

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



# 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



# Review



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



# 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

# 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

# Review

---

## Authentication

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

## 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

## 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





# 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

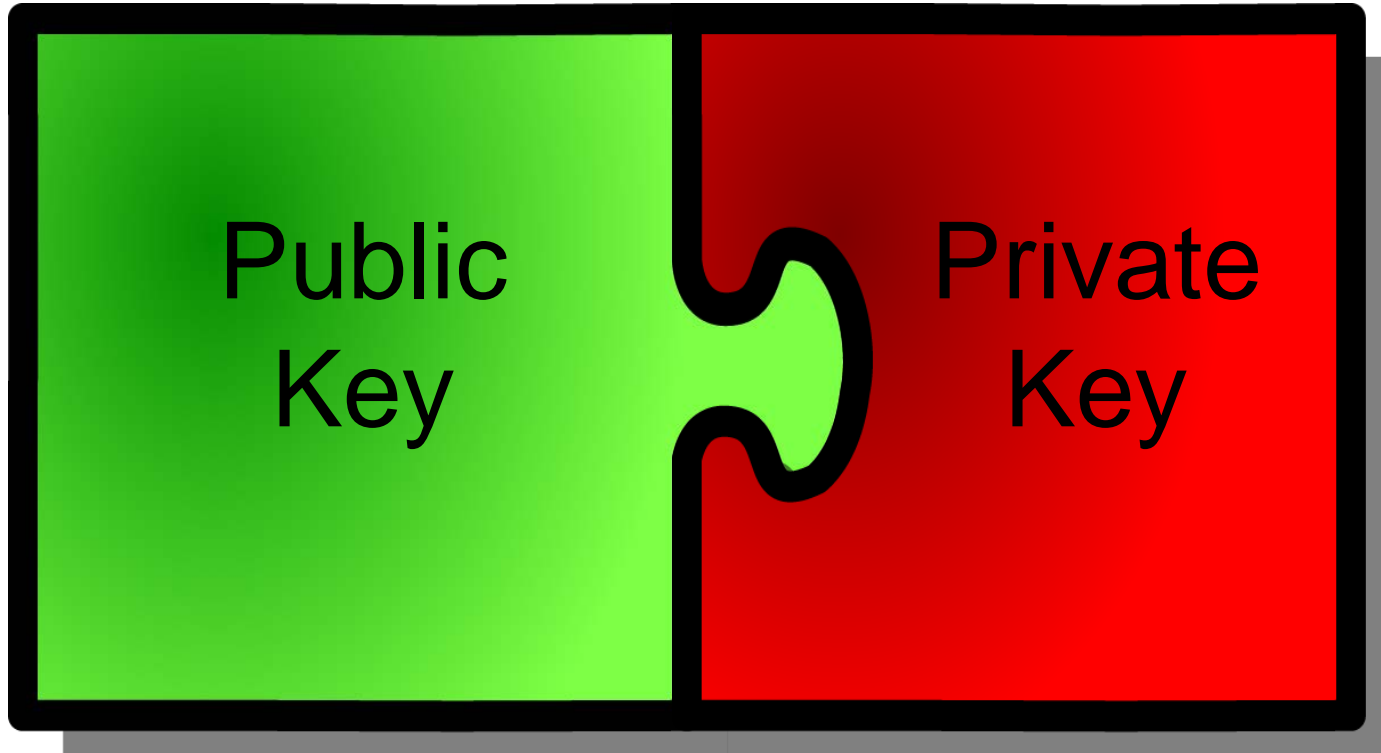


# SSL

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



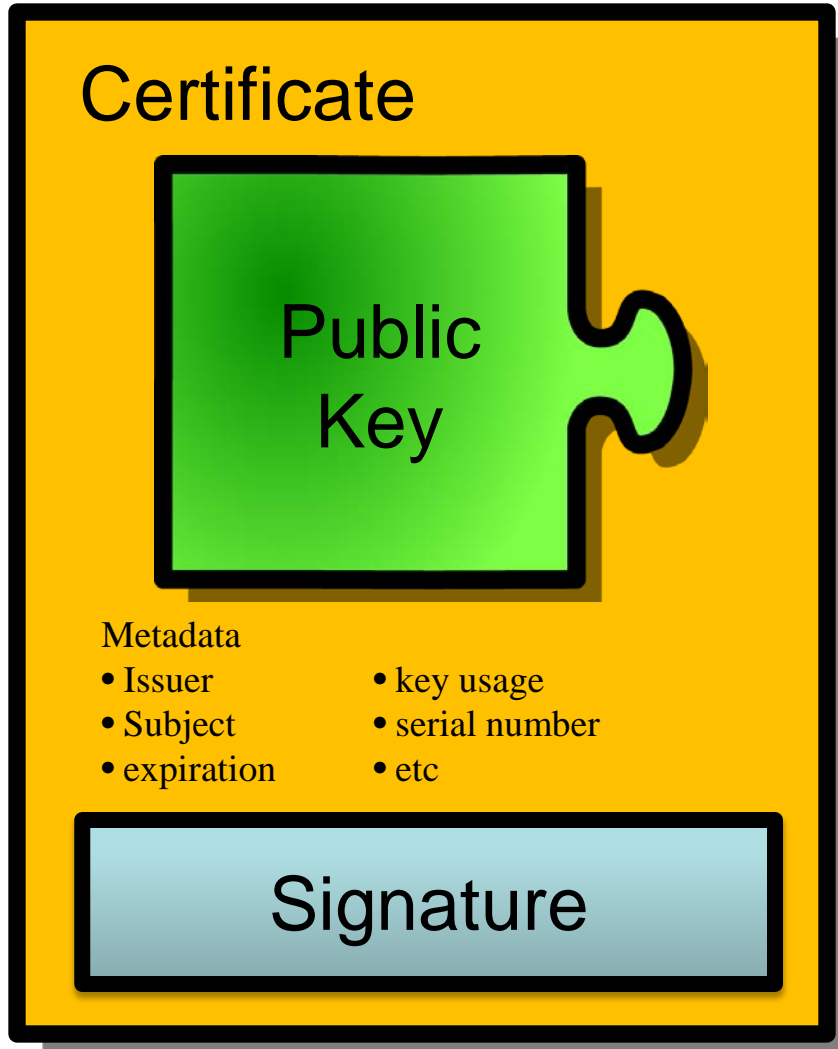
# SSL – Key Pair



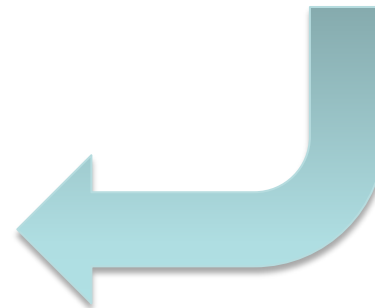
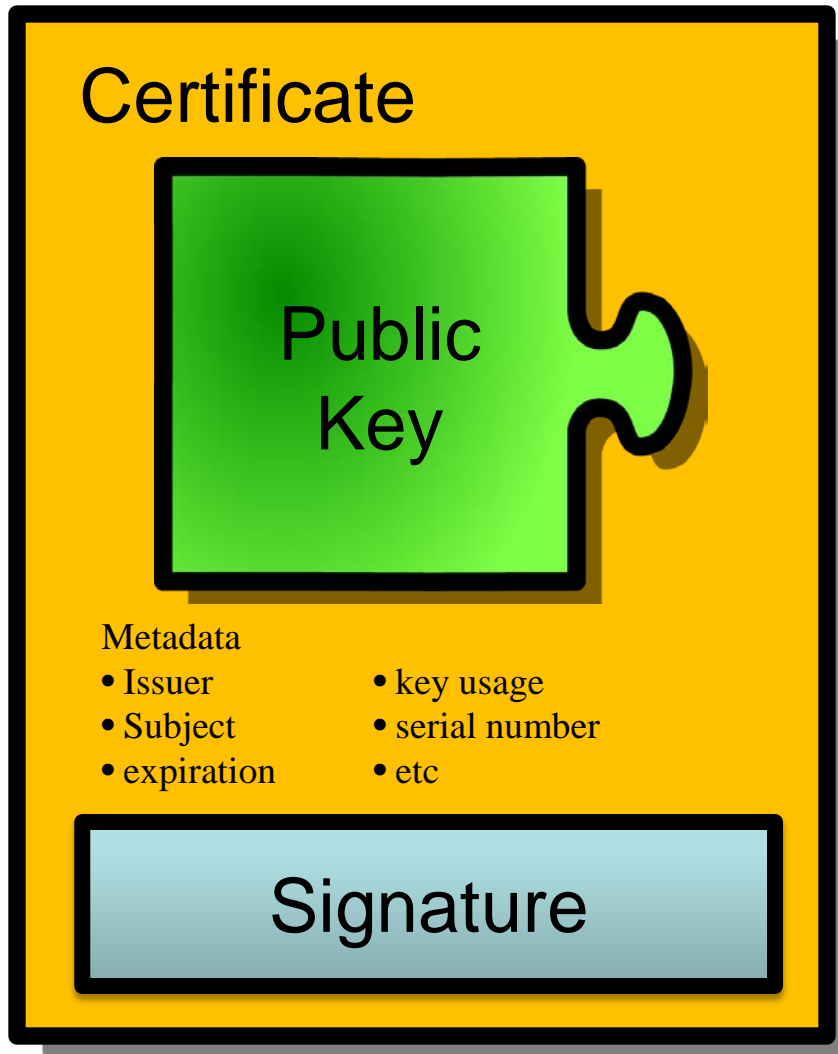
Common sizes: 1024 and 2048 bits



