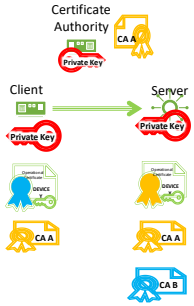


Trust and Network Authorization Through Certificate Authority (CA) Signatures

- One or Multiple trusted CAs as determined by Installation
- CA is Trust Anchor, creates Trust Scope, signs authorized Operational Device Certificates.

- Peers do trust another peer if its Operational Certificate Issuer Signature is of one of those CAs of which they have the CA Public Certificates (1 to many)
- Other Peer is accepted to connect if a presented Operational Certificate is signed by one of these CAs
- Certificate Authority chain is not relevant.
- No need to directly trust or otherwise know each other Device

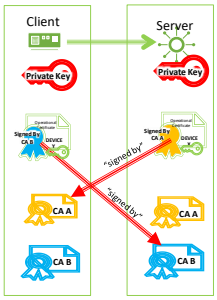
PKI, CA, Certificates



Public Key Infrastructure (PKI)

- Cryptography based on Public Keys, Private Keys and Signatures on X509 certificates for Identity
- Certificate Authority (CA) for proofing and signing Identities and the Public Key
- Identity, Public Key and CA Signature in X509 Certificates.
- Private Key never exchanged, except in some configuration methods (with tool, out-of-band)
- Peer Operational Certificate signature verified against trusted CAs

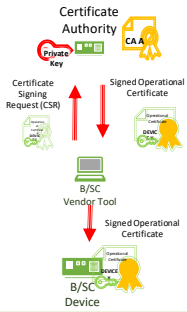
Cyber Security in BACnet/SC



Multiple CAs Used

- More than one Public CA Certificate in Client or Server
- Device Operational Certificate presented must be signed by one of these CAs
- Multiple Public CA Certificates more typical in a Server (Hub) than in a Client (Device)
- Can be helpful for CA Migration and Certificate Update Procedures
- Allows for Self-signed Certificate setups, but not recommended.

PKI, CA, Certificates

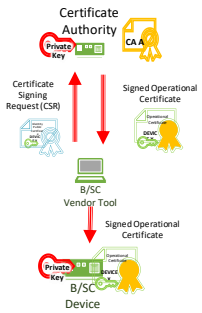


Certificate Authority (CA)

- Verifies Identity in Public Device Certificates
- May be delegated to Registration Authority (RA)
- Verifies and Accepts Device Identity Certificates presented in Certificate Signing Request (CSR)
- Signs the Public Identity Certificate to prove that the Identity and Public Key is valid and the Device can access network
- Proofs its Identity by a Public CA Certificate

- Can be an online Service
- May be an offline service (e.g. via Email, Flash)
- Not connected to the BACnet/SC network
- Used by Vendor Tools to request for signature on Operational Certificates (CSR)
- Provides its Public Key certificate as Operational CA Certificate.
- Must support .PEM File Formats for CSR and signed Operational Certificate exchange with Vendor Tool

PKI, CA, Certificates



Certificates

- Operational Device Certificates, CA Public Certificate
- Are all X509 Certificates
- Each Certificate contains
  - Identity of Subject (optional)
  - Names and Description of Subject (optional)
  - Public Key of Subject
  - Validity Time
  - Identity of Issuer (CA used to sign the Certificate)
  - Signature of Issuer from Issuer's Private Key

Certificates in Play

- Public Device Identity Certificate, for CSR
- Public Device Operational Certificate, signed by an accepted CA
- Accepted CA Public Certificates, can be self-signed (Root CA) or any Intermediate CA Certificate.

