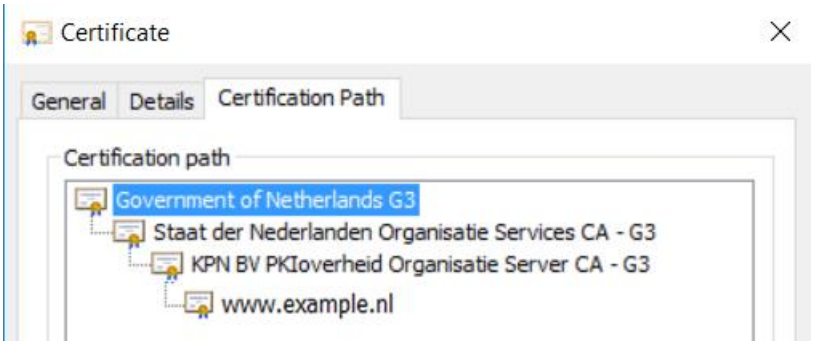
[English version]

Installatie KPN PKIoverheid G3 servercertificaat

KPN geeft **vanaf medio maart 2017** de PKIoverheid servercertificaten uit onder het Root CA certificaat "Staat der Nederlanden Root CA - G3" met daaronder twee Intermediate CA certificaten, te weten “Staat der Nederlanden Organisatie Services CA - G3” en daaronder de “KPN BV PKIoverheid Organisatie Server CA - G3”. De volledige CA hiërarchie[1] van een G3 servercertificaat ziet er als volgt uit[2]:



Het is van het grootste belang dat naast het G3 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 Root CA - G3" 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 dus door de server naar de client gepushed moeten worden zodat de CA certificate chain gemaakt kan worden en het G3 servercertificaat als trusted (geldig en vertrouwd) wordt beschouwd in de browser[3].

Download CA certificaten

Het Staat der Nederlanden Root CA - G3 certificaat is hier te downloaden. (Als het goed is al aanwezig in Certificate Store).

Het Staat der Nederlanden Organisatie Services CA - G3 certificaat is hier te downloaden.

Het KPN BV PKIoverheid Organisatie Server CA - G3 certificaat is hier te downloaden.

---

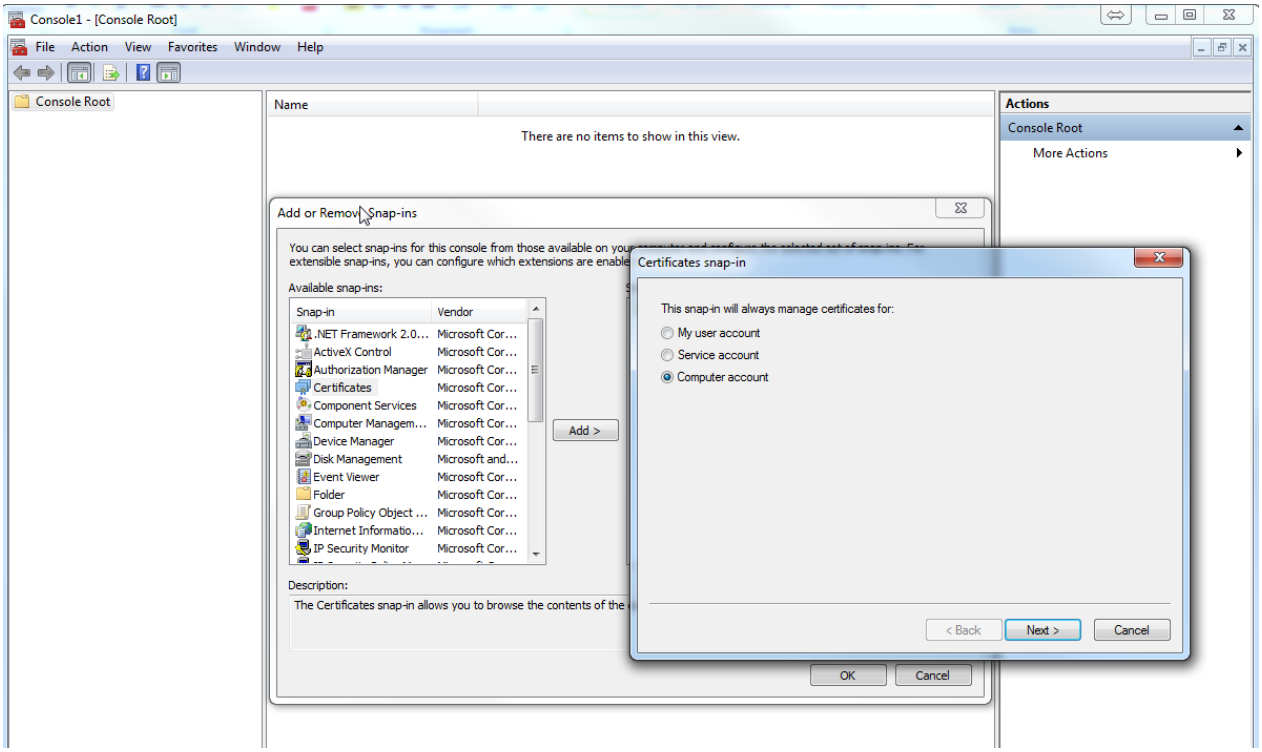
[1] Onder de G3 root CA zijn er voor pasgebonden certificaten andere Intermediate CA’s in gebruik. Zie hiervoor de toelichting op de G3 landingspage.

