CONNECTING
THE WORLD

Security from and to the building

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

Dominik Zühlke

TRIDIUM

ARMONK, NY and LONDON, UK 23 Feb. 22

IBM Security (NYSE:IBM) released is 2023 **X-Force Threat Intelligence Index**, which revelas the UK's **PBC-Services** and **Finance/Insurance** both where the country's top target for cyberattacks, accounting for **25%** off 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.

NF 23

TRIDIUM

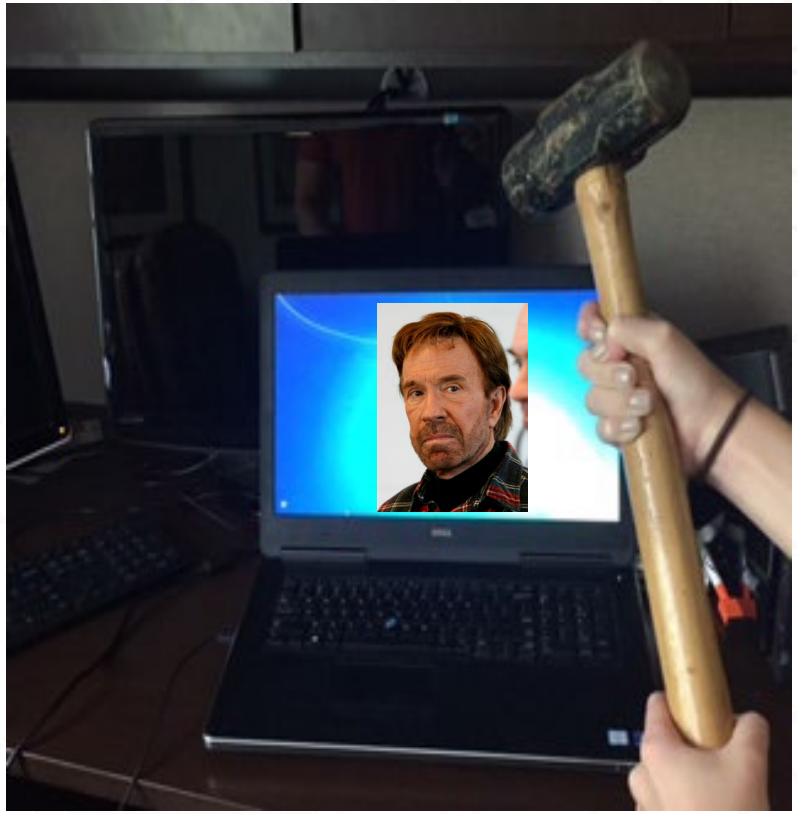
Iran Railways had to shut down its train system because a hacker group infiltrated an IT system and spread malware.

