



CONNECTING  
**THE WORLD**

niagara<sup>4</sup>



NF  
23

CONNECTING  
THE WORLD

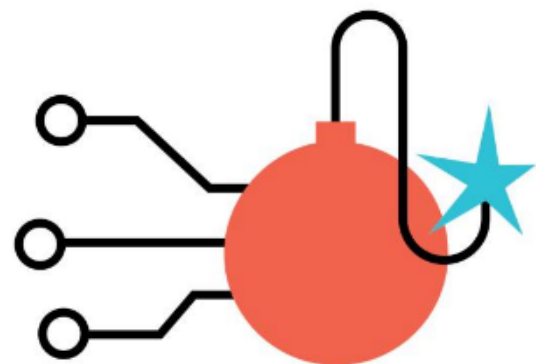
# Security from and to the building

*Dirk Speckhardt, Honeywell  
(former CentraLine), Trend, SBC*

*Dominik Zühlke*



# ARMONK, NY and LONDON, UK 23 Feb. 22



**CYBER ATTACKS**

**IBM Security (NYSE:IBM)** released its 2023 **X-Force Threat Intelligence Index**, which reveals the UK's **PBC-Services** and **Finance/Insurance** both where the country's top target for cyberattacks, accounting for **25%** of all incidents each, followed by Manufacturing **12%** of attacks. The UK became the **top** most attacked country in Europe in 2022, along with **Germany**, according to the report.



**Iran Railways had to shut down its train system because a hacker group infiltrated an IT system and spread malware.**



**Colonial Pipeline ransomware attack caused a gasoline shortage.**

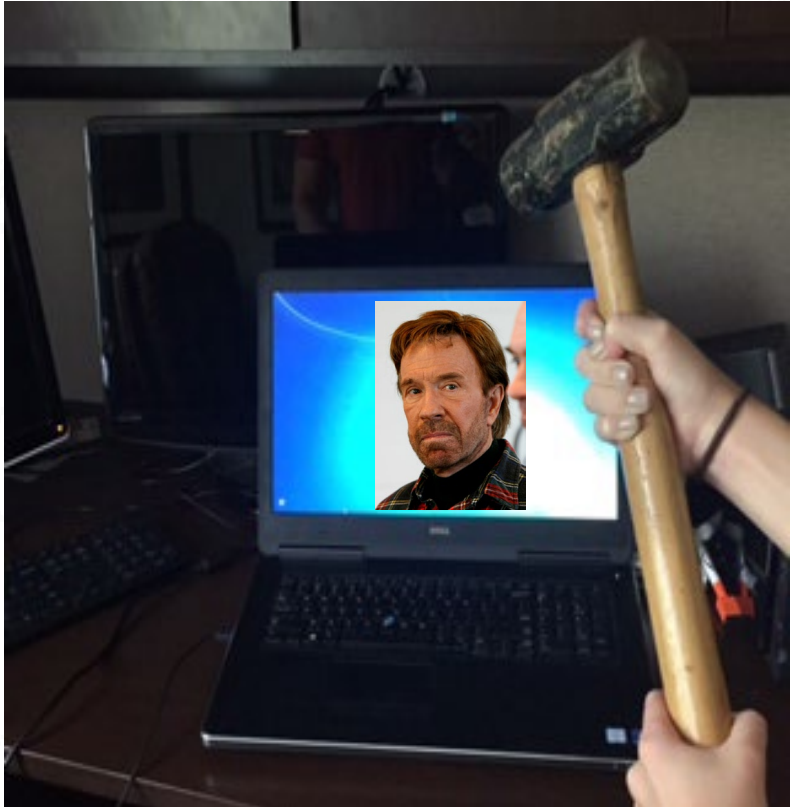


**European oil port of Hamburg, terminals affected by cyber attack.**



**German fuel supplier offline due to cyber attack.**

# Be prepared



- Attacks are inevitable; failure doesn't have to be!
- Don't forget physical security



