TRIDIUM

NS2022

ACCELERATING INNOVATION

TRIDIUM

Hackers Uninvited Guests

James Johnson - Tridium

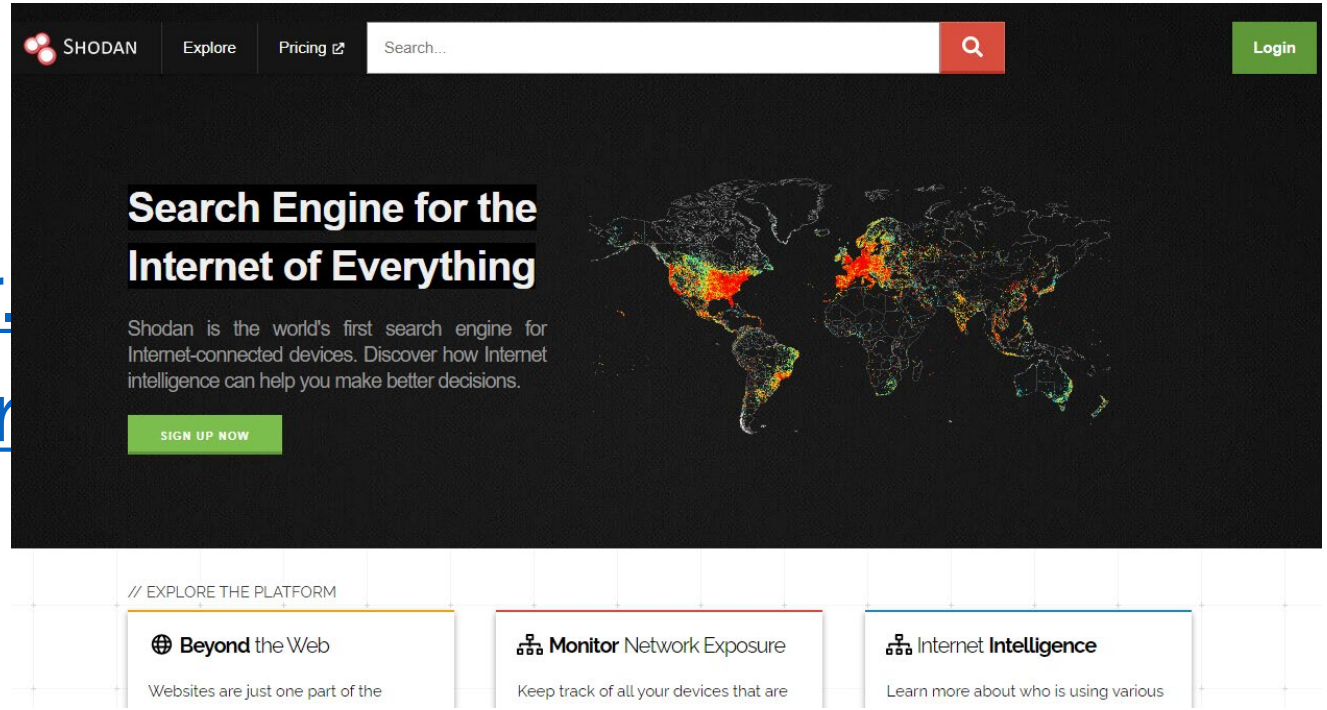
Objectives

- Why should you care about security?
- Best practices for hardening a Niagara application
- Security Service and Dashboard
- PKI certificates
- Code signing

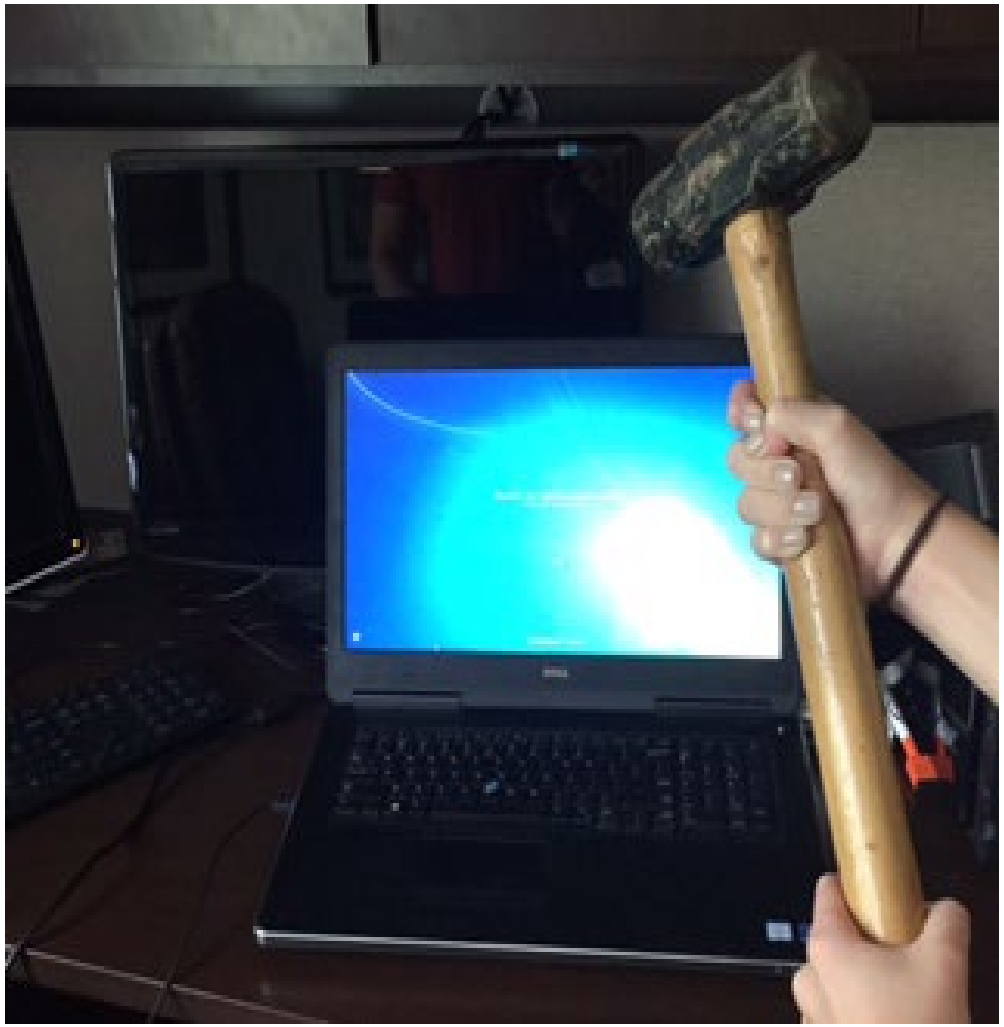
Why Should You Care?

