Digital Certificates for Web-Based DeltaV Applications

This document provides details on how to handle digital certificates for web-based DeltaV applications.

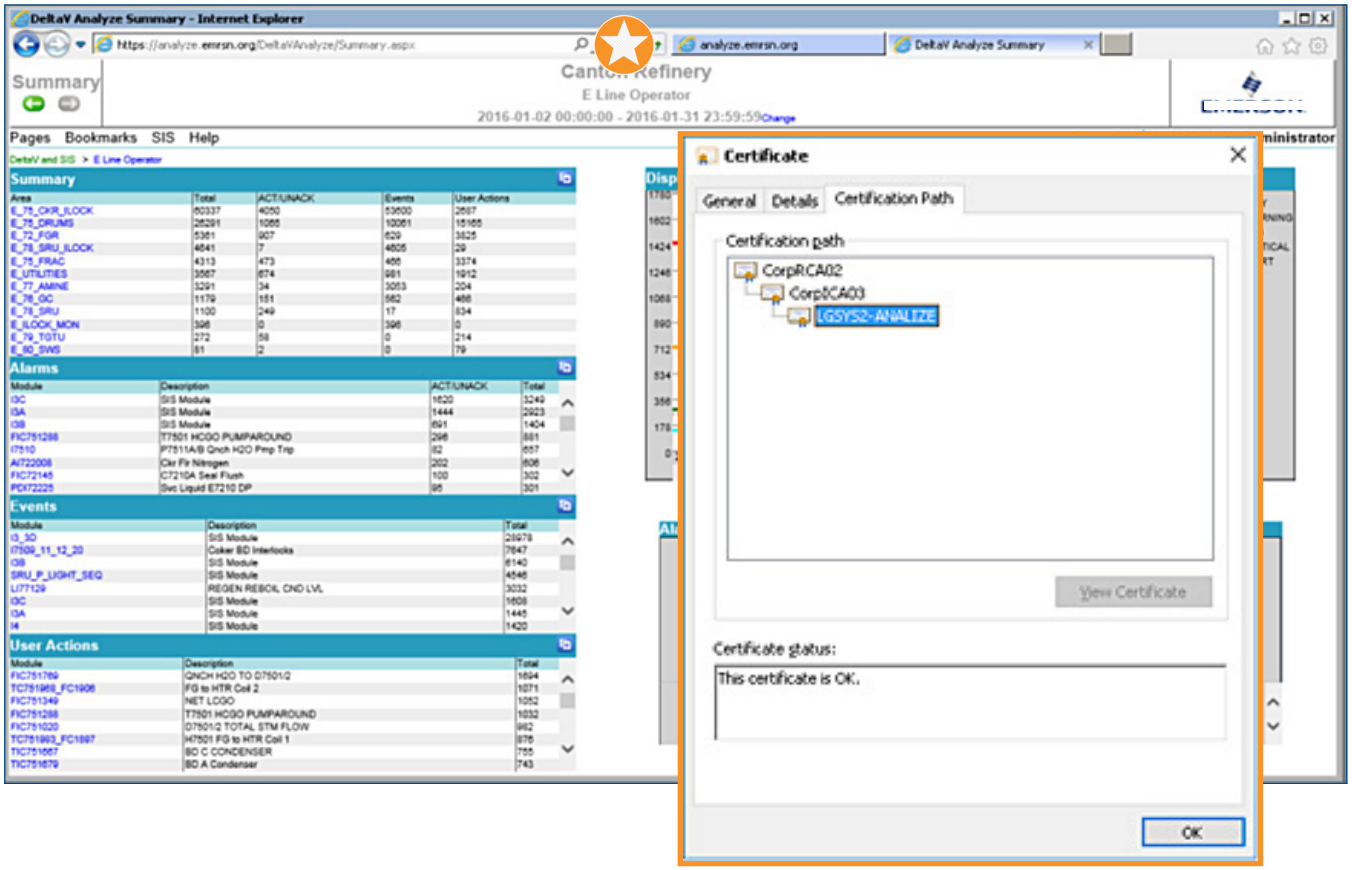

Table of Contents

1 Introduction

This whitepaper provides background information about digital certificates, how DeltaV applications utilize certificates to secure communications, and guidelines for managing certificates to ensure the security and trust of the system are properly maintained.

A digital certificate is an electronic mechanism that uniquely identify users, services, and endpoints so that they may exchange information securely in a network. In simpler implementations, digital certificates can be used to set the trust between two devices involved on a data exchange.

Both cases are based on the Public Key Infrastructure (PKI), where a key-pair – a public key and a private key – is used to simply set the trust when the Server digitally signs the information provided, or is used to encrypt the communications when both the Server and the Client share their public keys. Encrypted communications can only be decrypted using private keys, whereas the public keys are exchanged among the devices or applications.