Bundesamt  
für Sicherheit in der  
Informationstechnik



National Cyber  
Security Centre

a part of GCHQ



**CISA**  
CYBER+INFRASTRUCTURE



**ICS-CERT**

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



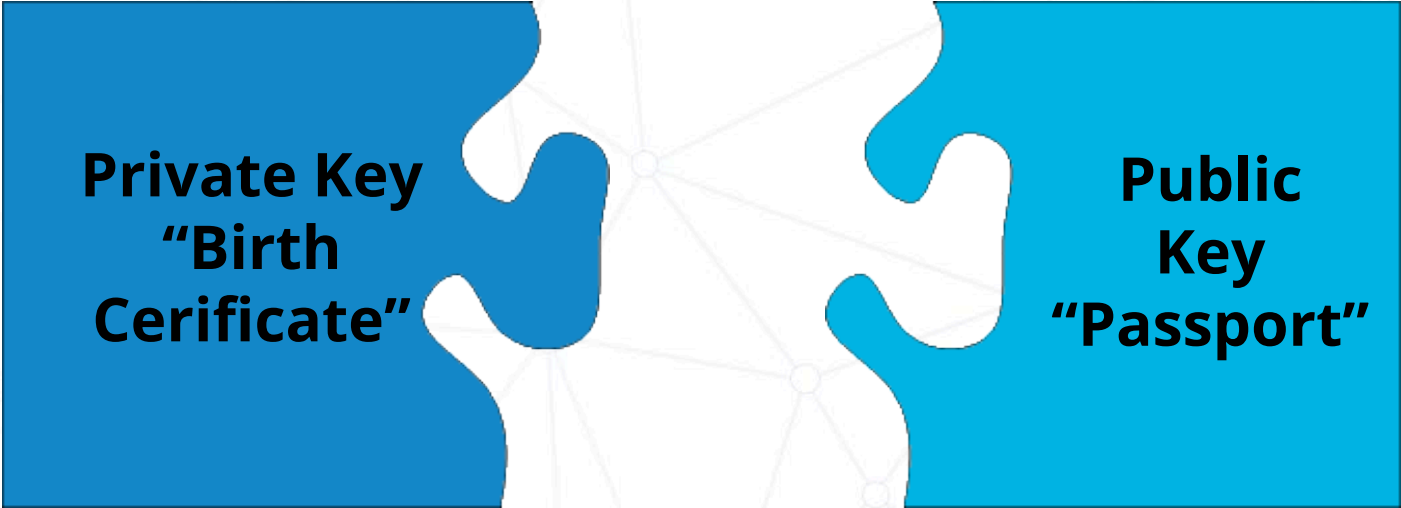
# \*Honeywell Bacnet Story\*





# Public Key Infrastructure\*

# Public Key Infrastructure (PKI)



The diagram consists of two interlocking puzzle pieces. The left piece is dark blue and has a wavy, irregular shape on its right side. The right piece is a lighter blue and has a matching wavy, irregular shape on its left side. They are positioned side-by-side, illustrating how they fit together.

**Private Key**  
"Birth  
Certificate"

**Public  
Key**  
"Passport"

# What does a TLS certificate offer?

## Security overview



This page is secure (valid HTTPS).

- Certificate - **valid and trusted**

The connection to this site is using a valid, trusted server certificate issued by Microsoft IT TLS CA 4.

[View certificate](#)

- Connection - **secure (strong TLS 1.2)**

The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE\_RSA with X25519 (a strong key exchange), and AES\_128\_GCM (a strong cipher).

- Resources - **all served securely**

All resources on this page are served securely.





# Certificate Authority (CA)

- In cryptography, an organization that issues **digital certificates**.
- A **trusted** third-party organization that verifies the organization that wants to have its certificate signed.
- The verification process varies depending on the type of certificate.
- The CA usually charges a fee for the process.
- Certificates are usually **only** valid for a period of **1 year**.
- Could be well-known public organizations like Thawte, GoDaddy or Verisign, or be a local authority.