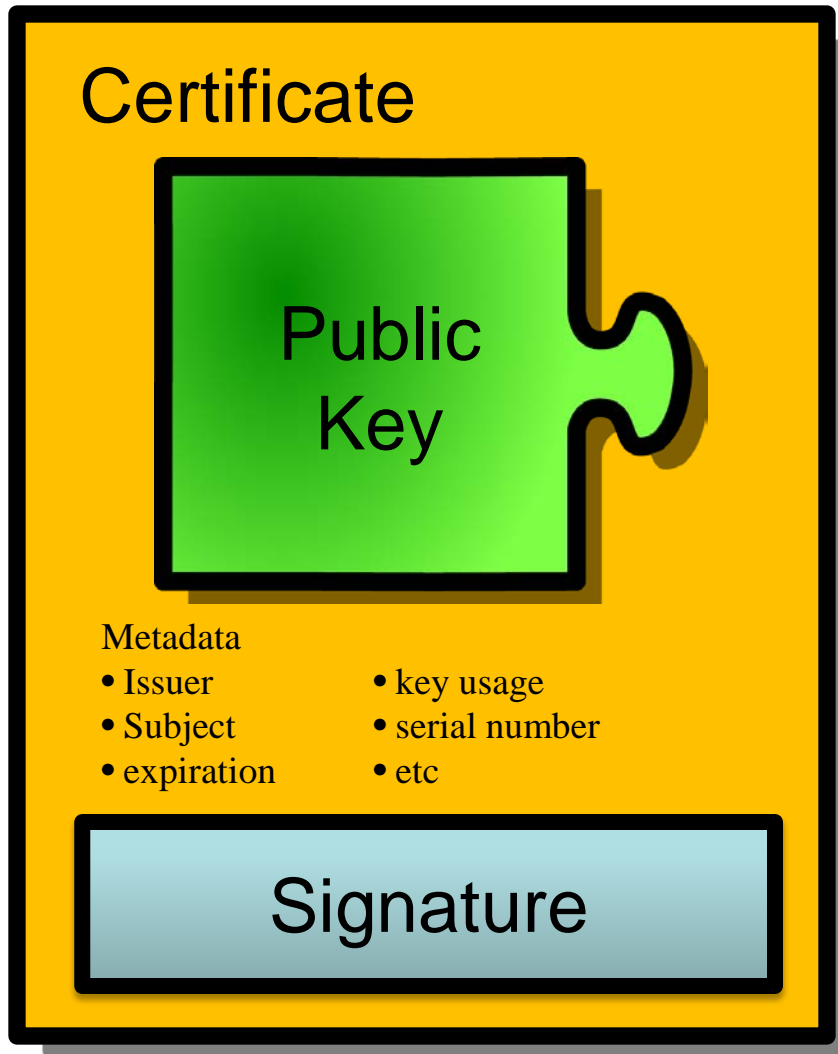
# SSL – Certificate



# SSL – Self Signed Certificate



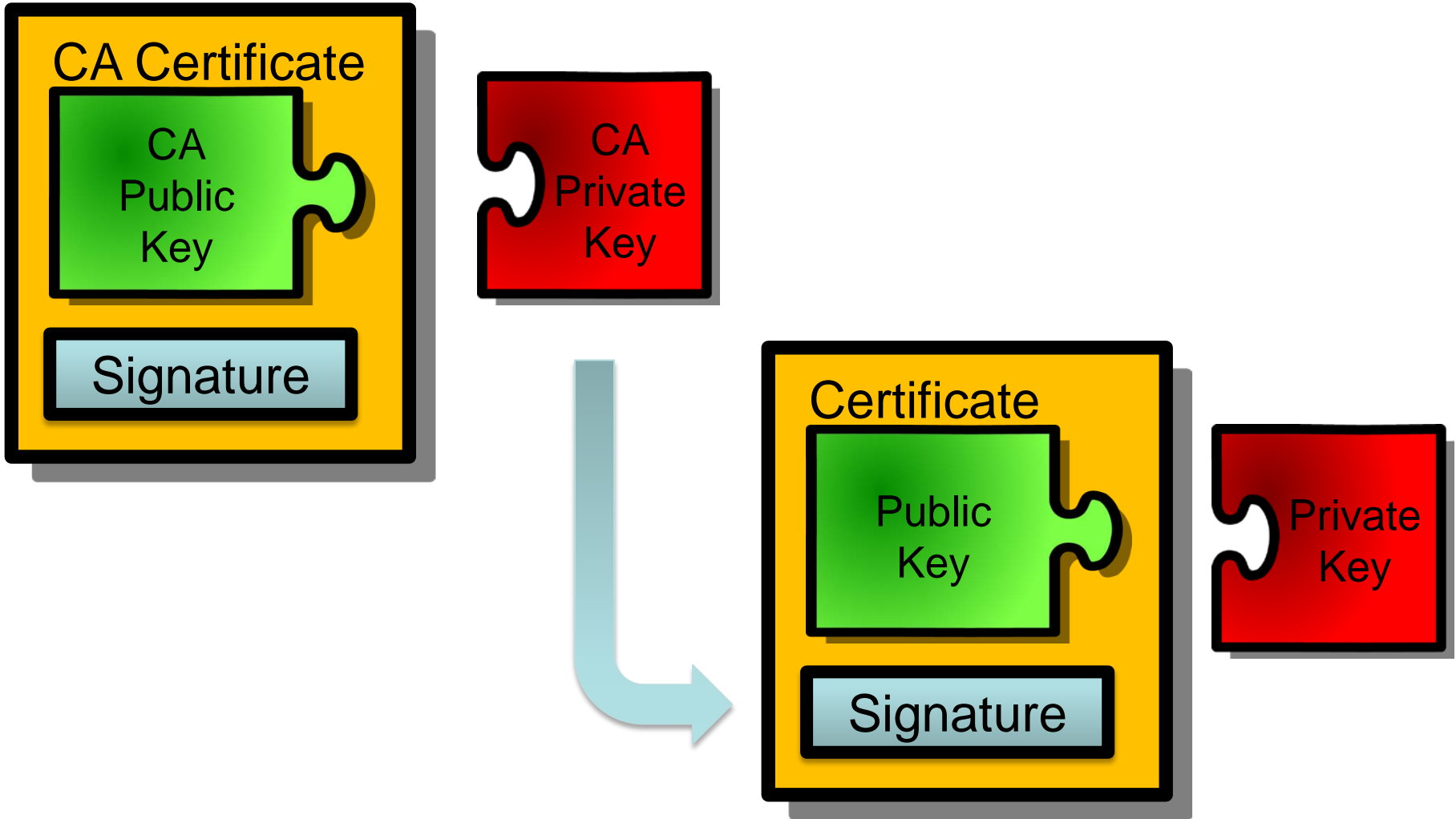
# SSL – Trusted Certificate



Trusted Source

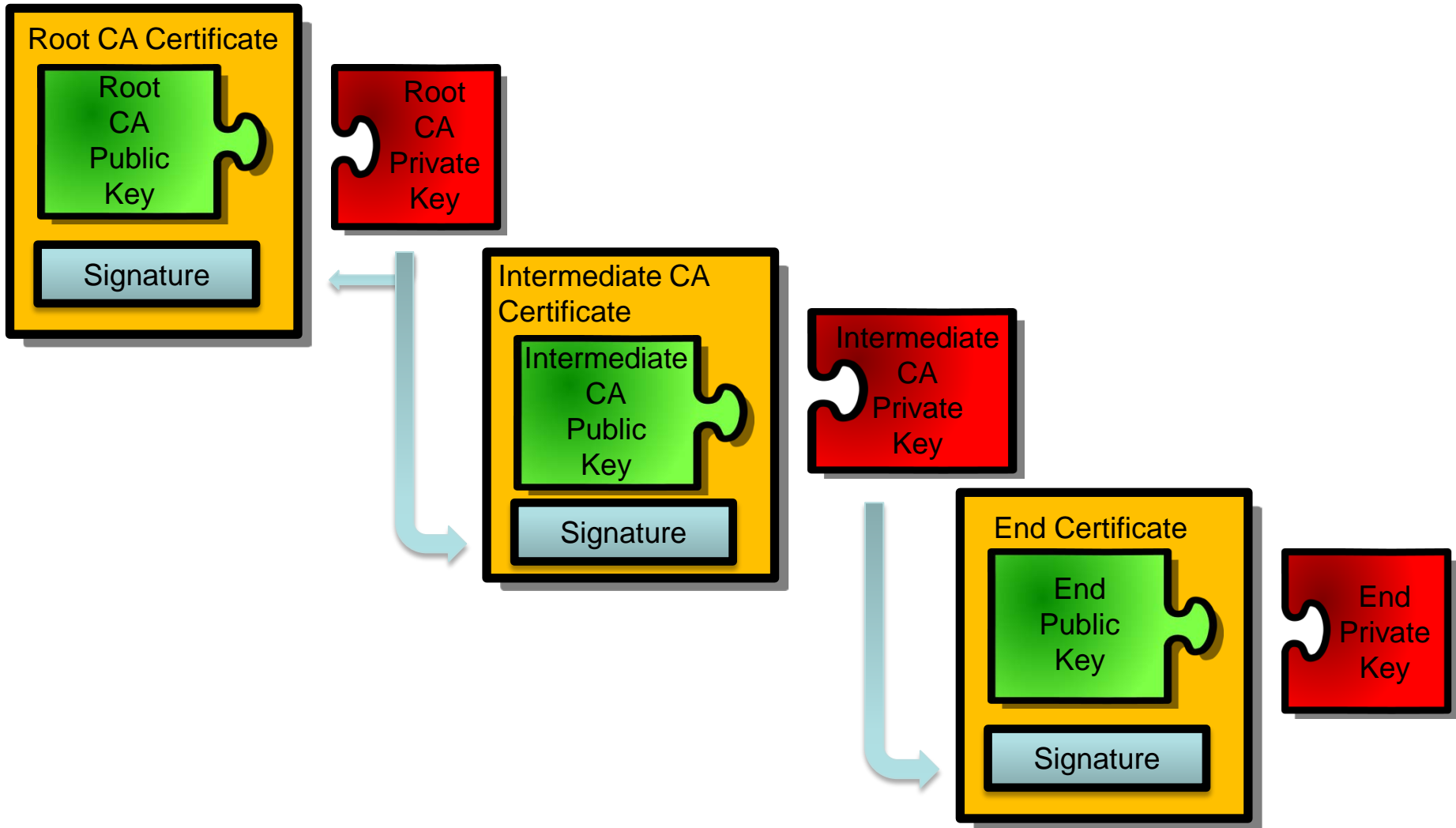


# SSL – Signed Certificate



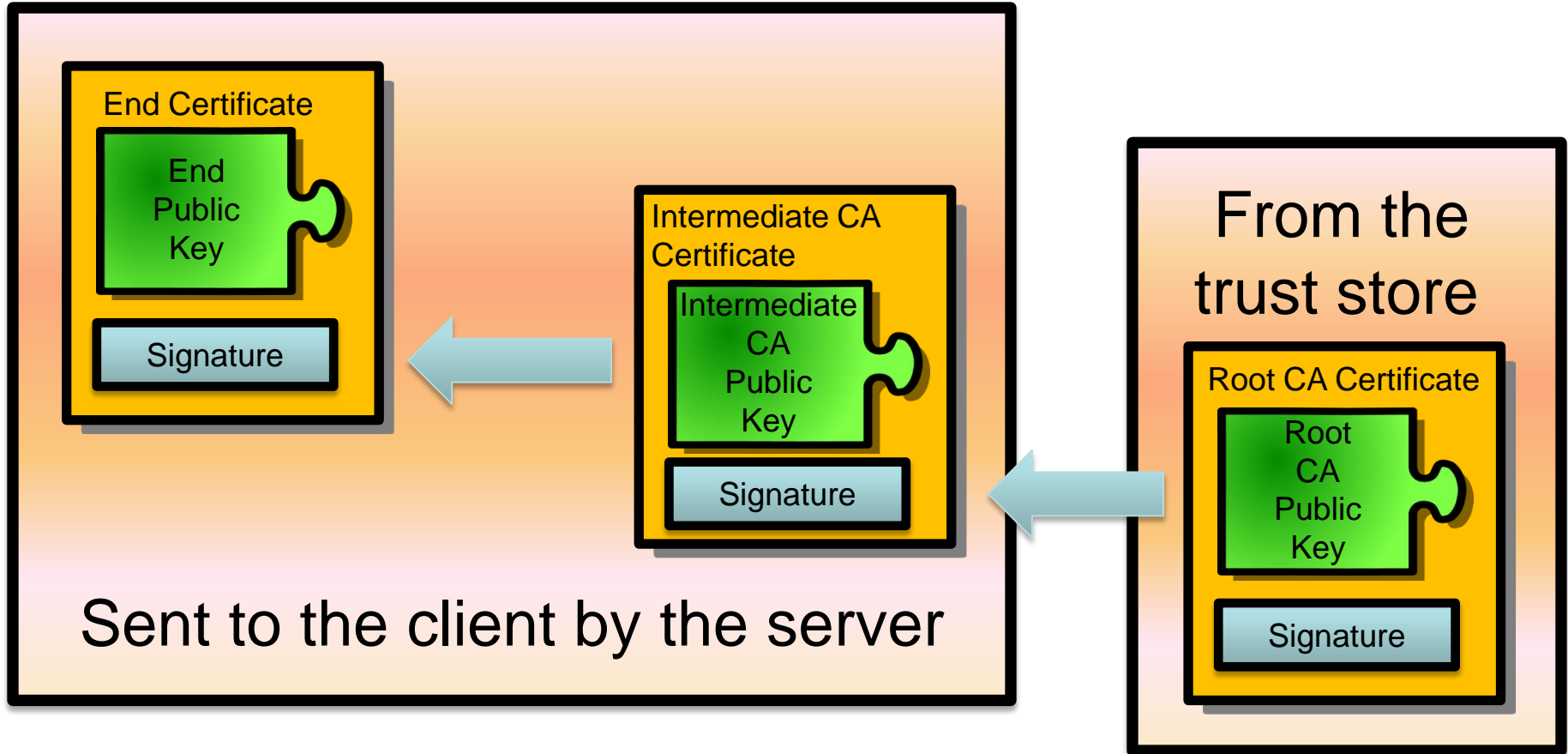


# SSL – Certificate Chain



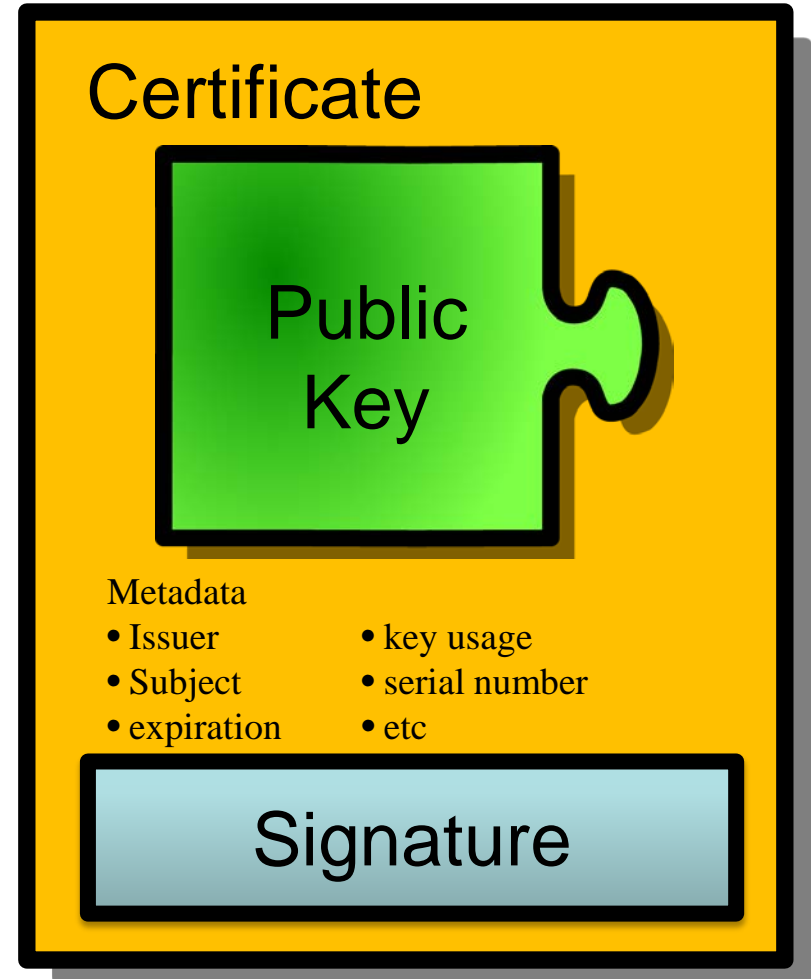


# SSL – Certificate Validation



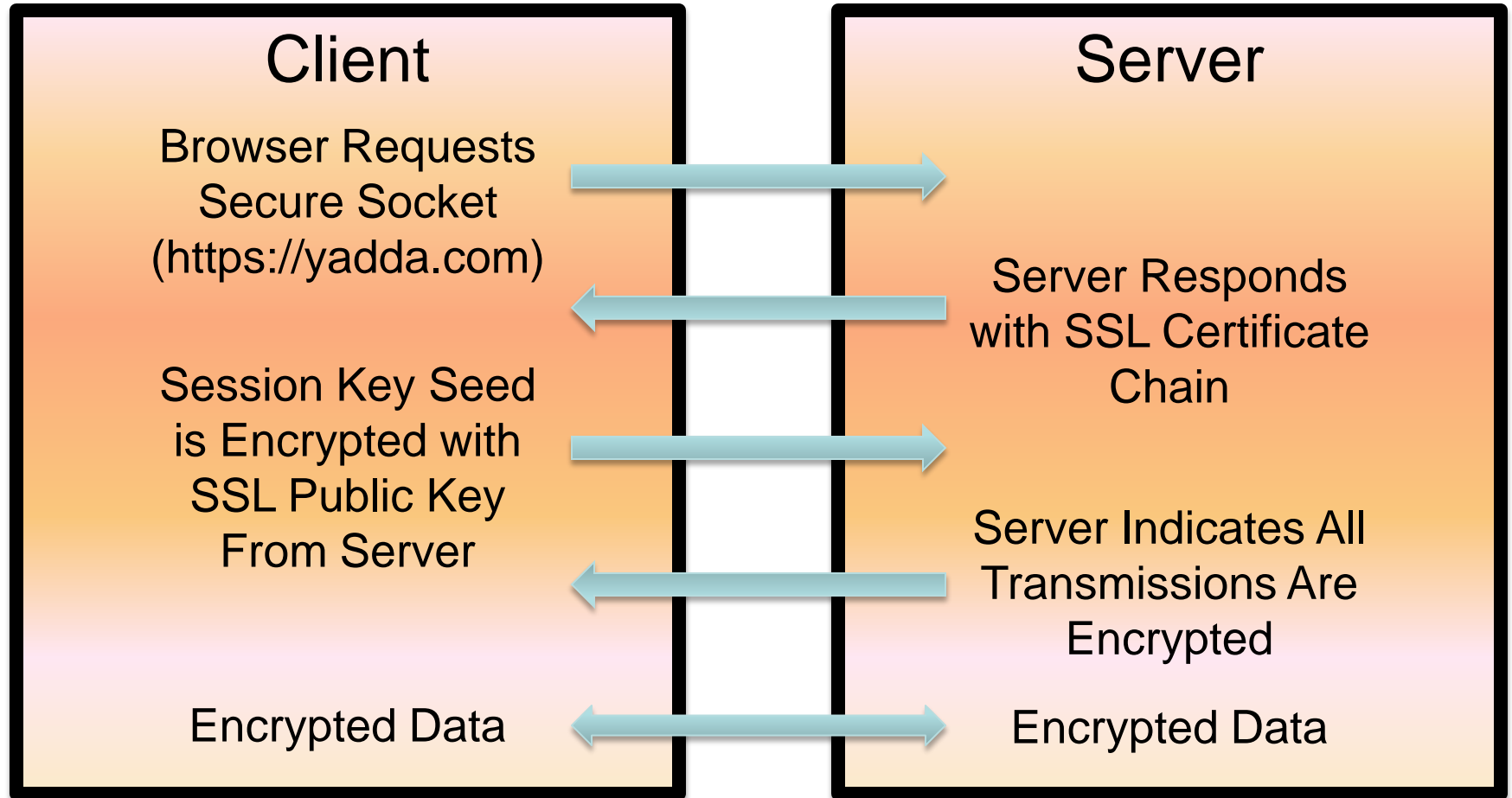
# SSL – Certificate Validation

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





# SSL – Handshake





# SSL – Certificate Tools

The screenshot shows a 'Certificate Request Info' dialog box for 'www.tridium.com'. The main dialog has a 'Properties:' section with a list of fields: Version (v3), Serial Number, Issued On, Issuer DN, Subject, Subject DN, Not Before, Not After, Key Algorithm, Key Size, Signature Algorithm, Signature, Basic Constraints, Key Usage, Extended Key Usage, MD5 Fingerprint, SHA1 Fingerprint, and Valid (true). A 'Certificate