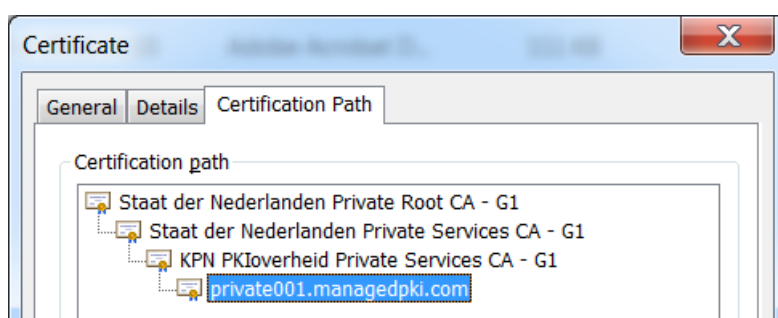




[English version](#)

Installatie KPN PKIoverheid Private servercertificaat G1

KPN geeft PKIoverheid Private servercertificaten uit onder het Root CA certificaat "Staat der Nederlanden Private Root CA - G1" met daaronder twee Intermediate CA certificaten, te weten "Staat der Nederlanden Private Services CA - G1" en de "KPN PKIoverheid Private Services CA - G1". De CA hiërarchie ziet er als volgt uit:



Het is van het grootste belang dat naast het Private SSL servercertificaat, in bovenstaand voorbeeld *private001.managedpki.com*, ook beide Intermediate CA certificaten op de server geïnstalleerd worden.

Standaard zal op geen enkele server of client browser het "Staat der Nederlanden Private Root CA - G1" certificaat aanwezig zijn. Dit zal dus handmatig geïnstalleerd moeten worden zoals beschreven is in dit document. Hetzelfde geldt voor de twee Intermediate CA certificaten. Hoewel deze Intermediate CA certificaten naar een client gepushed kunnen worden als onderdeel van de zogenaamde TLS handshake is het advies om deze altijd te installeren. Dit garandeert dat de volledige CA certificate chain aanwezig is waarmee het Private servercertificaat als trusted (geldig en vertrouwd) wordt beschouwd.

Download CA certificaten

Het [Staat der Nederlanden Private Root CA - G1](#) certificaat is hier te downloaden.

Het [Staat der Nederlanden Private Services CA - G1](#) certificaat is hier te downloaden.

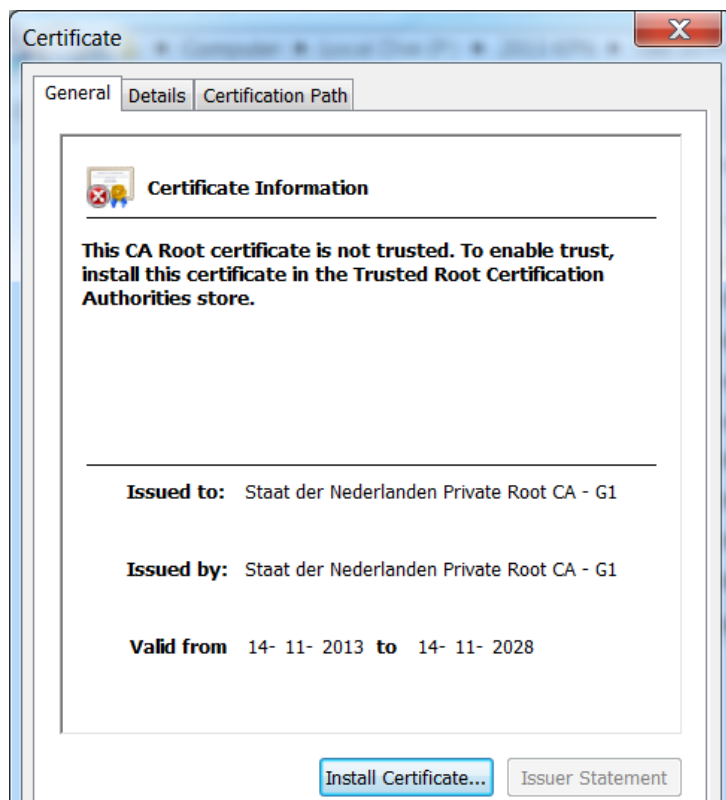
Het [KPN PKIoverheid Private Services CA - G1](#) certificaat is hier te downloaden.