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

NF
23

TRIDIUM

niagara4

Honeywell Bacnet Story

NF 23

TRIDIUM

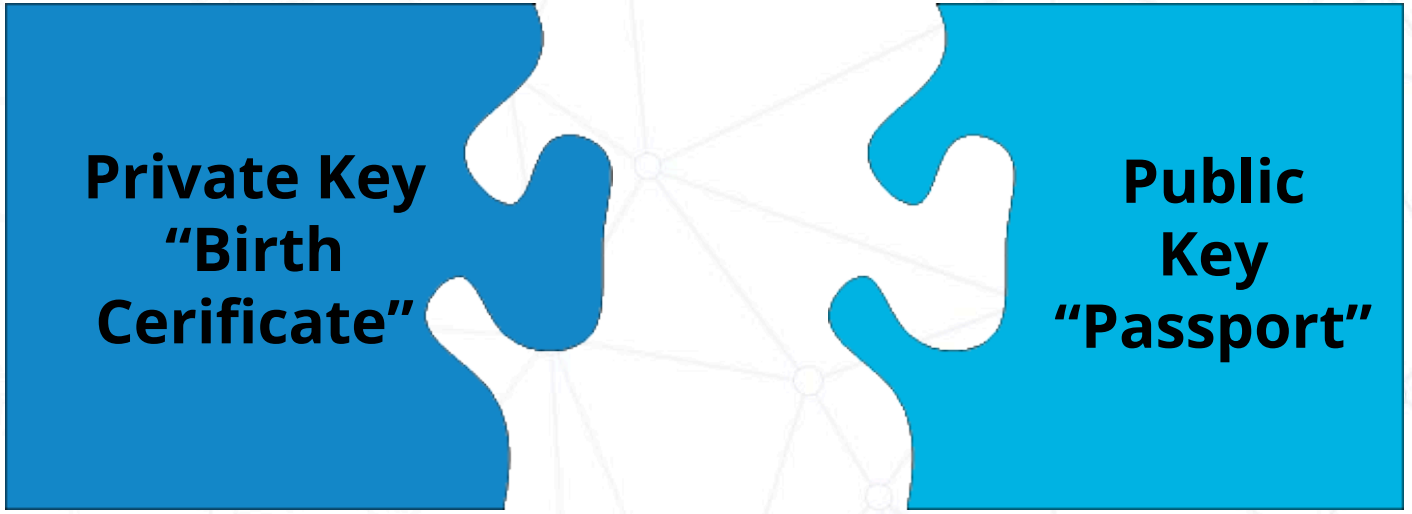
niagara4

Public Key Infrastructure*

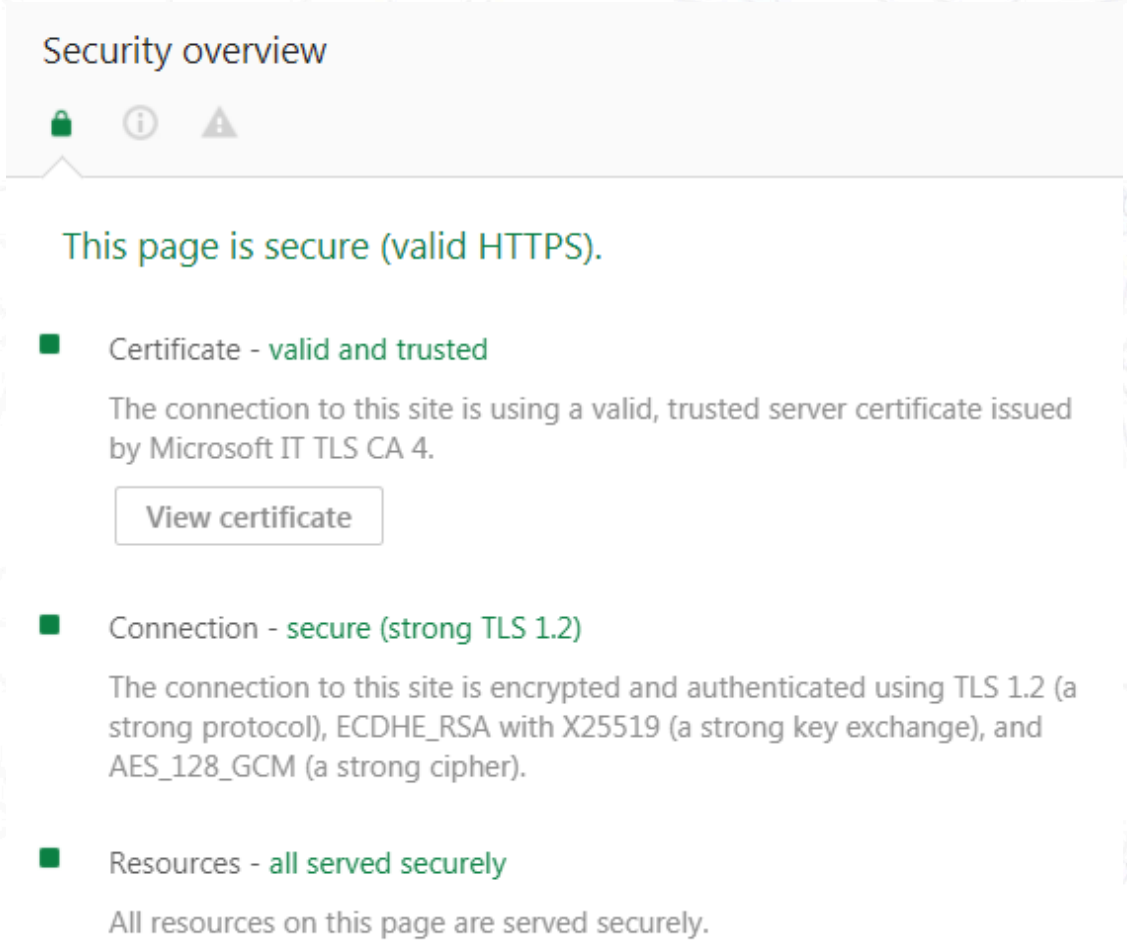
NF 23

TRIDIUM

Public Key Infrastructure (PKI)



What does a TLS certificate offer?