# Creating a Certificate Signing Request (CSR)

- Contains only the **public key** from the server's certificate.
- The original **private key** must remain in the server's keystore.



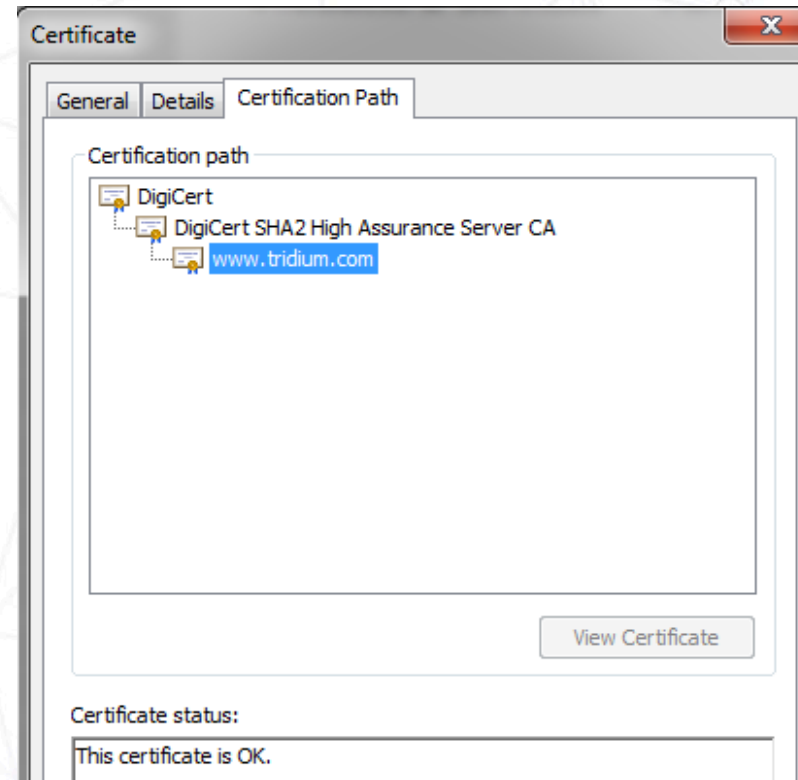
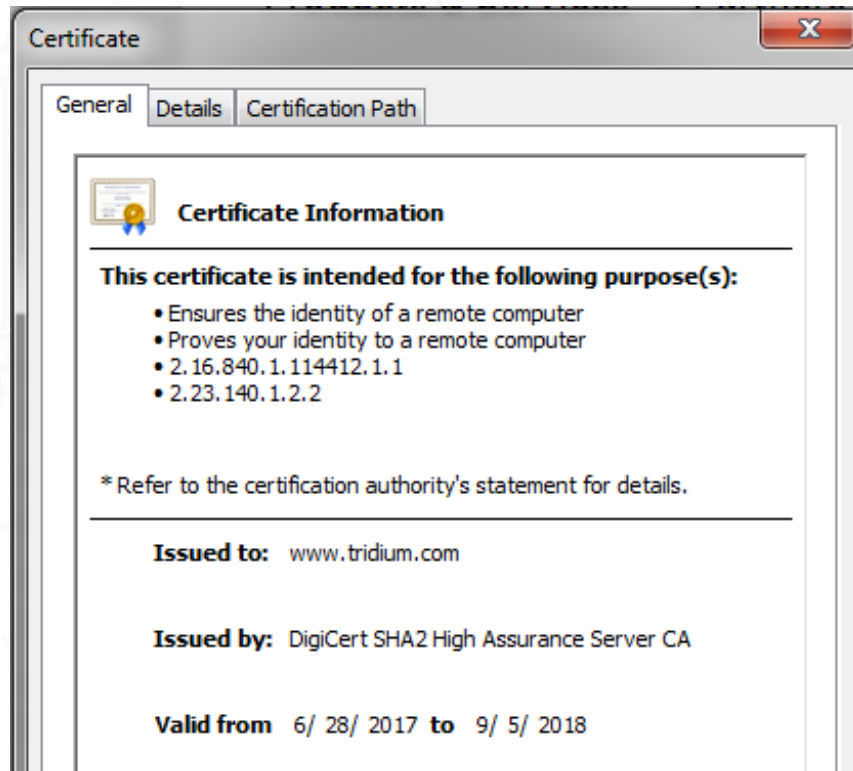
# Signing a Certificate Signing Request (CSR)

