Implementer Certificate

Installation Guide

February 05, 2016

Version 2.5

Document Change History

Version	Date	Items Changed Since Previous Version	Changed By
0.1 – 0.8		Initial Drafts	Nicholas Vennaro
0.9	06/01/2010	Consolidated with Entrust Process Guide; renamed guide; updated URLs and screen shots; added generate a CSR section; edited and formatted	Anand Perianayagam, Linda Toscano
1.0	07/07/2010	Following Nicholas Vennaro's review, advanced to version 1.0	Linda Toscano
1.1	02/22/2011	Updated logo and acronyms	Linda Toscano
1.2	09/12/2011	Added instructions for Java keystore installation; added list of figures; added section links	Alok Srivastava, Linda Toscano
1.3	10/30/2012	Added URL for accessing Production Certificate	Vijay Shah
2.0	08/18/2014	Update content, URLs, procedures, images and figures	Gonzalo Hernando
2.1	12/29/2014	Updated content and language for user readability	Gonzalo Hernando
2.2	01/13/2015	Minor edits and addition suggested by participants	Gonzalo Hernando
2.3	04/28/2015	Section 4.2 update	Gonzalo Hernando
2.4	06/29/2015	Organization Name change	Gonzalo Hernando
2.5	02/05/2016	Correcting typos and adding instructions for downloading root certificate	Gonzalo Hernando

Table of Contents

List of Figures

1 Overview

An important feature of a Participant's onboarding process with the Carequality is obtaining and using digital security certificates. This document will guide Participants through the certificate installation process as well as discuss the importance of best practices for certificate handling.

1.1 Definitions

The following terms are used throughout this document:

1. Participant – Refers to the organization that is onboarding to the Carequality such as an HIE, Hospital etc.
2. Subscriber – The individual within a participant that signed the Entrust contract in order to acquire a certificate
3. Proxy – The individual assigned by the Subscriber with the role of managing and installing the certificate.

1.2 Production Certificate Process Overview

During the Production onboarding process, Participants will submit a request to the Carequality Support Staff for a new certificate. After the Carequality Support Staff validates the appropriate documents (see section 2 of this document) a certificate acquisition "reference number" and "authorization code" will be sent by two separate ***modalities*** to the Subscriber or the Subscriber's Proxy. These codes will be utilized to create the Certificate Signing Request (CSR) as well as obtaining the signed certificate. After the certificate installation is complete the Organization will be able to perform partner testing and connect to other Participants in the Production environment.

2 Superseded Certificate Information

In the past there were some installation steps that are no longer required. This guide along with the links to the additional information contain the latest information with regards to your certificate installation guide. After installing all the certificates mentioned in this document ensure that your trust chain and certificates match what is mentioned.

Known superseded steps:

1. There is no longer a need for a Cross-Certificate. The only certificates that should be installed on your environment are your server, intermediate and root certificates mentioned in this document.

3 Information for Requesting a Certificate

3.1 Production Request Documents/Information

1. The following Identity Proofing forms (via hyperlinks) shall be completed for any Implementer who is designating/updating a Subscriber to receive the Certificate codes, or if the current forms are more than two years old. Note – these forms are valid for 2 years from the date they are Notarized and Certificates expire after one year's time.

   https://carequality.org/wp-content/uploads/2020/02/Subscriber-Identity-Verification-Form.pdf

   https://carequality.org/wp-content/uploads/2020/02/Subscriber-Agreement-Form.pdf

2. The Subscriber's approval for any renewal request shall be needed. (Include name, email address, and cell phone number)

3.2 Uploading the forms and next steps

Upon completion/Notarization of the required forms, an Implementer Representative uploads them along with photocopies of IDs to the appropriate Implementer folder on Box.

4 Overview of Proper Handling of Codes and Certificates

Before an Organization begins the final stage of the onboarding process, installing the Production certificate and moving into Production, it is imperative that the individual (Subscriber or Proxy) handling the codes and certificate understand the proper guidelines and procedures for dealing with them.

