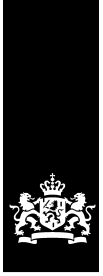


CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Het aanmaken en installeren van een Servercertificaat onder IIS7 / IIS8 en IIS10

Microsoft Internet Information Services 7 / 8 en 10

Versie 4.4

Datum 23 Juli 2019
Status Definitief

Inhoud

Versiehistorie

Versie	Datum	Status	Toevoegingen en wijzigingen
1.1	30 mrt 09	definitief	Aanpassingen: Toevoegen G2 hiërarchie
1.2	8 apr 09	definitief	Aanpassingen: - Toevoeging testen SBV-Z testtool - Extra toelichting OpenSSL - Voorbeeldnamen PKCS#10 request hernoemd
1.3	10 apr 09	definitief	Aanpassingen: - Hoofdstuk X hernoemd (toevoeging UZI-pas) - Hoofdstuk 3 aangevuld met FQDN naam - Bjilage toegevoegd: Toelichting systeemnaam
1.4	23 apr 09	definitief	Aanpassingen: - Hoofdstuk 3 aangevuld met reden gebruik IIS - Hoofdstuk 6: Generen PFX - Aanvulling op Bijlage: Toelichting systeemnaam
1.5	12 mei 09	definitief	Aanpassingen: Hoofdstuk 13: Troubleshoot Pending Request kan niet worden gemaakt
2.0	25 mei 09	concept	Afzonderlijke handleidingen samengevoegd tot 1 document (Apache – IIS + UZI)
2.0	21 jul 09	definitief	
3.0	6 okt 09	definitief	Aanpassing: Aparte versie voor II7 (Windows 2008 server) geschreven.
3.1	16 nov 10	definitief	Document aangepast wegens invoering SHA-2
3.2	24 dec 10	review	Feedback verwerkt
3.3	09 aug 12	definitief	Hoofdstuknummering gewijzigd
4.0	1 sept 15	concept	Aanpassingen: bijgewerkt voor IIS8 (Windows 2012 server) Verlopen CA hiërarchieën verwijderd Links naar CA bestanden bijgewerkt Aanvulling op Bijlage: Toelichting systeemnaam
4.1	16 juni 16	definitief	Links bijgewerkt
4.2	28 sept 18	Concept	Aanpassingen: bijgewerkt voor IIS10 (Windows 2016 server) Verlopen CA hiërarchieën verwijderd Links naar CA bestanden bijgewerkt Links naar externe websites bijgewerkt
4.3	06 nov 18	Definitief	Screenhots aangepast
4.4	23 juli 2019	Definitief	Inleiding aangepast

1 Inleiding

1.1 Inleiding

Dit document beschrijft de basisstappen voor het aanmaken en installeren van een servercertificaat voor het beveiligen van de communicatie tussen een client en een Microsoft Internet Information Server (IIS 7, IIS 8 of IIS 10). Wanneer er in dit document wordt gesproken over een client, dan bedoelen wij een willekeurig werkstation. Wanneer er in dit document wordt gesproken over een webserver dan wordt de server bedoeld waarop de internetpagina draait en waarvan de communicatie versleutelt moet worden. Verderop in het document wordt uitgelegd hoe u de gebruiker kan laten identificeren door middel van het tonen van een clientcertificaat, echter is dit geen vereiste.

Neem voor het aanmaken van het PKCS#10 bestand eerst contact op met uw softwareleverancier.

1.2 Disclaimer

Het aanmaken van een PKCS#10[1] bestand kan op vele manieren. Bekijk hiervoor de documentatie van de leverancier van uw server. Dit document kan als voorbeeld worden gebruikt voor het aanmaken van een PKCS#10 bestand. En als voorbeeld voor het installeren van het servercertificaat dat u van het UZI-register heeft ontvangen. Aan de inhoud van dit document kunnen geen rechten worden ontleend.

1 In dit document is 'PKCS#10 bestand' als naam gehanteerd voor het bestand waarin een aanvrager de publieke sleutel ter certificering aanbiedt aan het UZI-register. Deze naam is gebaseerd op de technische Public Key Cryptography Standards. Zie http://en.wikipedia.org/wiki/PKCS. Alternatieve naamgeving die veel voorkomt is Certificate Signing Request.