Signing' sub-dialog box is overlaid on top. The sub-dialog has a title bar 'Certificate Signing' and a message: 'Sign a certificate signing request with a selected CA certificate.' Below the message is a text box with a folder icon and the text 'Select a certificate signing request to sign:'. There are two date pickers: 'Not Before: 04-Apr-2012 03:15 PM EDT' and 'Not After: 04-Apr-2014 03:15 PM EDT'. There is a 'CA Alias:' dropdown menu and a 'CA Password:' text box. At the bottom of the sub-dialog are 'OK' and 'Cancel' buttons. The main dialog also has 'OK' and 'Cancel' buttons at the bottom.



# SSL – Client Interface

Identity Verification

**NiagaraAX**  
Unable to verify host identity

**The supplied certificate could not be validated:**

- the certificate was issued for a different address
- the certificate was not issued by a trusted authority

**Properties:**

Version	v3
Serial Number	45 c8 05 76 41 38 75 01 8a e5 aa 4e
Issued By	NiagaraAX
Issuer DN	C=US, O=Tridium, CN=NiagaraAX
Subject	NiagaraAX
Subject DN	C=US, O=Tridium, CN=NiagaraAX
Not Before	Mon Mar 26 10:29:25 EDT 2012
Not After	Tue Mar 26 10:29:25 EDT 2013
Key Algorithm	RSA
Key Size	1024
Signature Algorithm	SHA256withRSA
Signature Size	128
Basic Constraints	Subject Type: End Entity
Key Usage	Not Provided
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1), TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
MD5 Fingerprint	38:28:09:bc:85:6a:2d:71:84:c3:af:fc:22:ed:5f:33
SHA1 Fingerprint	a8:4a:dc:14:b6:f7:66:38:71:da:92:1c:fe:4c:0b:d1:2a:f2:ba:46
Valid	true

**Extensions:**

Accept Reject

Session Info for simple

You are connected as admin.

---

The identity of this host has not been verified.

- Server's certificate does not match the address.
- Server's certificate is not trusted.

[Certificate Information](#)

---

Your connection to simple is encrypted with 256-bit encryption. The connection uses TLSv1.

---

The connection is encrypted using AES\_256\_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.