IoT Search Engines

- https://www.shodan.io
- https://censys.io
- https://www.punkspider.
- https://www.zoomeye.or
- https://ivre.rocks



People Forget Physical Security



- Many successful cyber attacks begin with a physical attack.
- Malware can be introduced through USB devices.

Protect Against Ransomware

- Use anti-virus software.
- Perform periodic scheduled backups.
- Treat systems as mission-critical infrastructure, which means it shouldn't be used for surfing the web or checking email.

Patch Management is Critical

- Many organizations provide services internationally, reporting vulnerabilities in hardware and software.
- Advisories may affect millions of devices.
- Vendors release security patches and updates.
- An unpatched system on your network may be an attacker's avenue.

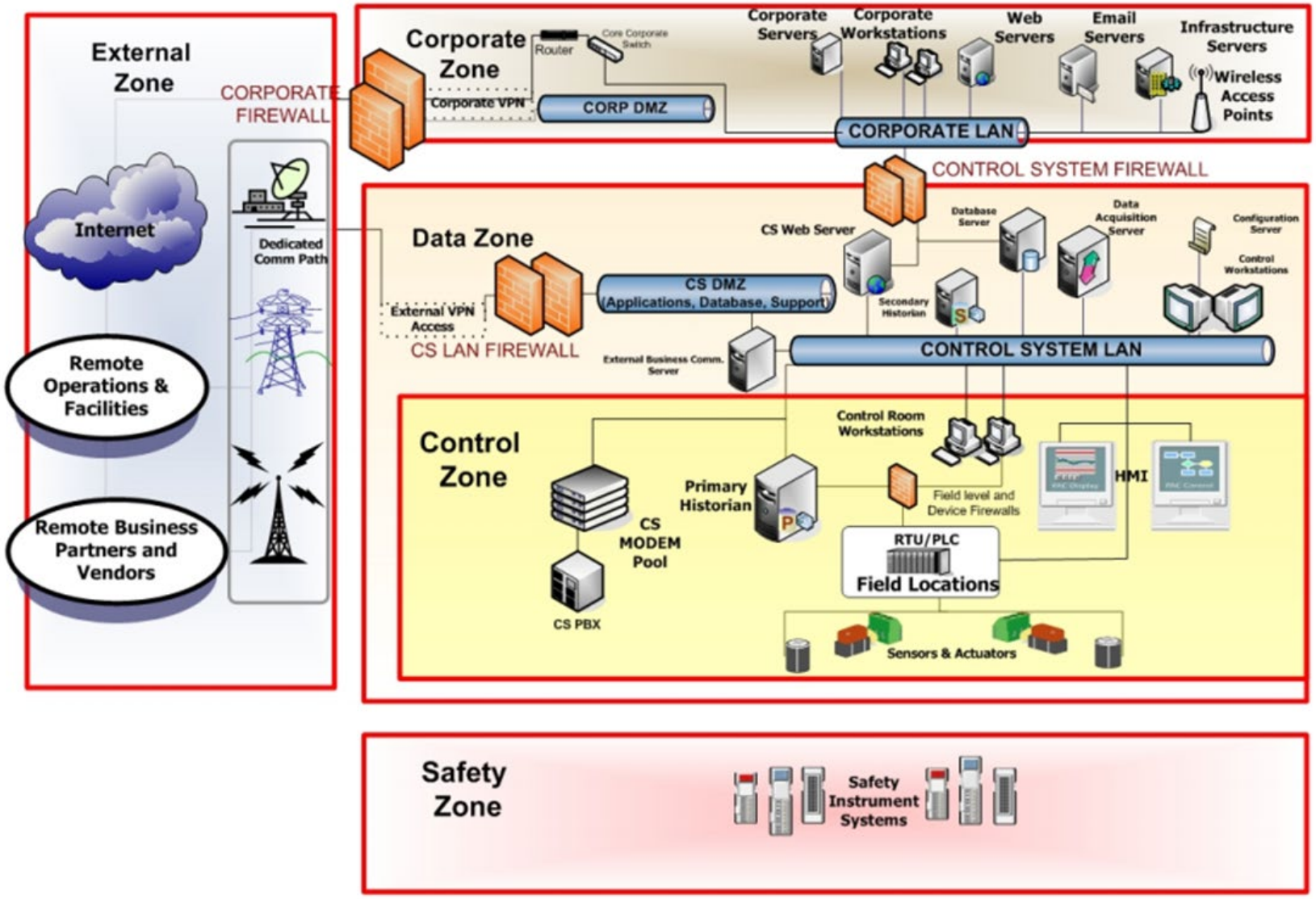
https://www.cisa.gov/

https://www.cisa.gov/uscert/ics

Network Defense In Depth

Recommended Practice: Improving Industrial Control Cybersecurity with Defense-In-Depth Strategies

DHS, ICS-CERT 2009



Good Behavior Through Technology

- Secure by Default
  - Forcing default credential changes upon commissioning
  - Strongest authentication mechanisms
  - Enforcement of strong passwords
  - Encrypted communications
- Encryption of sensitive information at rest
- Digitally signed code – validated for integrity at run time
- Secure Boot