4.1 Handling Codes

It is important to understand that, in Production, these codes are the keys to obtaining access to millions of patients' data, and therefore it is extremely important that they are handled correctly. The codes are issued by Carequality Support Staff directly to, and only to, the x.509 Subscriber or a person named by the Subscriber to act as his/her Proxy. These codes must ***not*** be shared with anyone; only the Subscriber ***or*** the Proxy should have them (not both). Also, a reminder that the use of these codes is covered in the Entrust agreements that you or your organization notarized and executed, and the associated Entrust and FBCA policies, and applicable state and federal law and regulations.

4.2 Handling Certificates

Your production certificate allows your organization to access the network and all of its patients' data. For this reason, it is required that your organization take the necessary precautions to ensure that this certificate remains secure. The following items should be followed (including but not limited to):

- Private key should never be shared.
- Private key should be created on the production server.

- Private key should never leave the production server.
- Individuals should become familiar with X.509 key management best practices.
- Individuals should be familiar with applicable law and FBCA procedures and policies.

In general individuals must agree to follow certificate best handling practices. For a list of similar or best practices organizations can and should review certificate PCI compliance. See: https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs (requires free registration).

5 Generate CSR

After the Organization receives the reference number and authorization code from the Carequality Support Staff, it starts the process of creating a certificate for a Web server. The first step is to generate a pair of cryptographic keys and a PKCS#10 Certificate Signing Request (CSR). The CSR contains information used to create the certificate. The following values should be used to fill out your Certificate Signing Request:

Note: depending on the tool used to generate the CSR a Keystore might need to be created before the CSR. Regardless the Keystore size needs to be set to 2048.

IMPORTANT: ensure that you follow the lower case/upper case of each value for your CSR e.g. the Organization 'O' for validation is all lower case 'nhin' while the Organizational Unit 'OU' is mixed.

5.1 CSR Values for Production

CN=<*registry.nhinonline.net*> (**Replace this value with your Reference Number**)
O=HHS-ONC
OU=CAREQUALITY
C=US

Note: Only enter the information after the equals sign '=' e.g. for the organization field enter 'HHS-ONC' (no quotes)

Note: The Common Name (CN) is an important piece of information required in the CSR. The CN **must** be the reference number sent by Carequality Support Staff to the Organization. Once the CSR is signed the resulting certificates CN should be an FQDN that resolves (not an IP).

Note: If City and State are required fields for your CSR enter the City and State of your organization.

For Windows IIS users: Leave the Cryptographic service provider as "Microsoft RSA SChannel Cryptographic Provider" and make sure to select a bit length of 2048.

6 Submit CSR

After the Organization generates the CSR for the Web server, it submits the certificate request through the Entrust Authority™ Enrollment Server for Web. Use the following steps to complete this procedure.

Using Internet Explorer go to the appropriate URL:

6.1 Production URL

https://enrollwebfed.managed.entrust.com/nfi/cda-cgi/clientcgi?action=start

Note: Please verify that the Organization is utilizing the latest endpoints by cross checking the information with question 1 on the following article:

https://carequality.org/wiki/carequality-certificates/

1. The Entrust Authority™ Enrollment Server for Web tool should appear.

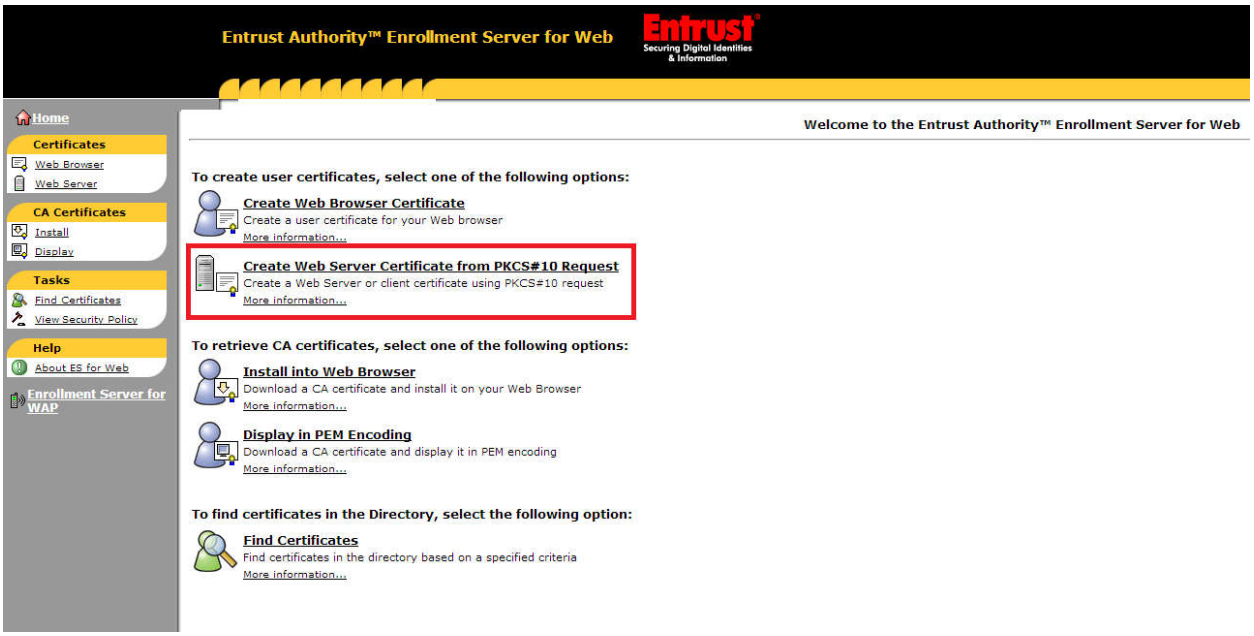

Figure 1. Entrust Authority™ Enrollment Server for Web Screen

Warning: The system may prompt you to install a Java Applet. Agree to the installation and follow the screen prompts to run the applet. **Note:** The system does not confirm installation.

