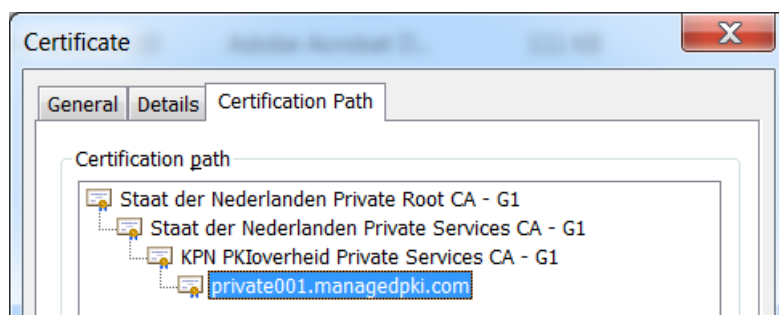


Installing KPN PKIoverheid Private server certificates G1

KPN issues PKIoverheid Private server certificates under the Root CA certificate "Staat der Nederlanden Private Root CA - G1" with two Intermediate certificates, named "Staat der Nederlanden Private Services CA - G1" and "KPN PKIoverheid Private Services CA - G1".

The CA hierarchy of a KPN PKIO Private server certificate is as follows:



Besides the Private server certificate (private001.managedpki.com in the example above) you need to install the two intermediate CA certificates in the servers certificate store.

The "Staat der Nederlanden Private Root CA - G1" certificate will not be installed in any operating system or browser by the vendor. It has to be installed manually as explained in this document. This also applies to the two Intermediate CA certificates. Although intermediate CA certificates can be pushed to the client during the so called TLS handshake KPN advises to install them on any system using the Private server certificates. This will guarantee the CA certificate chain is complete so the Private server certificate can be validated by the client and will be trusted.

Download CA certificates

The [Staat der Nederlanden Private Root CA - G1](#) certificate can be downloaded here.

The [Staat der Nederlanden Private Services CA - G1](#) certificate can be downloaded here.

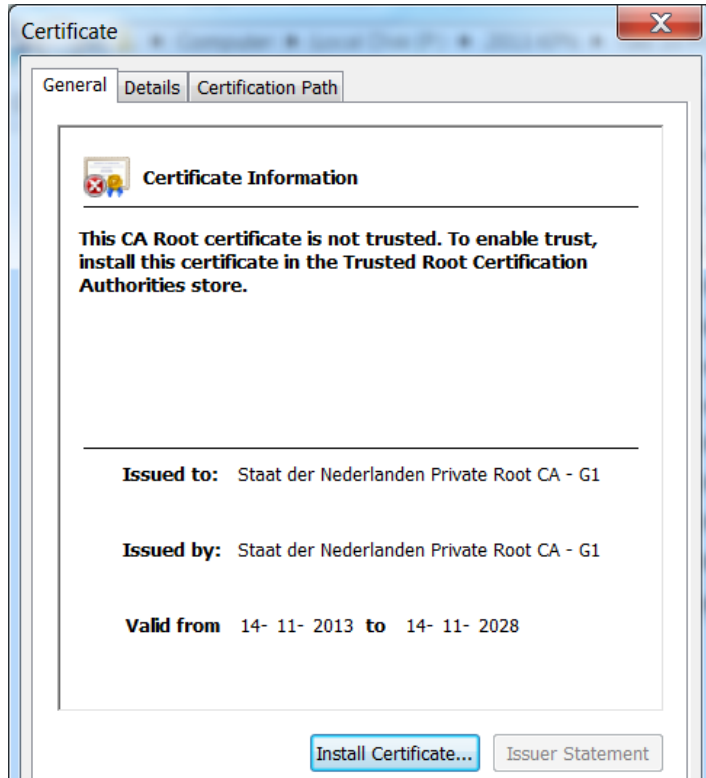
The [KPN PKIoverheid Private Services CA - G1](#) certificate can be downloaded here.

Installing the Private Root CA certificate on a Windows server

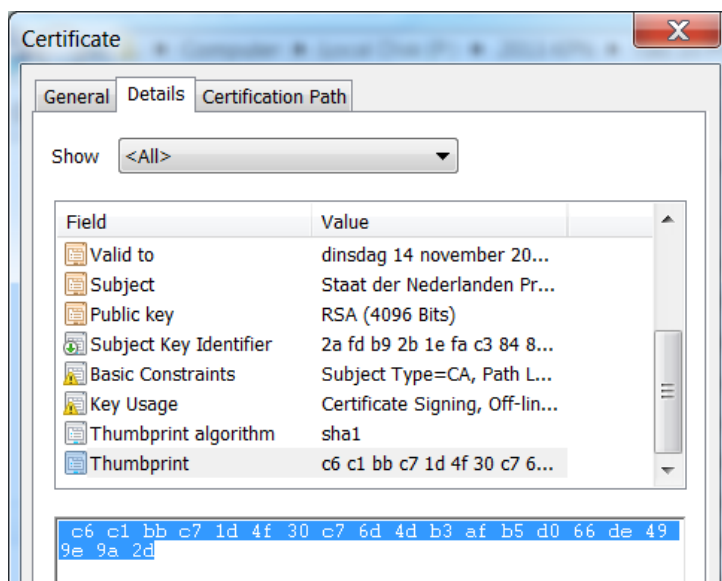
The 'Staat der Nederlanden Private Root CA - G1' certificate will not be installed in any operating system or browser by the vendor. This requires a manual installation of the Root CA certificate.