Flexible Authentication Schemes

- Lightweight Directory Access Protocol (LDAP) and Active Directory (AD) – integrates to existing directory information services.
- Security Assertion Markup Language (SAML) – works with popular on premise and cloud Identity Providers
- Client Certificate – utilizes PKI certificate authentication
- Google – provides two factor authentication using the Google Authenticator app

IEEE 802.1X

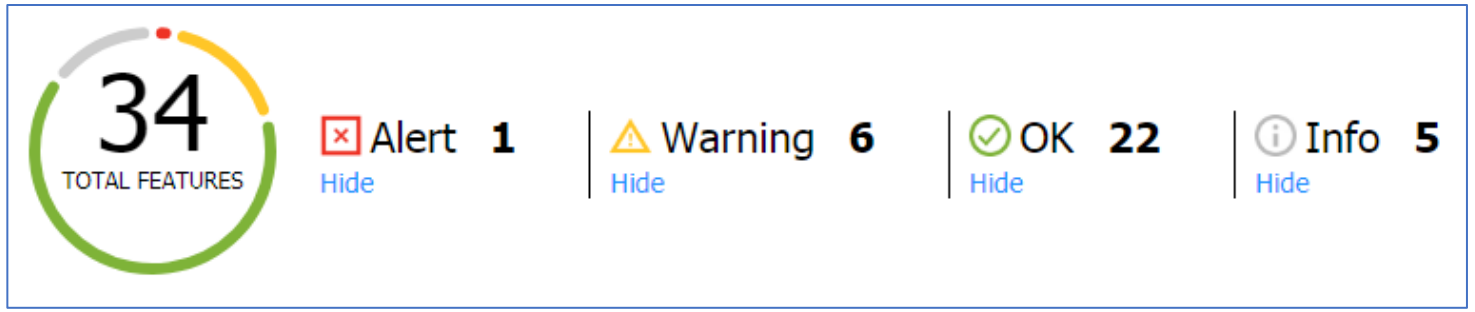
- Port-based Network Access Control (PNAC)
- Provides authentication mechanism to devices wishing to attach to a network
- Available for JACE-8 and Niagara Edge controllers with Niagara 4.8 or newer version.

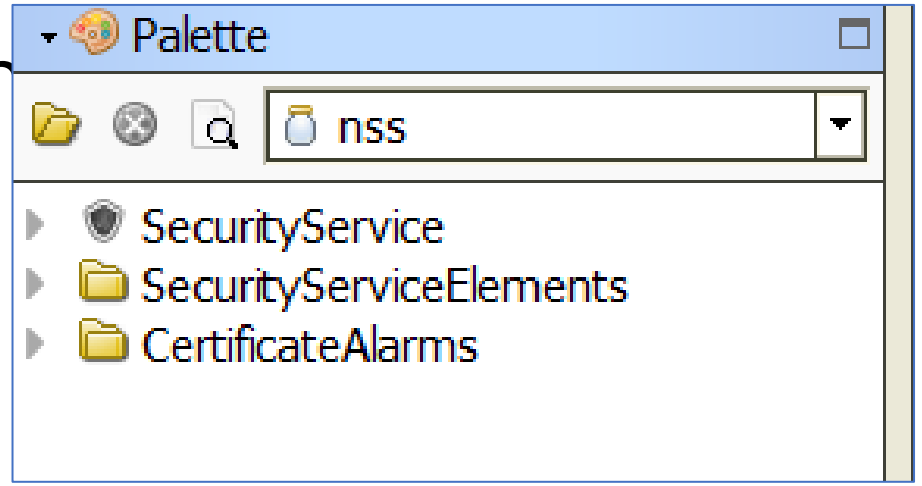
What are your assets and risks?

- Understand your organization's appetite for risk and determine a risk threshold using a CVSS score.
- Identify electronic assets to protect and document security requirements.
- Engage an independent team to ac threats and potential vulnerabilities you network and assets.
- Perform a periodic assessment bec assets and requirements change ov time.

