Secure Communication in Niagara - Putting the Pieces Together

October 29, 2026

A consolidated Q&A reference covering certificate creation, signing, trust stores, provisioning, and certificate lifetimes in Niagara.

1. How do I mass update security certificates across 200+ JACEs? I used to use the Provisioning Service, but that doesn't work anymore.

The Provisioning Service remains the expected workflow for bulk updates of certificates through the Niagara Network. Can you please clarify what you mean by "doesn't work anymore"?

2. What is the difference between AX Certificate Management and Certificate Management in the dashboard?

The "AX Certificate Manager" is a thick-client view implemented in Java and originally developed for AX, hence the name. It was carried forward into N4 as-is.

The "Certificate Manager" is a thin-client HTML5 view introduced in Niagara 4 for interacting with the same store.

The obsolete naming convention is dropped in Niagara 5. Both will be labeled "Certificate Management," with a custom toggle between view types.

4. I have been told that you should check Digital Signature and Non-repudiation. Does that matter?

That depends on how the certificate will be used. Digital Signature is a necessary usage for a certificate used to sign other certificates and is automatically selected for a CA certificate because that usage is implied by the certificate type.

Non-repudiation is a flag that is not required by the UI, but it has additional optional legal implications indicating that the certificate is valid for electronic signatures.

5. What are the pros and cons of using the "Use Global Certificate Password" checkbox?

Using the global certificate password protects all private keys with the same passphrase. Not using the global option protects each key with a unique passphrase. Your IT department may have guidelines on passphrase reuse that allow or require unique passphrases.

6. When using fully qualified domain names, should we put the IP address in the SAN field as a backup in case DNS cannot resolve the FQDN?

This generally is not recommended. If you are using a load balancer or dynamic IP addresses, adding the IP address is not very helpful. It can also force you to change the certificate if the server's IP address changes. Even if the IP address is static, users who expect to use the FQDN may not know the IP address, and requiring them to change the setup to use the IP address is not a good user experience.

7. How do I sign a CSR if the CA is created in the remote station?

The CA and its private key would need to be exported to Workbench to use the Workbench tools.

8. Why do we create the server certificate in the JACE rather than in the N4 Supervisor?

CA certificate workflows are most typically performed in the Supervisor and provisioned to subordinate devices. The tools do not prevent you from performing these activities in the JACEs themselves if you have a reason to do so.

9. When you create the CA, can you change the default CA certificate lifetime to more than one year? Is there a limit on how long the certificate can remain valid?

You should be able to select a custom lifetime for the CA certificate at certificate-generation time. The lifetime of an already-created certificate cannot be changed without regenerating the certificate.

The UI should permit any lifetime you choose, although your organization may have IT guidelines governing the limits allowed for production use.

10. Is there any reason to keep the CSR and PEM files after trust has been established?

A CSR generally does not need to be retained after the normal workflow is complete. The resulting PEM file from the CSR process may be retained to transfer the certificate elsewhere in your system, particularly to a system that is not running Niagara.

11. Is this procedure available in a PDF?

Some of this information can be found on Niagara Central. Much of the guidance used to prepare and validate this webinar came from Tridium documentation.

12. Can you suggest a process for removing certificates from the system trust store if a certificate in the system trust store is compromised?

The system trust store is read-only and cannot be modified. The best solution is to keep your Niagara installation up to date so that you receive the most recent security fixes.

13. If we get a CA from a trusted authority such as GoDaddy, can we distribute it among multiple PCs and JACEs, or do we need to install it individually?

You can use the Provisioning Service to install a certificate in the User Trust Store of all constituent stations in your Niagara Network.

However, certificates from public authorities are already likely to be present in the System Trust Store of all devices. This is the value of signing by enterprise CAs: they do not require custom imports before issued certificates are trusted.

14. What about certificates for modules? Is that the same process?

Code-signing certificates can be signed by a CA using the same process. To sign modules, use the signed or self-signed code-signing certificate in the Jar Signer Tool, or add code-signing tasks to the build process as part of your development workflow.

15. If the CA is created in the remote station and I do not want the private key to leave the JACE, can I sign a CSR without exporting the CA's private key?

The tools generally assume that signing will be performed by Workbench using the Certificate Signer Tool, or by a Supervisor using provisioning jobs or the signing service. It is recommended that you create and store your CA in one of those locations to facilitate signing across multiple devices in your network. To sign from the JACE, you would need to write custom code.

16. What is the maximum lifetime we can set for a certificate created in Niagara?

Follow your IT guidelines or industry best practices to determine the certificate lifetime. Niagara is a framework that supports many environments, so it does not set a maximum certificate lifetime. The default is one year, and that value can be adjusted based on your needs and the type of certificate being created.

17. I need to set up a third-party-signed certificate at the server level for web browsing. Is the process basically the same as the process shown for the JACE, except that I export the certificate request, send it to the third party, and import it later?

Yes. The process should be the same, except that you may need to manually assemble the file for import into Niagara. Niagara expects certificates to be imported as a PEM file containing the server certificate, any intermediate CA certificates, and the root CA certificate in a single file, in that order from top to bottom. Niagara 5 will also add the ability to import PKCS #12-formatted certificates.

18. The web-services industry is moving toward 45-day certificate validity. Another issue is that the CA is not in the browser store. CAs such as DigiCert provide signing services, but they add cost to projects. Could Tridium provide an automated service using a certified certificate for each SI?

There are no plans to do this at the moment. In most cases, Niagara installations should be deployed on internal networks that third-party CAs cannot verify. Some IT environments allow a trusted CA to be pushed to user devices or provide an internal signing mechanism that signs certificates with an internal CA. Tridium is working on ways to make that workflow easier, but nothing has been scheduled yet.

19. Can the Niagara CA be implemented in an IT CA environment as a subordinate CA?

Assuming "subordinate CA" means an intermediate CA, yes. You can export the CSR for the intermediate CA, have the IT team sign it, and then reimport the signed CA certificate into the key store.