IMPORTANT: Verify the downloaded Private Root CA certificate

- Open the root certificate by (double)clicking the .cer file on a Windows system. It will not be trusted as shown in the following picture.



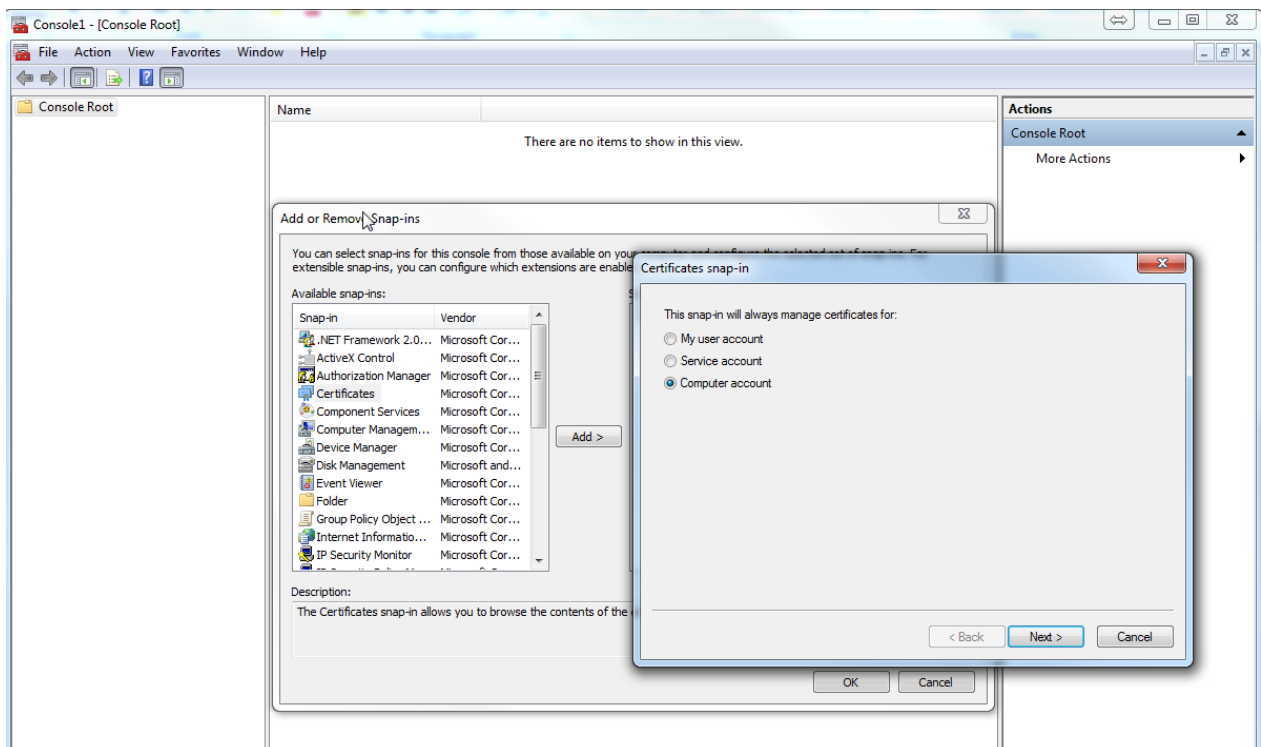
- Click on tab Details en check the Fingerprint of the root CA certificate. This must be:
C6 C1 BB C7 1D 4F 30 C7 6D 4D B3 AF B5 D0 66 DE 49 9E 9A 2D



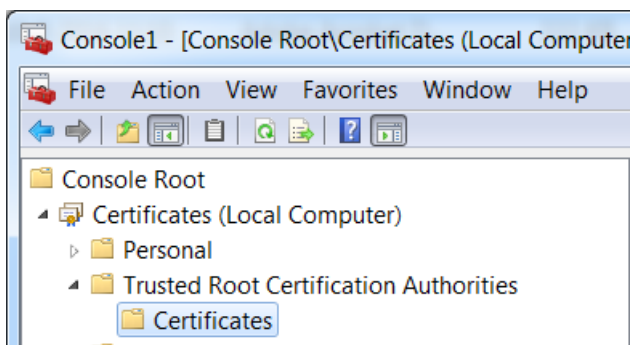
The security features of the 'Staat der Nederlanden Private Root CA - G1' certificate are officially published in the Staatscourant Nr. 6676, d.d. 12 maart 2015.