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)

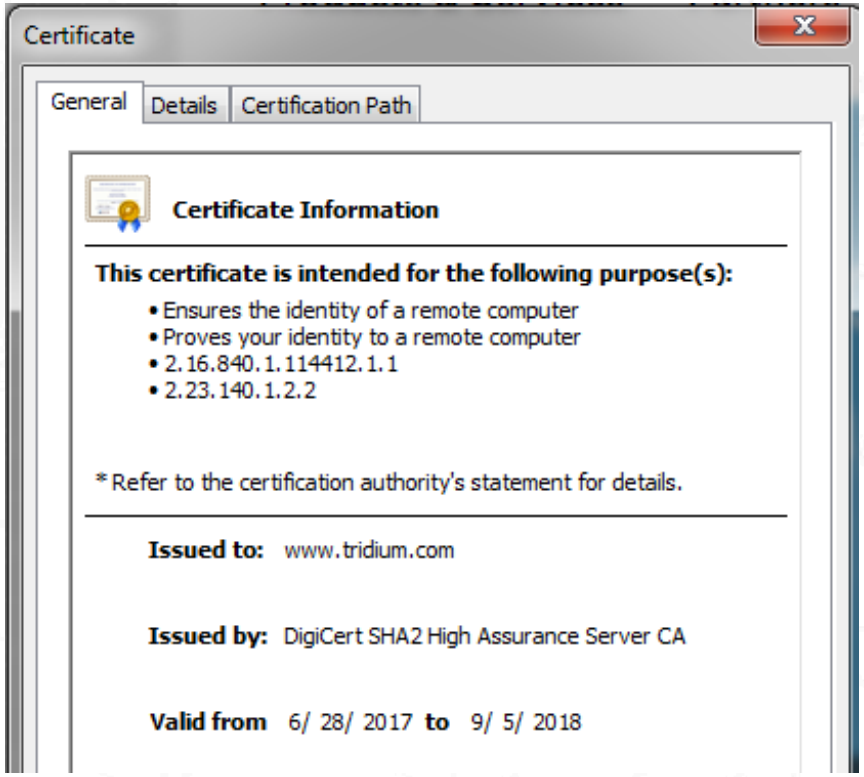
- Contains only the **public key** from the server's certificate.
- The original **private key** must remain in the server's keystore.

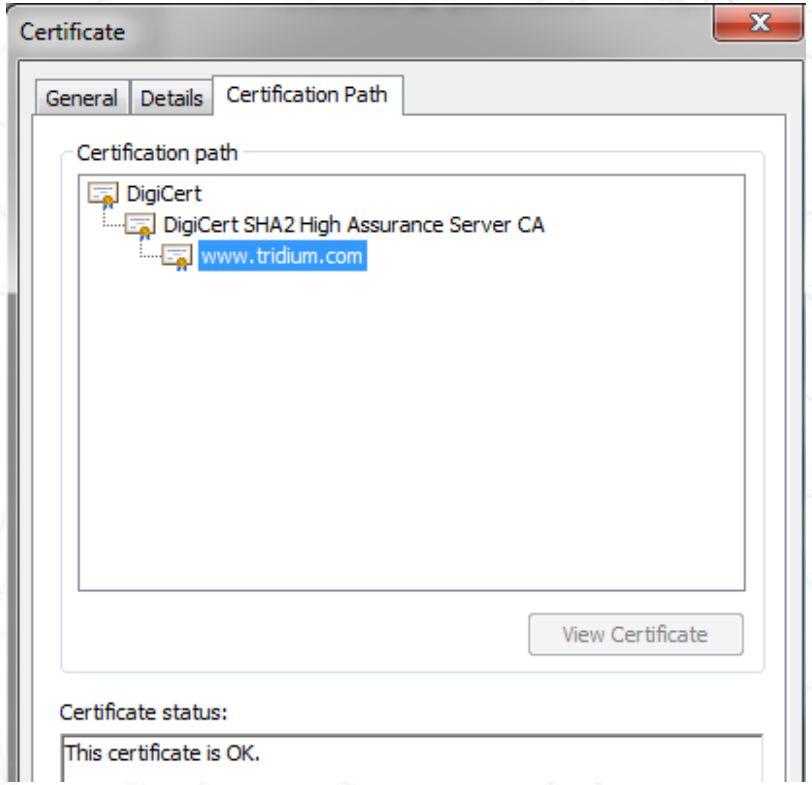
Signing a Certificate Signing Request (CSR)

