Information

- Questions will be answered at the end.
- Please submit questions to *Erick Mendoza* using the chat function.

TRIDIUM

Securing Niagara, Part 2

- Java 1.7.0.25 Update Announcement
- Review basic hardening steps
- Discuss basic usage of SSL functionality
- Discuss VPNs
- Highlight recent update changes
- The Future
- Questions

TRIDIUM

Review

- System security is like an onion:
  - No, not because it smells bad (although it can)
  - It is made up of **LAYERS**

TRIDIUM

Review

Passwords

- Change the Default Platform Credentials
- Use Strong Passwords
- Enable the Account Lockout Feature
- Use the Password History
- Use the Password Reset Feature
- Leave the “Remember These Credentials” Box Unchecked

TRIDIUM

Review

Account Management

- Use a Different Account for Each User
- Assign the Minimum Required Permissions
- Use a Single Super User
- Require Super User Permissions for Program Objects
- Use the Minimum Required Permissions for External Accounts

TRIDIUM

Review

Authentication

- Use “Digest” Authentication in the FoxService
- Set the FoxService Legacy Authentication to “Strict”
- Use “cookie-digest” Authentication in the WebService

TRIDIUM

Review

TLS/SSL & Certificate Management

- Enable Platform SSL Only (3.7+ only)
- Enable Fox SSL Only (3.7 only)
- Enable Web SSL Only
- Enable SSL on Other Services
- Set Up Certificates

TRIDIUM

Review

Additional Settings

- Disable FTP and Telnet
- Remove the serial shell jumper
- Disable Unnecessary Services
- Blacklist Sensitive Files and Folders
- Update NiagaraAX to the Latest Release

TRIDIUM

Review

External Factors

- Install JACEs in a Secure Location (locked room, wiring in conduit, etc)
- Make Sure that Stations Are Behind a VPN
- Even internally, make sure that stations are behind a firewall with only necessary ports open
- Protect your backups

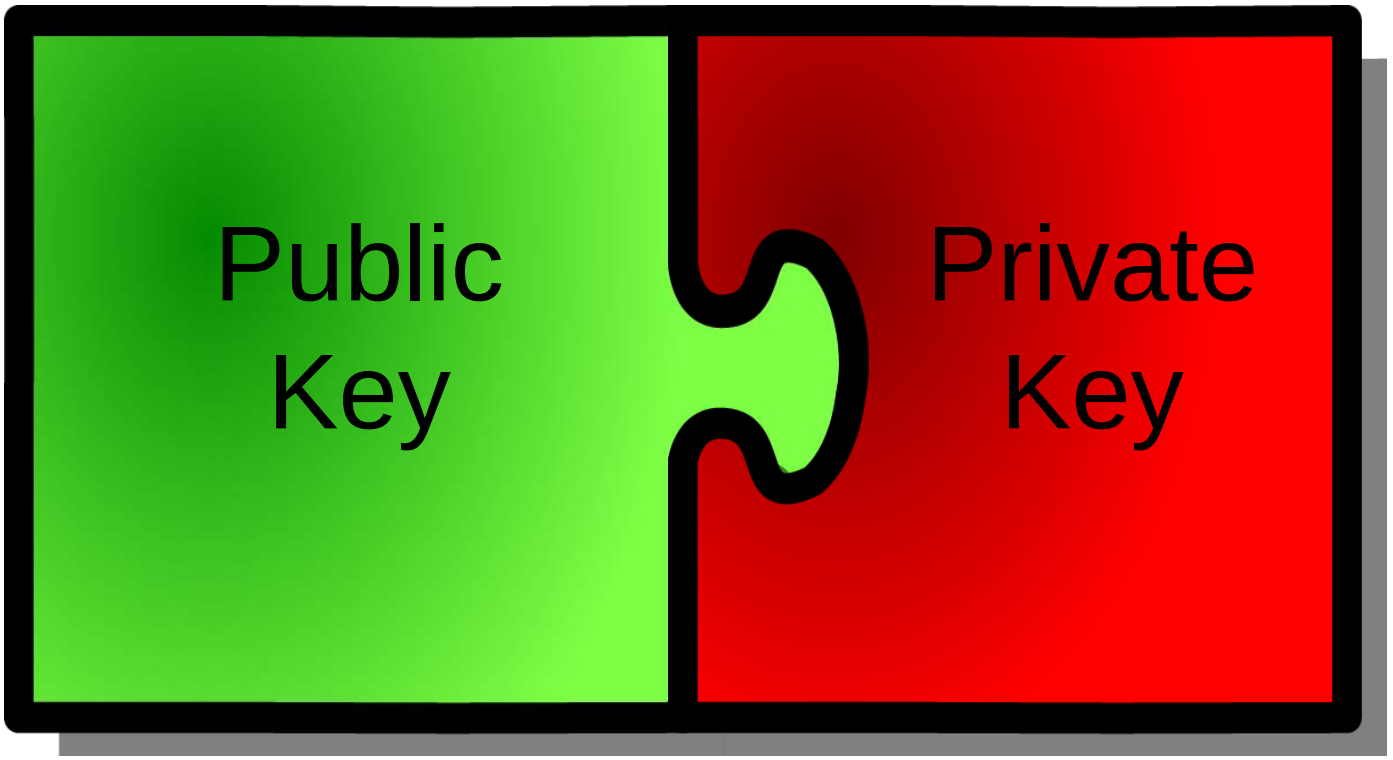
TRIDIUM

SSL

- Key Pair
- Certificate
- Self Signed Certificate
  - Trusted Certificate
- Certificate Authority (CA)
- Certificate Chain
- SSL Handshake
- SSL and NiagaraAX

