Explanation of SSL Certificate chain issues

Certificate chains are a PKI feature that allows root certificate authorities to delegate the work of certificate signing. Roughly one half of all sites have certificates that are signed by a trusted CA. Such sites need only provide the server's certificate in the handshake. The remaining half (of the sites) uses intermediate certificates (usually only one; it is rare to see a site with more than one such certificate). Such sites need to provide all the intermediate certificates in addition to the server's certificate.

Common SSL chain issues:

- **Missing intermediate certificates;** When a site does not provide the necessary intermediate certificates, a trust path cannot be established. Generally speaking, we cannot distinguish that case from a certificate signed by a custom CA. However, some server certificates include the information on which intermediate certificates are required, and also where to obtain them. SSL Labs will attempt to fetch missing certificates. If the intermediate certificates are found, then it's very likely that a trust path will be established. In such cases, the test will issue a warning. If you site receives the warning you should reconfigure the server to add the missing certificates.
- **Certificate chains that are too long;** Sites often include more certificates in the handshake than necessary. Of those, most include one extra certificate, and that is the actual trusted root certificate (which browsers already have in their storage). This last certificate is not needed for the validation process. Having an additional certificate in the chain wastes bandwidth and decreases overall performance slightly. A small number of sites will include a very large number of certificates as a result of misconfiguration. Such sites will typically suffer significant performance issues and need to be reconfigured.
- **Certificates given in incorrect order**; According to the standard, certificates must be presented in the order in which they are needed. The main, server, certificate must come first, followed by the certificate that signed it, followed by the next certificate in the chain, and so on. A small number of sites does not get this order right. Most SSL clients will deal with this problem silently, but there is a small number of platforms that will give up.

Solutions

To resolve chaining issues there are two main steps that must be completed:

- Verify that Thawte Intermediate CA are installed on the server.

Step 1: Obtain the Thawte Intermediate CA

Note: If you know you installed the PKCS#7 version of your SSL certificate, please skip to Step 3. The PKCS#7 version of the SSL certificate is available from Thawte Certificate Center (TCC) and includes the Thawte Intermediate CA and the SSL certificate. Microsoft IIS understands how to parse this type of file during the certificate installation.

If you downloaded the certificate in x509 format (.cer, .crt), obtain the Thawte Intermediate CA that is appropriate for your product from: INFO1384

Step 2: Adding the Certificates Snap-in to the Microsoft Management Console (MMC):

Microsoft IIS 5.0 or 6.0

1. From your Web server, go to **Start** > **Run**
2. Enter **mmc** in the text box
3. Click **OK**
4. From the Microsoft Management Console (MMC) menu bar, select **Console** > **Add/Remove Snap-in**
5. Click **Add**
6. Select **Certificates** from the list of snap-ins
7. Click **Add**
8. Select the **Computer account** option
9. Click **Next**
10. Select the **Local computer** (the computer this console is running on) option
11. Click **Finish**
12. Click on the **Close** button on the snap-in list window
13. Click on the **OK** button on the Add/Remove Snap-in window

Microsoft IIS 7.0

1. From the Web server, click **Start**
2. In the Search programs and files field, type **mmc**
3. From the Programs list, click **mmc.exe**
4. At the permission prompt, click **Yes**
5. From the Microsoft Management Console (MMC), click **File** > **Add/Remove Snap-in**
6. From the list of snap-ins, select **Certificates**
7. Click **Add**
8. Select **Computer account**
9. Click **Next**
10. Select **Local computer (the computer this console is running on)**
11. Click **Finish**
12. In the Add/Remove Snap-in window, click **OK**
13. Save these console settings for future use

Step 3: Install the Thawte Intermediate CA

1. Open the **Microsoft Management Console** (MMC)
2. Click on **Certificates** from the left pane
3. Double-click on **Intermediate Certification Authorities** from the right pane
4. Right-click on **Certificates** from the right pane and select **All Tasks** > **Import** to open the **Certificate Import Wizard**
5. Click **Next**
6. Specify the location of the **Thawte Intermediate CA** file obtained from Step 1 by clicking **Browse**
7. Click **Next**
8. By default, it will place the certificate in the Intermediate Certification Authorities store. Keep this selection and click on the **Next** button.
9. Click **Finish**
10. A message will appear confirming the successful import of the certificate. Click **OK**
11. Keep the Console open

Step 4: Verify certificate installation

1. Stop and start your Web server prior to any testing
   Note: In some cases the changes may not take place after restarting IIS Services and a re-boot is needed.
2. To verify the SSL certificate installation, use the **Thawte Installation Checker**

Reference Link:

Explanation of chain issues in SSL Labs tests

Resolving certificate chain issues with Thawte SSL123,SSL Web Server/Wildcard or Thawte SSL Extended Validation certificate for IIS 5.0, 6.0, or 7.0