2 Stappenplan servercertificaat

Dit stappenplan beschrijft de stappen van het maken, installeren en configureren van een servercertificaat binnen de IIS webserver onder een Windows Operating System.

Achter elke stap staat de naam van het document waarin deze stap uitgebreid beschreven staat.

Deze handleiding kunt u ook gebruiken voor het vernieuwen/vervangen van al bestaande servercertificaten. Bijvoorbeeld als het bestaande servercertificaat verlopen is.

Stap	**Beschrijving**	**Document**
1	Aanmaken van een PKCS#10 bestand	*Hoofdstuk 3*
2	Aanvragen servercertificaat	*Zie stappen op:* https://www.uziregister.nl/servercertificaat/servercertificaat-aanvragen
3	Installeren van het servercertificaat	*Hoofdstuk 4*
4	Beveiligen servercertificaat	*Zie pagina 'Veilig gebruik van uw servercertificaat' op* https://www.uziregister.nl/servercertificaat/veilig-gebruik-servercertificaat
5	Exporteren & installeren PFX	*Hoofdstuk 6 + 7*

*Stap 5 is van toepassing als het servercertificaat op meerdere servers geïnstalleerd moet worden of als er een back-up/restore gewenst is.

3 Aanmaken van het Certificate Signing Request

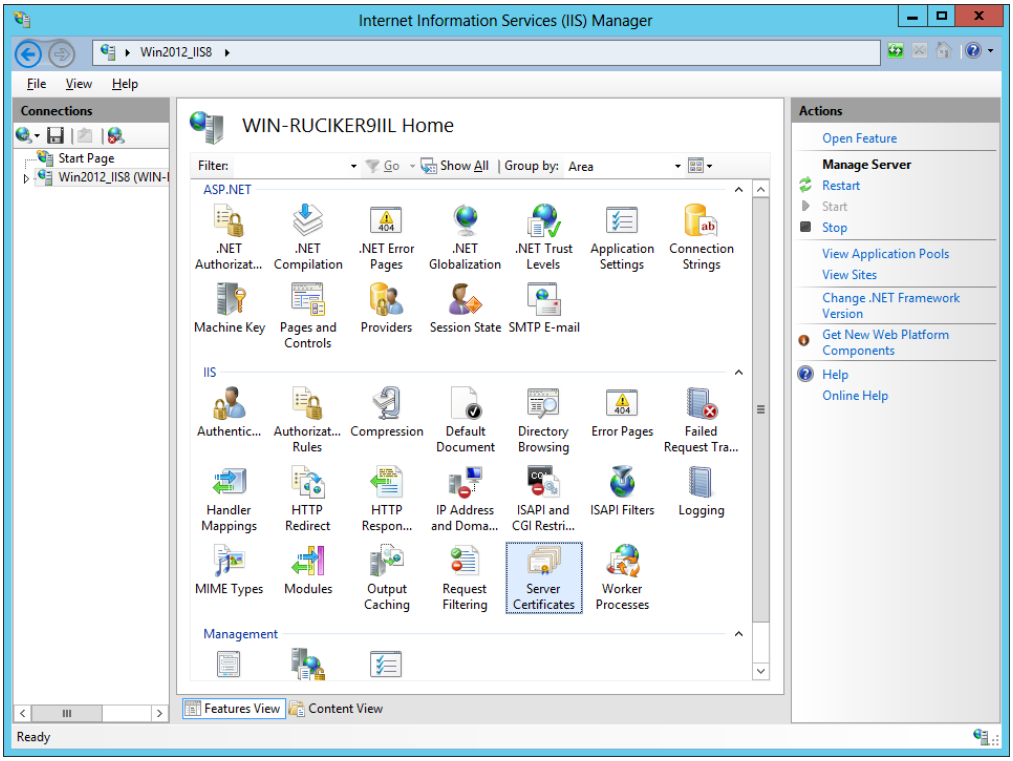
3.1 Wat heeft u nodig

Voor het aanmaken van een zogeheten Certificate Signing Request (PKCS#10 bestand) heeft u een werkende IIS webserver nodig.