Installatie Private Root CA certificaat op een Windows server

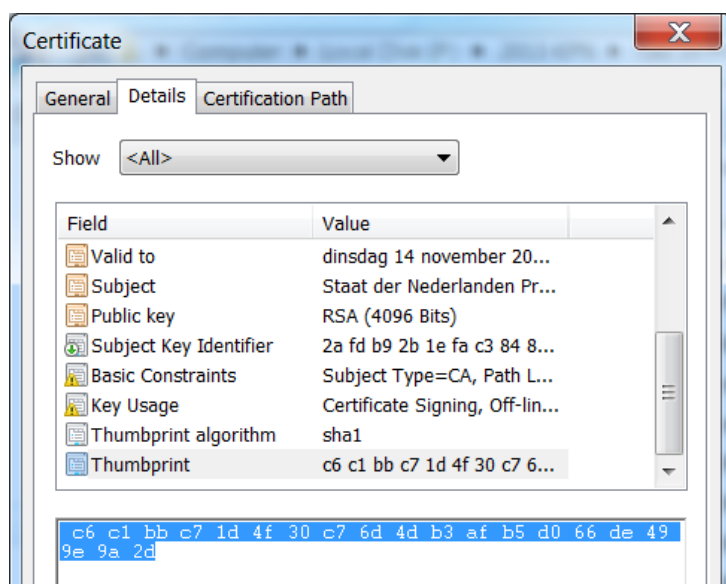
Omdat het 'Staat der Nederlanden Private Root CA - G1' certificaat niet standaard in de Operating Systemen is opgenomen is een vereiste stap om dit handmatig te doen.

BELANGRIJK: Verifieer eerst het gedownloadde Private Root CA certificaat

- Open het root certificaat door op het .cer bestand te (dubbel)klikken op een Windows systeem. Het zal standaard niet vertrouwd zijn in Windows.



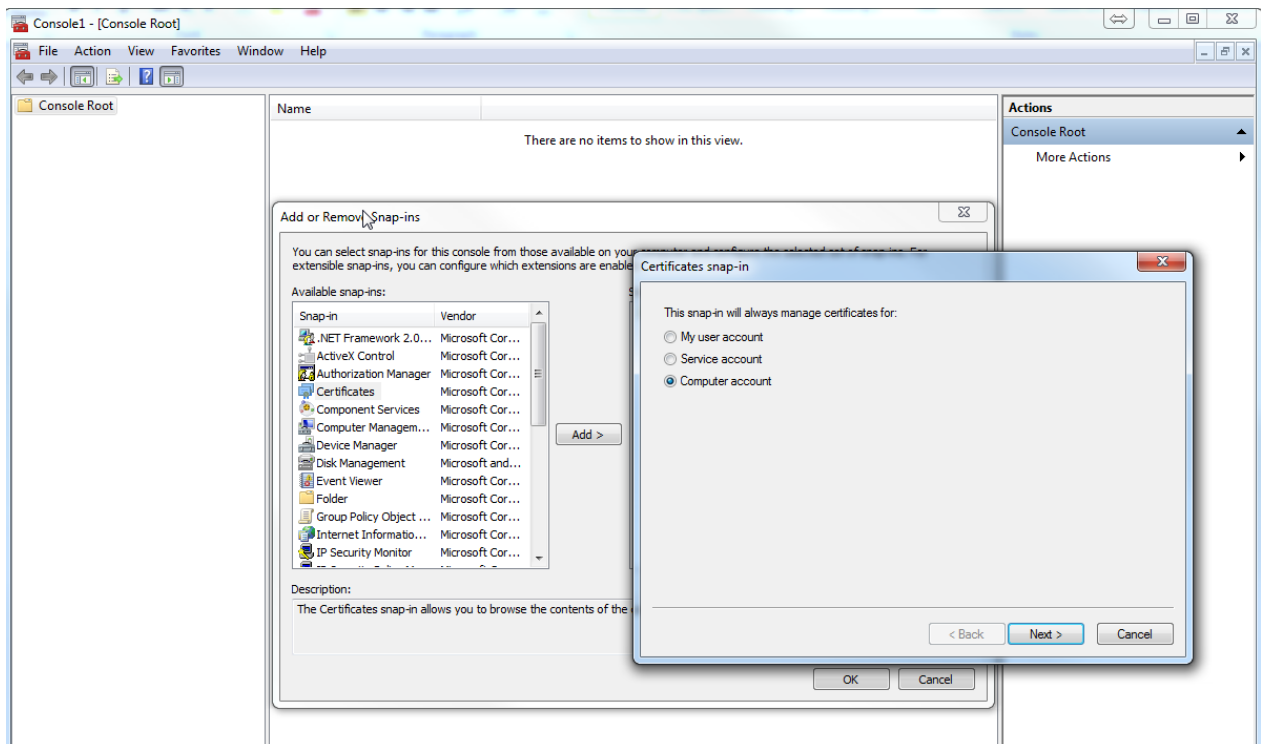
- Klik op tabblad Details en controleer de Fingerprint van het root CA certificaat. Dit moet zijn: C6 C1 BB C7 1D 4F 30 C7 6D 4D B3 AF B5 D0 66 DE 49 9E 9A 2D



