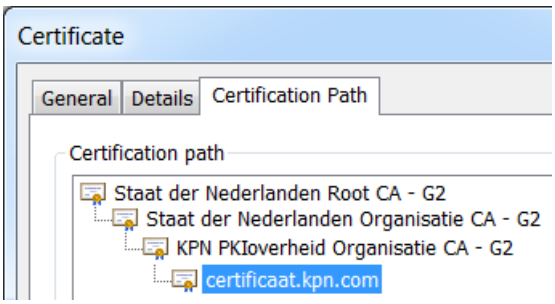
English version

KPN PKIoverheid server (SSL) certificaten G2

KPN geeft deze certificaten uit onder het Root CA certificaat "Staat der Nederlanden Root CA - G2" met daaronder twee Intermediate certificaten, te weten “Staat der Nederlanden Organisatie CA - G2” en **vanaf 1 april 2016** de “KPN PKIoverheid Organisatie CA - G2”.
De CA hiërarchie ziet er als volgt uit:



Het is van het grootste belang dat naast het server SSL certificaat, in dit voorbeeld *certificaat.kpn.com* ook beide Intermediate certificaten op de server geïnstalleerd worden.

Op de meeste servers en in de client browsers is het "Staat der Nederlanden Root CA - G2" standaard of via update aanwezig in de zogenaamde “Trusted Root Certification Authorities”. De twee Intermediate certificaten zijn meestal niet aanwezig in de client browsers en deze zullen dus door de server naar de client gepushed moeten worden zodat de certificate chain gemaakt kan worden en het SSL certificaat als trusted (geldig en vertrouwd) wordt beschouwd.

Hieronder zijn de linkjes opgenomen naar de genoemde CA certificaten opgenomen:

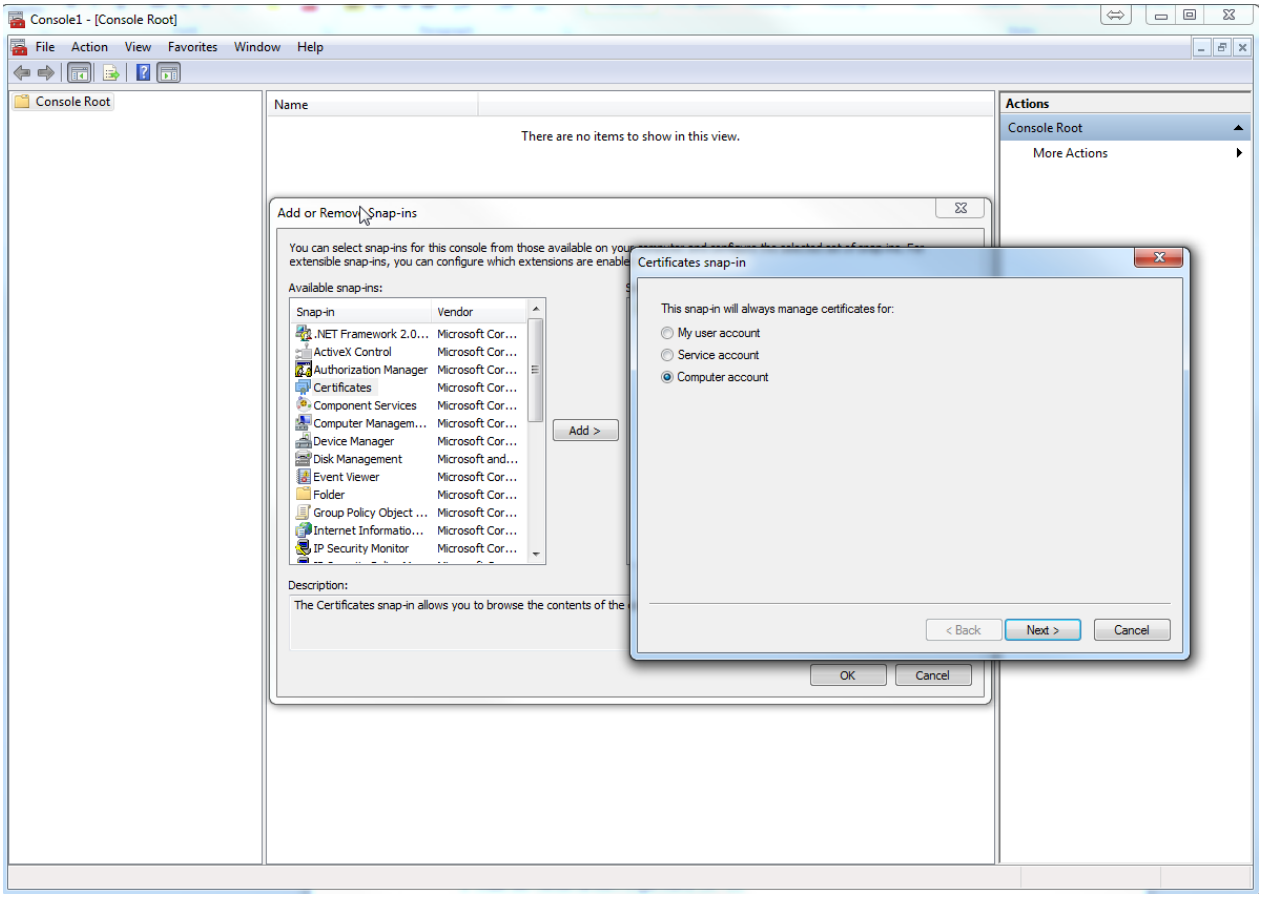
Staat der Nederlanden Root CA - G2 certificaat.