TRIDIUM

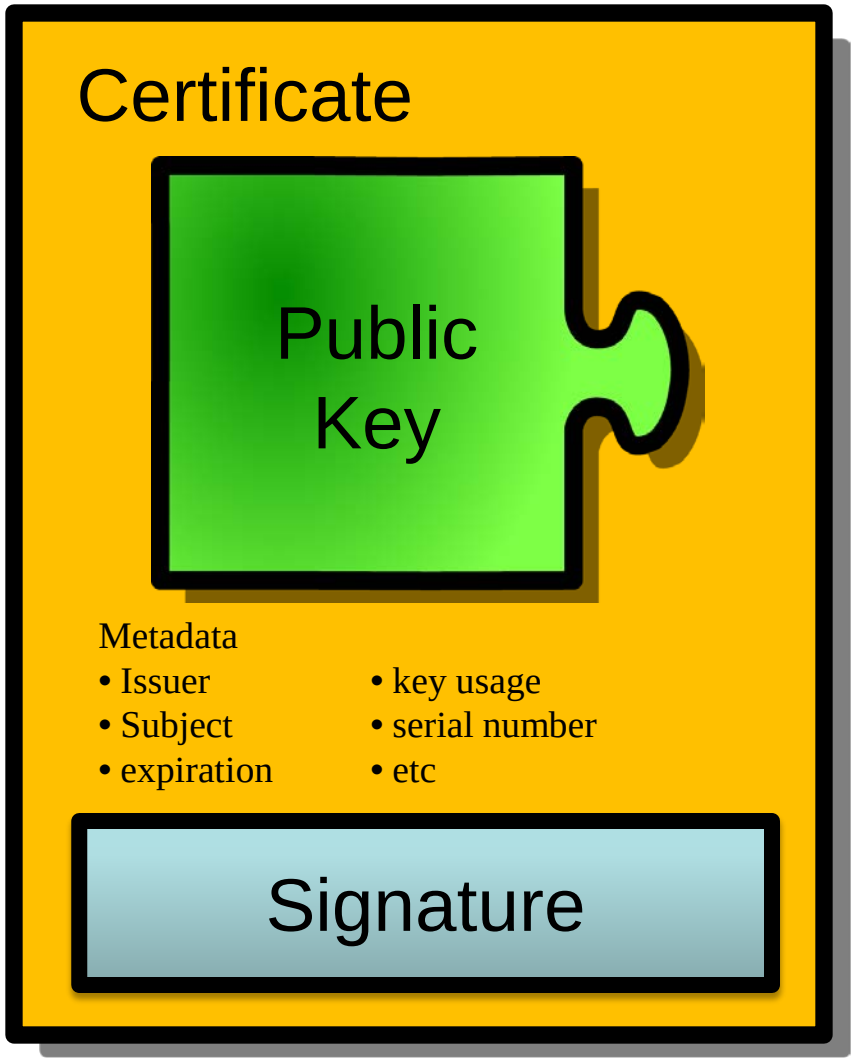
SSL – Key Pair



Common sizes: 1024 and 2048 bits

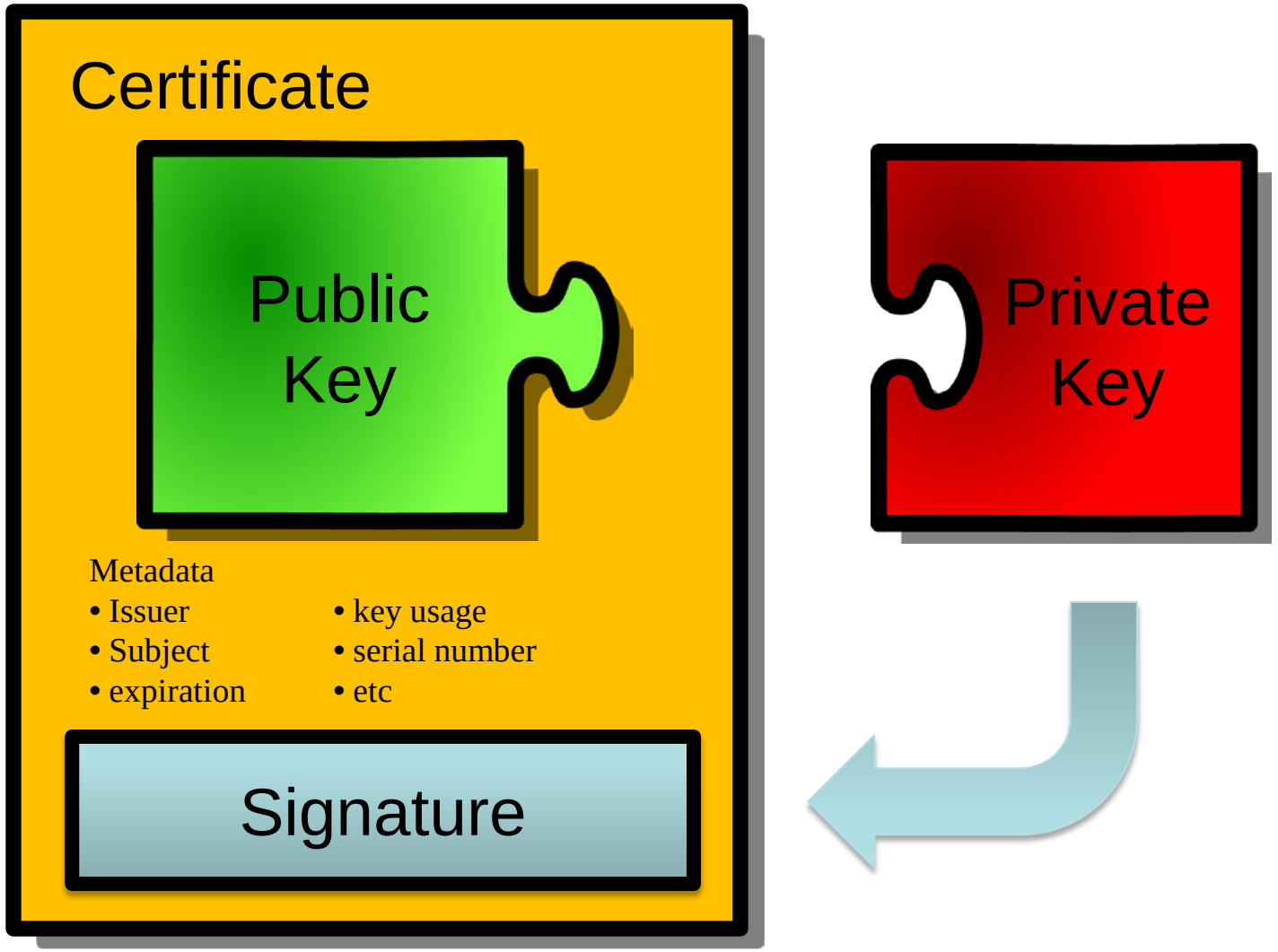
TRIDIUM

SSL – Certificate



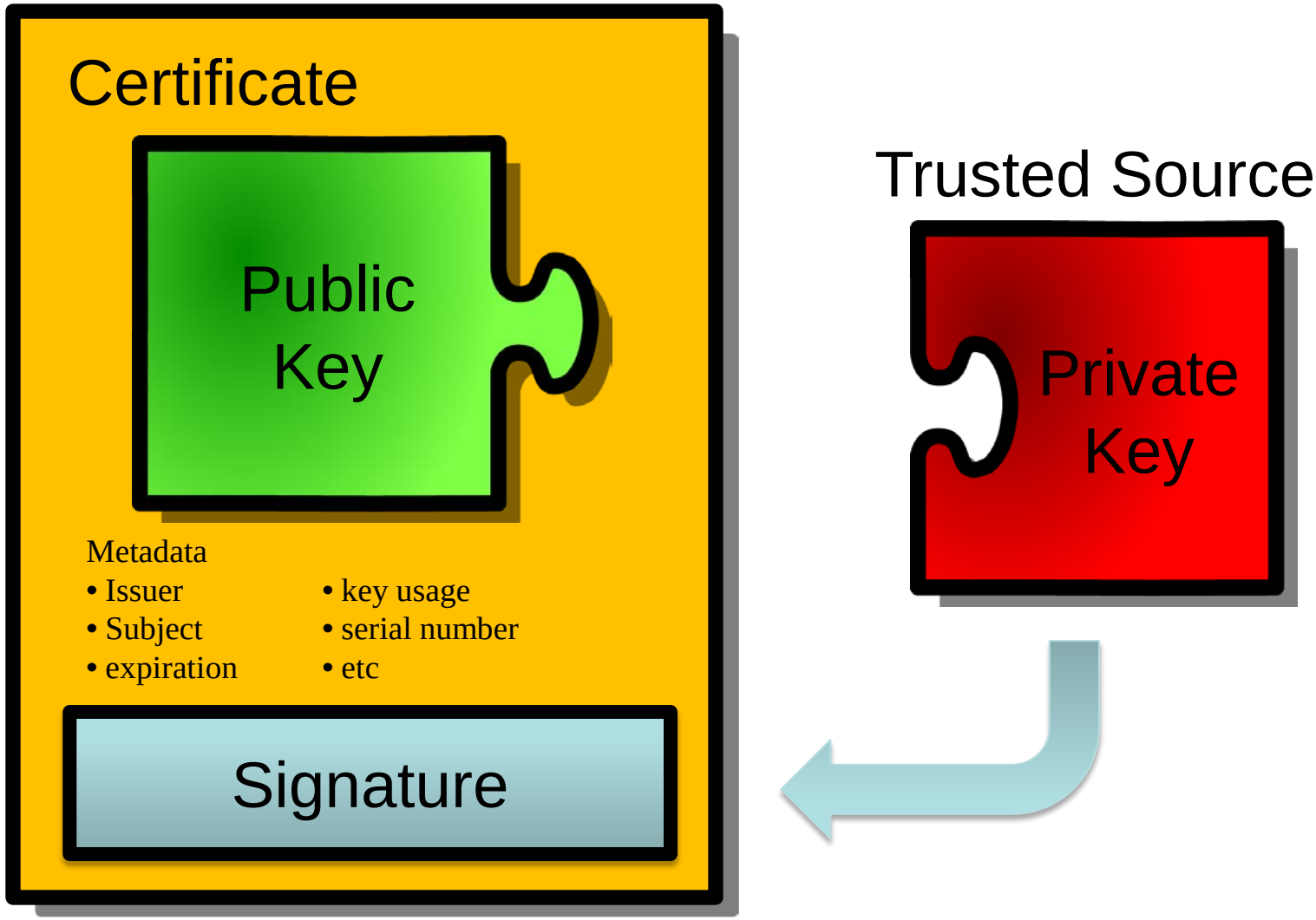
TRIDIUM

SSL – Self Signed Certificate