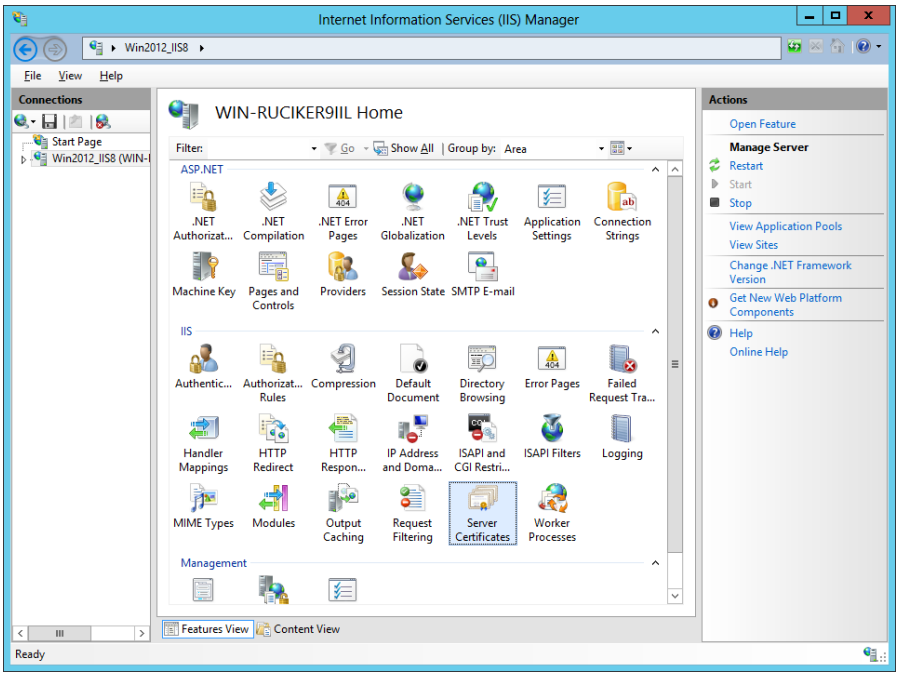
LET OP! IIS wordt gebruikt puur voor het generen van het sleutelpaar en het later koppelen van het door het UZI-register ondertekende publieke deel. Uiteindelijk wordt het servercertificaat in de Certificate Store opgeslagen.

3.2 Aanmaken van het Certificate Signing Request

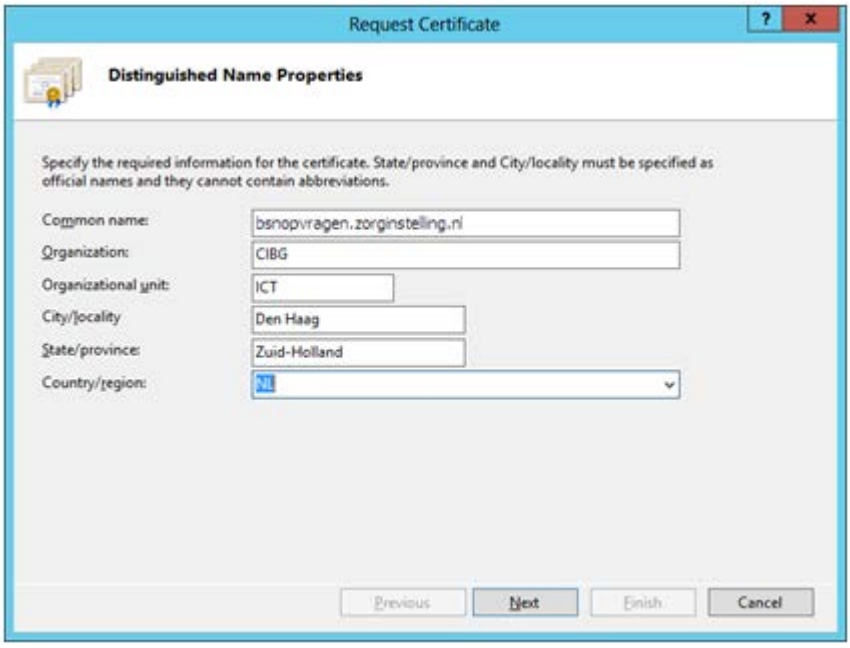
Open “Internet Information Services (IIS) Manager”, klik op de “Homepage” van de server en klik vervolgens op “Server Certificates”.