Security Service and Dashboard

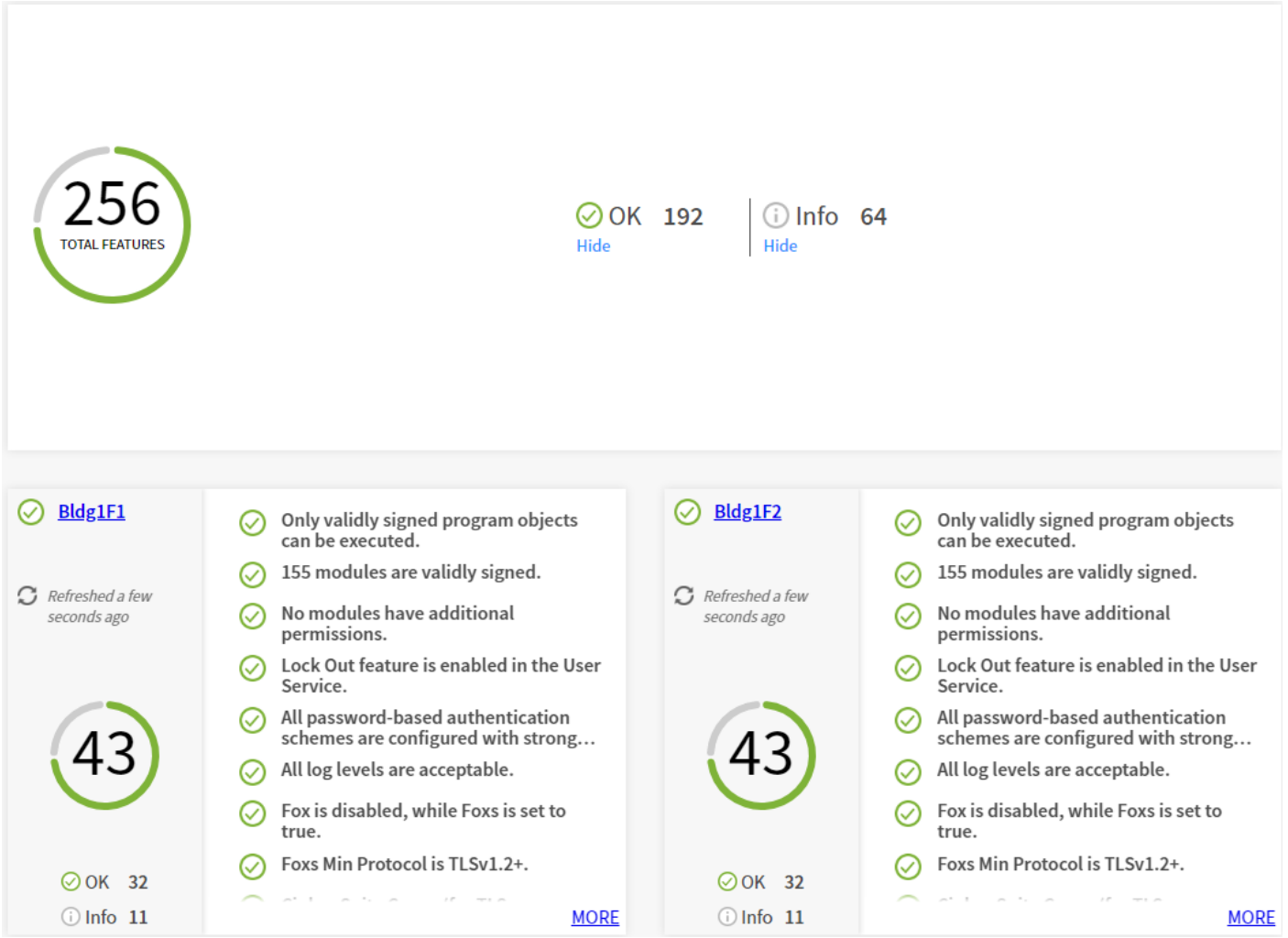
- Security Service provides a dashboard view to help assess the security posture of a Niagara application.
- Available in Niagara 4.8 for Supervisor, JACE and Edge controller stations.
- Optional certificate expiry alarm





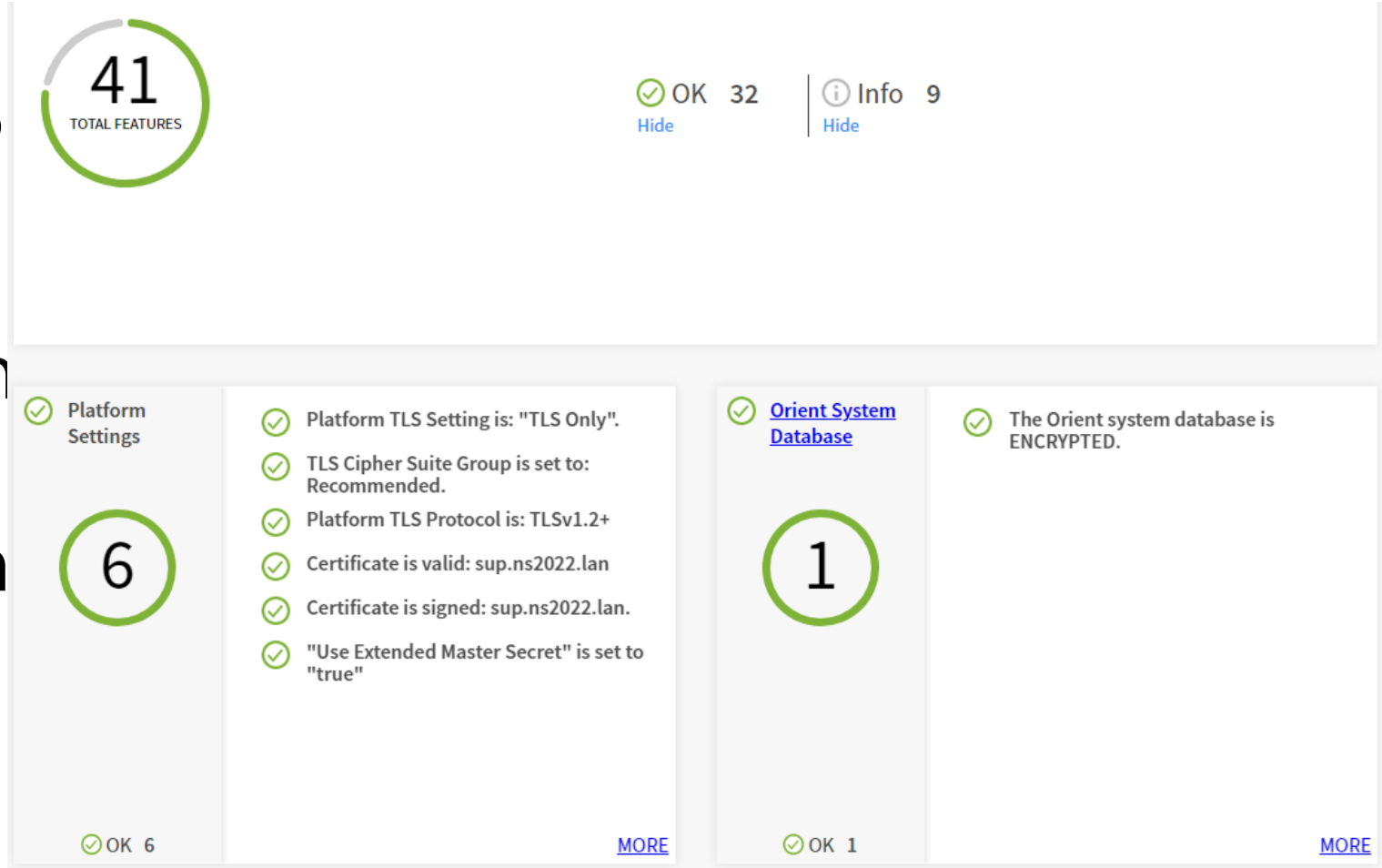
Security Dashboard – System View

- Scores the station and all Niagara network devices.
- Tiles show details for individual devices.
- Hyperlink to more detailed information.