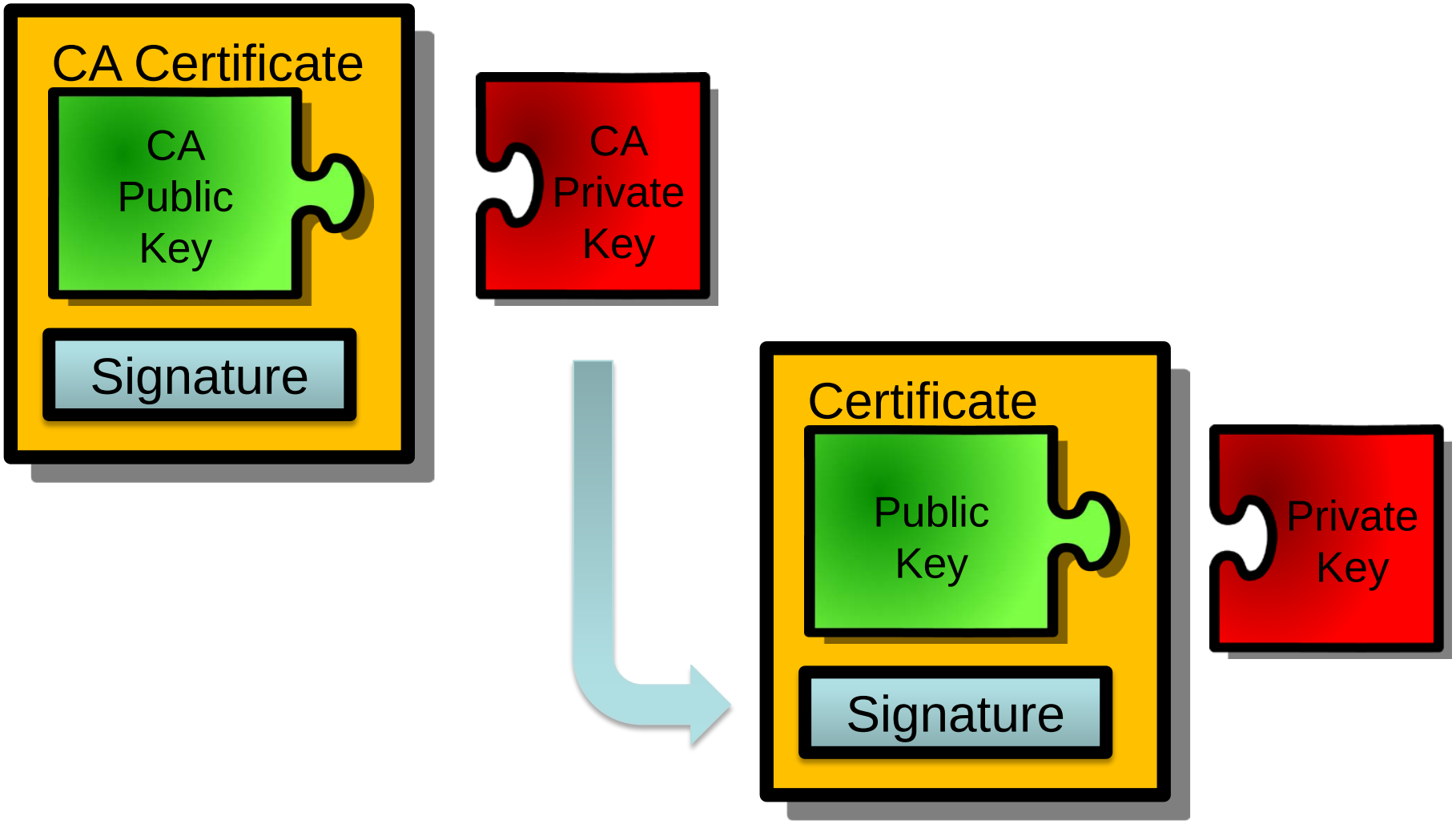
TRIDIUM

SSL – Trusted Certificate



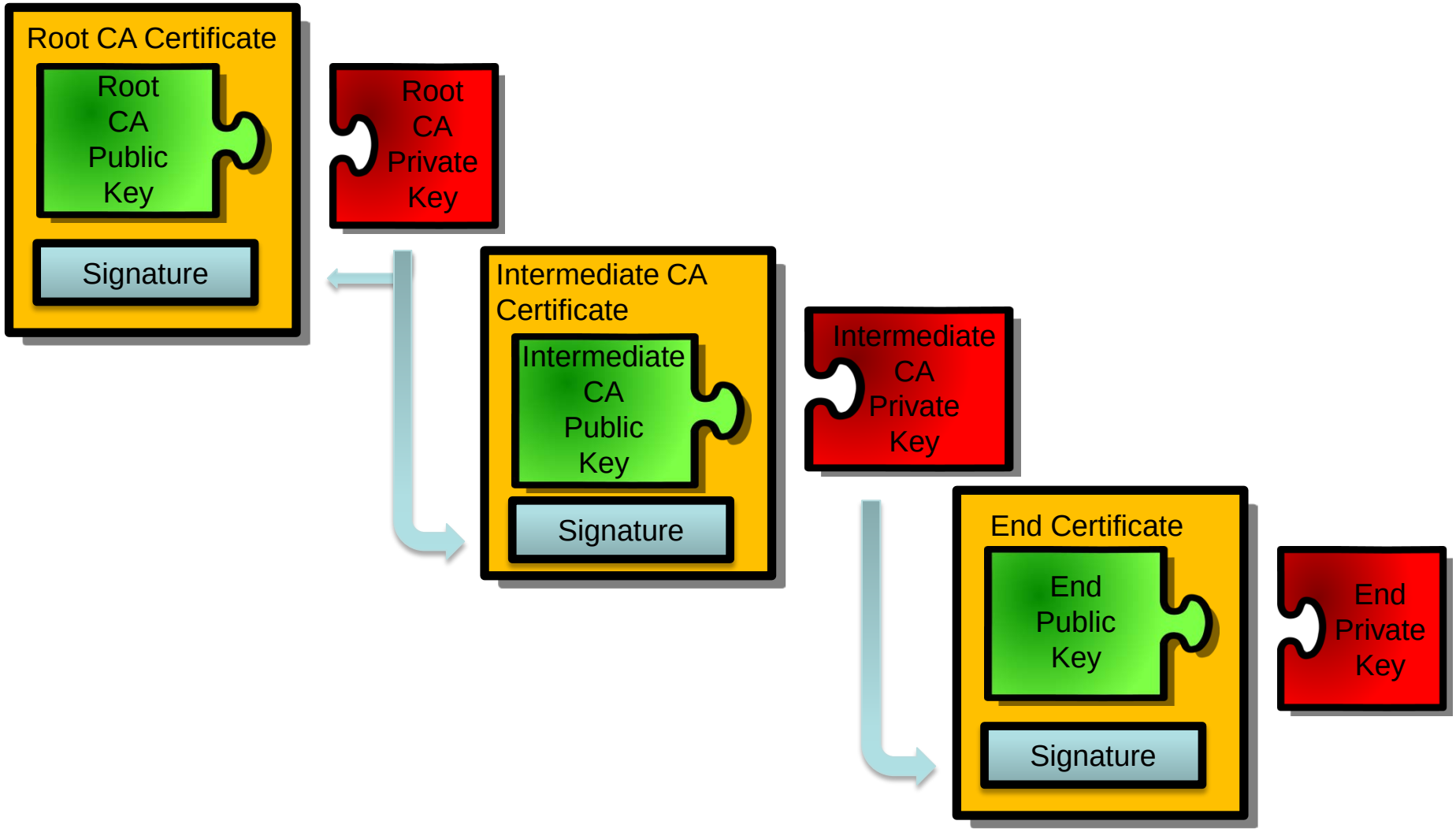
TRIDIUM

SSL – Signed Certificate



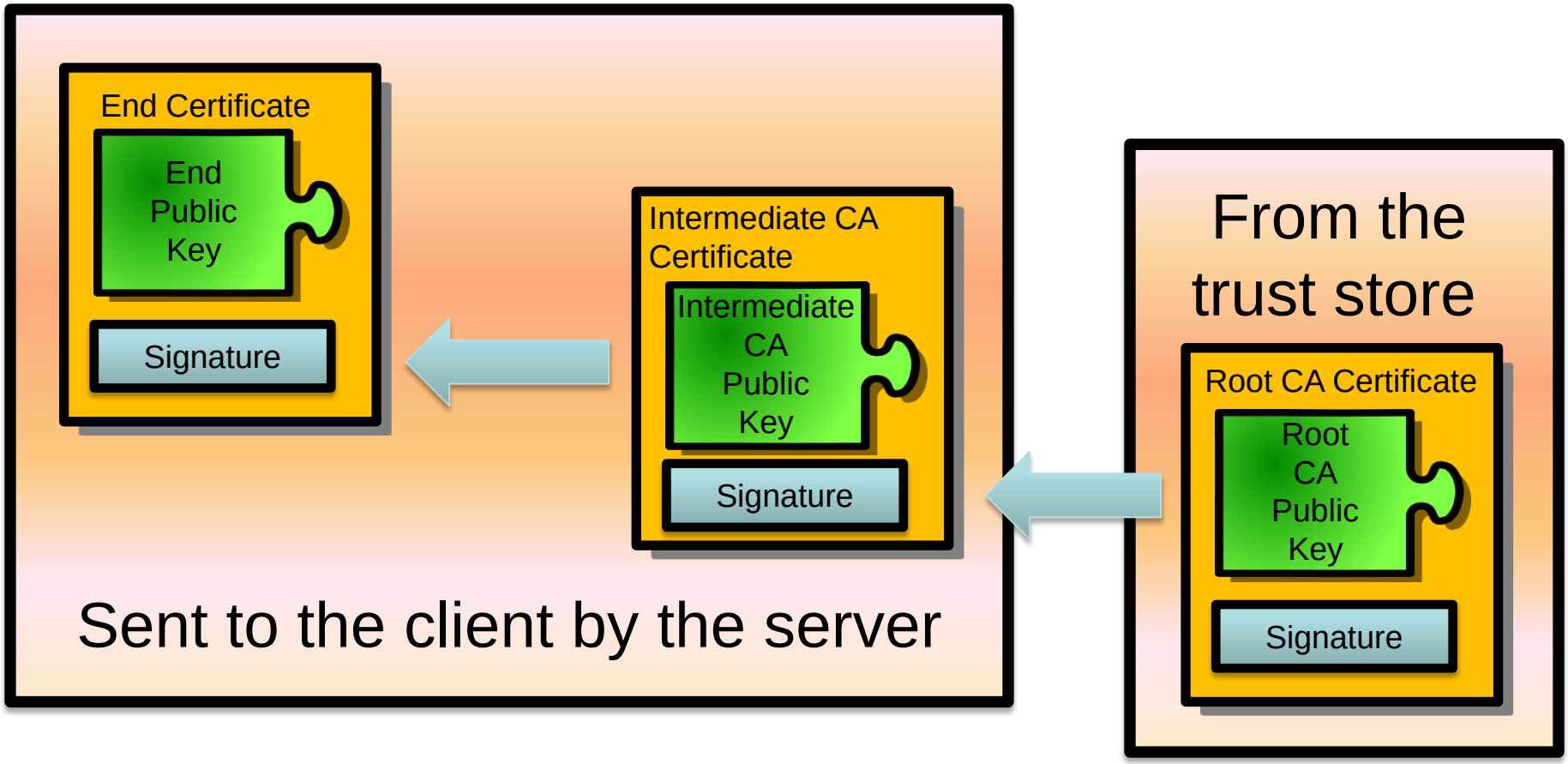
TRIDIUM

SSL – Certificate Chain



TRIDIUM

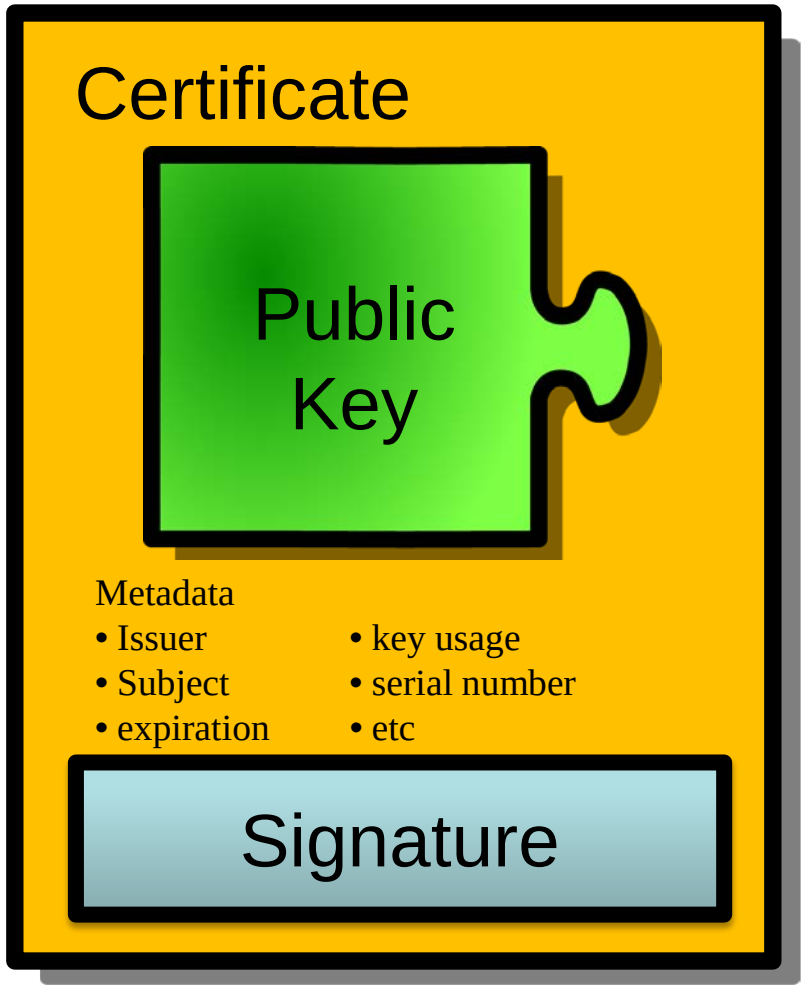