- After validating the request, the CA signs the CSR with its private key.
- The CA sends the signed certificate and other information to the subject.



# Certificate Chain of Trust

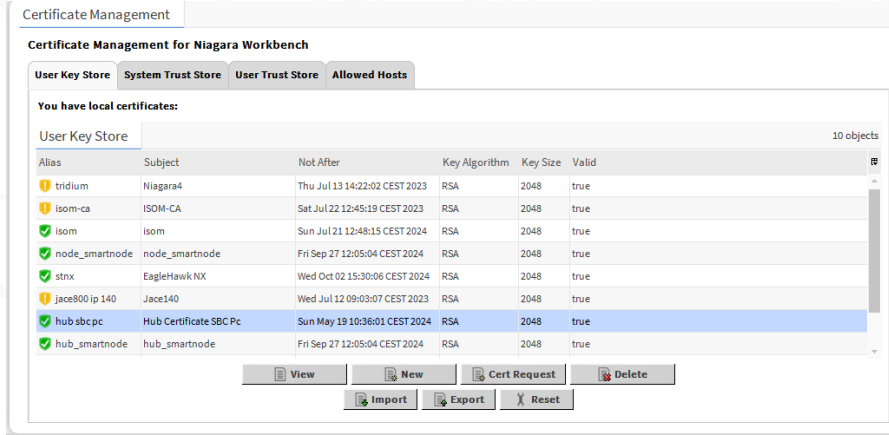
- Displays the chain of certificates used to digitally sign the certificate.
- Typically contains at least one intermediate and root certificates.





# Certificate Trust Store

- A collection of **root** and **intermediate** certificates, including their public encryption keys.
- Typically populated by the operating system or application provider with well-known public CAs.
- Can import additional certificates from other CAs.
- Use by the **client** to verify the digital signatures used in a certificate's chain of trust.



