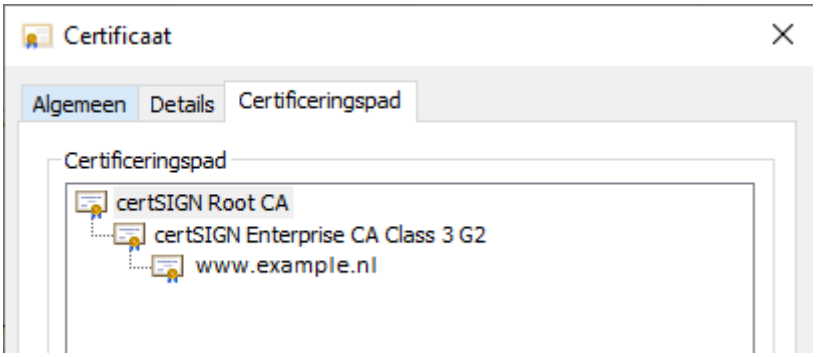
English version

Installatie certSIGN servercertificaat

KPN levert servercertificaten uit onder het Root CA certificaat "certSIGN Root CA" met daaronder één Intermediate CA certificaat, te weten “certSIGN Enterprise CA Class 3 G2”. De volledige CA hiërarchie van een certSIGN servercertificaat ziet er als volgt uit:



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

Op de meeste servers en in de client browsers is het "certSIGN Root CA" certificaat standaard of via update aanwezig in de zogenaamde “Trusted Root Certification Authorities”. Het Intermediate CA certificaat is 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 certSIGN servercertificaat als trusted (geldig en vertrouwd) wordt beschouwd in de browser[1].

Download CA certificaten

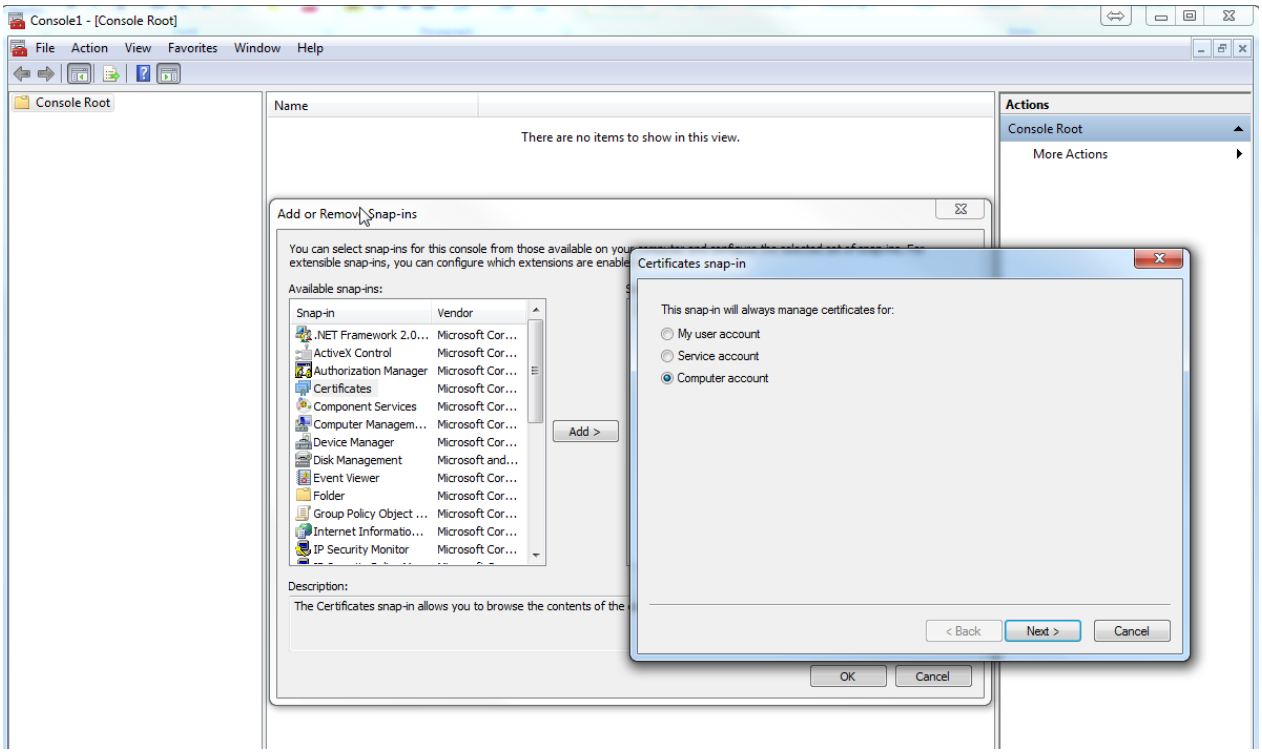
Het certSIGN Root CA certificaat is hier te downloaden. (Als het goed is al aanwezig in Certificate Store).

Het certSIGN Enterprise CA Class 3 G2 certificaat is hier te downloaden.

Installatie CA certificaten op een Windows server

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

[1] De certSIGN 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.



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

Importeer 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. certSIGN Enterprise CA Class 3 G2
2. certSIGN Root CA

Het bestand ca-bundle-certsign-server.pem is hier te downloaden en bevat de 2 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 certSIGN 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. certSIGN Enterprise CA Class 3 G2