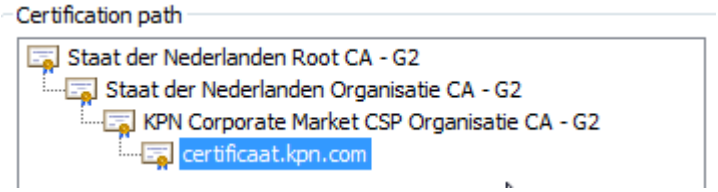
English version

PKIoverheid server (SSL) certificaten

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 “KPN Corporate Market CSP Organisatie CA – G2”.



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.

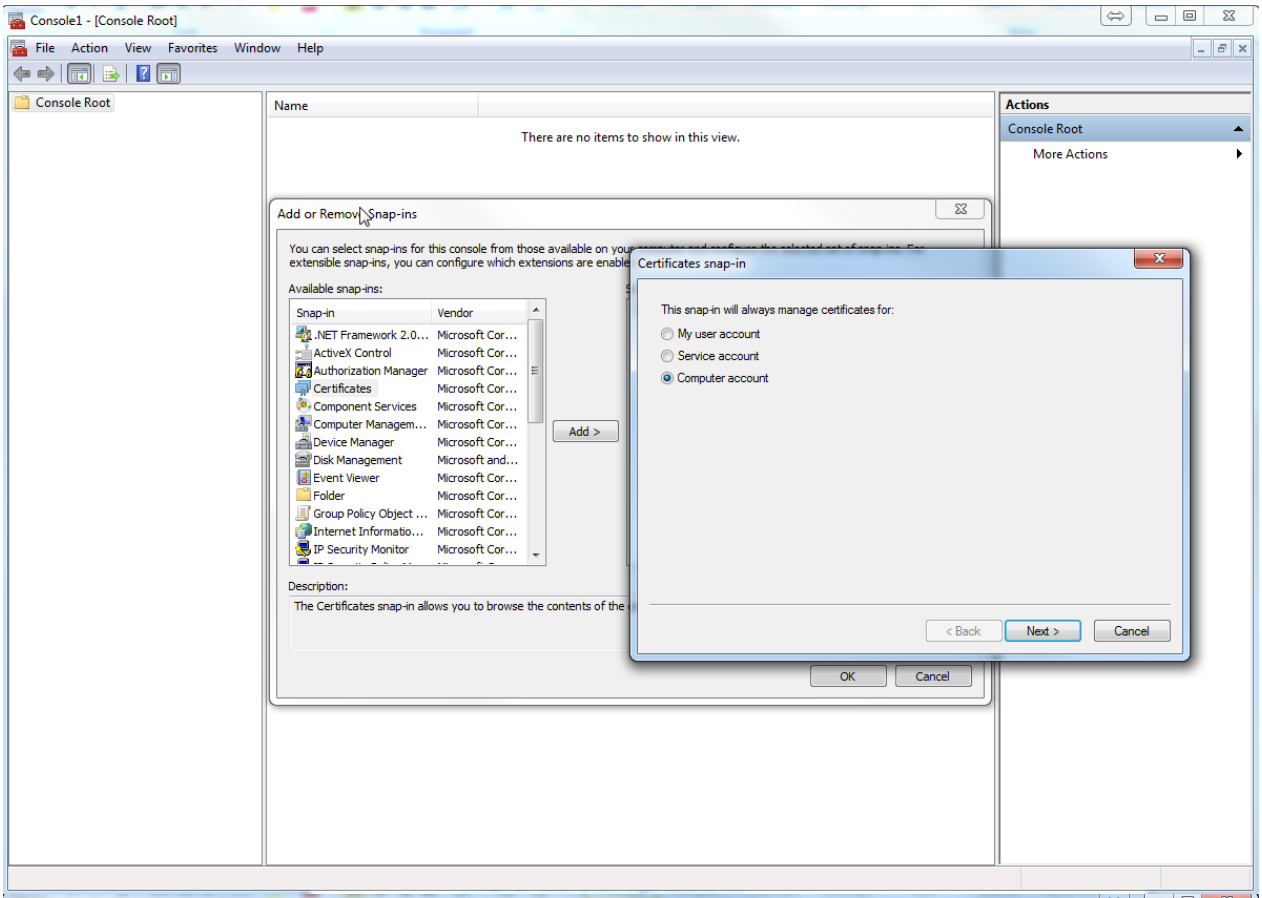
Op de meeste servers en in de client browsers is het "Staat der Nederlanden Root CA - G2" standaard of via update aanwezig in de zogenaamde “Trusted Root Certification Authorities”, de twee Intermediate certificaten zijn meestal niet aanwezig in de client browsers en deze zullen dus door de server naar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