Although intensively utilized over open/public networks (internet) for security reasons, digital certificates are also often used in the Industrial Control System (ICS) environment due to the number of available web-based applications that require additional security mechanisms. ICS also relies on digital certificates to at least allow Clients to check if the received data is coming from the trusted Server (Client/Server model).

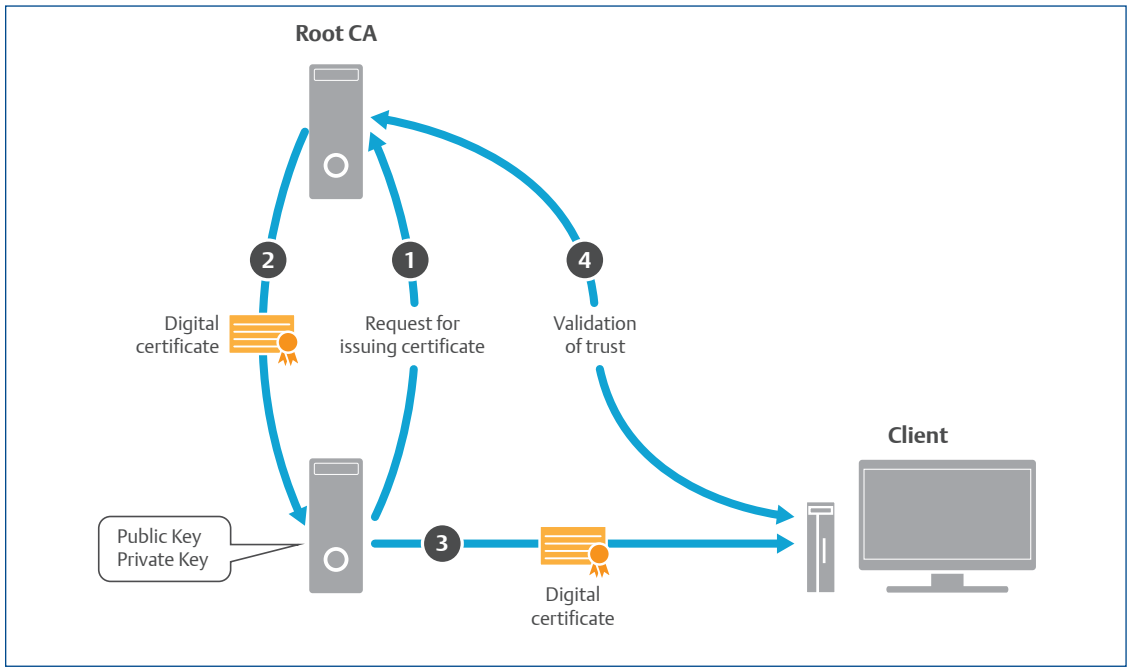

Figure 1 – Client/Server communication model based on PKI.

Since digital certificates are crucial to maintain the security level and the trust relationship, it is highly recommended that proper key management is done when managing the digital certificates. For open/public networks this is done by means of Commercial Certification Authorities (CAs).

The CA provides the digital certificates, manage the keys and is the trusted entity within the chain of trust, hence the CA can be referenced at any time to confirm that a certificate is still valid.

In November 2011, the Certification Authority/Browser Forum (CA/B Forum) adopted the baseline requirements for the issuance and management of publicly-trusted certificates that took effect in July 2012 and encompasses the following basic requirements:

- Commercial CAs should notify applicants prior to issuance that the use of certificates for private networks has been deprecated by the CA/B Forum.
- Commercial CAs should not issue certificates with an expiration date later than November 1st, 2015 for private networks.

The CA/B Forum is a voluntary group of CAs, vendors of internet browser software, and suppliers of other applications that use X.509 digital certificates for Secure Sockets Layer / Transport Layer Security (SSL/TLS) and code signing that chain to a trust anchor embedded in such applications. The CA/B Forum guidelines cover certificates used for the SSL/TLS protocol and code signing, as well as system and network security of CAs.

With the CA/B Forum in mind and understanding how their guidelines apply to ICS environments – where network segmentation and private/dedicated networks are broadly used – alternatives are presented in this document to help you have access to the security protections offered by digital certificates, but not necessarily giving up the chain of trust mechanism based on CAs.

There are different types of digital certificates depending on their issuance mechanism, and for simplicity in this white paper we will refer to the following three digital certificate types:

- Digital certificates issued by Commercial CAs
- Digital certificates issued by Private CAs (or intermediate servers)
- Self-Signed digital certificates

2 Hash Functions

Hash functions are used to generate a compressed/fixed size data stream that can be encrypted to generate digital signatures for large amounts of data.

There are different hash functions issued by different organizations today. The Secure Hash Algorithm (SHA) is a good example and, along with other hash function types such as MD5 or CRC32, it is a one-way hashing formula that is used to protect the integrity of data.