- 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.

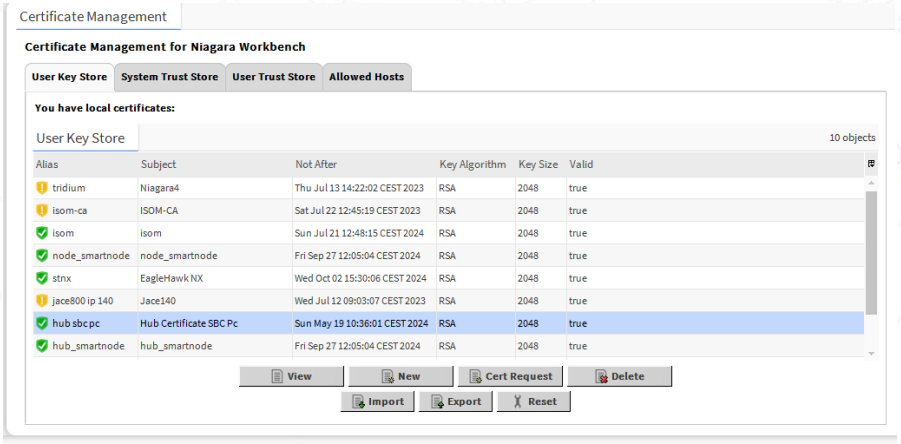
Certificate Chain of Trust

- 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.