SSL – Certificate Validation



TRIDIUM

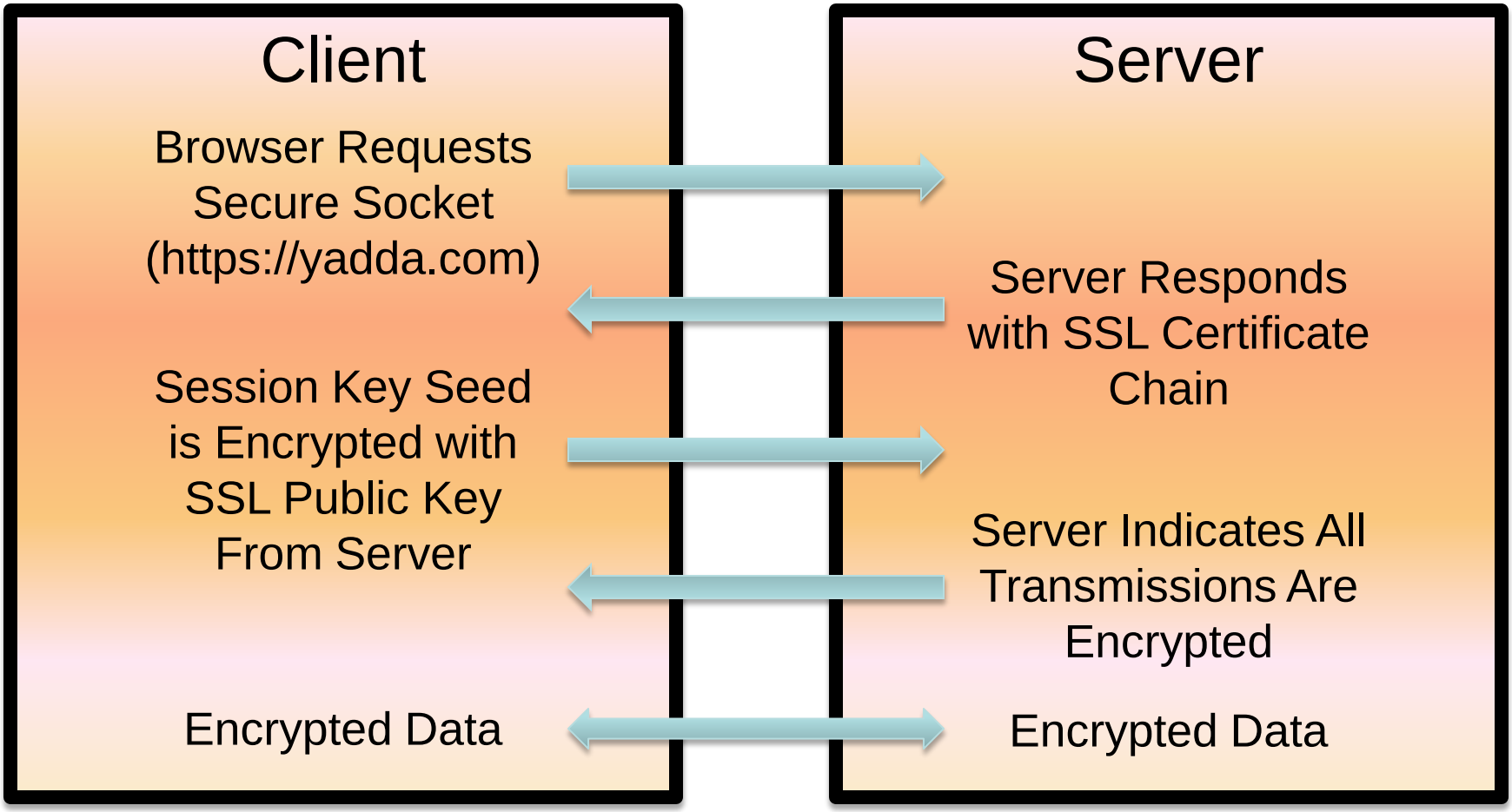
SSL – Certificate Validation

- Certificate chain is valid and trusted
- Distinguished name matches server address
- Key usage is valid
- Certificate is in the valid date range