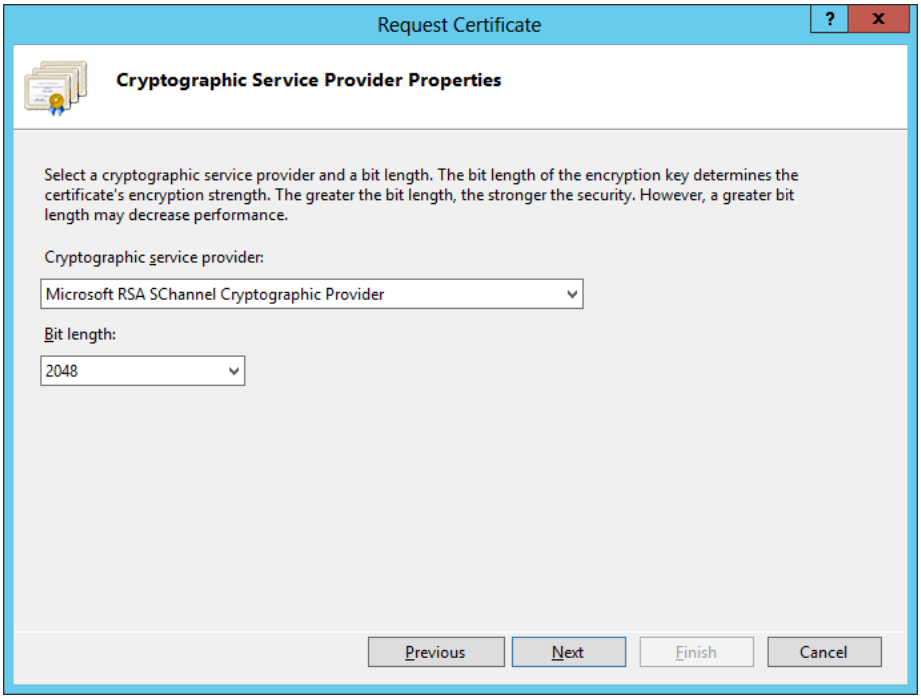
Klik onder “Actions” op: “Create Certificate Request”



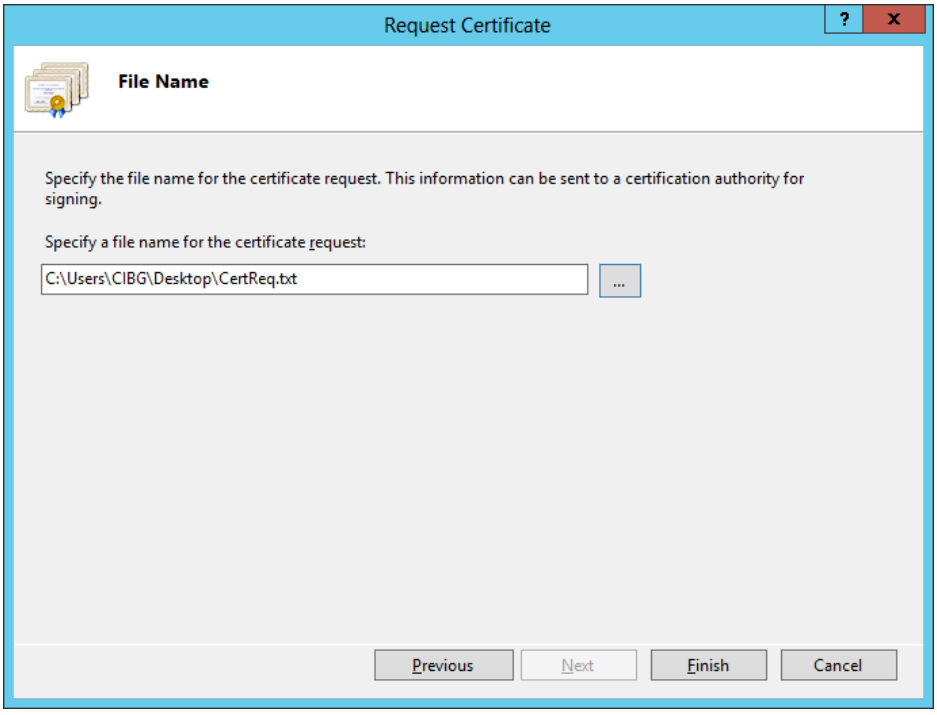
Voer in het eerste scherm de velden in. Bij “Common Name” moet dezelfde naam opgegeven worden als de systeemnaam (FQDN) op het aanvraagformulier. Klik daarna op “Next”.