Digital signatures based on SHA are dependent on the hash value size – the larger (bit-wise) the hash value the more complex is the encryption, hence harder to break the encryption. SHA-1 produces 160bit hash values, SHA-2 produces either 256bit (SHA-256) or 512bit (SHA-512) hash values, and so on.

In November 2013, Microsoft announced that they would not be accepting SHA-1 encryption after 2016 based on calculations that showed how breaking SHA-1 is becoming feasible – SHA-2 is now the next available option which is widely adopted by users, suppliers and vendors.

3 Web-Based DeltaV Applications

Certificates are used in DeltaV's web-based applications. These applications deliver an enhanced user's experience especially for client PCs that are not running DeltaV software on them. Each is accessible via an internet browser (e.g. Microsoft Internet Explorer) where the web-application Server is within a private network (DeltaV Area Control Network or L2.5 Network). For some DeltaV applications, certificates are used at the communications level by Windows services.

The web-based DeltaV application Servers provide the web pages using the https protocol (HyperText Transfer Protocol – Secure) which is the secure version of http and uses digital certificates to encrypt the communications between the Client and the Server.

Below is a list of web-based DeltaV applications/services referenced in this document:

- DeltaV Mobile Portal (formerly Executive Portal)
- DeltaV Web Server
- DeltaV Logbooks
- DeltaV OPC .Net Remote
- DeltaV Analyze
- DeltaV History Analysis
- DeltaV Batch Analytics
- DeltaV History Web Service
- DeltaV Plant Messenger

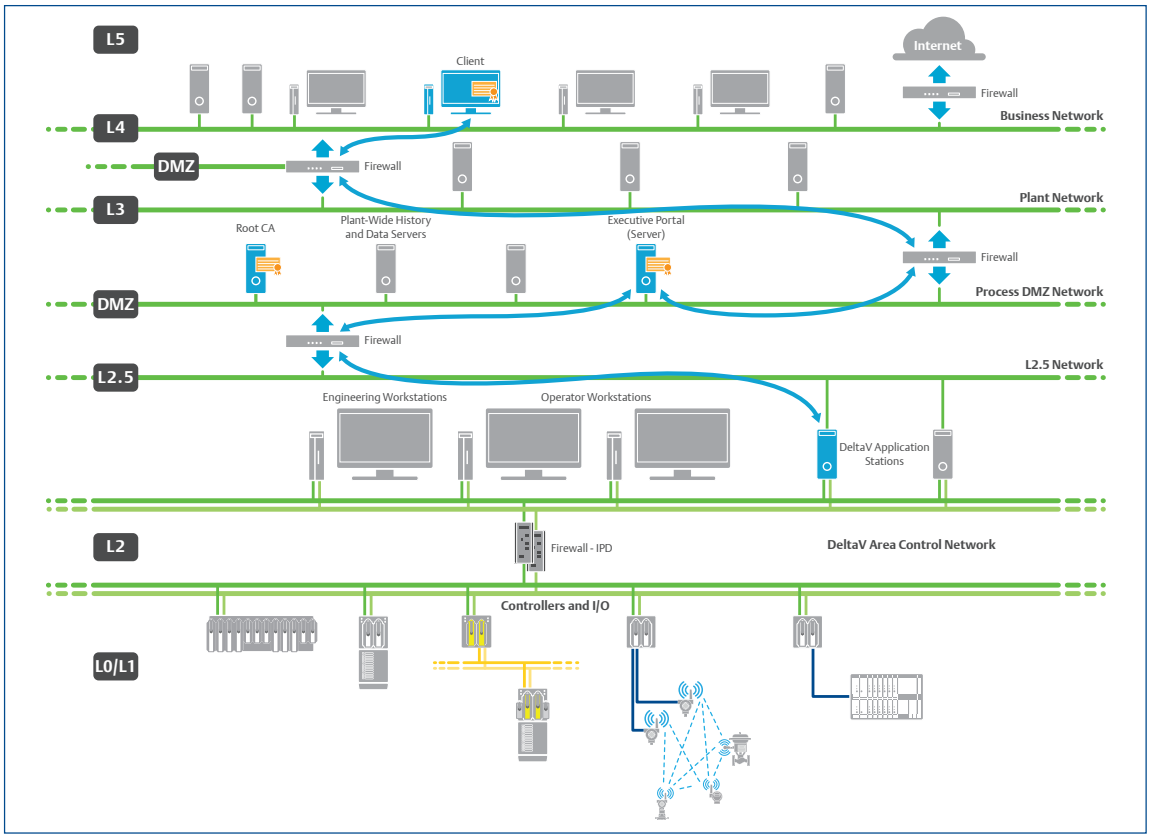

Figure 2 – Reference architecture showing a web-based DeltaV application.