[2] De weergave ‘Government of Netherlands G3’ betreft de zogenaamde Friendly Name van de ‘Staat der Nederlanden Root CA - G3’ en is de weergave op Microsoft Windows systemen.

[3] De G3 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 ook trager. Vandaar het advies om altijd de volledige CA certificate chain te installeren op de server.

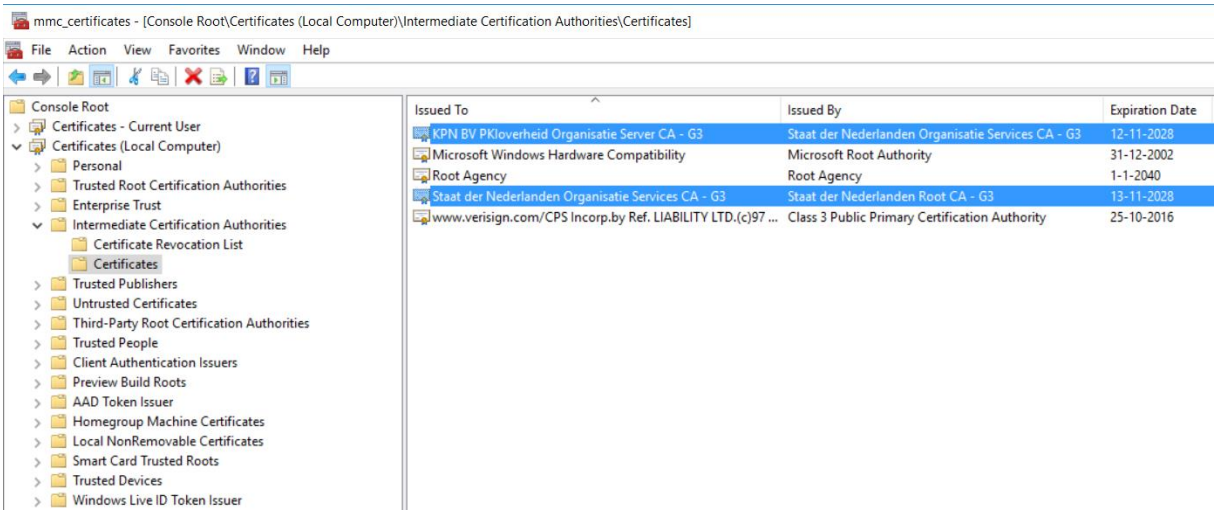
Installatie CA certificaten op een Windows server

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, te weten:

1. KPN BV PKIoverheid Organisatie Server CA - G3
2. Staat der Nederlanden Organisatie Services CA - G3
3. Staat der Nederlanden Root CA - G3

Het bestand ca-bundle-kpn-pkio-g3-server.pem is hier te downloaden en bevat de 3 genoemde CA certificaten in PEM formaat[4].

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 BV PKIoverheid Organisatie Server CA - G3
3. Staat der Nederlanden Organisatie Services CA - G3
4. Staat der Nederlanden Root CA - G3

[4] De linkjes onder ‘Download CA certificaten’ verwijzen naar de CA certificaten in DER format.