New Sectigo Cross-Signed Intermediates in Microsoft

Sectigo has provided this workaround to build the cross-signed intermediate into the chain of trust on Microsoft servers.

What you need:

- The intermediate certificate (Sectigo Public Authentication Server CA DV/OV/EV)
- The cross-signed intermediate certificate (Sectigo Public Authentication Server CA Root)
- The root (USERTrust RSA Certification Authority)

These three certificate files are included in your certificate downloads folder but can also be downloaded from the links provided in this guide.

1. Run MMC to Add Certificates

1. Open the Microsoft Management Console (MMC): open Start -> Run -> Type mmc and Click 'OK' or hit Enter on your keyboard.
2. Open 'Add/Remove Snap-in' Window
3. File -> Add/Remove Snap-in
4. Add the Certificates Snap-in
5. Click 'Add' then double-click 'Certificates'
6. Select 'Computer Account' and click 'Next'
    1. Note: This step is very important. It must be the 'Computer Account' and no other account
7. Select 'Local Computer' and click 'Finish'
8. Close the 'Add Standalone Snap-in' window and click 'OK' in the 'Add/Remove Snap-in' Window.

Will now be returned to the MMC.

Click on the (+) sign by “certificates (local computer), to add each certificate as follows.

2. Import the Cross-Signed Root

Expand the Certificates section by clicking on the plus (+) sign and turn it to a minus (-) sign to expose the 'Certificates' tree and select "Trusted Root Certification Authorities", sub-folder "Certificates"

Right Click on "Certificates" folder > "All Tasks" > "Import" the Root Certificate "USERTrustRSACertificationAuthority.crt"

- Review certificate https://crt.sh/?id=1199354
- Direct download link https://crt.sh/?d=1199354

3. Import the Cross-signed Intermediate

Expand the Certificates section by clicking on the plus (+) sign and turn it to a minus (-) sign to expose the 'Certificates' tree and select "Intermediate Certification Authorities", sub-folder "Certificates"

Right Click on "Certificates" folder > "All Tasks" > "Import" the Cross-signed Intermediate Certificate SectigoPublicServerAuthenticationRootR46_USERTrust.crt

- Review certificate https://crt.sh/?id=11405654893
- Direct download link https://crt.sh/?d=11405654893

4. Important the Product type Intermediate

- DV - Sectigo Public Server Authentication CA DV R36 (https://crt.sh/?d=4267304690)
- OV - Sectigo Public Server Authentication CA OV R36 (https://crt.sh/?d=4267304698)
- EV - Sectigo Public Server Authentication CA EV R36 (https://crt.sh/?d=4267304687)

Expand the Certificates section by clicking on the plus (+) sign and turn it to a minus (-) sign to expose the 'Certificates' tree and select "Intermediate Certification Authorities", sub-folder "Certificates"

Right Click on "Certificates" folder > "All Tasks" > "Import" the Product type Intermediate Certificate from the list above (subject to the customers purchased certificate type)

5. Cross-Signed Workaround

If possible, disable the self-signed Root Certificate "Sectigo Public Server Authentication Root R46" on Windows Server. (Please **do not remove** the root)

It might be necessary to disable certificate via Windows' MMC to ensure that the correct certificate chain is used.

1. Open the Windows Run dialog by clicking Run in the Start Menu or using the Win+R shortcut. Then type mmc and click OK.
2. Click on the File menu then on Add/Remove Snap-in.
3. Click on Certificates then on Add.
4. Select your Windows Account type then completes the information required (generally - Computer Account)
5. Then click OK.

Disabling a certificate within the "Trusted Root Certification Authorities" / sub-folder store "Certificates"

6. Select "Sectigo Public Server Authentication Root", right-click the certificate Then, select Properties.
    1. Note: Please check that this certificate is “Issued By: Sectigo Public Server Authentication Root” before disabling. Do not disable the certificate Issued by USERTrust.
7. In the General tab, in the field Certificate Purpose, select "Disable all purposes" for this certificate
8. Then click OK.

The certificate is now disabled.

This should then allow the cross-signing chain to be shown and used.