Note: *Emerson is updating all web-based DeltaV applications to be installed with SHA-2 encrypted self-signed digital certificates that expire in 90 days.*

For DeltaV applications, an initial 90-day self-signed digital certificate is generated at the time of installation to provide the user secure out-of-the-box assurance that the newly installed web-based DeltaV application is really serving its users (trusted Server). This initial 90-day self-signed certificate is not based on a root CA and should only be used for evaluation or test of the web-based DeltaV application. Emerson recommends you to replace the provided self-signed certificate by another alternative that can be used for the long-term, and with proper key management to secure the communication channel between the Client browser and the trusted Server.

4 Digital Certificates Solutions for DeltaV Applications

Web-based DeltaV application Servers are installed on private networks within your organization, and often times do not have Fully Qualified Domain Names (FQDN). As mentioned in the Introduction of this white paper, Commercial CAs are no longer allowed by the CA/B Forum to issue digital certificates for private networks and therefore self-signed digital certificates issued by Root CAs, or digital certificates issued by Private CAs can be utilized instead.

Self-signed certificates issued by the web-based application Server (without a Root CA) must not be used for the long-term as they do not have the necessary security protections this type of solution require.

Additionally, managing self-signed certificates present some challenges as listed below:

- Need for technical expertise to deploy and manage the self-signed certificates.
- Harder to make sure the key management is secure (and not compromised).
- If compromised, it is not simple to revoke certificates across the private network.
- Cost to deploy may vary and cannot be anticipated very well.
- Increased risks based on misuse or mishandling.

4.1 Self-Signed Digital Certificates issued by Root CAs

If the User decides to use self-signed certificates for the web-based DeltaV applications, the first thing to consider is that a Root CA has to be deployed. The self-signed certificate provided upon the web-based DeltaV application installation will not be re-issued, and once expired (after 90 days) the certificate will need to be replaced. The Root CA in this case is usually a server-type machine that is hardened and installed following security guidelines to make sure the keys involved in the certificates issuance are not exposed – only system administrators should have access to the Root CA.

There are multiple ways to deploy Root CAs, including Microsoft's guidelines – Root CA is one of the server roles that can be enabled on a Microsoft Windows Server O/S. Emerson can provide support to set up the Root CA in your infrastructure, please contact your local Emerson sales office and ask for a quote from Performance Services if you need assistance setting up a Root CA for self-signed certificates issuance to be used with web-based DeltaV applications.

Note: *It is highly recommended that the Root CA is a different server-type machine than the Professional Plus machine, or any other DeltaV server machine – preferably the self-signed Root CA should be running independently from other applications, roles and services.*

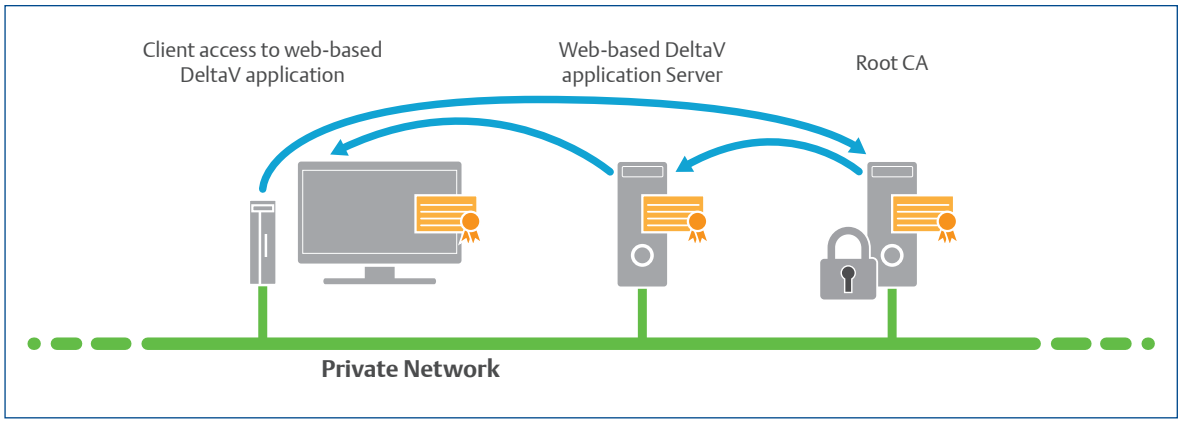

Figure 3 – Self-signed Root CA architecture overview.

4.2 Digital Certificates Issued by Private CAs

Deploying and managing Root CAs for local self-signed certificates can be complex. It requires management and server-type machines that have specific features (e.g. Secure Boot, Trusted Platform Module, etc.). If your Organization is not equipped with an Information Technology (IT) department that is available to support the Root CA deployment, then management overhead or eventually misuse and mishandling become real challenges.