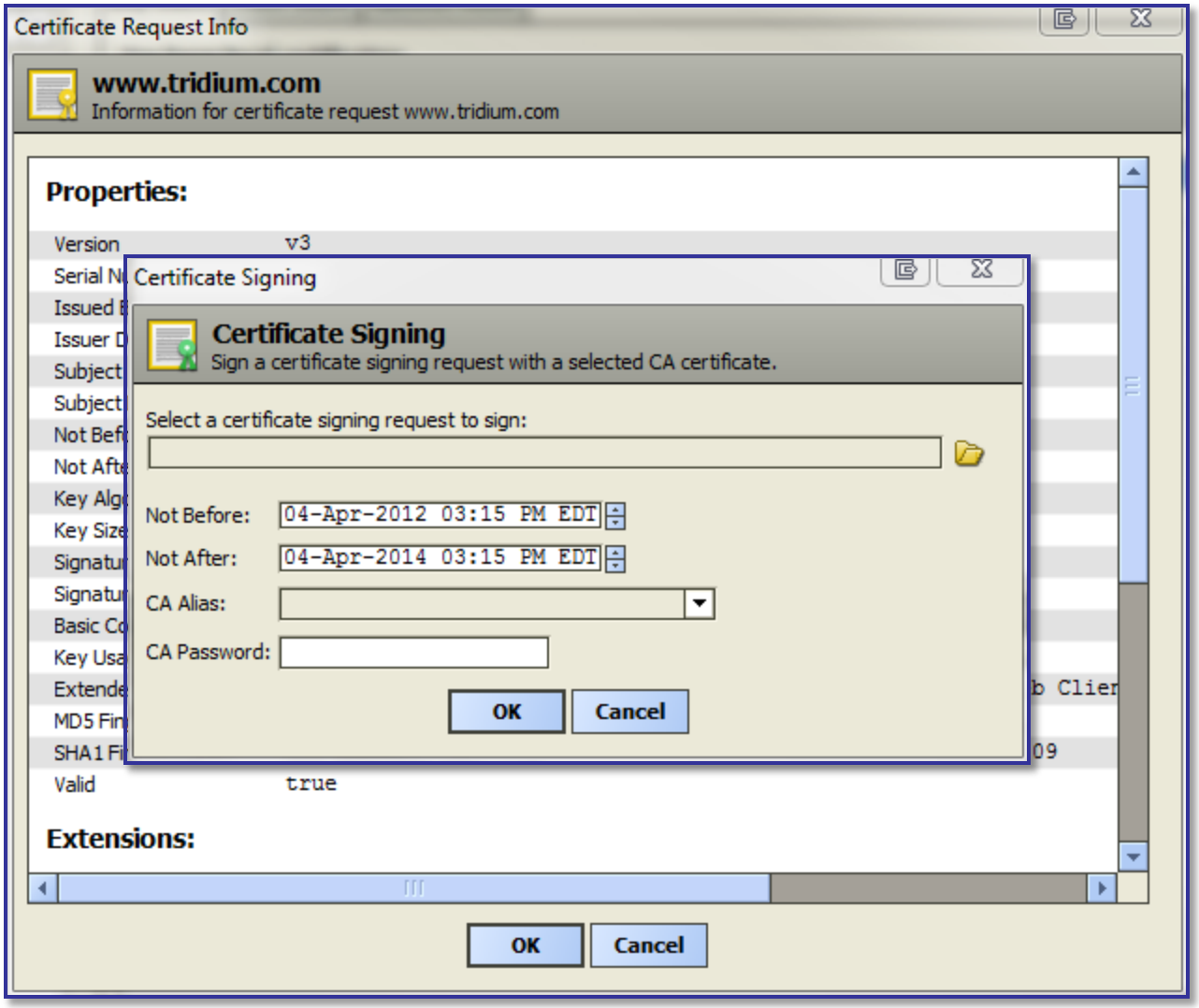
TRIDIUM

SSL – Handshake



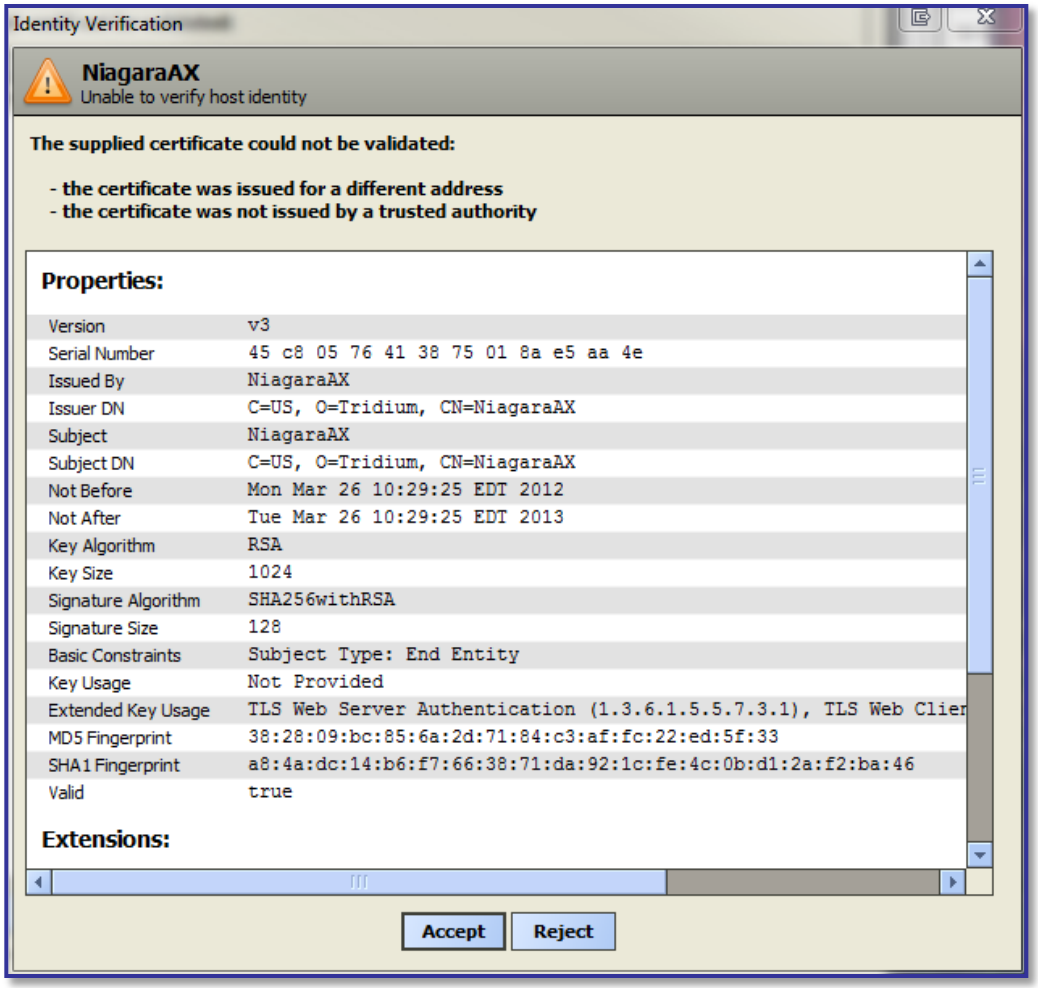
TRIDIUM

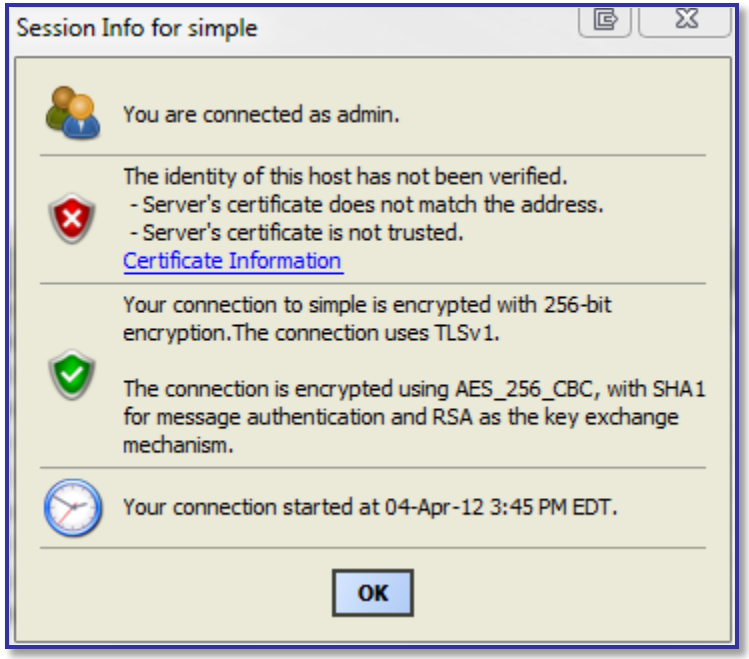
SSL – Certificate Tools



TRIDIUM

SSL – Client Interface