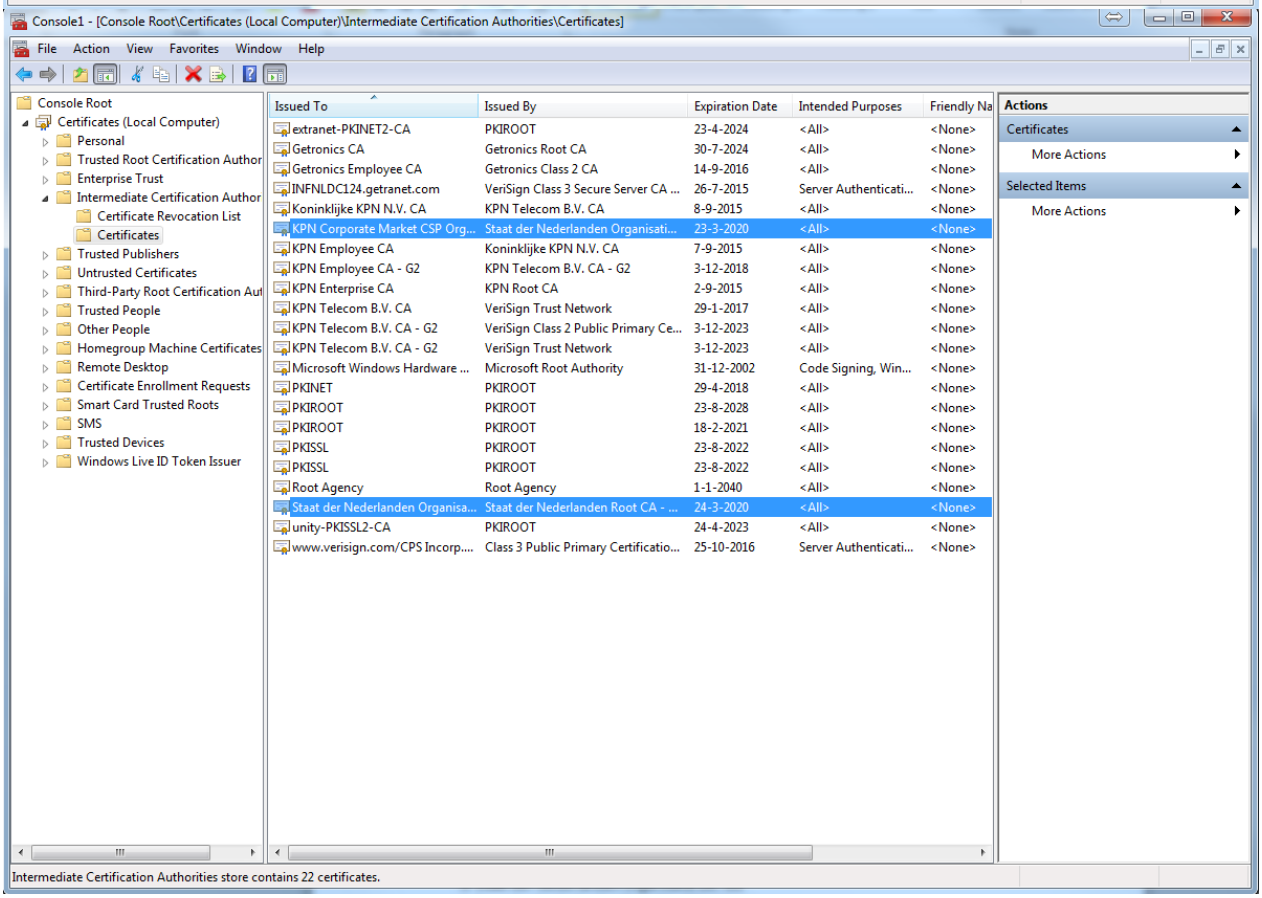
Het Staat der Nederlanden Organisatie CA - G2 certificaat is hier te downloaden.

Het KPN Corporate Market CSP Organisatie CA – G2 certificaat is hier te downloaden

Het Staat der Nederlanden Root CA - G2 certificaat is hier te downloaden

Op een Windows server kan dit via MMC ➔ Add snap-in Certificates





En dan via All Task ➔ import de twee Intermediate certificaten die gedownload zijn

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 Corporate Market CSP Organisatie CA – G2
2. Staat der Nederlanden Organisatie CA - G2
3. Staat der Nederlanden Root CA - G2

Het ca-bundle.pem is hier te downloaden

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. certificaat.kpn.com
2. KPN Corporate Market CSP Organisatie CA – G2
3. Staat der Nederlanden Organisatie CA - G2
4. Staat der Nederlanden Root CA - G2