Certain vendors can provide an alternative solution that runs on an intermediate server which works as a dual-homed server station connected to the public network (internet) with an FQDN, as well as to the private network where the web-based DeltaV applications are running. This solution allows you to avoid risks, errors, and hidden costs associated with self-signed Root CA's deployments, and at the same time it complies with the CA/B Forum guidelines. This alternative solution is called private SSL (Secure Sockets Layer), and is based on the deployment of a Private CA infrastructure.

The biggest advantage of using Private CAs is that all work and expertise associated to manage the keys for digital certificates is outsourced in this case. Some companies that can provide this type of Solution as a Service (SaaS) are listed below:

- Symantec – http://www.symantec.com/private-ssl
- GlobalSign – https://www.globalsign.com/en/certificate-authority-root-signing
- Entrust – https://www.entrust.com/private-ssl-certificates
- Other companies may offer the same of similar.

The Private CA solution is not provided by Emerson at this time, but you are free to discuss solutions with vendors that provide this type of service as indicated above.

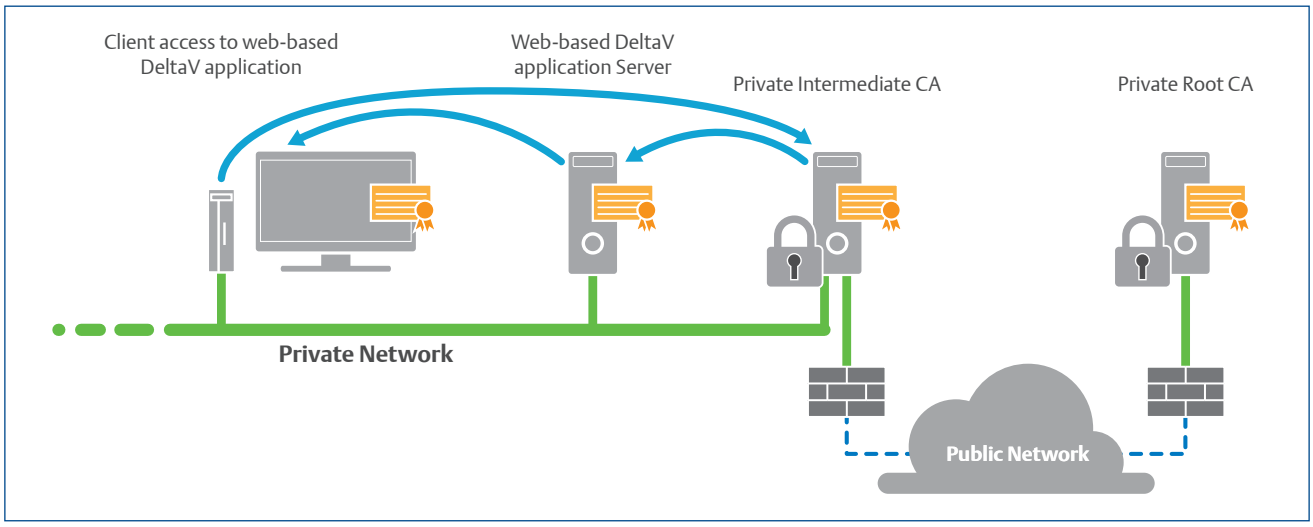

Figure 4 – Private CA architecture overview.

Emerson recommends the use of digital certificates to enable Clients to verify if the web-based DeltaV application Server is the trusted Server. All web-based DeltaV applications are being updated to only accept connections based on the https protocol, therefore digital certificates are required for a fully featured user's experience. When the self-signed certificate issued by the web-based DeltaV applications expires, the DeltaV application will continue to work, but the Client will be presented with a certificate error message at the top of the supported internet browser indicating there is an issue with the provided certificate (in this case caused by the expiration date).

Users are encouraged to define and implement the CA solution of choice and have it ready before the provided self-signed certificates expire. Table 1 provides details of which versions of each web-based DeltaV application are considering the approach described in this white paper.

Application	Version	Protocol	Hash Function	Self-Signed Certificate Expiration
DeltaV Web Server	v13.3.1 or higher	https only	SHA-256	90 days
DeltaV Logbooks	v5.6.5 or higher			
DeltaV Analyze	v4.1 or higher			
DeltaV History Analysis	v13.3.1 or higher			
DeltaV Batch Analytics	v13.3.1 or higher			
DeltaV History Web Service	v13.3.1 or higher			
DeltaV Plant Messenger	v1.6 or higher			

Table 1 – Web-based DeltaV applications

Note: Some web-based DeltaV applications are not listed here as they have not yet been changed to meet the requirements listed in this table. They will be added to this white paper once they meet the requirements.