- Staat der Nederlanden Organisatie CA - G2 certificaat.

- - KPN PKIoverheid Organisatie CA - G2 certificaat.

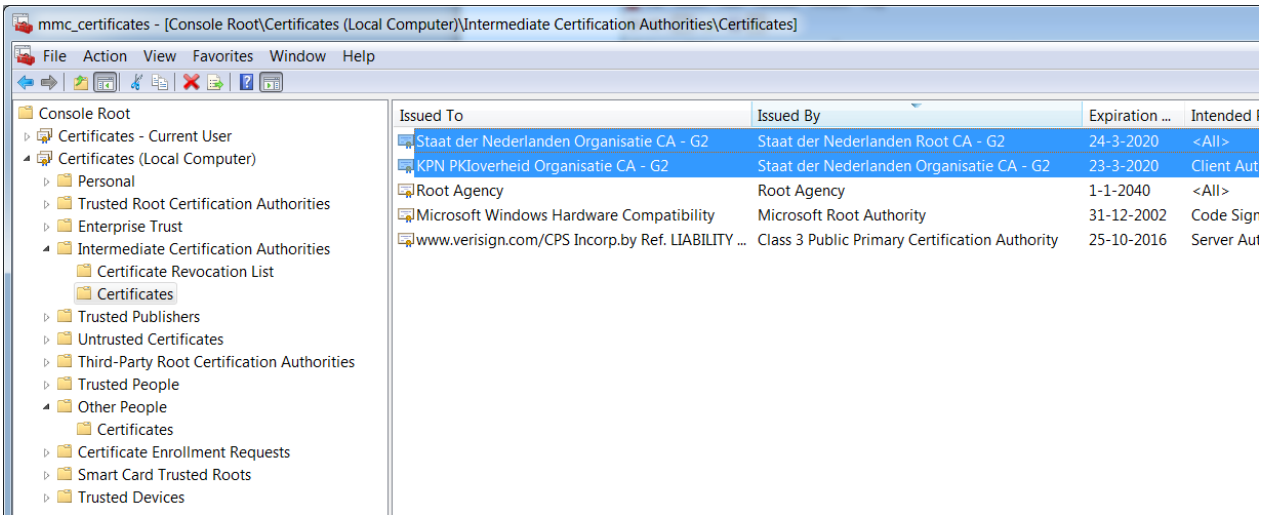
Toevoegen intermediate CA's op een Windows server

Dit kan via MMC ➔ Add snap-in Certificates. Kies voor Computer account



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. Dit zijn de:

1. KPN PKIoverheid Organisatie CA - G2
2. Staat der Nederlanden Organisatie CA - G2
3. Staat der Nederlanden Root CA - G2

Het ca-bundle-kpn-g2.pem bestand bevat de drie genoemde CA certificaten in PEM formaat.

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 certificaat geïnstalleerd is, moet men in deze key store ook de certificate chain en het server certificaat van de doel server opnemen:

1. (in dit voorbeeld) certificaat.kpn.com
2. KPN PKIoverheid Organisatie CA - G2
3. Staat der Nederlanden Organisatie CA - G2
4. Staat der Nederlanden Root CA - G2