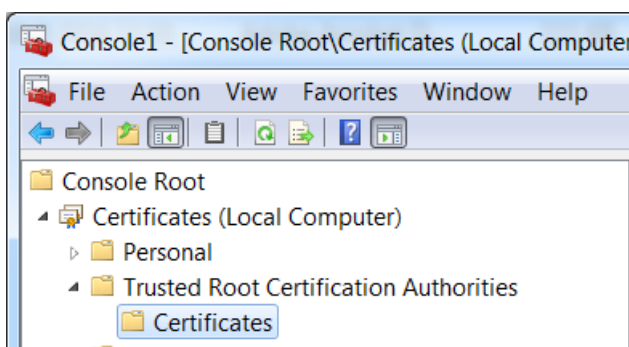
De echtheidskennmerken van het 'Staat der Nederlanden Private Root CA - G1' certificaat zijn officieel gepubliceerd in de Staatscourant Nr. 6676, d.d. 12 maart 2015.

Installatie Root CA certificaat met Microsoft Management Console (MMC)

- Open MMC
- Add snap-in
- Certificates
- Selecteer 'Computer account'

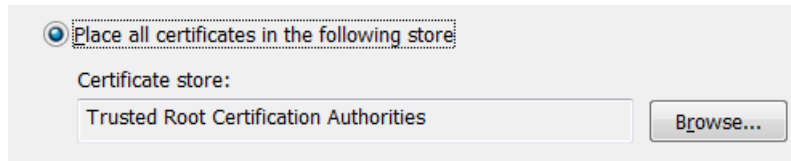


- Next. Selecteer 'Local Computer'
- Finish
- Selecteer de juiste Certificate store voor plaatsing van het Root CA certificaat

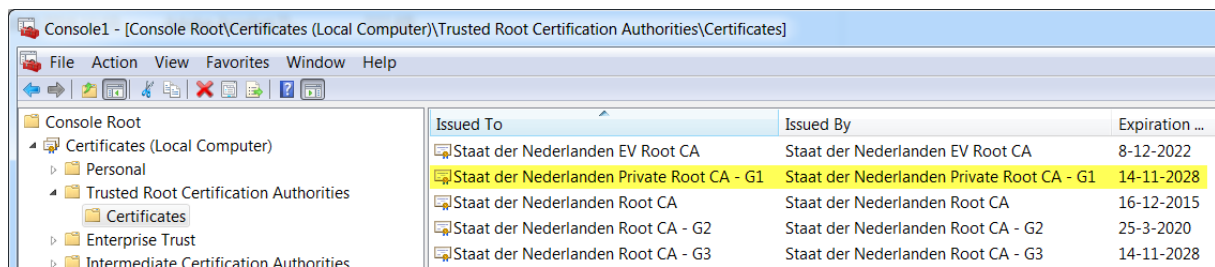


Instaleer vervolgens via Action → All Tasks → import het Root CA certificaat dat gedownload is.