2. Click **Create Certificate from PKCS#10 Request**. The Web Server PKCS#10 Certificate Request screen appears.

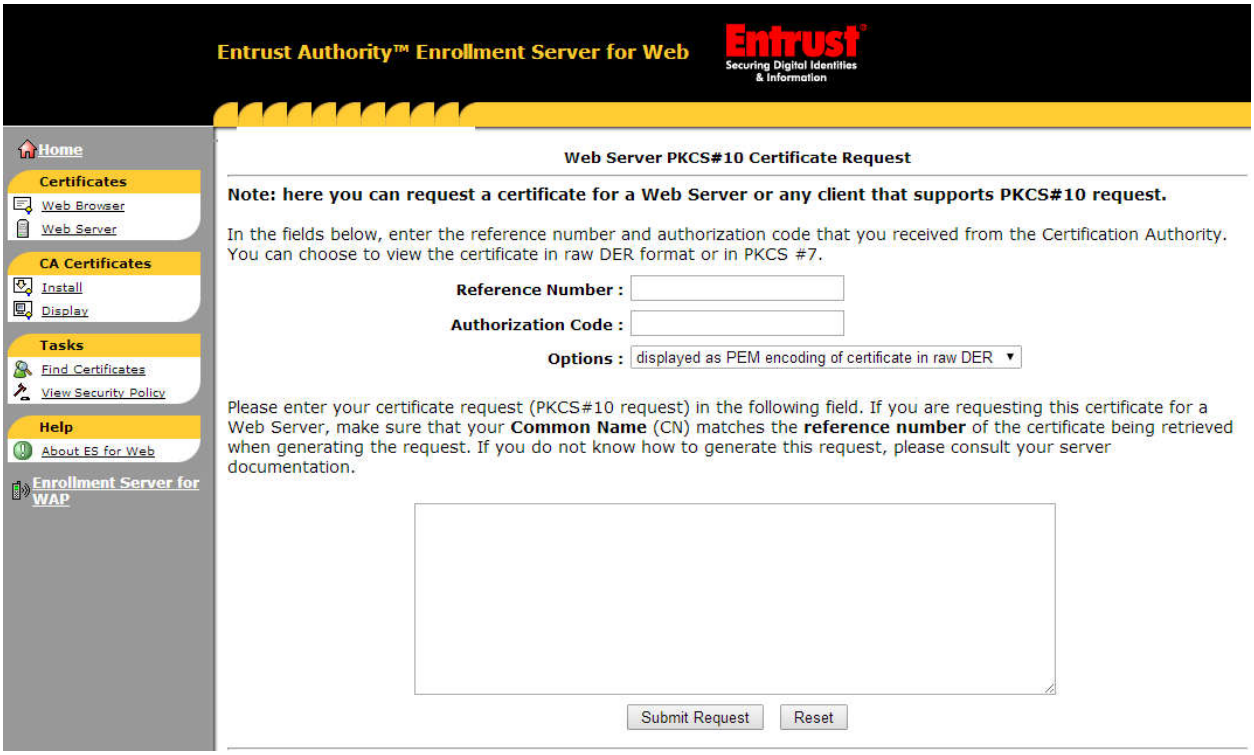

Figure 2. Web Server PKCS#10 Certificate Request Screen

3. In the *Reference Number:* field, enter **(Reference Number)** (or use copy/paste) issued by Carequality Support Staff.
4. In the *Authorization Code:* field, enter **(Authorization Code)** (or use copy/paste) issued by Carequality Support Staff.
5. Leave the *Options:* field with the default selection.
6. Copy the **(CSR)** you stored earlier in Notepad. (Include the *BEGIN* and *END* lines)
7. In the *Certificate Request* field, paste the **(CSR)** into the large text box.
8. Click **Submit Request**. Managed Services generates a Web server certificate and sends it to the Enrollment Server for Web.