Security Dashboard – Station View

- Scores the station.
- Tiles show details fo individual networks, services and configuration option
- Hyperlink to more detailed information



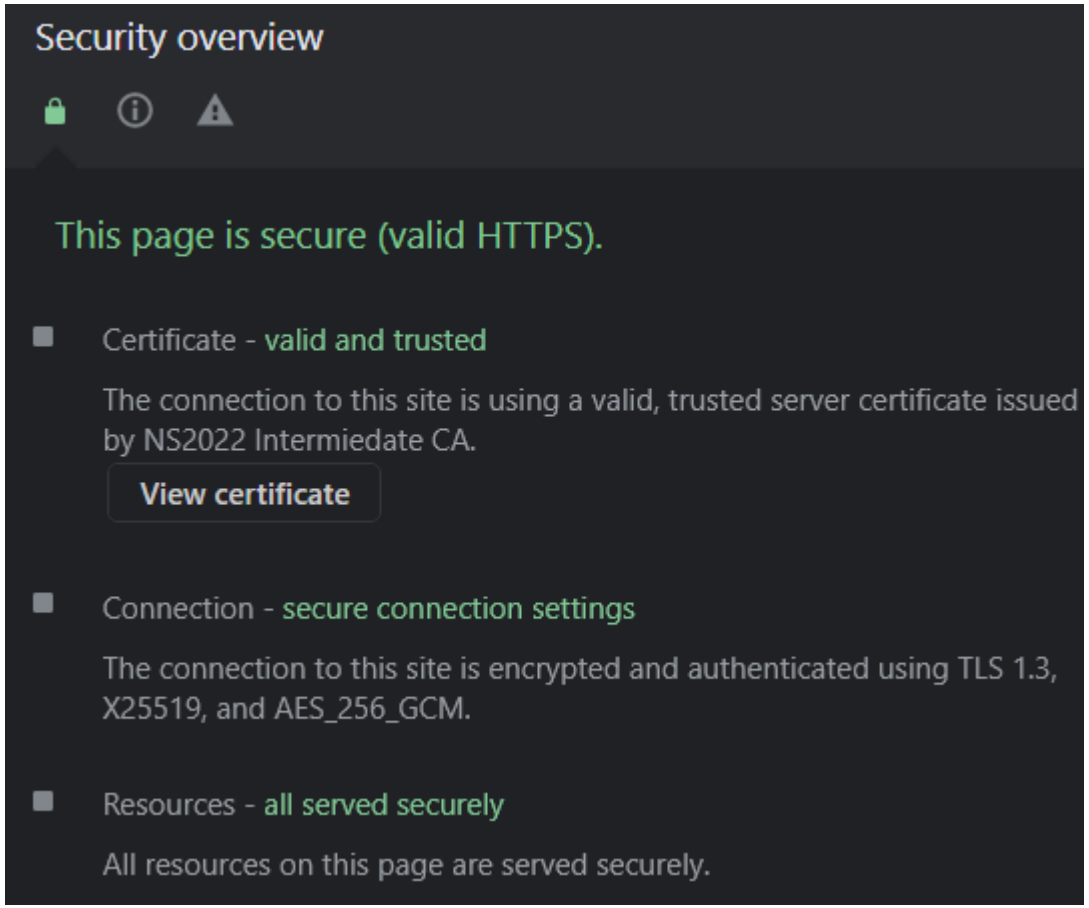
Public Key Infrastructure (PKI)

- An infrastructure that supports the distribution of certificates containing public identification keys that are used to both securely identify entities and provide confidentiality of transmissions.
- A Certificate Authority (CA) is an organization which issues and signs digital certificates.
- A digital certificate is an electronic document used to identify an entity, digitally signed by a trusted CA.

Public Key Cryptography

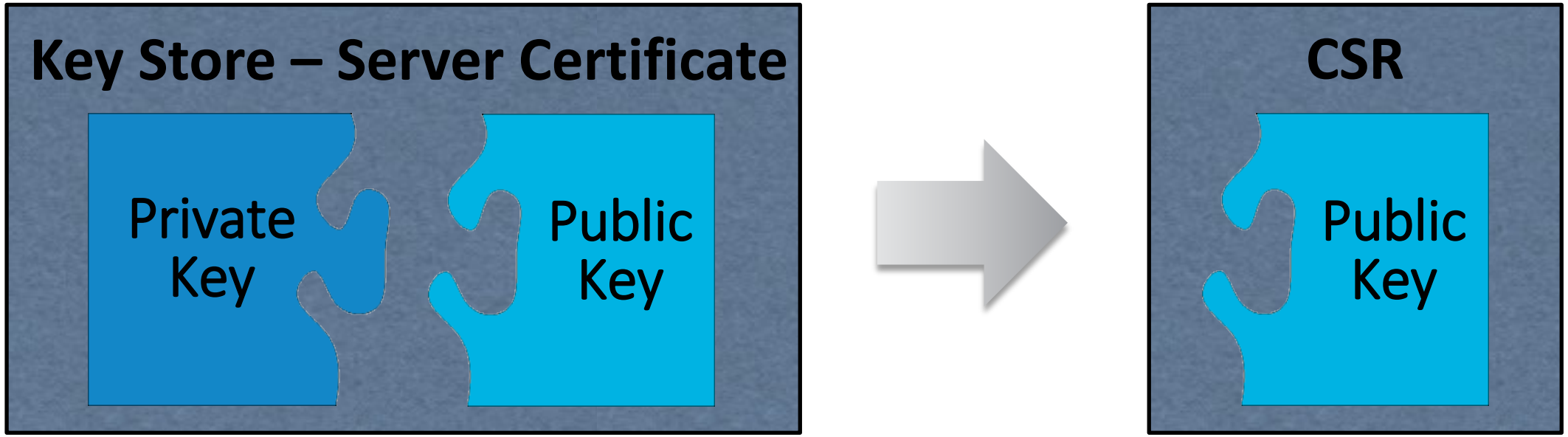
- Uses a **private** and **public key pair**, used together for encrypting and signing.
- Keys are asymmetric, meaning each key is unique but only two specific keys work together.
  - The public key is not a secret and is available to everyone.
  - Each participant keeps its private key a secret.
  - A **sender encrypts data** with a **recipient's public key** and only the **recipient with the private key** can decrypt the data.
  - A sender can **sign data** with **their private key** and **everyone** can validate the sender signed the data using the **sender's public key**.