NF 23

TRIDIUM

niagara4

Emerging Standards
BACnet/SC

NF 23

TRIDIUM

Benefits

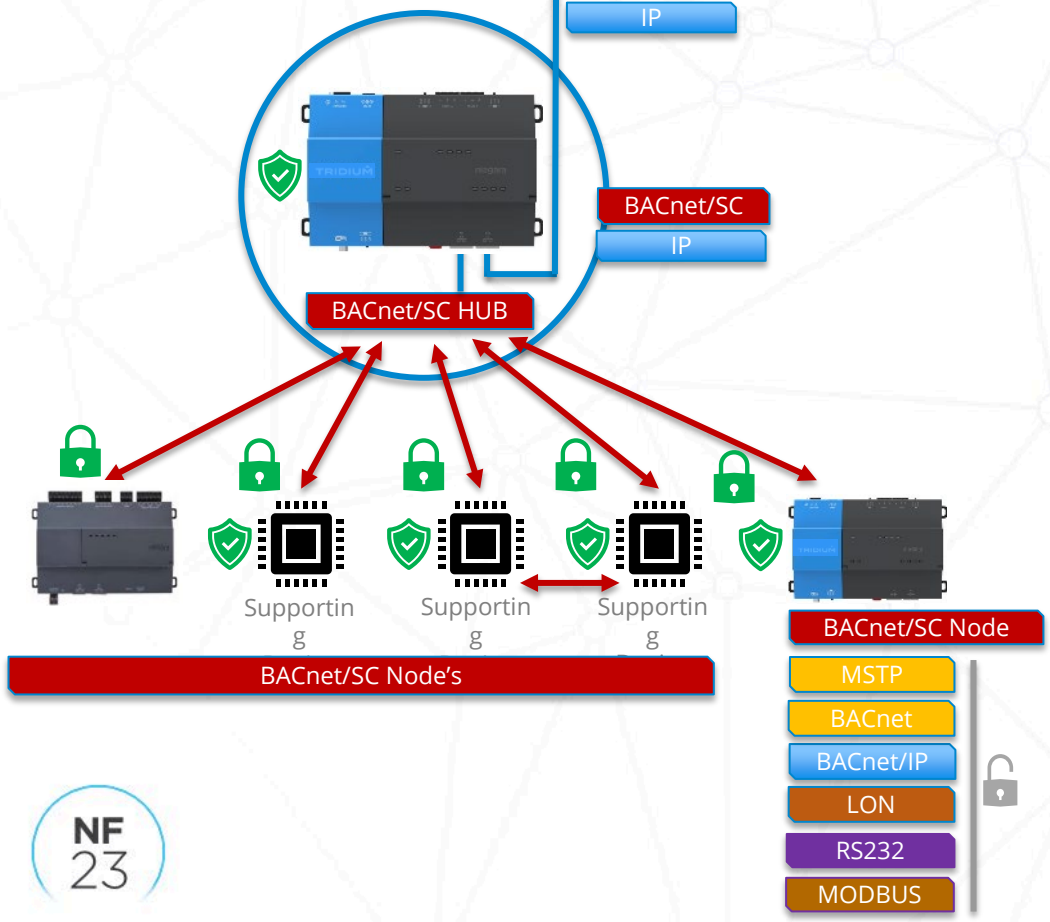
- BACnet/SC is a supplement to the BACnet protocol
- Encryption on the Wire.
- PKI-Deviceauthentication.
- More "IT-friendly" than BACnet IP.
- Backwards compatible with existing BACnet systems.
- Uses **secure** websockets instead of UDP.

