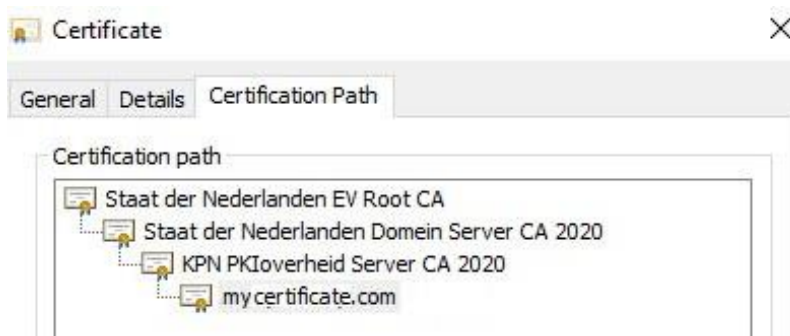




Installatie KPN PKIoverheid CA 2020 servercertificaat

KPN geeft **vanaf augustus 2020** de PKIoverheid servercertificaten uit onder het Root CA certificaat "Staat der Nederlanden EV Root CA" met daaronder twee Intermediate CA certificaten, te weten "Staat der Nederlanden Domein Server CA 2020" en daaronder de "KPN PKIoverheid Server CA 2020". De volledige CA hiërarchie van een CA 2020 servercertificaat ziet er als volgt uit:



Het is van het grootste belang dat naast het CA 2020 servercertificaat, in bovenstaand voorbeeld *www.example.nl*, ook beide Intermediate CA certificaten op de server geïnstalleerd worden.

Op de meeste servers en in de client browsers is het "Staat der Nederlanden EV Root CA" certificaat standaard of via update aanwezig in de zogenaamde "Trusted Root Certification Authorities". De twee Intermediate CA certificaten zijn meestal niet aanwezig in de client browsers en deze zullen door de server naar de client gepushed moeten worden zodat de CA certificate chain gemaakt kan worden en het CA 2020 servercertificaat als trusted (geldig en vertrouwd) wordt beschouwd in de browser¹.

Download CA certificaten

Het [Staat der Nederlanden EV Root CA](#) certificaat is hier te downloaden. (Als het goed is al aanwezig in Certificate Store).

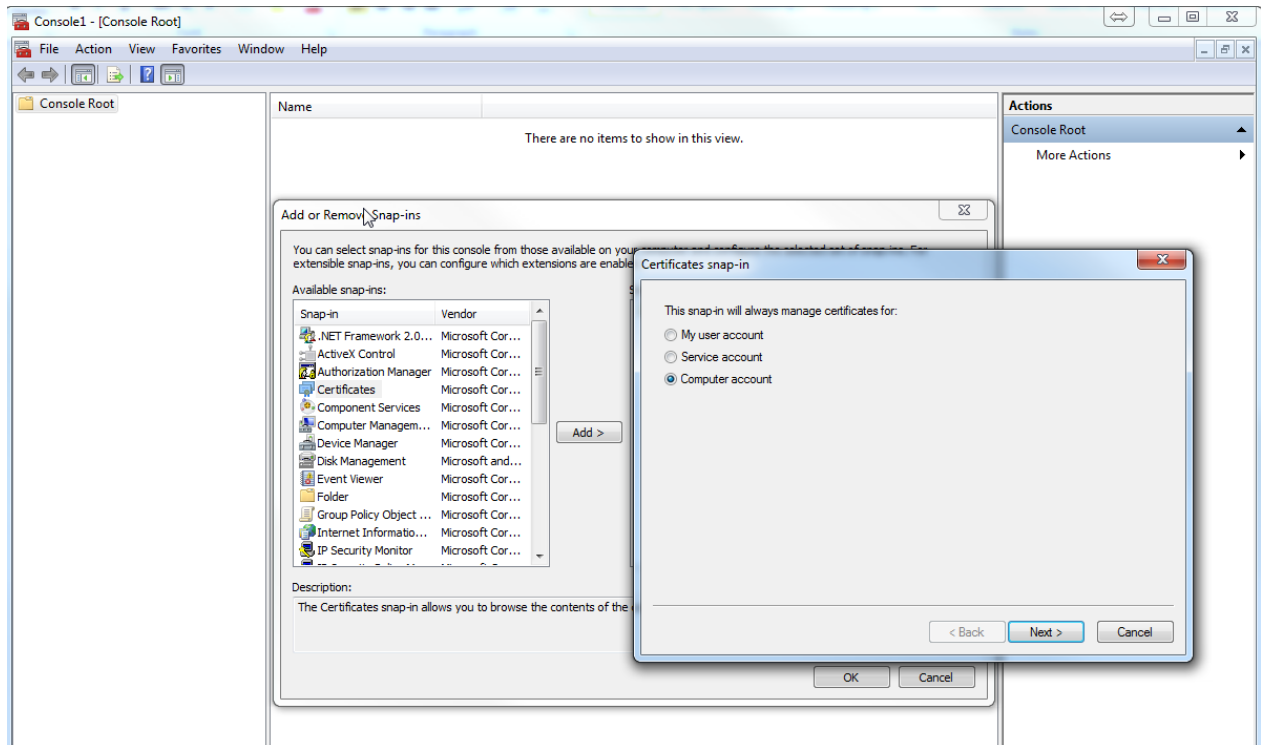
Het [Staat der Nederlanden Domein Server CA 2020](#) certificaat is hier te downloaden.