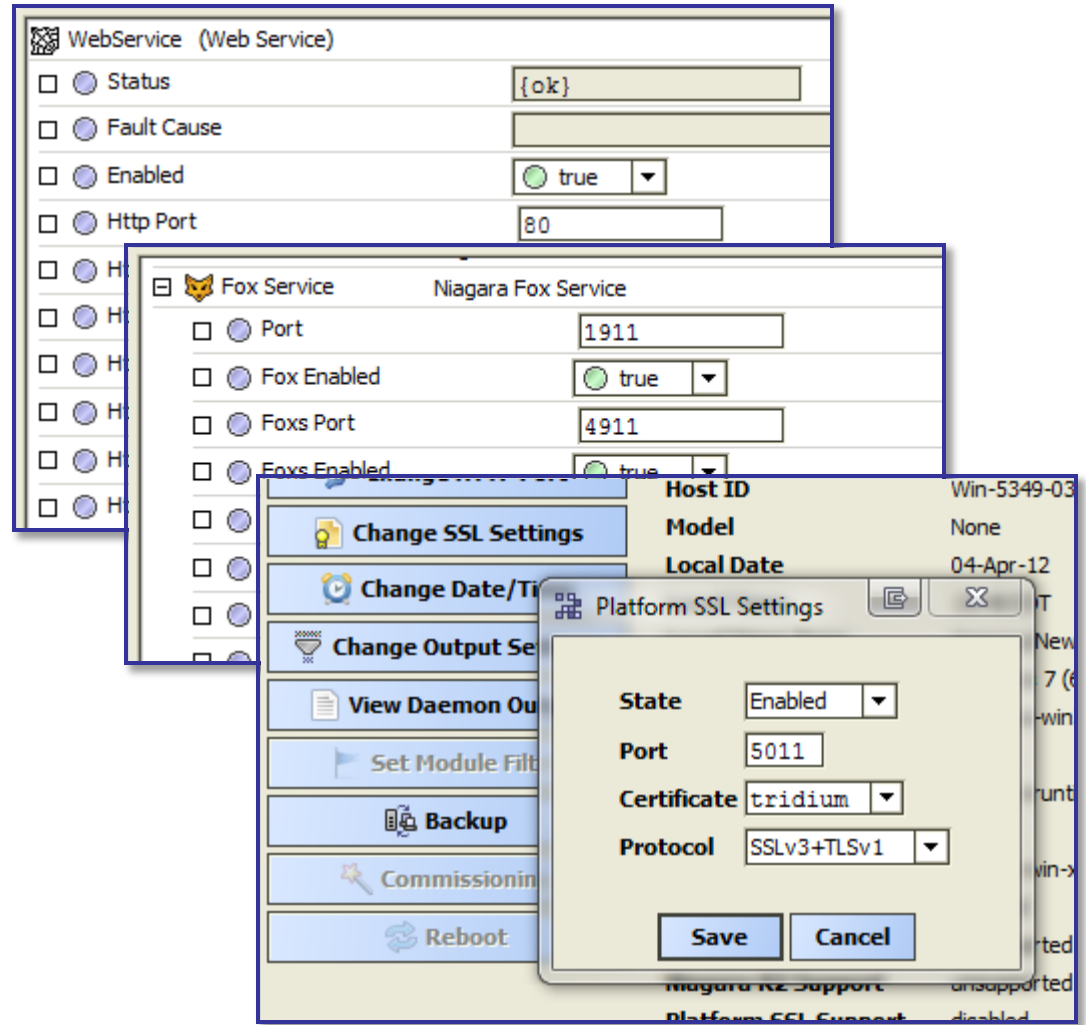
---

Your connection started at 04-Apr-12 3:45 PM EDT.

OK

# SSL – Server Configuration

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

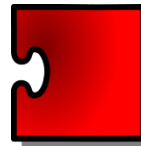
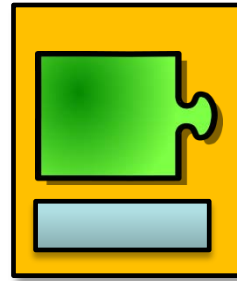


The image shows a series of overlapping configuration windows from a management interface. The top window is for 'WebService (Web Service)' with fields for Status, Fault Cause, Enabled (set to true), and Http Port (80). Below it is the 'Niagara Fox Service' window with fields for Port (1911), Fox Enabled (true), and Foxs Port (4911). The bottom-most window is the 'Platform SSL Settings' dialog, which is open over a 'Change SSL Settings' button. This dialog shows State (Enabled), Port (5011), Certificate (tridium), and Protocol (SSLv3+TLSv1). Other buttons visible in the background include 'Change Date/T...', 'Change Output Se...', 'View Daemon Ou...', 'Set Module Fil...', 'Backup', 'Commissionin...', and 'Reboot'.