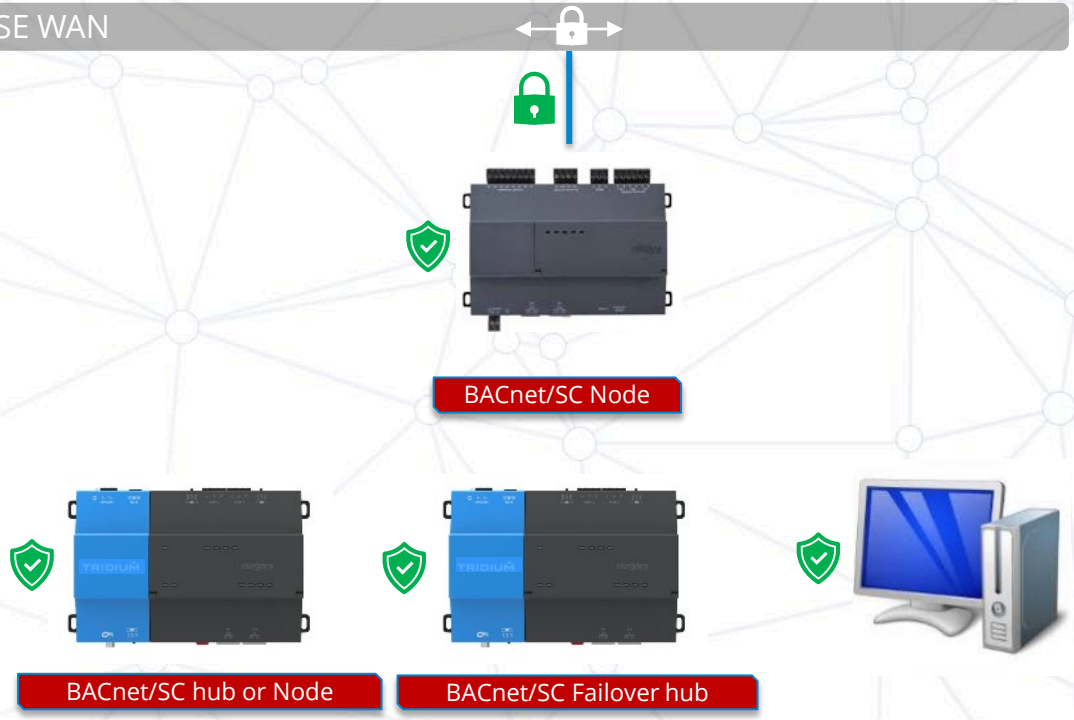
Encrypted

Device Certificate

BUILDING LAN / ENTERPRISE WAN

Hub and Spoke Design

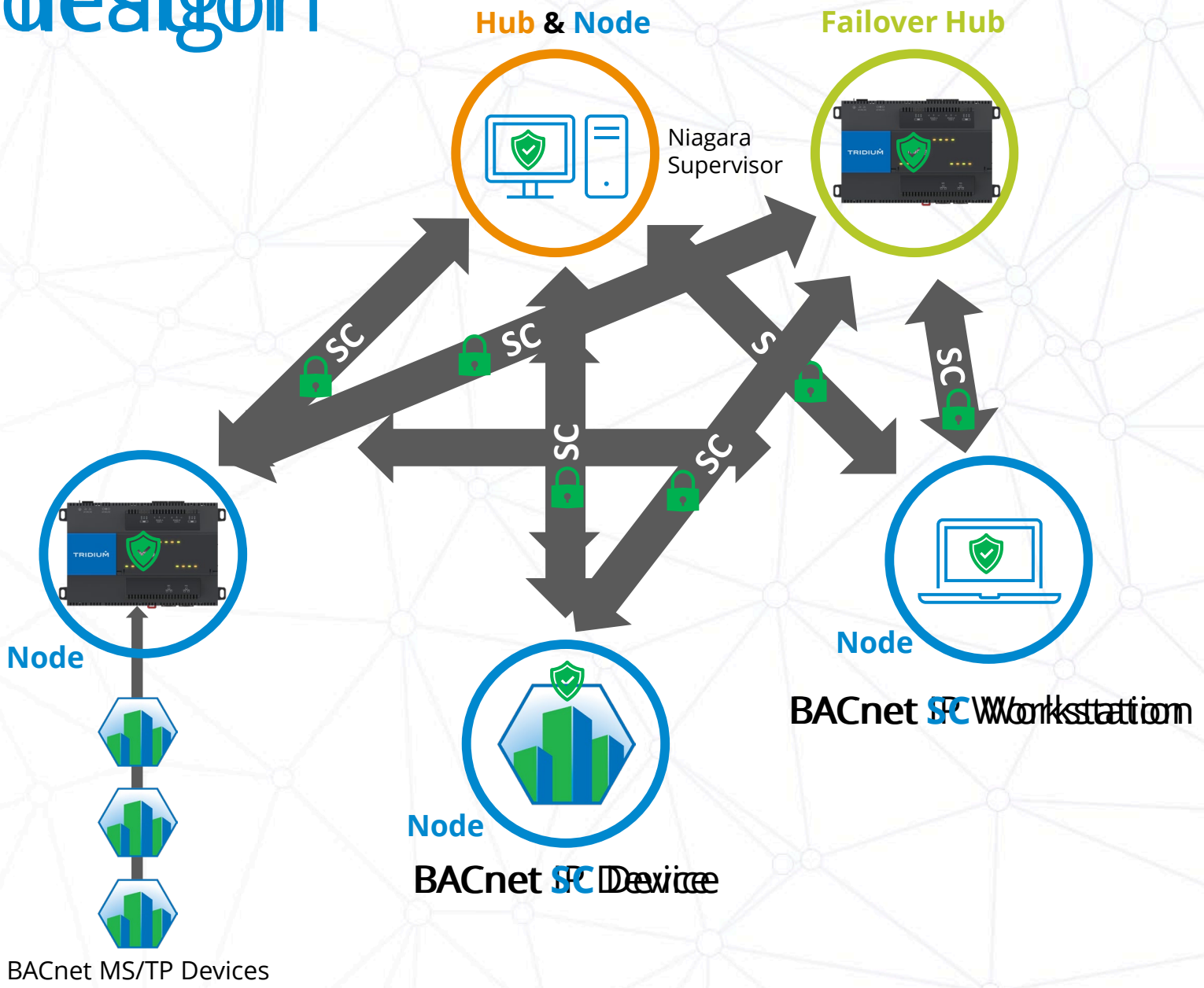




NF 23

TRIDIUM