Specification of BACnet/SC incl. Security

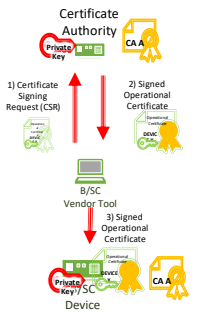
Protocol Implementation Conformance Statement (PICS)

Indication of BACnet/SC and BACnet/SC Routing Support by a Device

- Support of BACnet/SC as Node
- Support and maximum number of initiated Direct Connections
- Support and maximum number of accepted Direct Connections
- Support of BACnet/SC Hub Function and maximum number of accepted Hub Connections
- HTTPS Proxy Support by supported Proxy Types
- Additional cipher suites beyond those required by TLS V1.3
- Additional TLS Versions supported
- Can generate Private Key and CSR internal in device
- DNS Name Resolution support
- Support of BACnet/SC to BACnet/SC and to other datalink routing

➢ BACnet/SC support does not require Implementation of Protocol Revision 22 or higher
➢ BACnet/SC can be supported in any Protocol Revision!

PKI, CA, Certificates



Certificate Signing

1) Device with help of Vendor Tool sends Certificate Signing Request, including Device Public Key.
2) The CSR is verified by the CA, the Certificate is signed using the Private Key of the CA (= Issuer)
3) Signed Operational Device Certificate is given to the Device, currently by Vendor Tool

To create a reliable and secure trust:

- Vendor Tool gets CA's Public Certificates from CA Services
- Vendor Tool configures Accepted CA Certificates into Devices
- Vendor Tool configures signed Device Operational Certificate into Device

Private Key of Devices

- Stored in Device, generated by Device or Vendor Tool
- Related to the Public Key published in the Device Operational Certificate.

a) Generated by Tool before CSR and configured into Device, or
b) Generated by Device and base for Identity Certificate for CSR

Specification of BACnet/SC incl. Security

BIBBs

NM-SCH-B: Network Management-Secure Connect Hub-B

- Device supports a Network Port with BACnet/SC Hub Function accepting Hub Connections.

NM-SCDC-A: Network Management-Secure Connect Direct Connect - A

- Device supports at least one BACnet/SC network port that implements the node switch and is able **to initiate** at least one direct connection

NM-SCDC-B: Network Management-Secure Connect Direct Connect - B

- Device supports at least one BACnet/SC network port that implements the node switch and is able **to accept** at least one Direct Connection

Device Profile

B-SCHUB: BACnet Secure Connect Hub

- Part of Miscellaneous Family, can be claimed with other Device Profiles
- BACnet Device that is able to perform the BACnet Secure Connect hub Function and accepting Hub Connections
- This device can be used as Primary Hub or as Failover Hub without change

Specification of BACnet/SC incl. Security

Specification Items

Specification Item	Who	Description
BACnet/SC Hubs and Devices	Specifier	BACnet/SC Hubs, Failover Hubs, BACnet/SC Devices, BACnet/SC Routers by Device Profiles, BIBBs, and PICS
Scopes and CAs to be used	Specifier / IT	One or multiple CAs that are to be used to sign Device Operational Certificates, Scope of the CAs
IP Names, Validity Times	Specifier / IT	Domain Name Support, Host Names, Certificate validity time
TLS Version	Specifier / IT	TLS V1.3 supported by all BACnet/SC Devices TLS V1.2 Support is a possible implementation option but not required for BACnet/SC.
IP Network	Planner / IT	The IP network and infrastructure to connect BACnet/SC Devices and Hubs (Switches, Hot Spots, DNS Servers, IP Routers)
BACnet/SC Networks	Planner	Which Devices belong to which BACnet/SC Network, BACnet/SC to BACnet/SC Routers, and to other BACnet networks
WebSocket URI of (Primary) Hub	Planner	For all Devices of a BACnet/SC Network, to connect to the Primary Hub.
WebSocket URI of Failover Hub	Planner	For all Devices of a BACnet/SC Network, to connect to Failover Hub. Optional, only if Failover Hub is used

Setup and Maintenance of Security

Initial Commissioning

Item	Who	Description
Get CA Service Running	CA Operator	The CA, or multiple CAs, need to be accessible and in service. May need criteria on which devices are getting a signature.
Configure Device Operational Certificates	Installer	Create CSR for Device, get Signature from CA, install Device Operational Certificate in Device May require Key Generation and Private Key configuration by Tool if Device cannot do internally
Configure CA Certificates	Installer	Configure the Public Certificates of the accepted signing CAs into Devices and Hubs
Configure Hub's WebSocket URIs into Devices	Installer	Configure the Primary Hub URI, and optionally the Failover Hub URI into the Devices.
Get Hub Running	Installer	For a smooth startup, it is ideal to have the hub running before Devices
Get Devices running and connected to the Hubs	Installer	Configured Devices will attempt to connect to the Hubs based on the WebSocket URIs and the Operational Certificate configured.