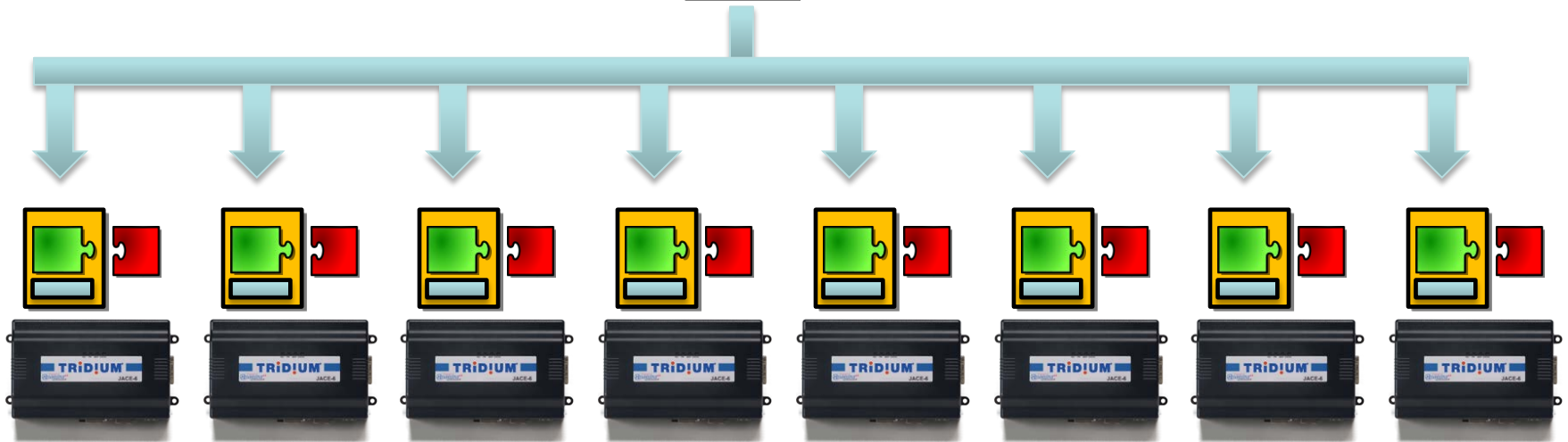


# SSL – Small Network Example

CA Certificate Installed  
on Client Machines  
in Their Trust Store

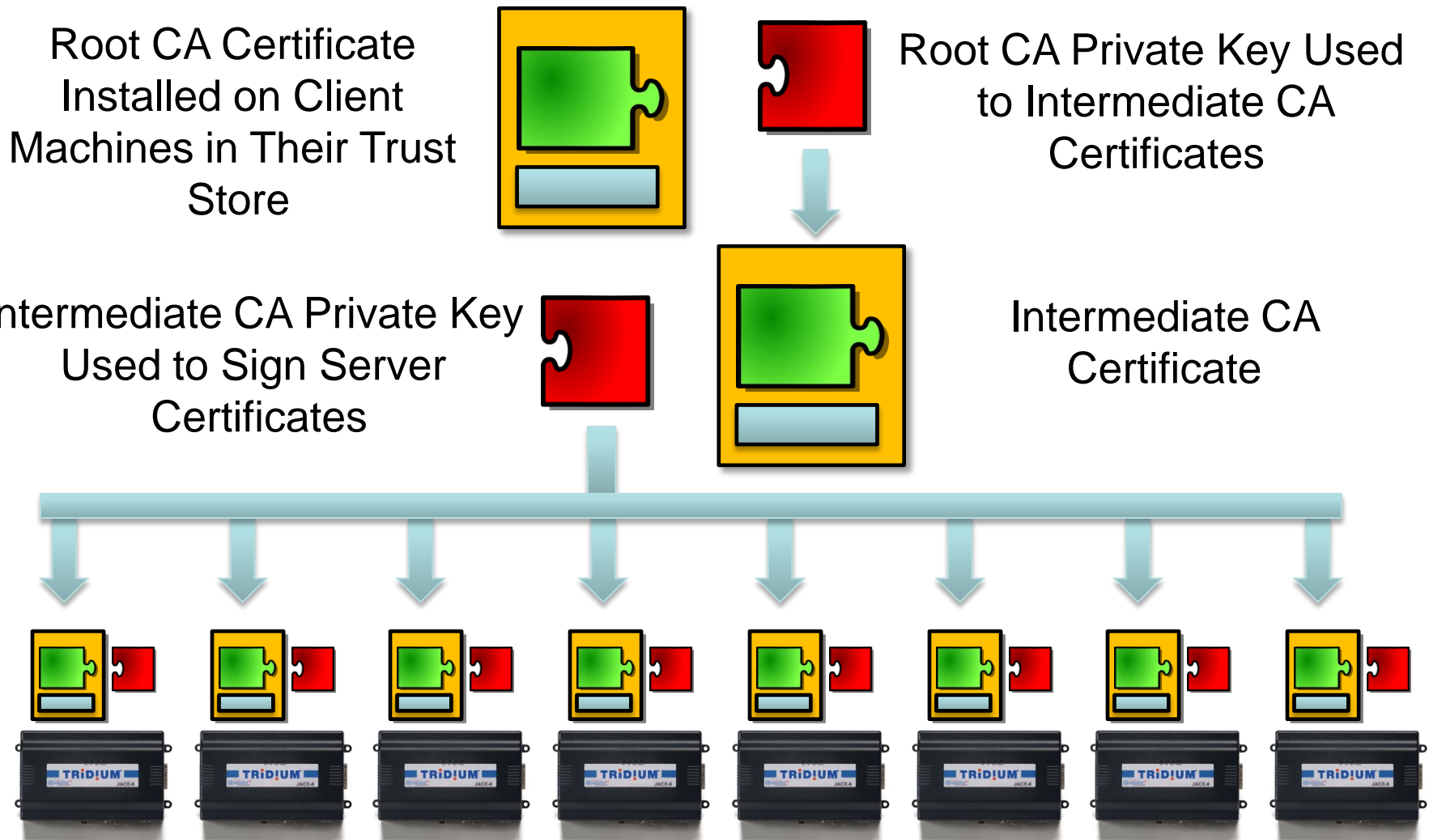


CA Private Key Used to  
Sign Server Certificates





# SSL – Large Network Example

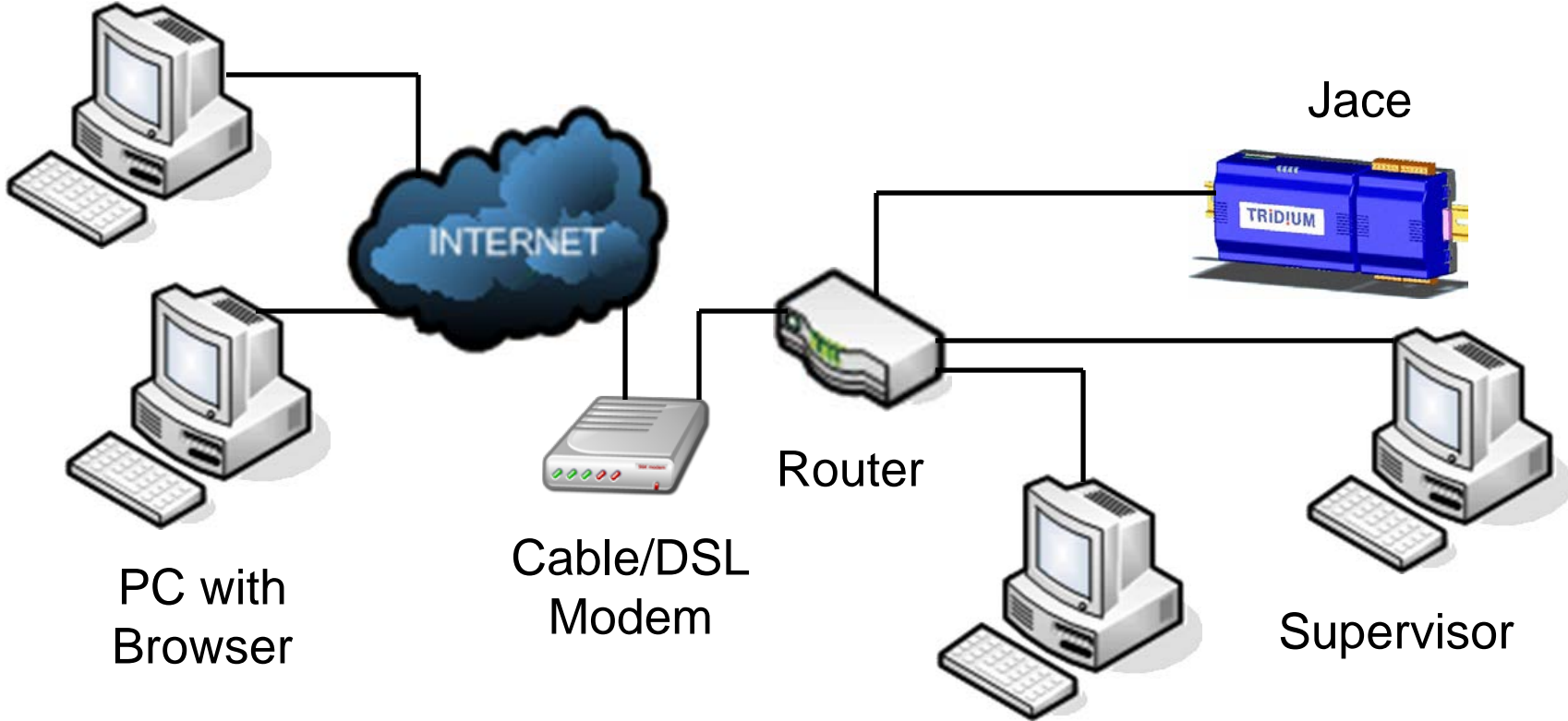






# VPN

Workbench PC



