

# **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 <u>Staat der Nederlanden Private Services CA - G1</u> certificate can be downloaded here.

The <u>KPN PKIoverheid Private Services CA - G1</u> 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 be trusted as shown in the following picture.

Certificate General Details	Certification Path
This CA Ro install this Authoritie	tificate Information ot certificate is not trusted. To enable trust, certificate in the Trusted Root Certification s store.
Issue	d to: Staat der Nederlanden Private Root CA - G1
Issue	d by: Staat der Nederlanden Private Root CA - G1
Valid	from 14- 11- 2013 to 14- 11- 2028
	Install Certificate Issuer Statement

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

General Details Certification	1 Path	
Show <all></all>	-	
Field	Value	
📴 Valid to	dinsdag 14 november 20	
🔄 Subject	Staat der Nederlanden Pr	
📴 Public key	RSA (4096 Bits)	
🗊 Subject Key Identifier	2a fd b9 2b 1e fa c3 84 8	
🜆 Basic Constraints	Subject Type=CA, Path L	=
<u>ଲ</u> Key Usage	Certificate Signing, Off-lin	-
🔄 Thumbprint algorithm	sha1	
🛅 Thumbprint	c6 c1 bb c7 1d 4f 30 c7 6	*
L		



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'

🚰 Console1 - [Console Root]						
🚡 File Action View Favorites Window Help						
Console Root	Name		Actions			
	There are no items to show in this view		Console Root			
		More Actions				
	- X					
	Vo					
	extensible snap-ins, you can configure which extensions are enable Certificates snap-in					
	Available snap-ins:					
	Snap-in Vendor This snap-in will a	Iways manage certificates for:				
	ActiveX Control Microsoft Cor Service acco	unt				
	Authorization Manager Microsoft Cor E	ount				
	Certificates Microsoft Cor					
	Computer Managem Microsoft Cor					
	Device Manager Microsoft Cor  Disk Management Microsoft and					
	Event Viewer Microsoft Cor					
	Folder Microsoft Cor Group Policy Object Microsoft Cor					
	PInternet Informatio Microsoft Cor					
	P Security Monitor Microsoft Cor					
	Description:					
	The Certificates snap-in allows you to browse the contents of the					
		< Back	Next > Cancel			
		OK Cancel				
I						

- 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'.

Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities	B <u>r</u> owse

Completing the import Wizard will result in:

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]								
Image: Second Secon								
Console Root	Issued To	Issued By	Expiration					
A 🐺 Certificates (Local Computer)	🖙 Staat der Nederlanden EV Root CA	Staat der Nederlanden EV Root CA	8-12-2022					
Personal	🖙 Staat der Nederlanden Private Root CA - G1	Staat der Nederlanden Private Root CA - G1	14-11-2028					
Irusted Koot Certification Authorities	🖙 Staat der Nederlanden Root CA	Staat der Nederlanden Root CA	16-12-2015					
Enterprise Trust	🖙 Staat der Nederlanden Root CA - G2	Staat der Nederlanden Root CA - G2	25-3-2020					
Intermediate Certification Authorities	🛱 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:





# **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 <u>ca-bundle-kpn-pkio-private-g1.pem</u> 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