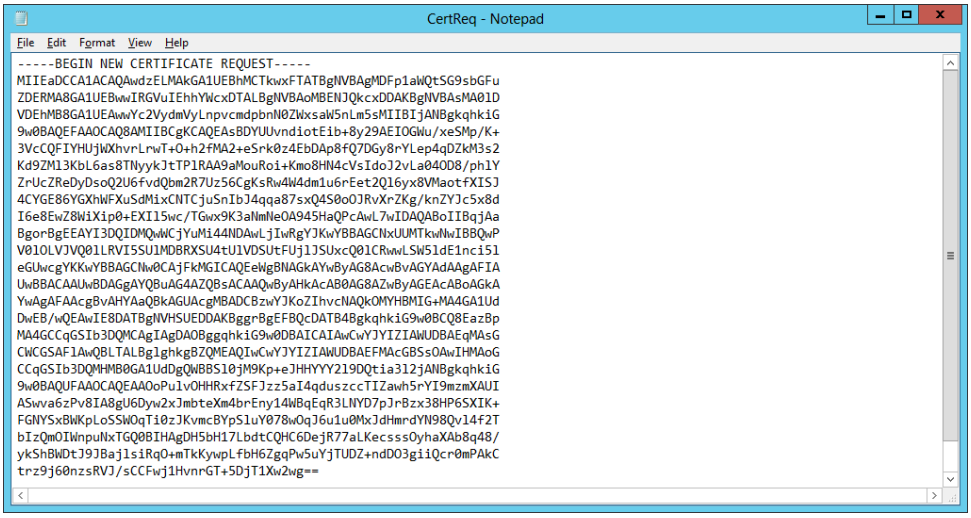
De bitlengte moet 2048 bit zijn voor het aanvragen van een UZI-servercertificaat. Wijzig dit in het volgende scherm zo nodig naar 2048 bit en klik daarna op “Next”.



Voer in onderstaand scherm de bestandsnaam op waar het Certificate Request opgeslagen moet gaan worden en klik op “Finish”.



Op het bureaublad komt nu het Certificate Request te staan. Dit bestand moet– samen met het aanvraagformulier – naar het UZI-register verzonden worden.



3.3 Het aanvragen van een servercertificaat

Ga verder met stap 3 van de aanvraagprocedure voor het aanvragen van het servercertificaat. De stappen staan op https://www.uziregister.nl/servercertificaat/servercertificaat-aanvragen

Wanneer u uw servercertificaat in uw bezit heeft kunt u verder met hoofdstuk 4.

4 Het installeren van een servercertificaat

4.1 Wat heeft u nodig

Voor de installatie van het servercertificaat heeft u het volgende nodig:

- Een geldig en getekend X.509 certificaat in DER-Encoding;
- De certificaten van de complete ‘certificate chain’ tot en met het Root CA certificaat.

Na de aanvraag voor een servercertificaat stuurt het UZI-register deze naar het e-mailadres van de bij het UZI-register geregistreerde aanvrager.

(UZI-register)

De Root CA keten bestaat uit de volgende CA’s en kan verschillen per generatie servercertificaat.

Voor de servercertificaten CA – G1 generatie:

-> Staat der Nederlanden Private Root CA - G1
->Staat der Nederlanden Private Services CA - G1
->UZI-register Private Server CA G1