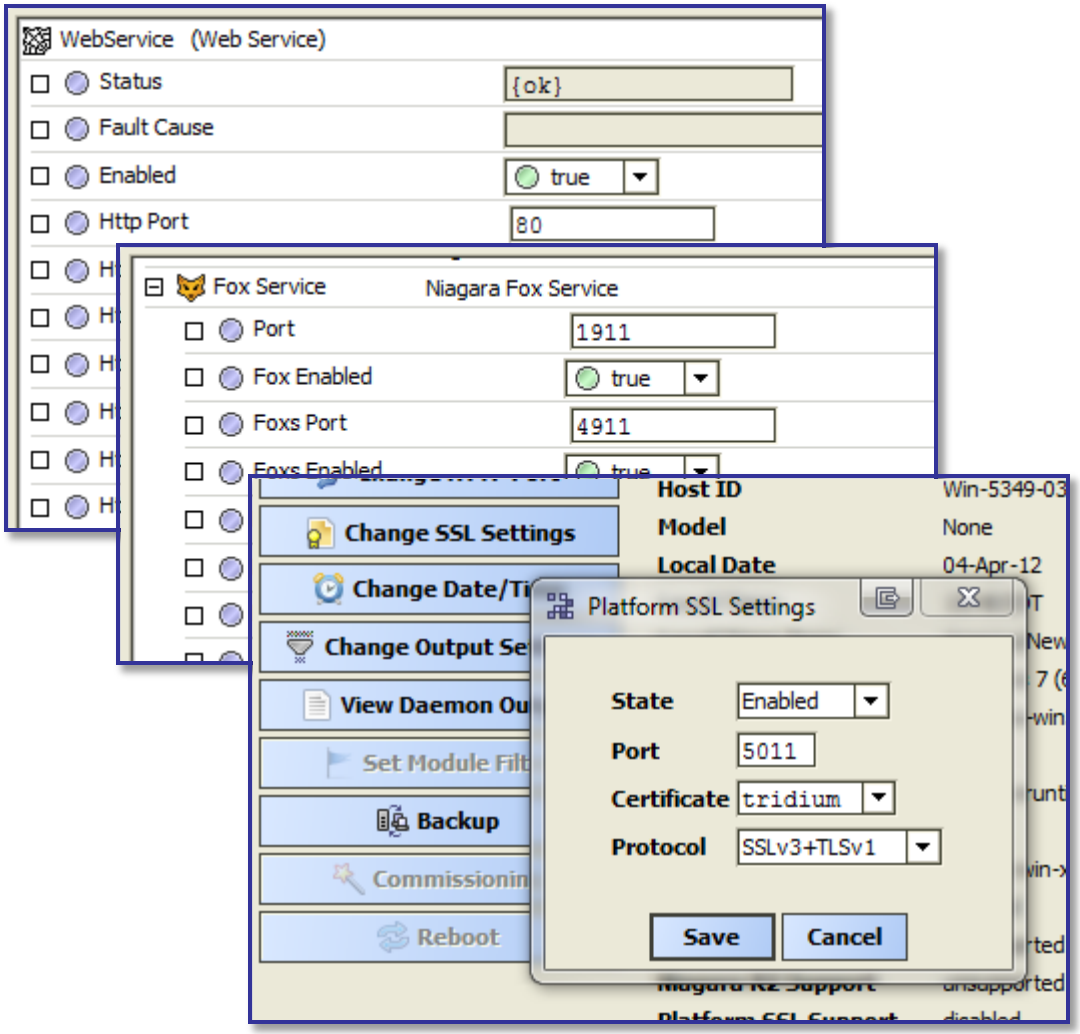




TRIDIUM

SSL – Server Configuration

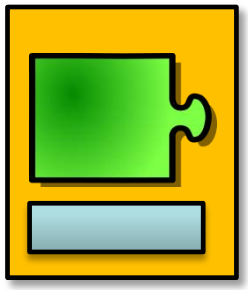
- Web Service (port 443)
- Fox Service (port 4911)
- Niagarad (port 5011)