What Does a TLS Certificate Provide



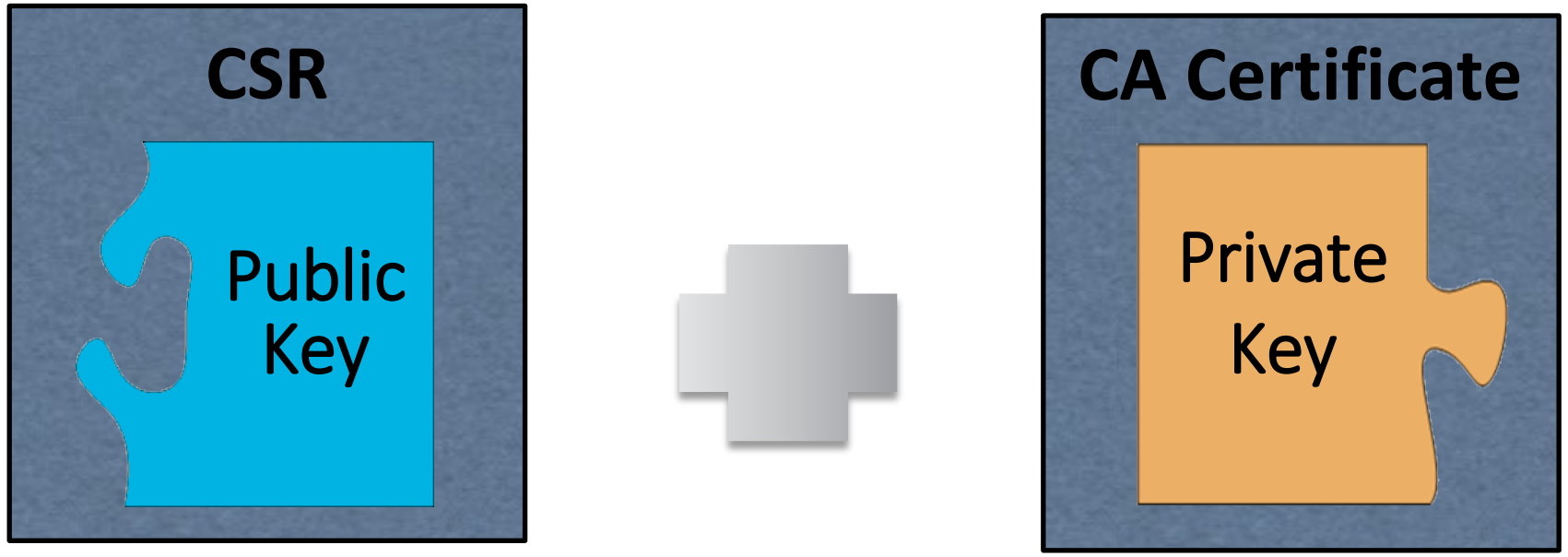
- The client establishes an **encrypted connection** with the server.
- **Verifies the identity** of the server.
- **Validates the authenticity** of the server's certificate.
- A connection can be encrypted without verifying the server's identity or validating the certificate authenticity

Certificate Signing Request (CSR)



- Only includes the public key from the server's certificate.
- The original private key must remain in the server's key store.