5 Importing Digital Certificates to the DeltaV Applications

Independent from which type of CA the digital certificate was issued, the process of importing it into the web-based DeltaV applications is the same. Once the digital certificate is available, the steps provided below can be followed for any of the web-based DeltaV applications (in this example the applications DeltaV Logbooks and History Web Services were used):

5.1 Obtain digital certificates

Once deployed, either the Root CA or the Intermediate Server provide digital certificates to allow for the proper implementation of your PKI. You must provide a minimum set of certificates to be bound into your DeltaV infrastructure.

Private CA	Self-Signed Root CA	Description
Private Root CA certificate	Self-Signed Root CA certificate	This is the root certificate that identifies the CA. It has the higher trust in the certificate path. For Private CA this certificate is linked to the private network via the Intermediate CA.
Intermediate CA certificate	N/A	This certificate applies to Private CA deployments, and is the root certificate within the private network, but it sits between the web-based DeltaV application certificate and the Private Root CA certificate in the certificate path.
Web-based DeltaV application certificate	Web-based DeltaV application certificate	This is the certificate used by the Web-Based DeltaV application to confirm it is the trusted Server for any given Client in the private network.

Table 2 – Different types of certificates applicable to a web-based DeltaV applications deployment.

Figure 5 shows the certificate path of the web-based DeltaV application certificate whereas: 'CorpRCA02' is the Private Root CA certificate, 'CorpICA03' is the Intermediate CA certificate, and 'LGSYS2-LOGBOOKS' is the web-based DeltaV application certificate.

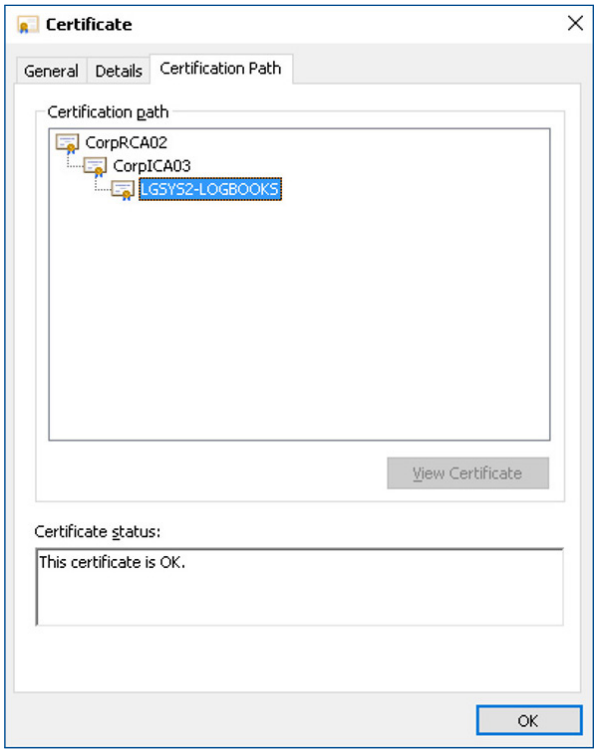

Figure 5 – Web-based DeltaV application certificate properties showing the certificate path.

5.2 Importing Root CA certificates

The Root CA certificates are available to the web-based DeltaV application Servers and Clients in the infrastructure. This is done using the Group Policy Management Editor on the Domain Controller of the given networks where the Servers and Clients are connected to.

The Self-Signed Root CA certificate or the Private Root CA certificate is imported to the Trusted Root Certification Authorities folder (Computer Configuration / Policies / Windows Settings / Security Settings / Public Key Policies).

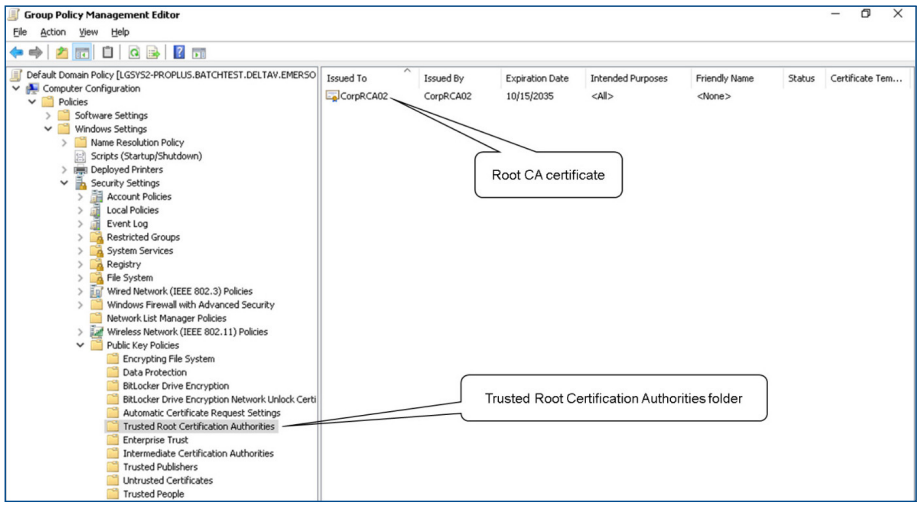

Figure 6 – Certificate in the Trusted Root Certification Authorities folder.