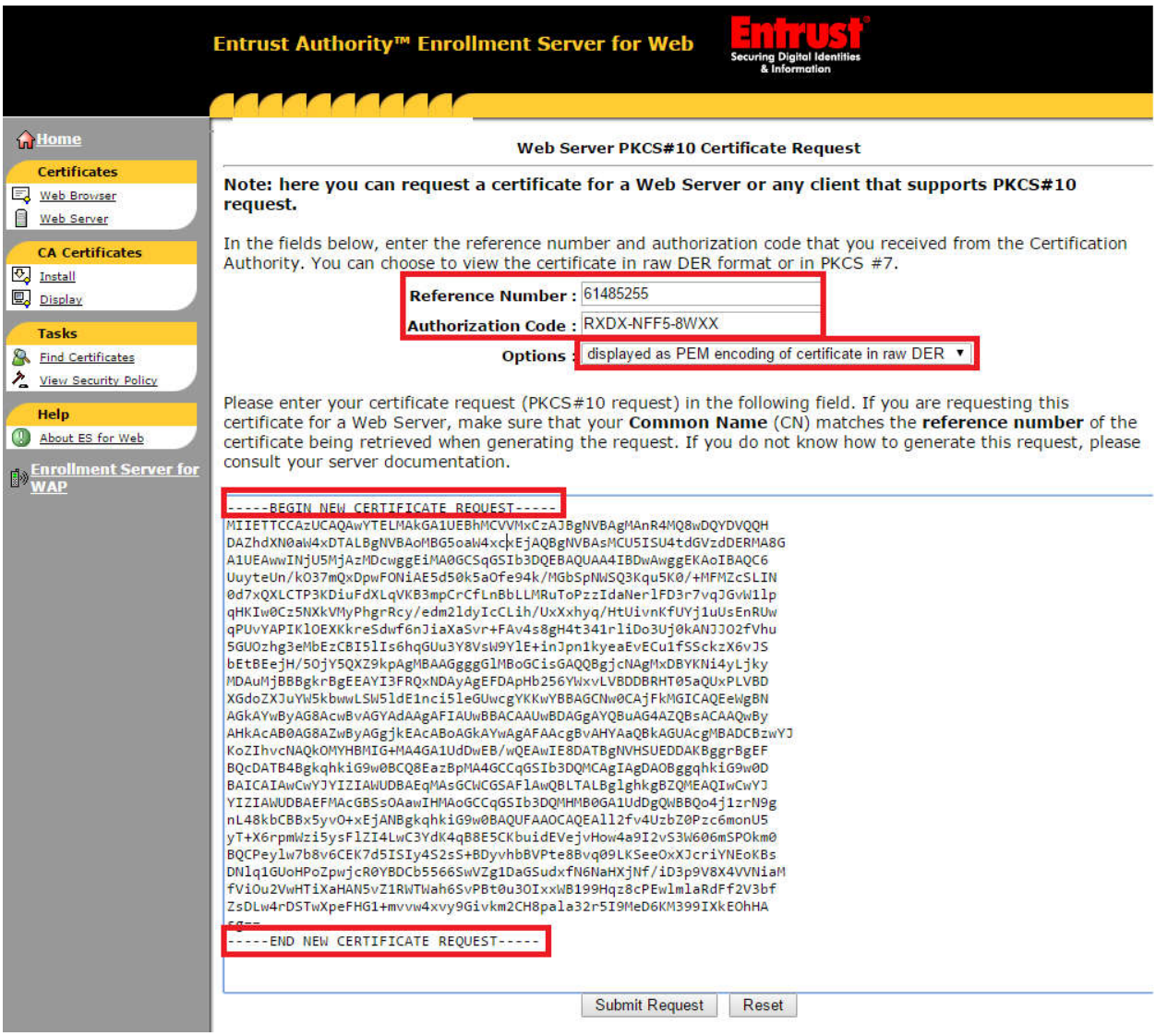

Figure 3. Web Server PKCS#10 Certificate Request Screen Filled

Note: Figure 3 does not contain accurate data, is for reference only.

Note: If an issue occurs during the submission process, after verifying that all the information was entered correctly on the CSR and website, and the correct URL was utilized please contact the Carequality Support Staff.

9. Click **Download** on the page displaying your certificate. A dialog box appears. **Note:** Depending on your browser, the dialog box could vary, but the steps are similar.
    a. In Internet Explorer:
        i. In the **File Download** dialog box, click **OK** to save this file to disk.

ii. In the **Save As** dialog box, choose a name and path of a text file to save the certificate.
iii. Click **Save**.

b. In Firefox:
i. In the **Opening** dialog box, select **Save to Disk**.
ii. Click **OK**. Firefox saves the file to the desktop.

If the system saves the certificate in the text file; the file extension may be `.bin` or `.cer`.

Note: If the download does not contain the right extension, copy and paste the certificate text to a text editor and save as a .cer file

You have submitted the certificate request.

7 Import Web Server Certificate

Because every system is unique and has different configurations it will be left up to the organization to properly and securely install the signed certificate to the web server.

8 Acquiring Root and Intermediate CA Certificate into Web Server

The following steps guide the Organization with instructions to acquiring the Intermediate and Root certificates.

Note: Previously there was a need for a Cross-Certificate to be installed. Please ensure that the Cross-Certificate is not present on the certificate trust chain and that only the following intermediate and root are present.

Note: Some systems will derive the incorrect intermediate and root certificate ensure that the certificate trust chain matches the certificates mentioned on section 9.

Note: Be sure to NOT install the FBCA cross-signed certs instead of the Carequality/Entrust FBCA certs unless you have good reason.

8.1 Retrieve CA Certificate from Managed Services

1. Using a Web browser go to the Production URL used to sign your CSR. See section 4.1 and 4.2. The Entrust Authority™ Enrollment Server for Web tool appears.
2. On the left side of the screen, under CA Certificates, click **Install**.
   Note: Depending on your browser, the dialog box could vary, but the steps are similar.