# Emerging Standards

## *BACnet/SC*

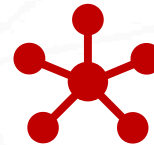
# Benefits

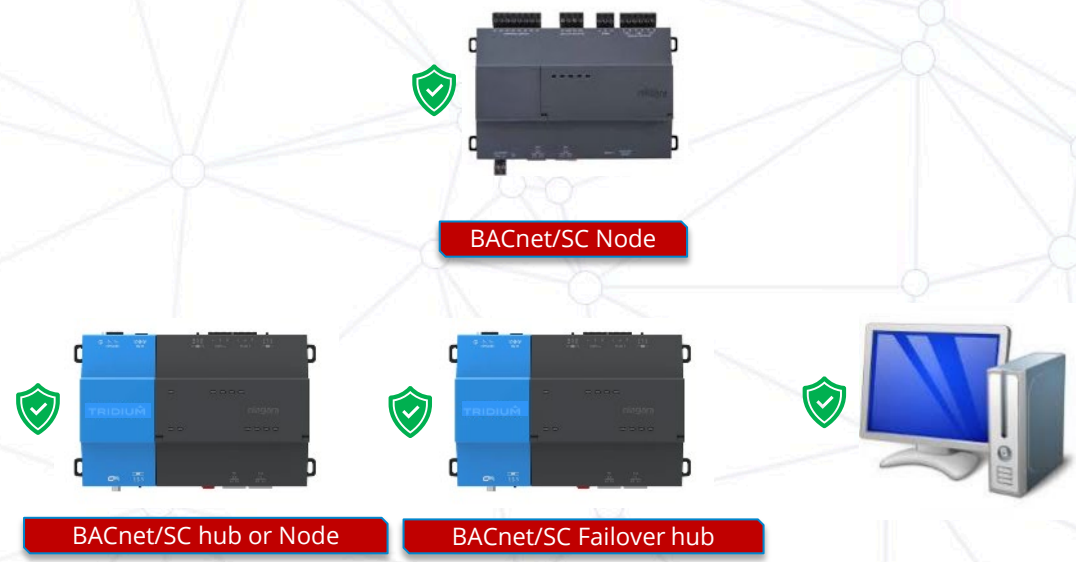
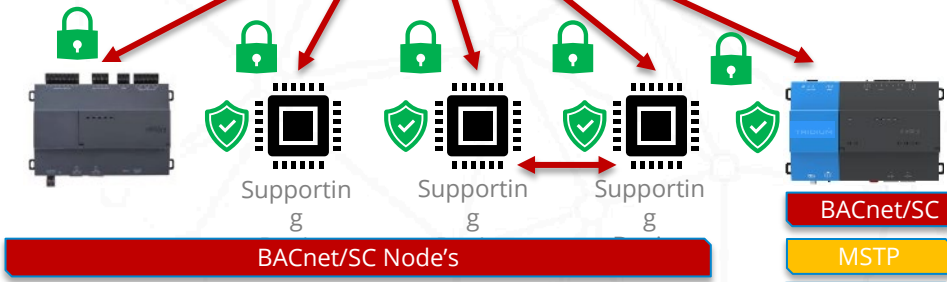
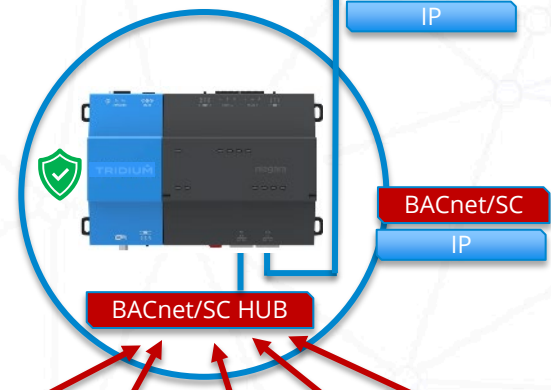
- BACnet/SC is a supplement to the BACnet protocol
- Encryption on the Wire.
- PKI-Device authentication.
- More "IT-friendly" than BACnet IP.
- Backwards compatible with existing BACnet systems.
- Uses **secure** websockets instead of UDP.