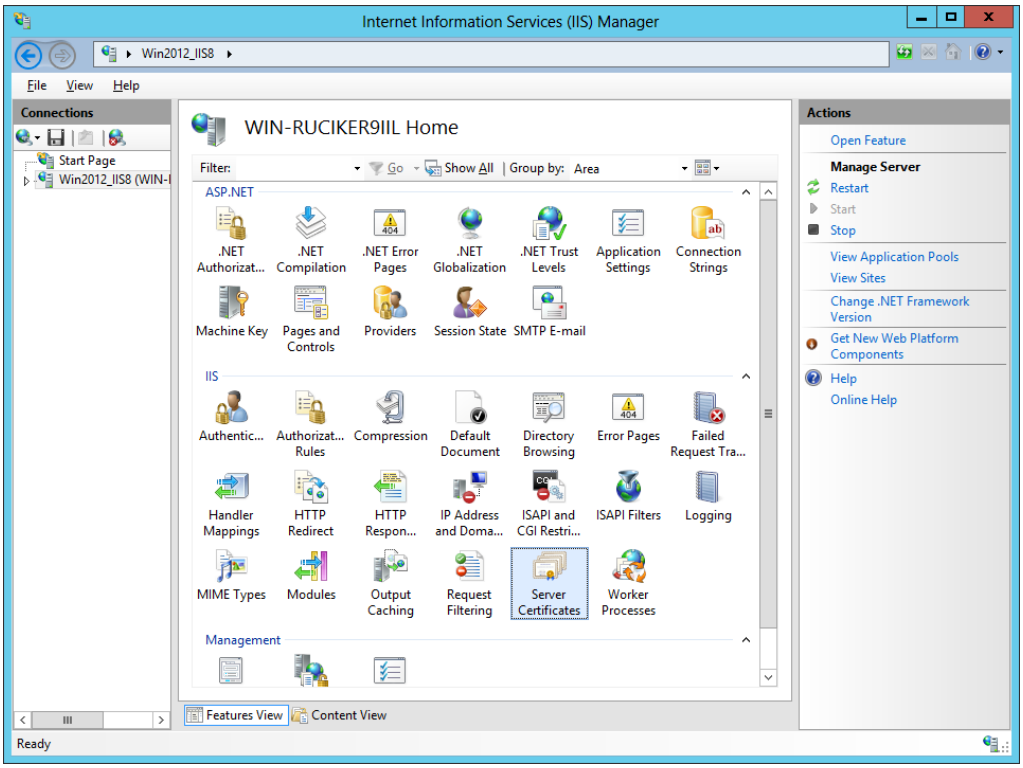
Oudere versies van de UZI-register CA certificaten kunt u altijd vinden op:
https://www.zorgcsp.nl/ca-certificaten

Pas wanneer u client authenticatie door middel van clientcertificaten wilt vereisen, zijn andere CA certificaten noodzakelijk.
Zie https://cert.pkioverheid.nl/cert-pkioverheid-nl.htm

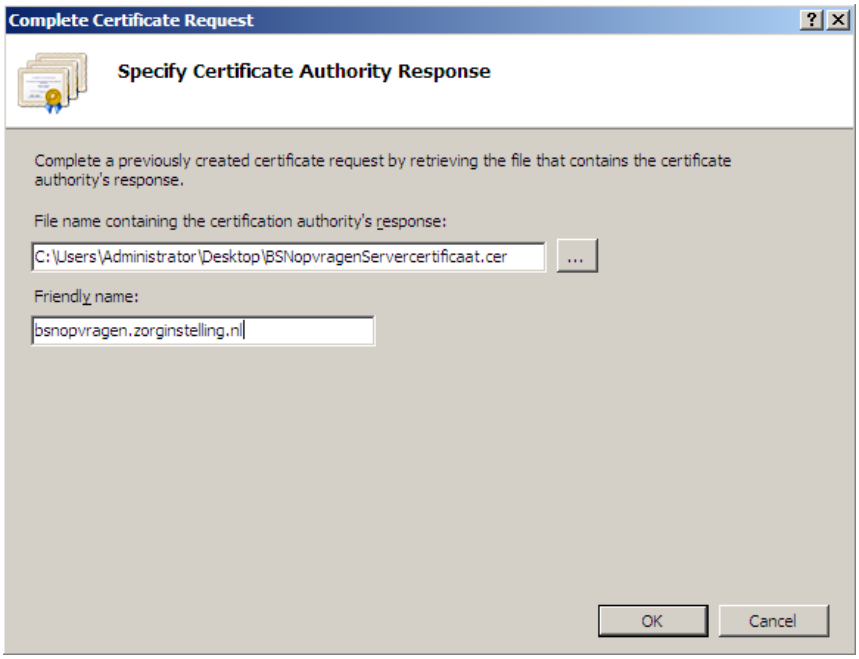
Voor test authenticatiemiddelen zijn afzonderlijke CA certificaten noodzakelijk. Deze kunt u downloaden via: https://acceptatie.zorgcsp.nl/ca-certificaten

Installeren van een servercertificaat
Open “Internet Information Services (IIS) Manager” en klik op de Homepage van de server en klik op “Server Certificates”.