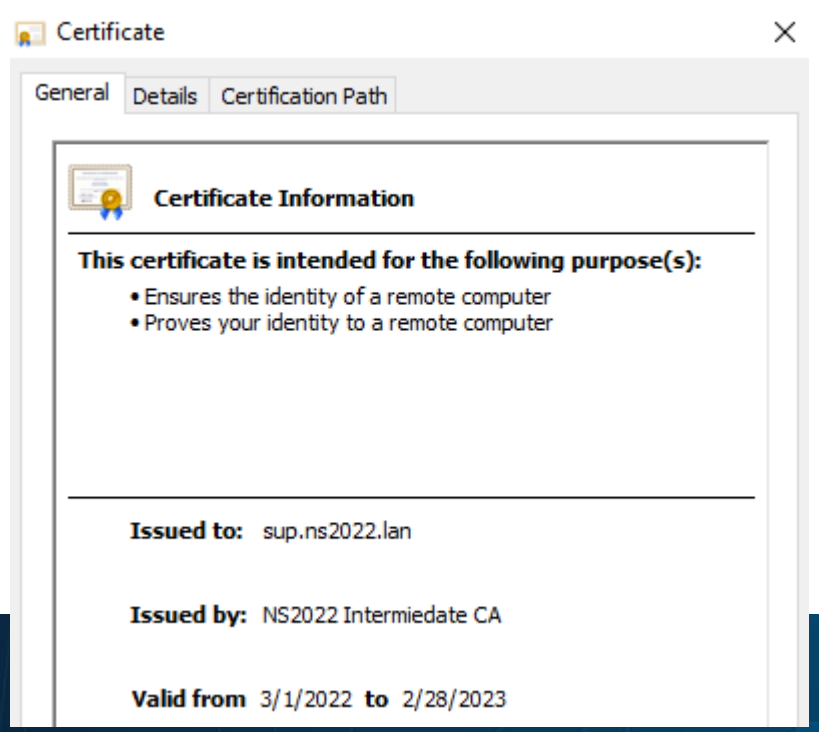
Signing a Certificate Signing Request

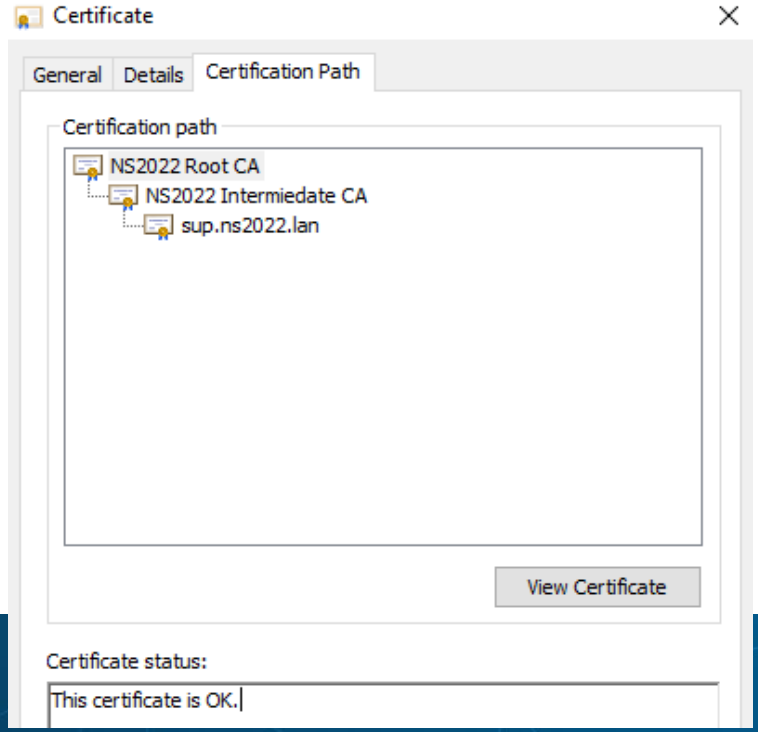


- Only includes the public key from the server's certificate.
- The original private key must remain in the server's key store.

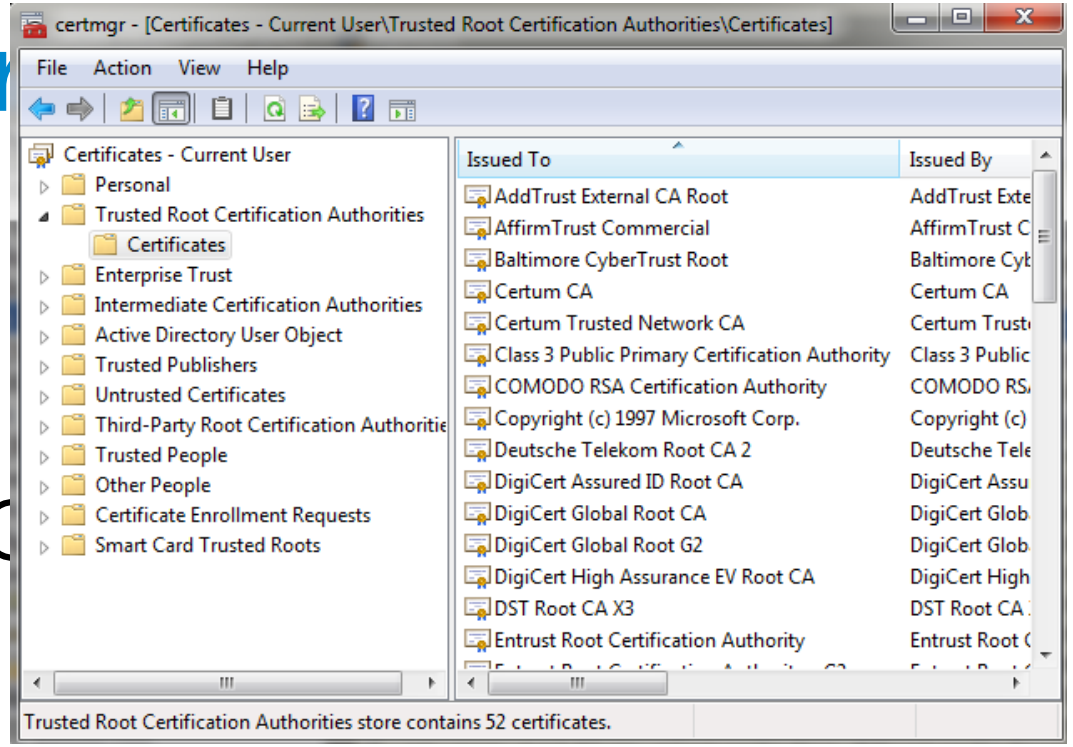
Chain of Trust

- Shows the **chain of certificates** used to digitally sign the certificate.
- Typically includes at least an intermediate and root certificate.





Certificate Trust Stor



- Collection of root and intermediate certificates including their public keys.
- Typically populated by the C or application provider with well-known public CAs.
- Can import additional certificates from other CAs.
- Used by client to validate the digital signature in a certificate's chain of trust.