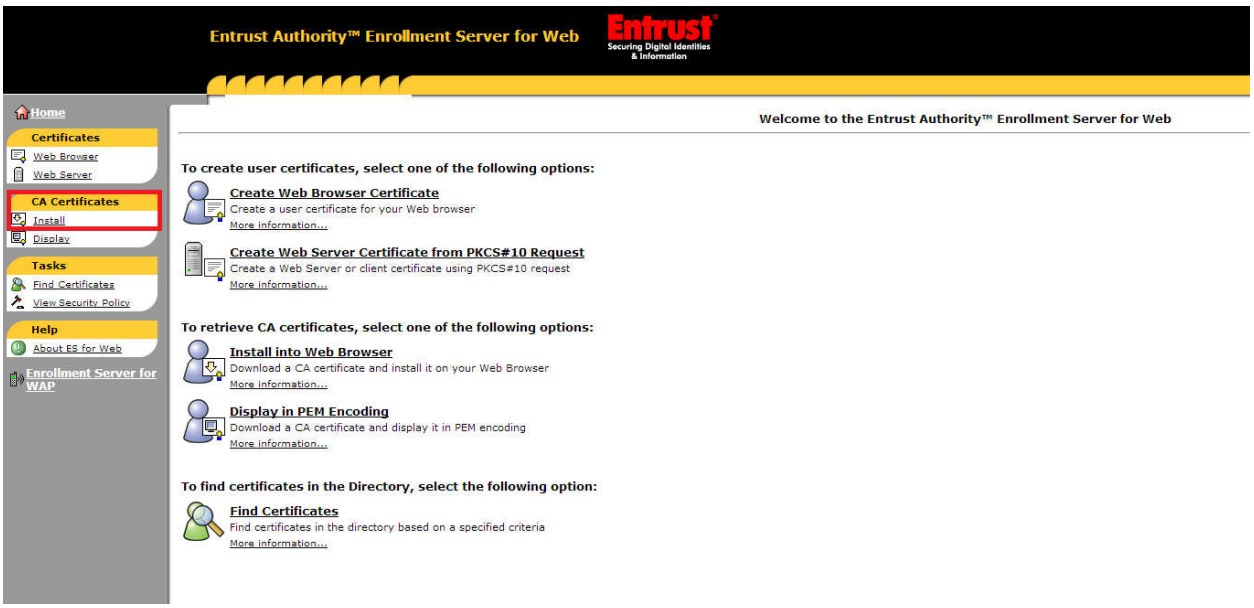

Figure 4. File Download – Security Warning Dialog Box

3. Save the certificate on the server. Ensure that the extension is *.cer*

Note: this download will have both the intermediate and root ensure that each certificate gets installed on the appropriate location.

Important: some systems will not derive the root out of the intermediate (mainly linux machines). If you are having issues with extracting the root certificate for your chain please contact Carequality Tech Support.

8.2 Installing Root and Intermediate CA Certificate

It will be left up to the organization to properly and securely install the signed certificate to the web server. These two certificates should be installed on your server based on the Organization's policies and procedures. Once installed ensure that the information on each certificate is accurate by comparing the detailed information of the certificate with the information in section 8 of this document.

9 Verifying Root, Intermediate and Server Certificates

After an Organization has installed all three CA certificates (Root, Intermediate and Server) in order to ensure that the correct certificates have been installed verify that the following information agrees with your installed certificates.

9.1 Production Certificate Details

The Entrust Root (self-signed) CA cert:

- serial number: 4A:A8:A6:0D
- issued 11/16/2017
- valid until 12/17/2027
- issuer OU = Entrust Managed Services NFI Root CA, OU = Certification Authorities, O = Entrust, C = US
- subject OU = Entrust Managed Services NFI Root CA, OU = Certification Authorities, O = Entrust, C = US

The Entrust Intermediate (Signing) CA cert:

- serial number: 4A:A8:B9:EA
- issued 5/16/2017
- valid until 12/17/2027
- issuer OU = Entrust Managed Services NFI Root CA, OU = Certification Authorities, O = Entrust, C = US
- subject OU = Entrust NFI Medium Assurance SSP CA, OU = Certification Authorities, O = Entrust, C = US

Your Server cert:

- serial number/dates (customer specific)
- issuer OU = Entrust NFI Medium Assurance SSP CA, OU = Certification Authorities, O = Entrust, C = US
- subject CN = (your FQDN), OU = CAREQUALITY, O = HHS-ONC, C = US

10 Best Practices

This certificate is the key to the Carequality ecosystem. The organization is responsible for following all best practices with regards to certificate handling and installation. The organization (as well as the individual installing the certificate) needs to be familiar with our minimum certificate best practices (See section 3 of this document). In addition, keys need to be handled using industry best practices. For example, see the PCI DSS Self-Assessment Questionnaire D questions 3.5 and 3.6 which may be found at https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs (requires free registration). Last but not least, ensure familiarity with the Carequality's X.509 certificate article https://carequality.org/wiki/carequality-certificates/

11 Troubleshooting

Troubleshooting is largely dependent on one's environment. A few troubleshooting items that should be common to most environments are as follows:

- See question 22 of https://carequality.org/wiki/carequality-certificates/ for information on smoke testing and partner testing.
- Section 8 of this document should be used to verify that you have the correct certificates installed.