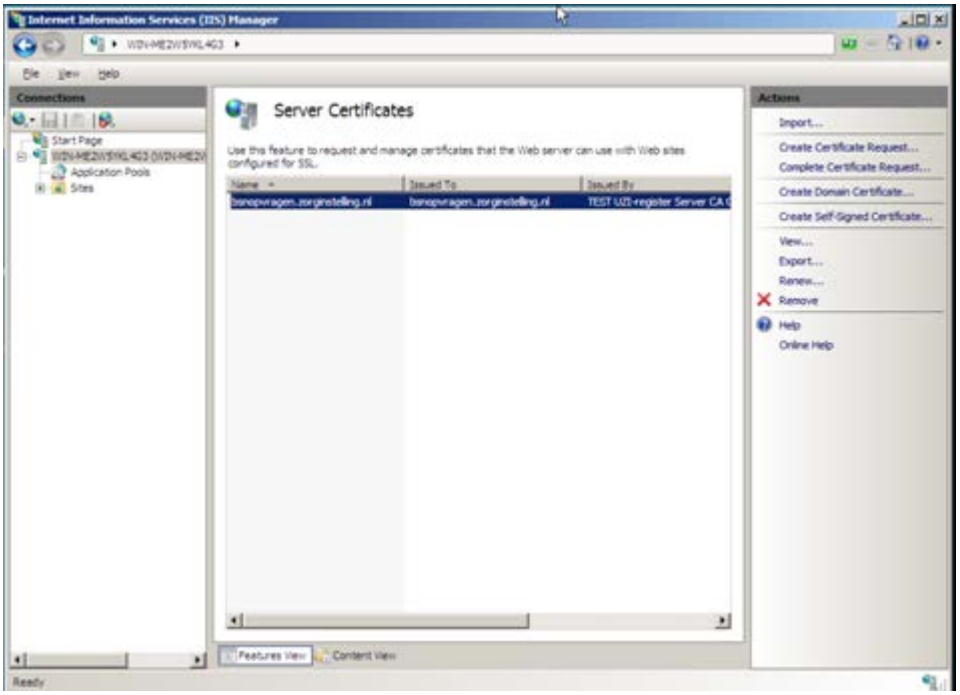
Kies voor “Complete Certificate Request”.



Selecteer in het scherm het certificaat dat u heeft ontvangen van het UZI-register. Vul bij “Friendly name” een eenvoudige naam in, bijvoorbeeld de systeemnaam. Klik daarna op “OK”.

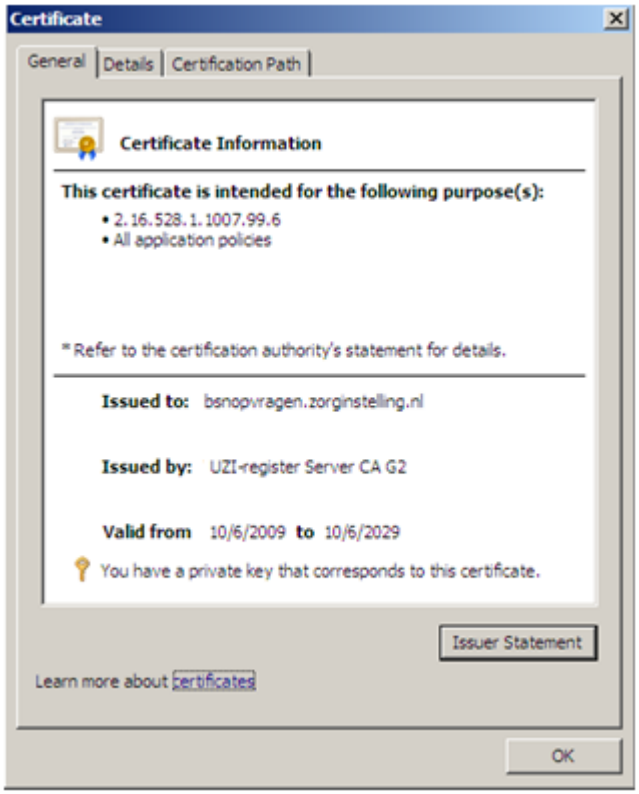


Hierna verschijnt het servercertificaat in de lijst met Server Certificates.