Setup and Maintenance of Security

Update of CA and Operational Certificates

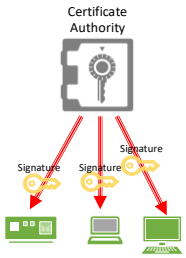
Item	Who	Description
Keep CA Service Running	CA Operator	The CA, or multiple CAs, need to be accessible and in service. May need acceptable devices list
Get new CA Certificates	Maintenance / Service	Get the new CA Certificates, and install in all Hubs in addition
Configure New Device Operational Certificates	Maintenance / Service	Create new CSR for Devices, get Signatures from CAs, install Device Operational Certificate in Device May require Key Generation and Private Key configuration if Device cannot do internally Can be done in steps, Device by Device
Configure CA Certificates	Maintenance / Service	Get the new CA Certificates, and install in all Devices in addition
Configure New Device Operational Certificates for Hubs	Maintenance / Service	Create new CSR for Hubs, Get Signatures from CA, install Device Operational Certificates in Hubs May require Key Generation and Private Key configuration if Hub cannot do internally
Cleanup old CA Certificates	Maintenance / Service	Remove the old CA Certificates from all Devices and Hubs

Outlook

The BACnet Committee is considering the following extension for security in BACnet/SC

- Interoperable Configuration of Hubs and Devices (no Vendor Tool required)
- Authorization of Requests by adding Authorization Tokens (OAuth 2.0 Concepts)
- Autonomic Security Configuration
- Automatic Discovery of Hubs
- Use of MQTT Brokers and other Services as Hub Function

Security Life Cycle and Roles



Security Life Cycle

- Security must be maintained over the entire life cycle of the installation
- Sometimes for 30+ Years
- Many Roles and Persons involved
- CAs comparable to a key vault
- Signature on Operational Certificate hands out a key for a Device to join Network

Questions to be asked over life cycle:

- What device wants a key?
- When should the key be valid for access?
- Which networks are allowed to be accessed?
- Why does it want a key?

Conclusion

- BACnet/SC uses modern IT security concepts
- Security requires proper specification
- Security requires maintenance along the entire lifecycle of an installed system
- Many roles, persons and workflows are involved in this, beyond the technical solution
- The manual work for configuration will be reduced over time

Security Life Cycle and Roles

Roles in Security Life Cycle

Who	Time	System Connection	Description
CA Operator	Long-term to entire life cycle	No	The CA, or multiple CAs, need to be accessible and in service as long as Operational Certificates signed by this CA are used.
Specifier	Initial Specification, Modifications	No	Specifies system and security policies with IT, but is not involved in installation
IT	Sporadic over life cycle	No	IP Infrastructure setup and maintenance IT Security Policies
Planner	Initial Planning, Modifications	No	Plans the details of Hubs and Devices
Installer per Vendor	Initial Commissioning	Yes, by Vendor Tool	Needs to create CSRs, configure and run Devices. Tools for network diagnostics and reports
Maintenance / Service per Vendor	Sporadic but short duration over life cycle	Yes, by Vendor Tool	CA Certificate Updates Operational Certificate Updates Device Replacement, Repair, Diagnosis

Bibliography

- Addendum bj to ANSI/ASHRAE Standard 135-2016, BACnet/SC ASHRAE, November 2019
- BACnet Secure Connect White Paper, ASHRAE, May 2019
- PKI, CA, X509 Certificates, TLS see Wikipedia, IETF RFCs and other public documentation

Questions?

Bernhard Isler

bernhard.isler@siemens.com