Het [KPN PKIoverheid Server CA 2020](#) certificaat is hier te downloaden.

Installatie CA certificaten op een Windows server

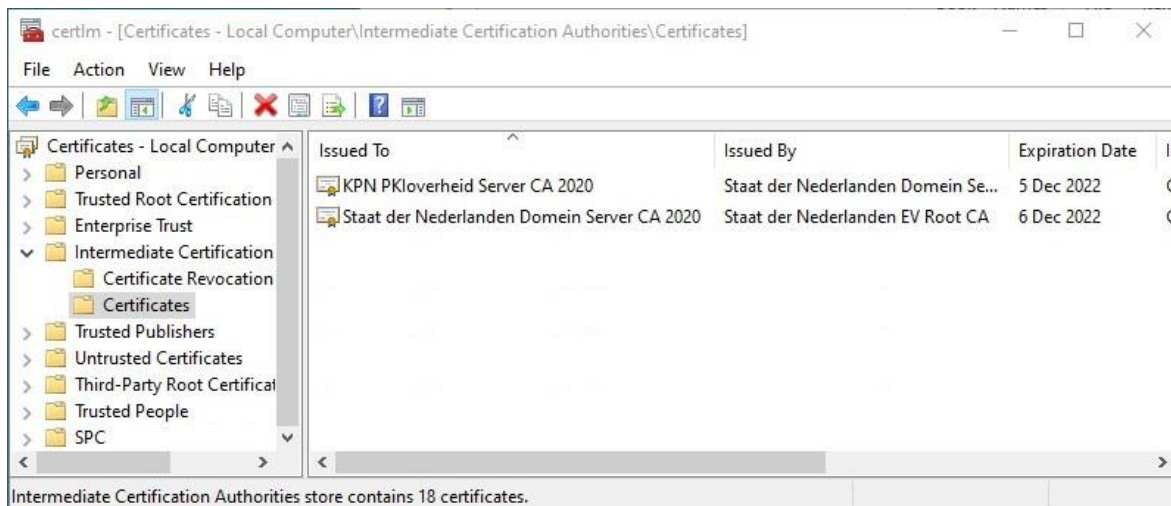
Dit kan via MMC → Add snap-in Certificates. Kies voor Computer account (of direct op te starten via windows startmenu met 'certlm.msc')

¹ De CA 2020 servercertificaten bevatten ook een URL met een link naar het bovenliggende intermediate CA certificaat. In theorie zou een client hiermee zelf de CA certificate chain kunnen ophalen maar dit wordt niet altijd ondersteund en is bovendien trager. Vandaar het advies om altijd de volledige CA certificate chain te installeren op de server.



Selecteer Certificates (Local Computer) → Intermediate Certification Authorities → Certificates.

Importeer dan via All Task → Import de twee Intermediate certificaten die gedownload zijn. Het resultaat is als volgt zichtbaar:



Apache Webserver

In een Apache omgeving is het advies om in de file (default ca-bundle.xxx) waarin verwezen wordt door het statement "SSLCertificateChainFile" in de ssl.conf de drie certificaten van de certificate chain op te nemen, te weten:

1. KPN PKIoverheid Server CA 2020
2. Staat der Nederlanden Domein Server CA 2020
3. Staat der Nederlanden EV Root CA



Het bestand [ca-bundle-kpn-server-ca-2020.pem](#) is hier te downloaden en bevat de 3 genoemde CA certificaten in PEM formaat².

Java keystore

Mochten er via een client certificaat in een java keystore (jks) van een andere server een verbinding opgezet worden naar de server waar het PKIOverheid G3 servercertificaat geïnstalleerd is, moet men in deze key store ook de certificate chain en het server certificaat van de server opnemen:

1. (in dit voorbeeld) www.example.nl
2. KPN PKIoverheid Server CA 2020
3. Staat der Nederlanden Domein Server CA 2020
4. Staat der Nederlanden EV Root CA

² De linkjes onder 'Download CA certificaten' verwijzen naar de CA certificaten in DER format.