Installing the Root CA certificaat using Microsoft Management Console (MMC)

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



- Next. Select 'Local Computer'
- Finish
- Select the Certificate store intended for installation of the Root CA certificate

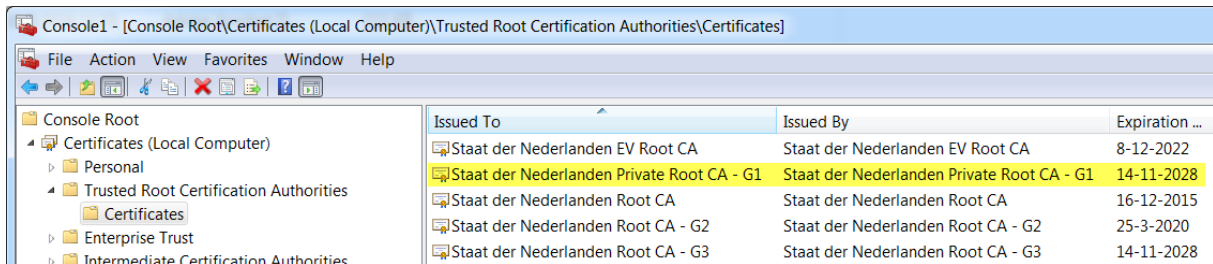


Select Action → All Tasks → import to install the downloaded Root CA certificate.

The Certificate Import Wizard will start. The radio button 'Place all certificates in the following store' should already be prefilled with 'Trusted Root Certification Authorities'.



Completing the import Wizard will result in:

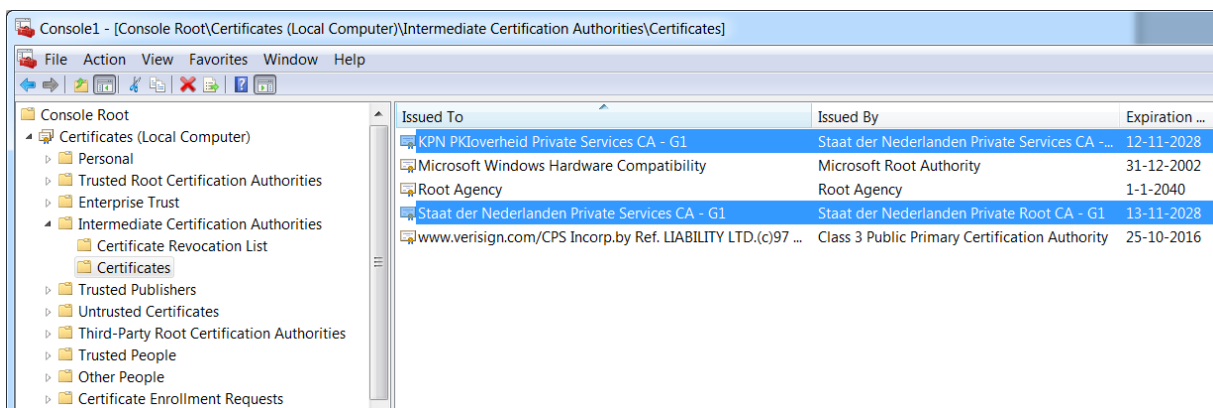


Issued To	Issued By	Expiration ...
Staat der Nederlanden EV Root CA	Staat der Nederlanden EV Root CA	8-12-2022
Staat der Nederlanden Private Root CA - G1	Staat der Nederlanden Private Root CA - G1	14-11-2028
Staat der Nederlanden Root CA	Staat der Nederlanden Root CA	16-12-2015
Staat der Nederlanden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

Installing Intermediate CA certificates on a Windows server

This can also be accomplished using the MMC.

- Select the Certificate store (Local Computer, Intermediate Certification Authorities) intended for installation of the Intermediate CA certificates.
- Select Action → All Tasks → import to import the two downloaded Intermediate certificates. This results in:



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 Incomp.by Ref. LIABILITY LTD.(c)97 ...	Class 3 Public Primary Certification Authority	25-10-2016



Apache Webserver

On an Apache web server we advise to add the three CA chain certificates from the certificate to the file (default ca-bundle.xxx) to which is referred in the statement “SSLCertificateChainFile” in the ssl.conf:

1. KPN PKIoverheid Private Services CA - G1
2. Staat der Nederlanden Private Services CA - G1
3. Staat der Nederlanden Private Root CA - G1

The file [ca-bundle-kpn-pki-private-g1.pem](#) can be downloaded here and contains the 3 CA certificates in PEM format.

Java keystore

If you use a Client certificate, stored in a java keystore (jks) on another server, to make a connection to the server where you installed the PKIOverheid Private server certificate, you need to add the certificate chain and server certificate from the target server in that java keystore:

1. (in this example) 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