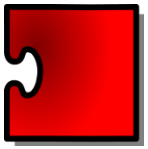


TRIDIUM

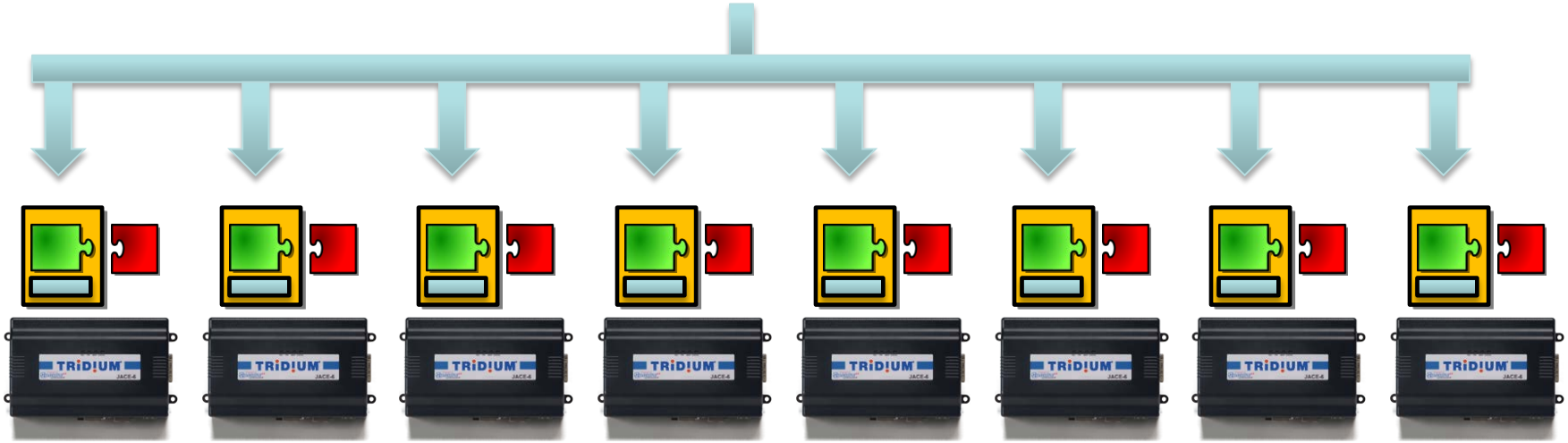
SSL – Small Network Example

CA Certificate Installed
on Client Machines
in Their Trust Store





CA Private Key Used to
Sign Server Certificates



TRiDiUM

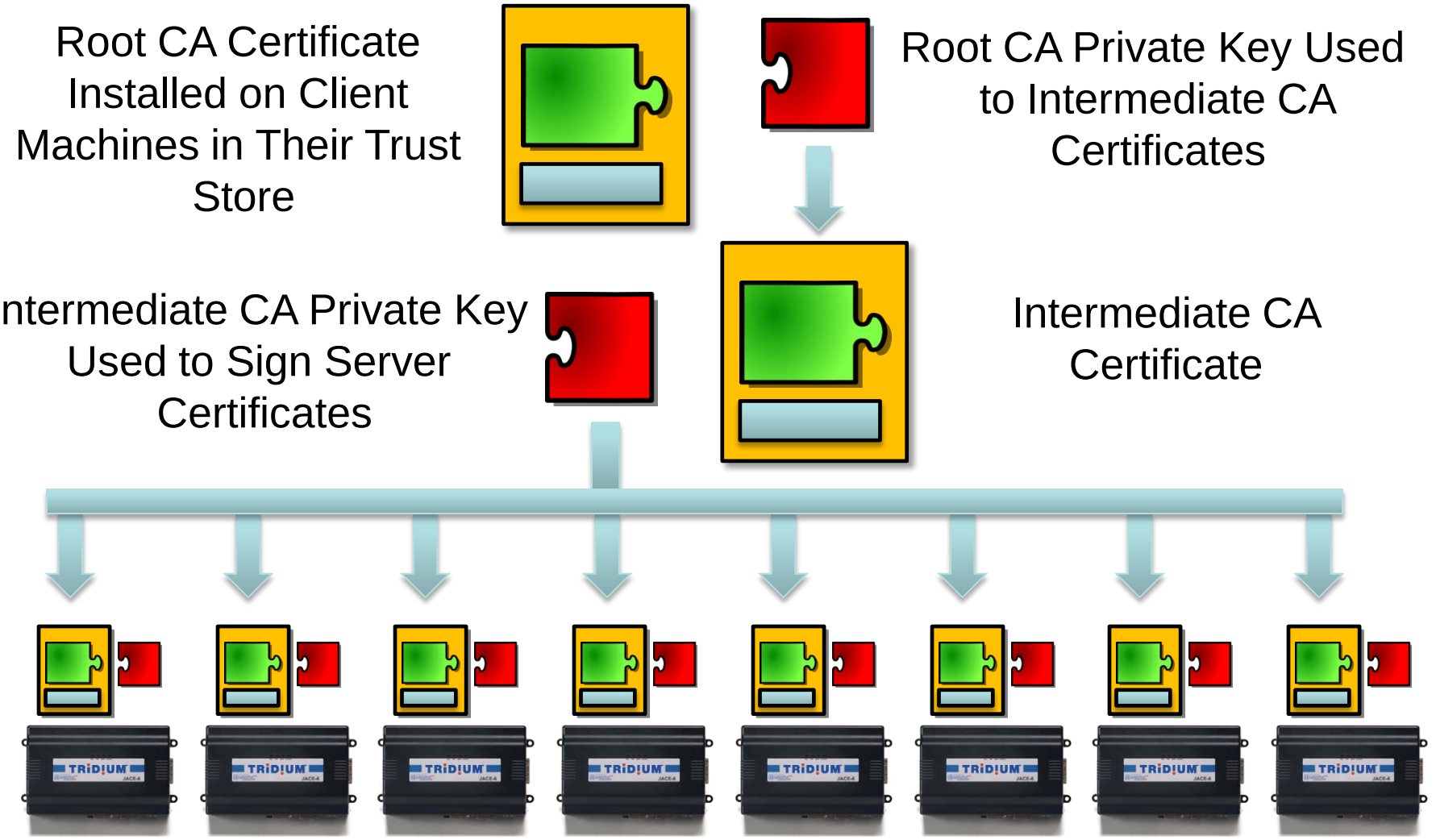
SSL – Large Network Example

Root CA Certificate Installed on Client Machines in Their Trust Store

Root CA Private Key Used to Intermediate CA Certificates

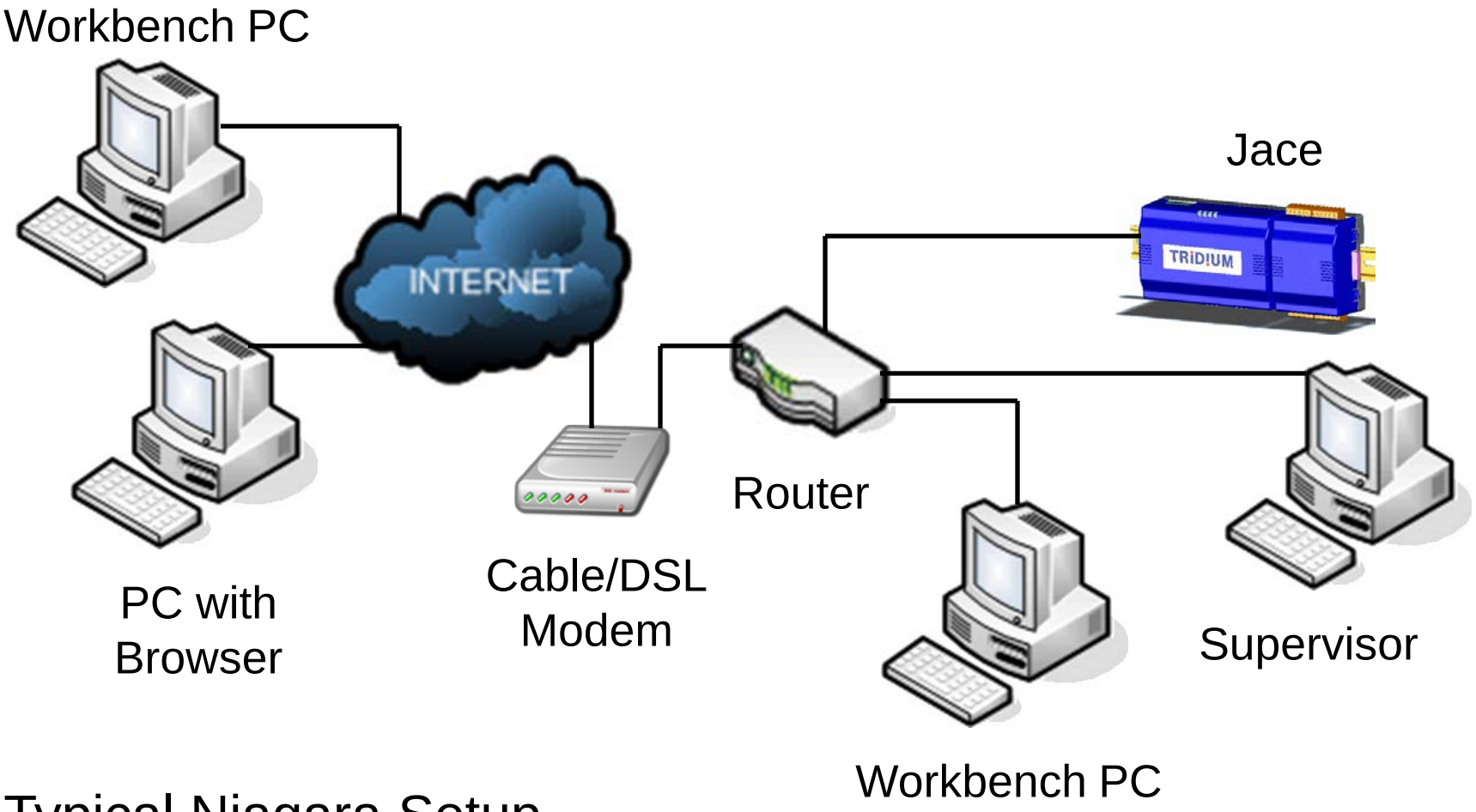
Intermediate CA Private Key Used to Sign Server Certificates