Code Signing

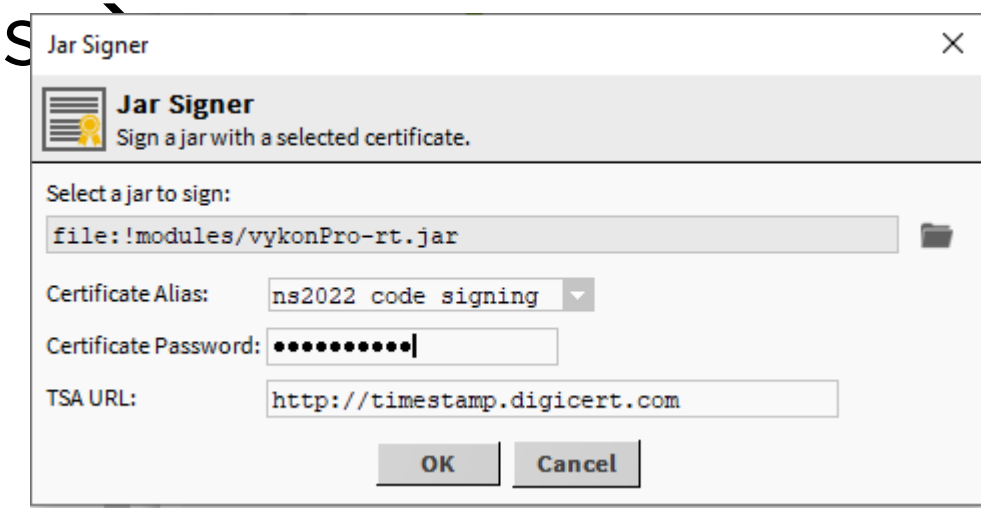
- Process of digitally signing executables and scripts to confirm the software author and guarantee the code has not been altered or corrupted since it was signed.
- Trusted timestamping is the process of securely tracking the creation and modification times of a document.
- Timestamping Authority (TSA) URL – server which timestamps the code signature.

Code Signing – Verification Modes

- **Low (4.8 default)** – modules that are not signed or are signed with an untrusted or expired certificate will cause warnings but still function normally. Errors occur if a signed module is modified and installation of such modules is not allowed.
- **Medium (4.9 default)** – modules must be signed be a valid trusted certificate, but this certificate may be self-signed. Installation of unsigned or invalidly signed modules is not allowed.
- High – modules must be signed by a valid trusted CA signed certificate. Installation of modules with a self-signed certificate is not allowed.

Code Signing – Jar Signer Tool

- Workbench menu select Tools > Jar Signer Tool.
- Used to code sign an already compiled module.

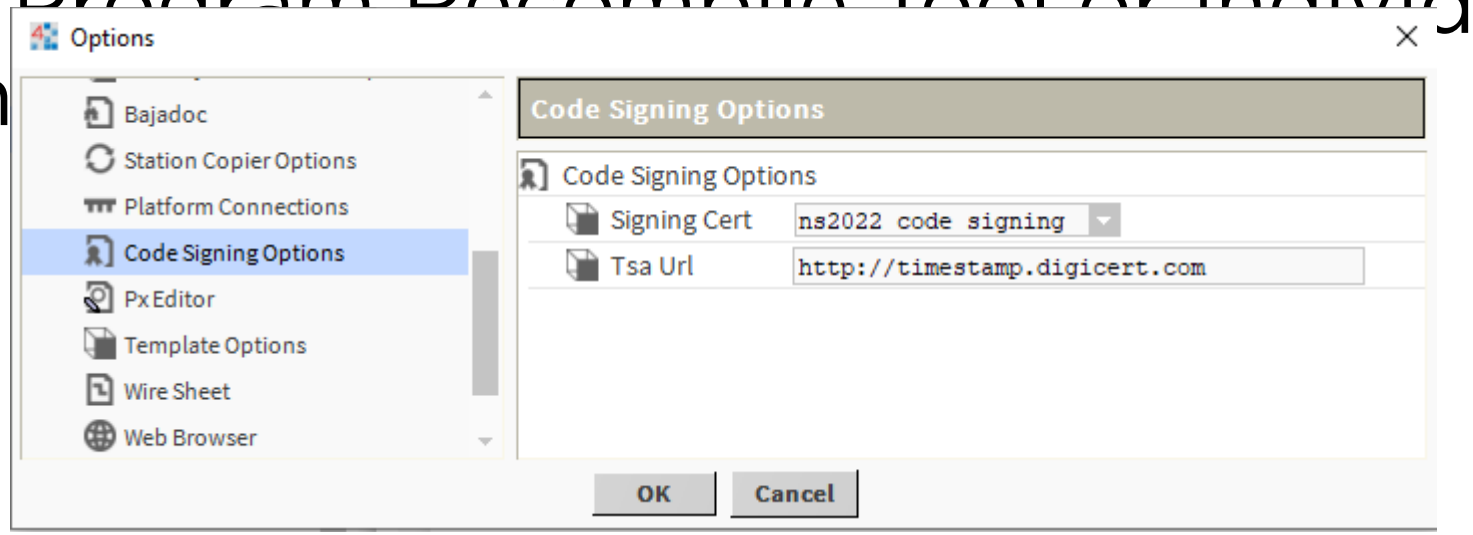


Code Signing – A Code Repository

- module://docDeveloper/doc/security/codeSigning.html

Code Signing – Program Objects

- Workbench menu select Tools → Options → Code Signing Options.
- Used to code sign a program object when compiling.
- Can use Program Recompile Tool or individual Program



Provisioning – Security Related Job Steps

- Certificate
  - Generate Certificate – in remote key store (4.6)
  - Import Signed Certificate – in remote key store (4.6)
  - Install Certificate – in remote user trust store (4.3)
  - Sign Certificate – in remote key store (4.6)
  - Export Certificate Signing Request – from remote key store (4.7)
  - Set Certificate Alias – used by Fox, Web and Platform Services (4.6)
- Station Users
  - Add Station User (4.8)
  - Remove Station User (4.8)
  - Set Station User Password (4.7)

Provisioning – Security Related Job Steps

- Platform
  - Set Platform Credentials (4.6)
  - Set System Passphrase (4.6)
  - Remove Platform User (4.12)
  - Set Platform User Password (4.12)
- Network Connection
  - Set Station Connection Credentials (4.8)
  - Setup Reciprocal Connection (4.6)
  - Set TLS Level – for Platform, Fox, Web (4.6)
- General
  - Set Property (4.8) / Remove Property (4.12)
  - Configure Niagara IdP and SAML Scheme (4.9)

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 conducting security audits.
- PKI certificates are used to **establish trust** between a client and server by verifying identities and **encrypting data exchanged over the network**.
- Security Dashboard helps **assess the security posture**.
- Code signing confirms software author and

Questions

NS2022
ACCELERATING INNOVATION

TRIDIUM