For Private CA deployments, both the Intermediate CA certificate and the Private Root CA certificate are imported to the Intermediate Certification Authorities folder (Computer Configuration / Policies / Windows Settings / Security Settings / Public Key Policies). After importing, the certificates need to be propagated to all workstations linked to the GPOs based on Microsoft's recommendations.

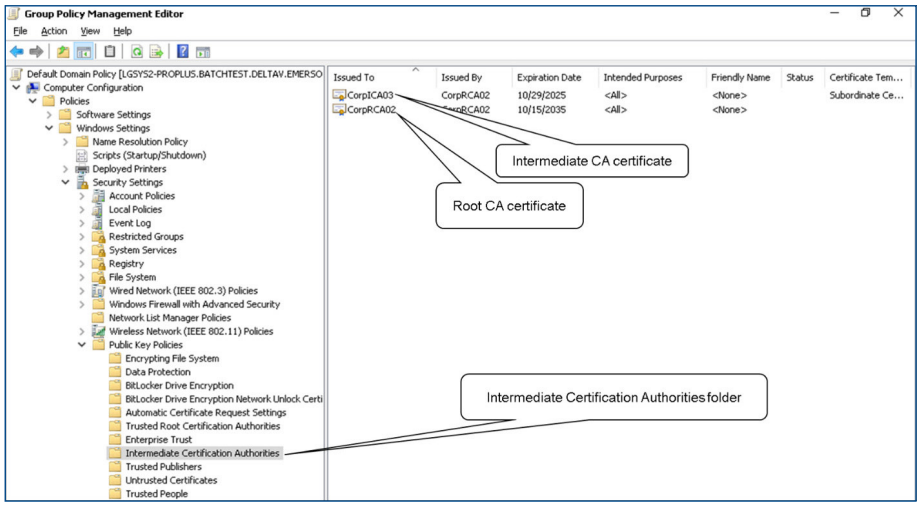

Figure 7 – Certificates in the Intermediate Root Certification Authorities folder.

5.3 Binding the certificates within Microsoft Internet Information Services (IIS)

Finally, the certificates are bound in the Server's IIS where the web-based DeltaV application is running. Figures 8 and 9 show the steps to bind them.