Failover redundancy design



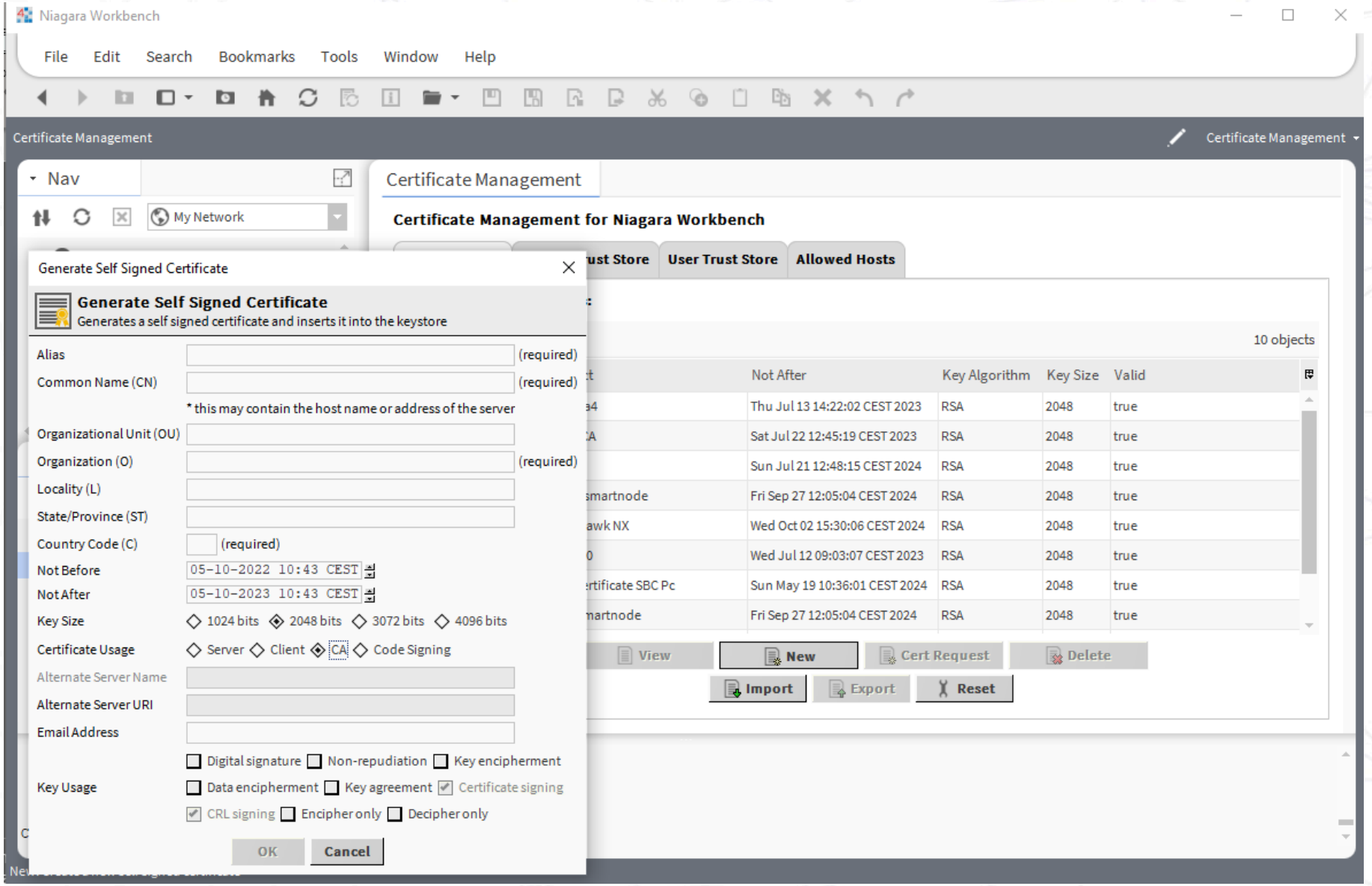
Failover design –

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

Device Certificate

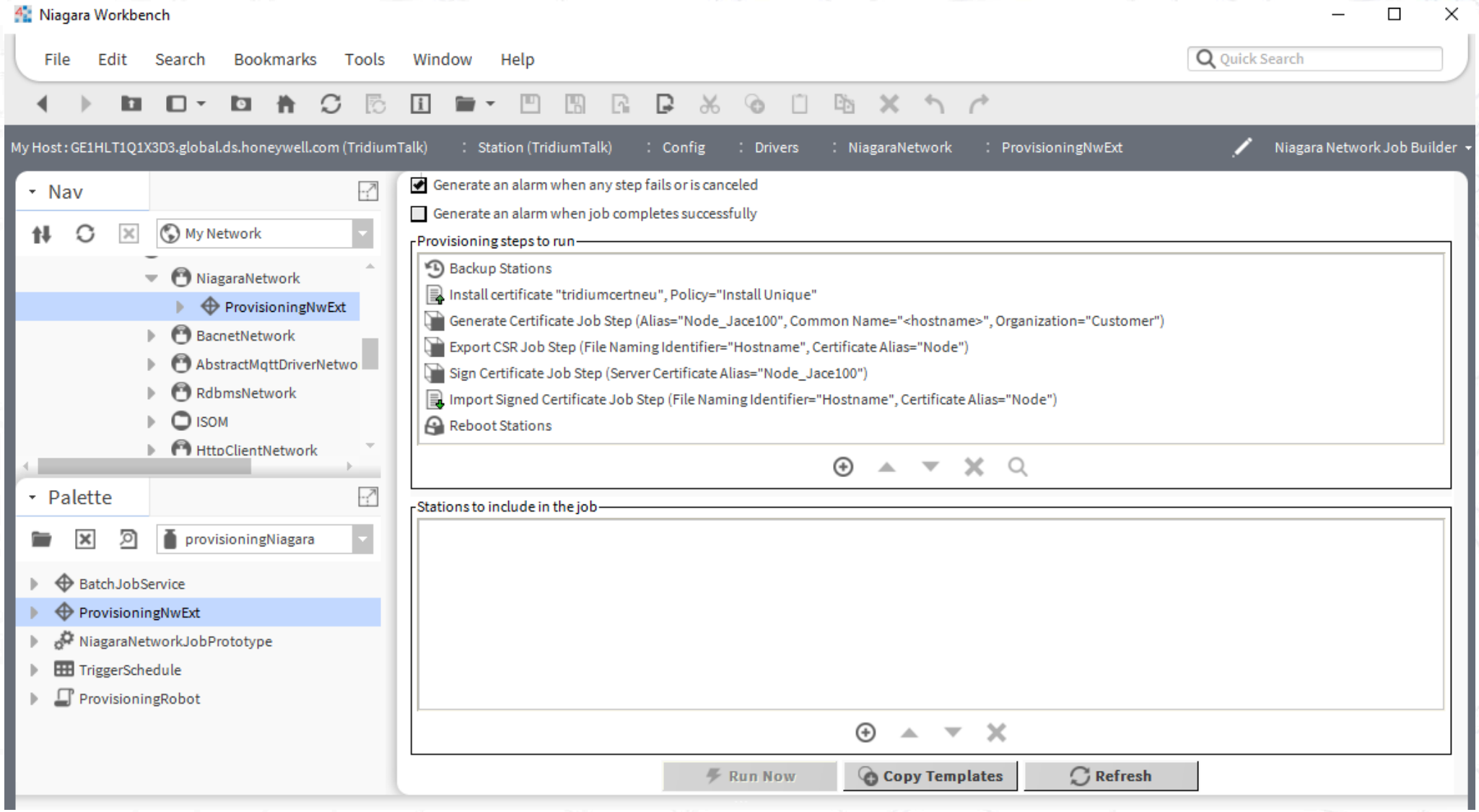
Encrypted

TRIDIUM



NF 23

TRIDIUM



NF 23

TRIDIUM

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

niagara4

Q&A

NF 23

TRIDIUM

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