 Encrypted  
 Device Certificate

 BUILDING LAN / ENTERPRISE WAN 

 Hub and Spoke Design



NF  
23

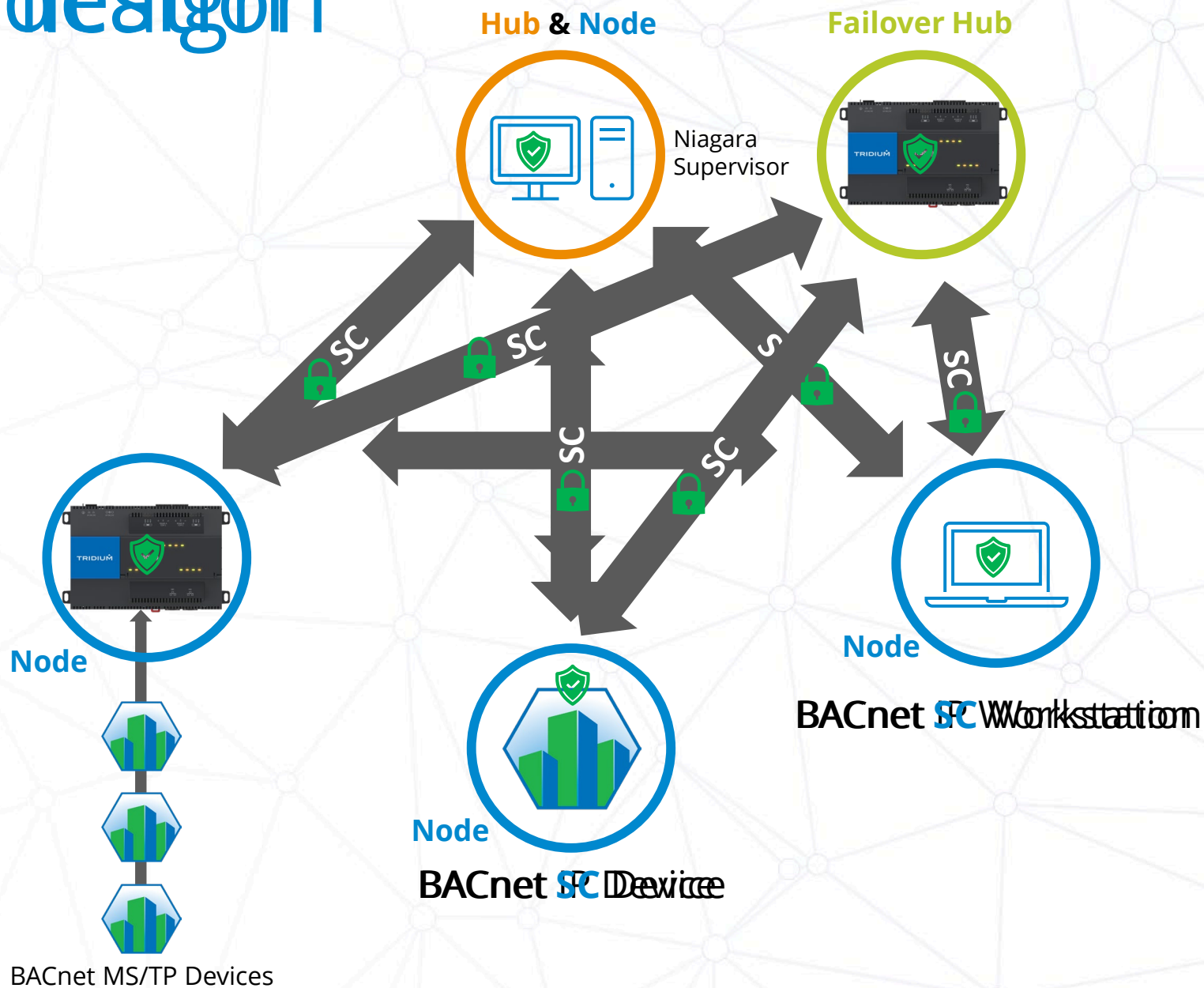
- BACnet/SC Node
- MSTP
- BACnet
- BACnet/IP
- LON
- RS232
- MODBUS



# Failover design

## Failover design –

- All nodes must be capable of connecting to a **Failover Hub** in the event the **Primary Hub** is unavailable



 Device Certificate  
 Encrypted

**TRIDIUM**

Niagara Workbench

File Edit Search Bookmarks Tools Window Help

Certificate Management

Nav Certificate Management

My Network

Certificate Management for Niagara Workbench

Trust Store User Trust Store Allowed Hosts

Generate Self Signed Certificate

Generate Self Signed Certificate  
Generates a self signed certificate and inserts it into the keystore

Alias (required)

Common Name (CN) (required)  
\* this may contain the host name or address of the server

Organizational Unit (OU)

Organization (O) (required)

Locality (L)

State/Province (ST)

Country Code (C) (required)