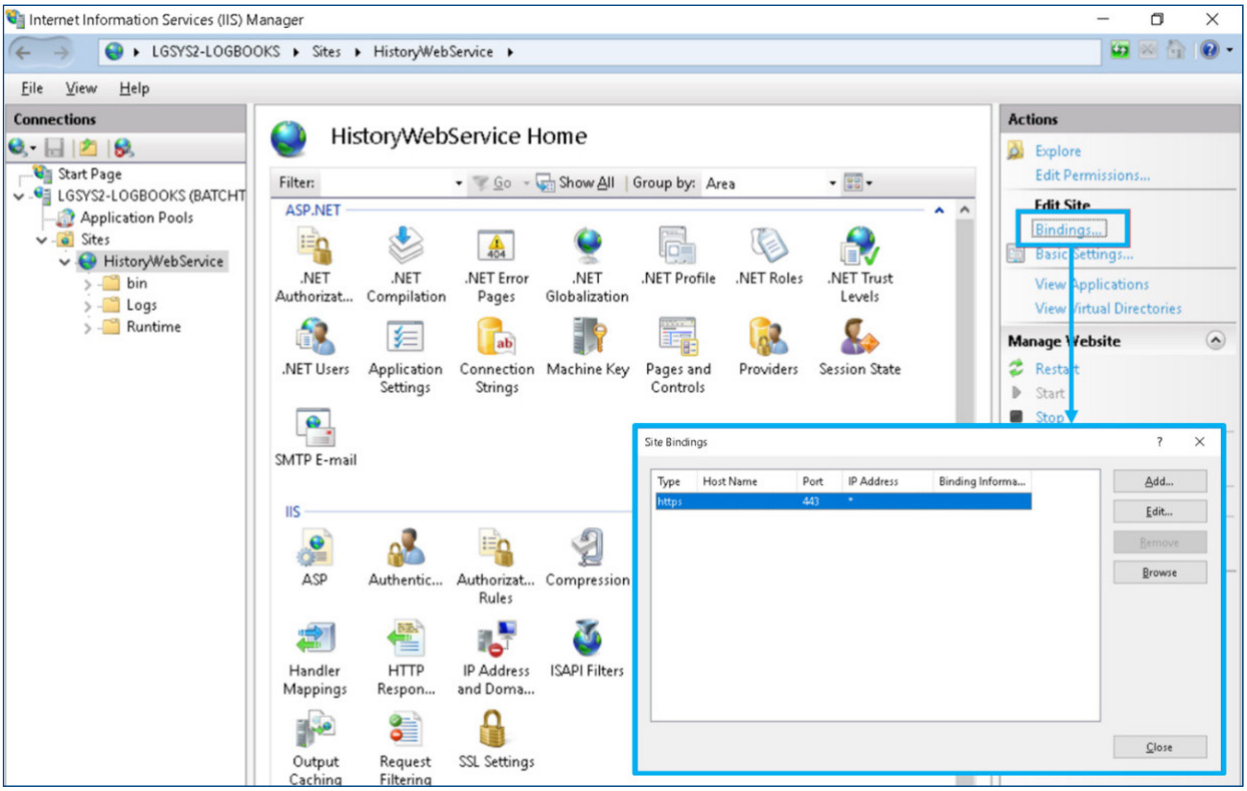

Figure 8 – Accessing IIS Manager to bind the certificates.

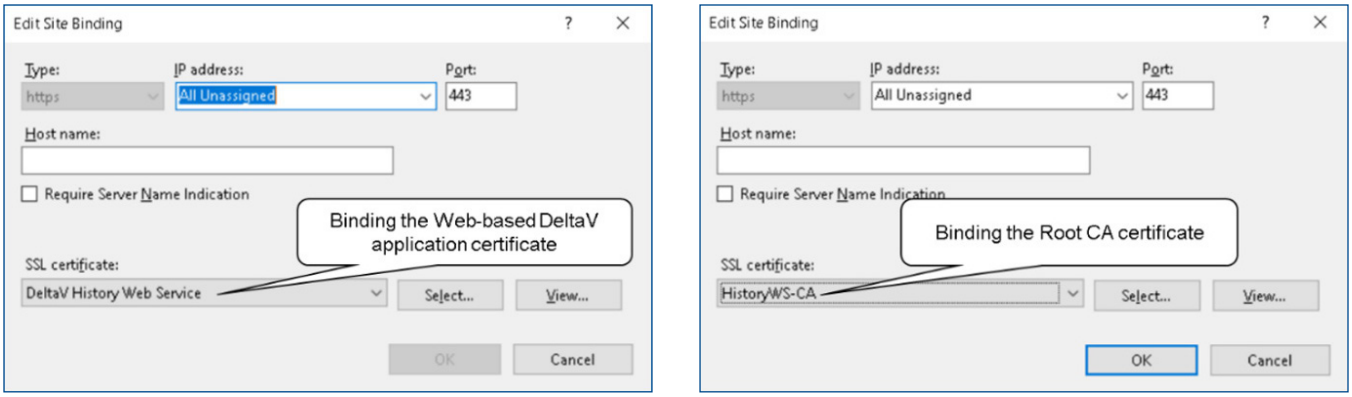

Figure 9 – Binding certificates.

Note: *If certificates are imported to any GPOs on any DeltaV workstation or server, they need to be backed up prior to any DeltaV upgrade or migration. DeltaV System Hardening does not take into account certificates that were previously imported into a running DeltaV system and therefore will delete the certificates as part of the DeltaV installation procedure.*

The certificates can be manually exported before the upgrade/migration, and re-imported once the procedure is complete. Alternatively, GPOs can be backed up and restored and instructions to do so are available in Emerson's Guardian Support Portal.

6 Conclusions

Starting with Microsoft Windows 10 Anniversary Update, Microsoft Edge and Internet Explorer will no longer consider websites protected with a SHA-1 certificate as secure. Emerson is already providing a solution for this issue by providing SHA-2 certificates with the web-based DeltaV applications.

The provided self-signed certificates for web-based DeltaV applications are valid for 90 days, and their main purpose is to allow you to evaluate and test the web-based DeltaV applications during Factory or Site Acceptance Tests, etc. The full long term solution needs to be provided by either a self-signed Root CA or a Private CA, whichever better suits your security posture as well as business decision. Please contact your local Emerson sales office in case you need support with any of the presented options in this document.

The main purpose of using digital certificates on web-based DeltaV applications is to verify that the Server providing the web pages can be trusted, and since it is a security protection, the certificates' keys must be managed appropriately. Self-signed certificates based on lower encryption hash function (e.g. SHA-1) cannot be simply deemed acceptable, and are also deprecated by the CA/B Forum guidelines.

The following references are available as additional literature about the topics presented in this white paper:

- CA/B Forum website - **https://cabforum.org/**
- Windows Enforcement of SHA-1 Certificates - **http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-sha1-certificates.aspx**
- DeltaV Security Manual - **http://www2.emersonprocess.com/siteadmincenter/pm%20deltav%20documents/manuals/cs_deltav_security_manual-toc%20only.pdf**
- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile - **https://tools.ietf.org/html/rfc5280**

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
+65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/deltav

DELTAV™

EMERSON™