Intermediate CA Certificate



TRIDIUM

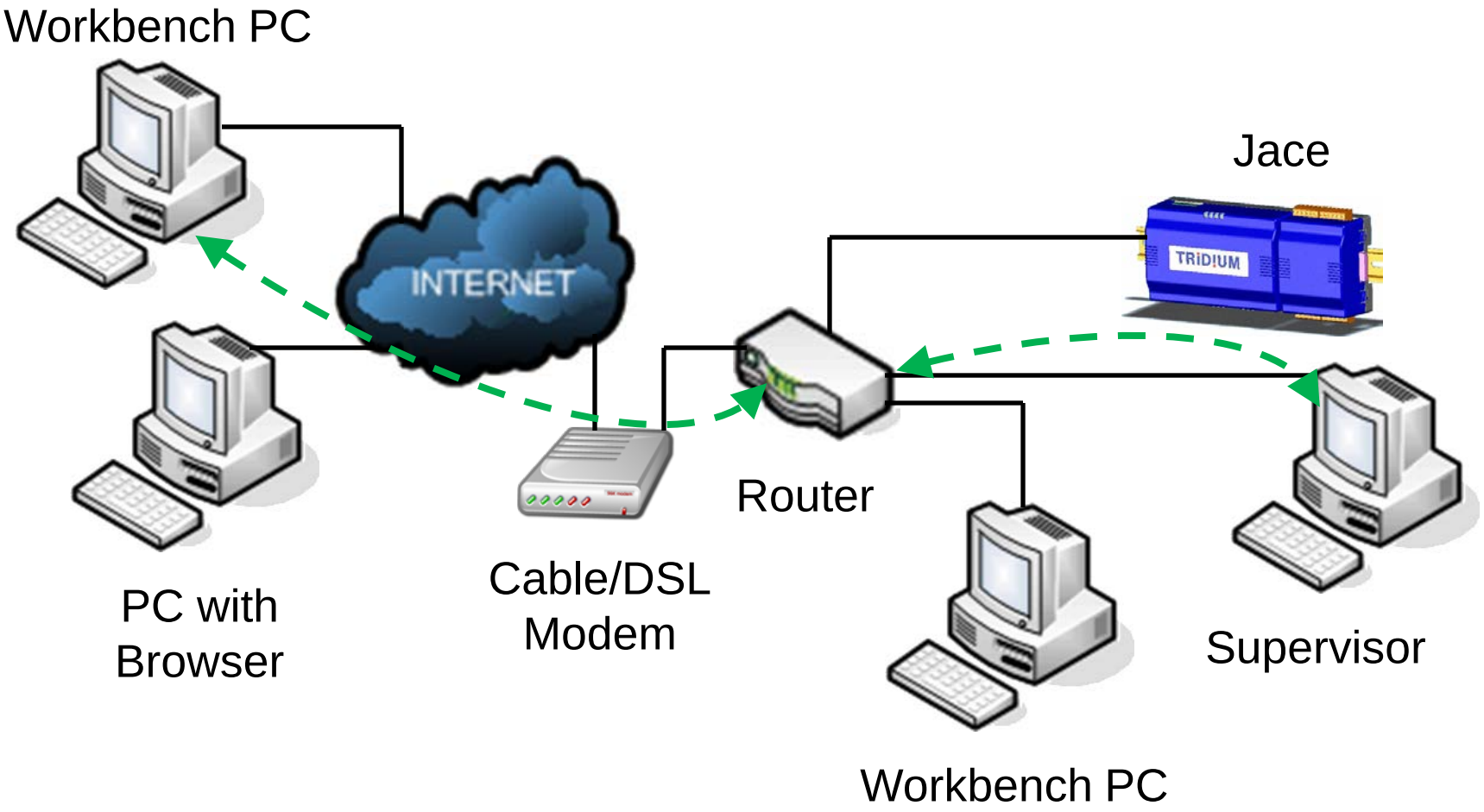
VPN



Typical Niagara Setup

- with all ports forwarded, it gives full access to web, fox, niagarad

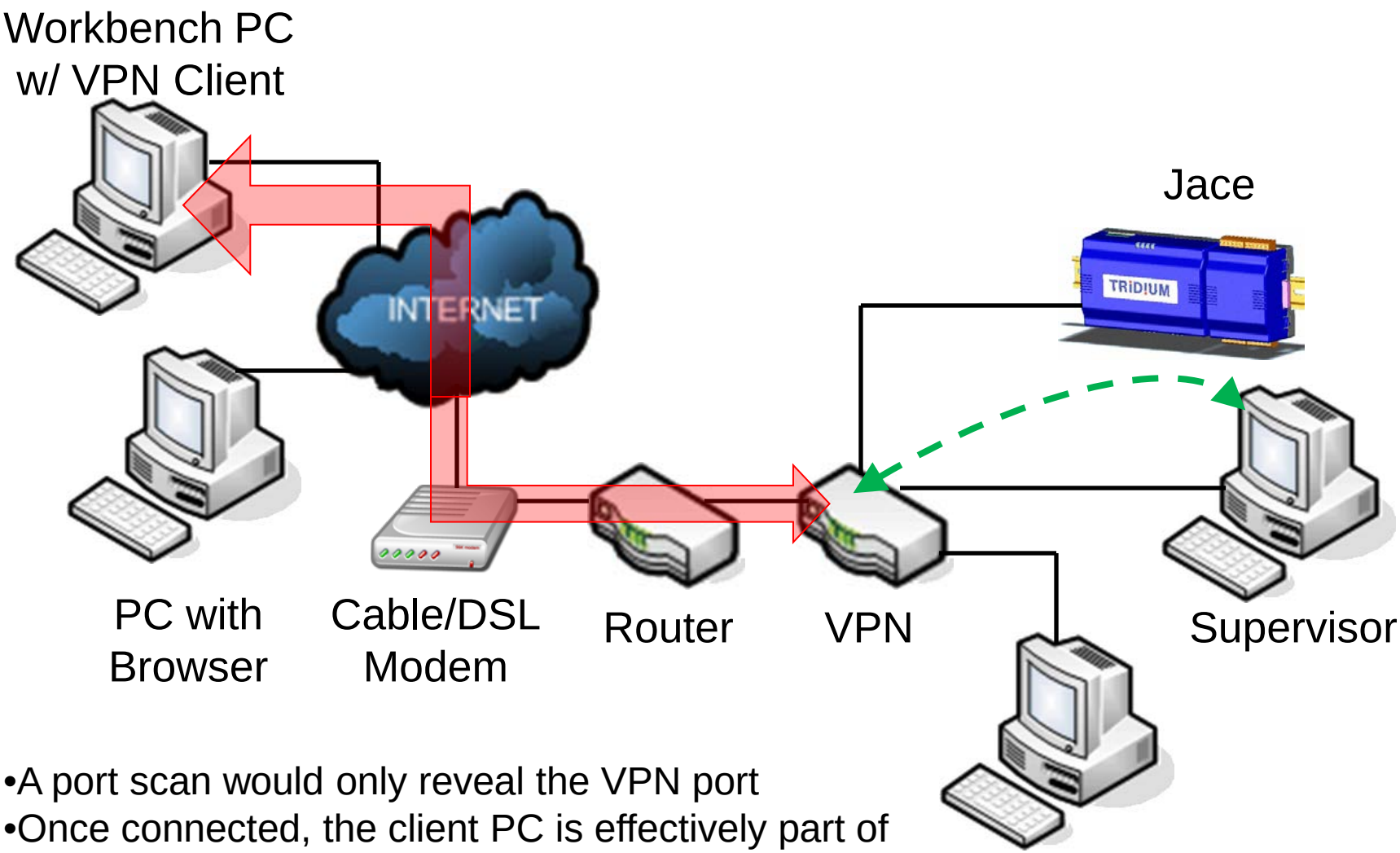
VPN



•A port scan would reveal all open Niagara ports
•Attackers could use weak credentials or known vulnerabilities to exploit the system.

TRIDIUM

VPN



- A port scan would only reveal the VPN port
- Once connected, the client PC is effectively part of the local network.

TRIDIUM

VPN

- The VPN Guide discusses all this in great detail
- It also provides an example setup using a ZyWall USG 20
- Supports the built in VPN clients in Windows, Android and iOS.
- In addition to client to server connections, a VPN can also support a persistent connection between remote networks
  - Station to station connections

TRIDIUM

Niagara Updates

- Enhanced password management
  - PBKDF2-SHA256
  - AES-256
- Enhanced digest authentication
  - SCRAM-SHA256
- Miscellaneous other security fixes

TRIDIUM

The Future…

- Always improving!
- Encrypted backups
- Rolling keys
- Two factor authentication
- Sandboxing
- …and more!!

TRIDIUM

FAQ

- Won’t SSL slow things down?
- What is the difference between a firewall and a VPN?
- If I’m using a VPN, do I need to use SSL?
- If I’m using SSL, do I need to use a VPN?
- If Tridium is pushing “secure by default”, why isn’t SSL enabled by default?

TRIDIUM

Sources for Good Information

- Niagara Hardening Guide
  - Available next week
- VPN Guide
  - Available next week
- Niagara SSL Documentation (docSSL)
  - In 3.7 release
- SNA Forum on LinkedIn
- ICS-CERT
  - http://ics-cert.us-cert.gov/
- Niagara Central
  - http://www.niagara-central.com
- Schneier on Security
  - http://www.schneier.com/

TRIDIUM

Questions

TRIDIUM