Not Before 05-10-2022 10:43 CEST

Not After 05-10-2023 10:43 CEST

Key Size 1024 bits 2048 bits 3072 bits 4096 bits

Certificate Usage Server Client CA Code Signing

Alternate Server Name

Alternate Server URI

Email Address

Key Usage  
☐ Digital signature ☐ Non-repudiation ☐ Key encipherment  
☐ Data encipherment ☐ Key agreement ☒ Certificate signing  
☒ CRL signing ☐ Encipher only ☐ Decipher only

OK Cancel

10 objects

|                    | Not After                     | Key Algorithm | Key Size | Valid |
|--------------------|-------------------------------|---------------|----------|-------|
|                    | Thu Jul 13 14:22:02 CEST 2023 | RSA           | 2048     | true  |
|                    | Sat Jul 22 12:45:19 CEST 2023 | RSA           | 2048     | true  |
|                    | Sun Jul 21 12:48:15 CEST 2024 | RSA           | 2048     | true  |
| smartnode          | Fri Sep 27 12:05:04 CEST 2024 | RSA           | 2048     | true  |
| hawk NX            | Wed Oct 02 15:30:06 CEST 2024 | RSA           | 2048     | true  |
|                    | Wed Jul 12 09:03:07 CEST 2023 | RSA           | 2048     | true  |
| certificate SBC Pc | Sun May 19 10:36:01 CEST 2024 | RSA           | 2048     | true  |
| smartnode          | Fri Sep 27 12:05:04 CEST 2024 | RSA           | 2048     | true  |

View New Cert Request Delete Import Export Reset

## Nav

- My Network
- NiagaraNetwork
    - ProvisioningNwExt
  - BacnetNetwork
  - AbstractMqttDriverNetwo
  - RdbmsNetwork
  - ISOM
  - HttpClientNetwork

## Palette

- provisioningNiagara
- BatchJobService
  - ProvisioningNwExt
  - NiagaraNetworkJobPrototype
  - TriggerSchedule
  - ProvisioningRobot

☒ Generate an alarm when any step fails or is canceled☐ Generate an alarm when job completes successfully

## Provisioning steps to run

- Backup Stations
- Install certificate "tridiumcertneu", Policy="Install Unique"
- Generate Certificate Job Step (Alias="Node\_Jace100", Common Name="<hostname>", Organization="Customer")
- Export CSR Job Step (File Naming Identifier="Hostname", Certificate Alias="Node")
- Sign Certificate Job Step (Server Certificate Alias="Node\_Jace100")
- Import Signed Certificate Job Step (File Naming Identifier="Hostname", Certificate Alias="Node")
- Reboot Stations

## Stations to include in the job

Run Now

Copy Templates

Refresh

# Summary

- Multiple layers of security provide **defense in depth**.
- Secure systems **require active management** including but not limited to managing certificates, installing software patches and performing periodic security audits.
- PKI certificates are used to **establish trust** between a client and server by verifying the identities and **encrypting data exchanged over the network**.
- Security Dashboards help to access the security posture of the applications.
- Insist your specifications include the most secure protocols and options



# Q&A

# Acronyms

| AD        | Active Directory                                                          |
|-----------|---------------------------------------------------------------------------|
| ASHRAE    | American Society of Heating, Refrigeration and air-conditioning Engineers |
| BACnet    | Building Automation Control network                                       |
| BACnet/IP | BACnet over IP                                                            |
| BACnet/SC | BACnet/Secure Connect                                                     |
| CA        | Certificate Authority                                                     |
| CSR       | Certificate Signing Request                                               |
| CVSS      | Common Vulnerability Scoring System                                       |

| IdP    | Identity Providers                    |
|--------|---------------------------------------|
| LON    | Local Operating Network               |
| LDAP   | Lightweight Directory Access Protocol |
| MODBUS | Data communications protocol          |
| MSTP   | Master Slave Token Passing            |
| PKI    | Public Key Infrastructure             |
| SAML   | Security Assertion Markup Language    |
| TLS    | Transport Layer Security              |
| UDP    | User Datagram Protocol                |