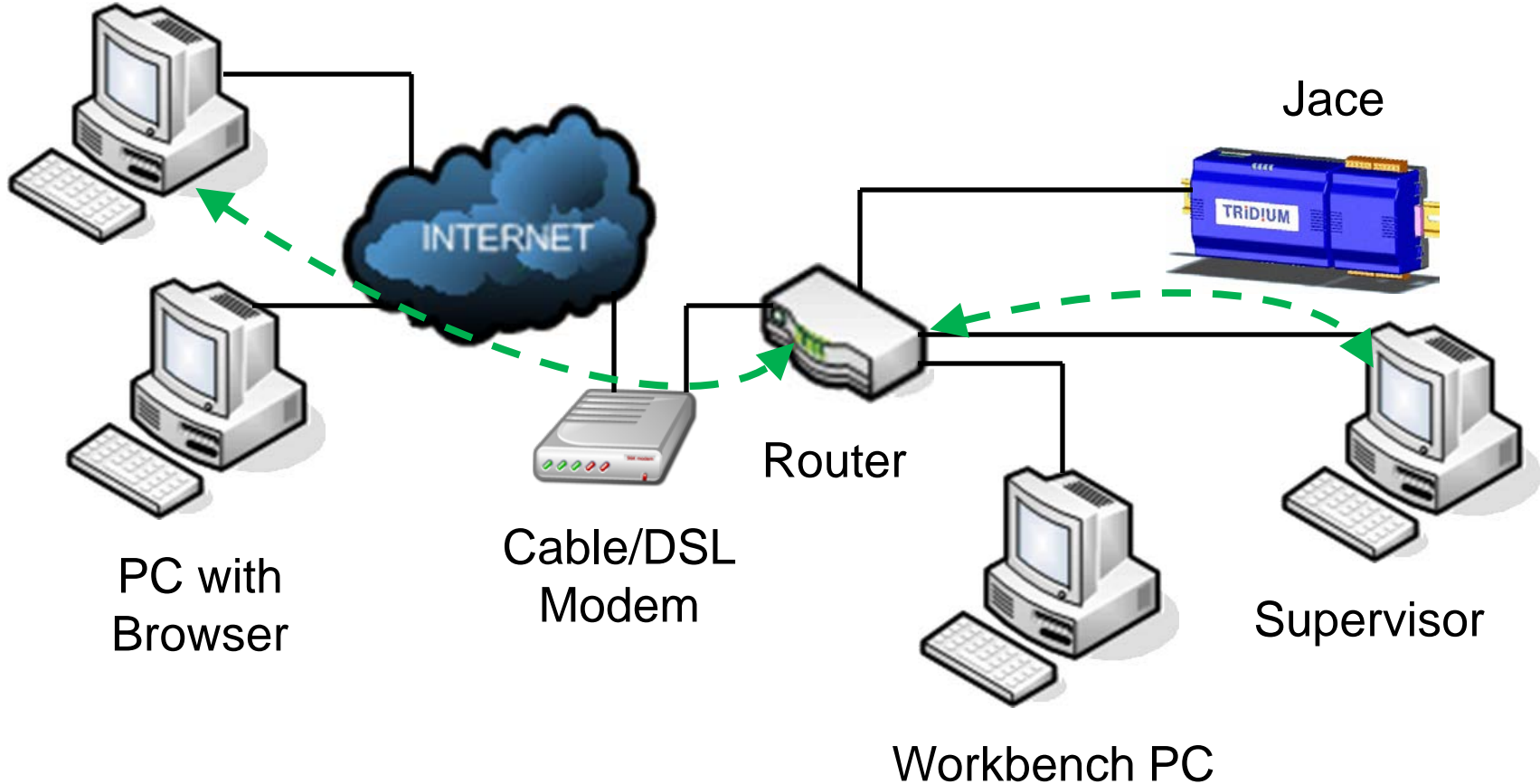
## Typical Niagara Setup

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



# VPN

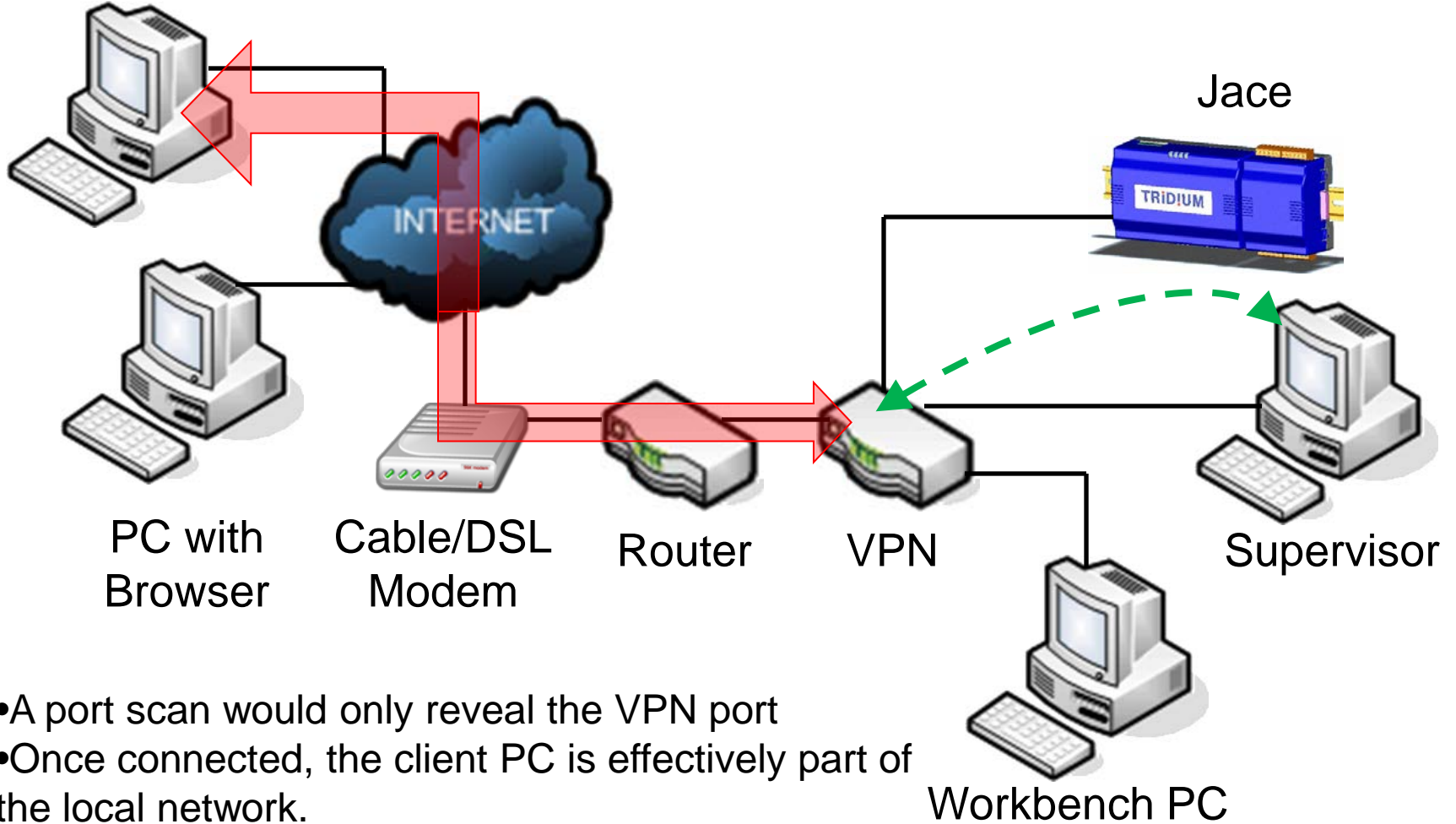
Workbench PC



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

# VPN

Workbench PC  
w/ VPN Client



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



# 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



# Niagara Updates

---

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



# The Future...

---

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

# 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?

# 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/>



# Questions

---