De Certificate Import Wizard open. Als het goed is, is de radio button 'Place all certificates in the following store' al correct gevuld met 'Trusted Root Certification Authorities'.



Afronding van de import Wizard heeft het volgende resultaat:



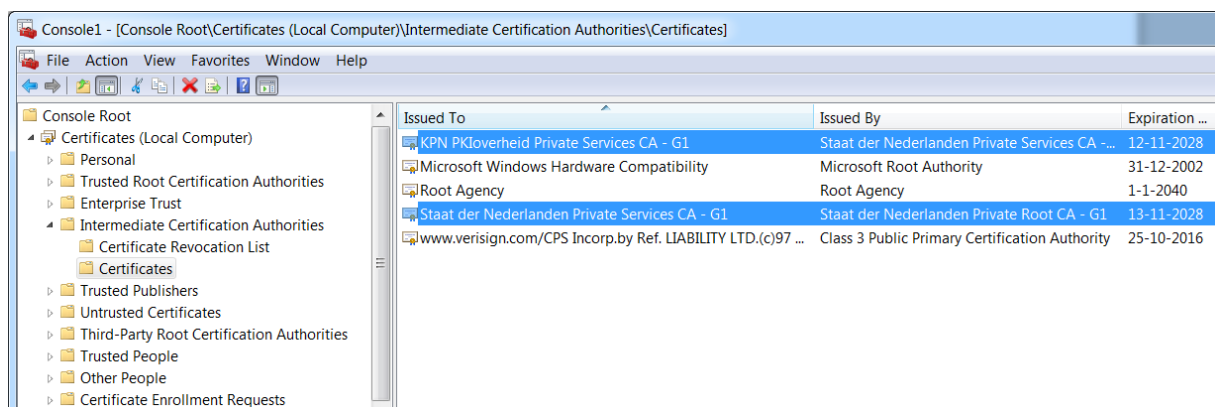
Issued To	Issued By	Expiration ...
Staat der Nederlanden EV Root CA	Staat der Nederlanden EV Root CA	8-12-2022
Staat der Nederlanden Private Root CA - G1	Staat der Nederlanden Private Root CA - G1	14-11-2028
Staat der Nederlanden Root CA	Staat der Nederlanden Root CA	16-12-2015
Staat der Nederlanden Root CA - G2	Staat der Nederlanden Root CA - G2	25-3-2020
Staat der Nederlanden Root CA - G3	Staat der Nederlanden Root CA - G3	14-11-2028

Installatie Intermediate CA certificaten op een Windows server

Ook dit kan via het MMC.

- Selecteer de juiste Certificate store (Local Computer, Intermediate Certification Authorities) voor plaatsing van de Intermediate CA certificaten.

Installeer vervolgens via **Action** → **All Tasks** → **import** de twee Intermediate certificaten die gedownload zijn. Dit heeft het volgende resultaat:



Issued To	Issued By	Expiration ...
KPN PKIoverheid Private Services CA - G1	Staat der Nederlanden Private Services CA - ...	12-11-2028
Microsoft Windows Hardware Compatibility	Microsoft Root Authority	31-12-2002
Root Agency	Root Agency	1-1-2040
Staat der Nederlanden Private Services CA - G1	Staat der Nederlanden Private Root CA - G1	13-11-2028
www.verisign.com/CPS Incorporation by Ref. LIABILITY LTD.(c)97 ...	Class 3 Public Primary Certification Authority	25-10-2016



Apache Webserver

In een Apache omgeving is het advies om in de file (default ca-bundle.xxx) -waarnaar 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 Private Services CA - G1
2. Staat der Nederlanden Private Services CA - G1
3. Staat der Nederlanden Private Root CA - G1

Het bestand [ca-bundle-kpn-pki-private-g1.pem](#) is hier te downloaden en bevat de 3 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 Private servercertificaat geïnstalleerd is, dan moet men in deze key store ook de certificate chain en het servercertificaat van de doel server opnemen:

1. (in dit voorbeeld) private001.managedpki.com
2. KPN PKIoverheid Private Services CA - G1
3. Staat der Nederlanden Private Services CA - G1
4. Staat der Nederlanden Private Root CA - G1