



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:

Certificate	
General Details Certification Path	
Certification gath	
Staat der Nederlanden Private Root CA - G1	
KPN PKIoverheid Private Services CA - G1	
private001.managedpki.com	

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 <u>Staat der Nederlanden Private Root CA - G1</u> 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 gedownloade 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.

Cert	tificate	
G	eneral Details Cer	tification Path
	This CA Root ce install this certi Authorities stor	te Information rtificate is not trusted. To enable trust, ficate in the Trusted Root Certification re.
	Issued to:	Staat der Nederlanden Private Root CA - G1
	Issued by:	Staat der Nederlanden Private Root CA - G1
	Valid from	14- 11- 2013 to 14- 11- 2028
		Install Certificate Issuer Statement

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

eneral Details Certification	n 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>ल</u> Key Usage	Certificate Signing, Off-lin	=
🔄 Thumbprint algorithm	sha1	
🛅 Thumbprint	c6 c1 bb c7 1d 4f 30 c7 6	-

Mini install KPN PKIoverheid PRIVATE G1 servercertificaat (versie 1.0, februari 2016)



De echtheidskenmerken 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'

Console1 - [Console Root]					
🚟 File Action View Favorites Wind	dow Help				_ & ×
Console Root	Name				Actions
		There are no items to	a show in this view.		Console Root 🔺
	There are no items to show in this view.			More Actions	
	Add or Remov Snap-ins			22	
		In G ener Manne av stabile an vers			
	extensible snap-ins, you can configur	e which extensions are enable	Certificates snap-in		
	Available snap-ins:				
	Snap-in Vendor	<u> </u>	This snap-in will always manage certificates for:		
	ActiveX Control Microso	ft Cor ft Cor	My user account Sequine account		
	Authorization Manager Microso	ft Cor ≡	Computer account		
	Certificates Microso	ft Cor ft Cor			
	Computer Managem Microso	ft Cor Add >			
	Device Manager Microso Disk Management Microso	ft Cor			
	Event Viewer Microso	ft Cor			
	Folder Microso	ft Cor			
	Internet Informatio Microso	ft Cor			
	IP Security Monitor Microso	ft Cor 👻			
	Description:				
	The Certificates snap-in allows you t	o browse the contents of the			
				< Back	Next > Cancel
		L. L.			
			OK C	ancel	
)	

- 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 opent. Als het goed is, is de radio button 'Place all certificates in the following store' al correct gevuld met 'Trusted Root Certification Authorities'.

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

Afronding van de import Wizard heeft het volgende resultaat:



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:





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