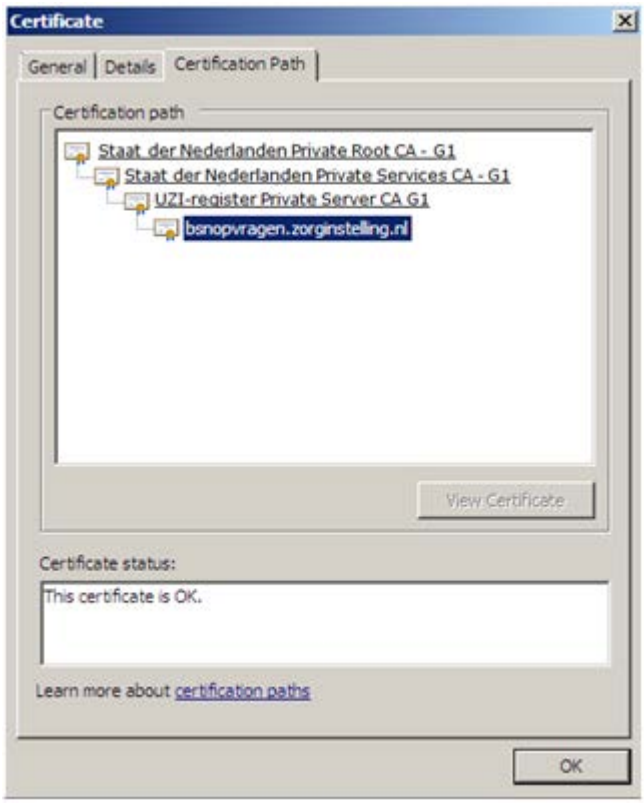


Dubbelklik op het certificaat.

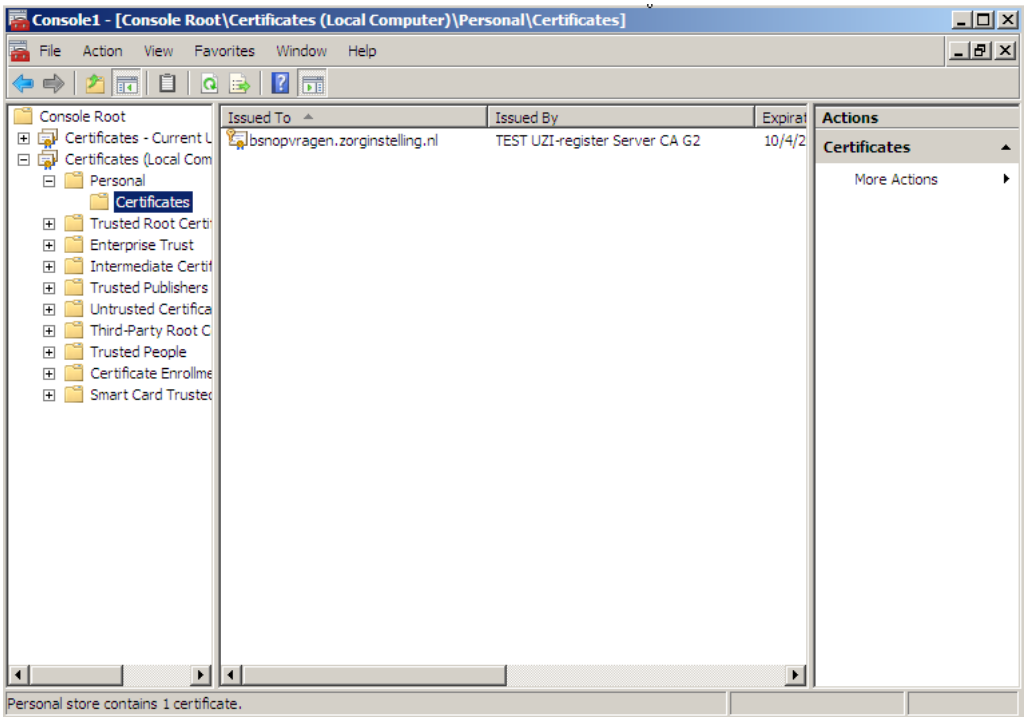
Tabblad “General”:



Tabblad “Certification Path” (na de installatie van de hiërarchie):



In de Certificate Store van de “Local Computer” is het certificaat terug te vinden:



4.2 Installatie Root CA certificaten

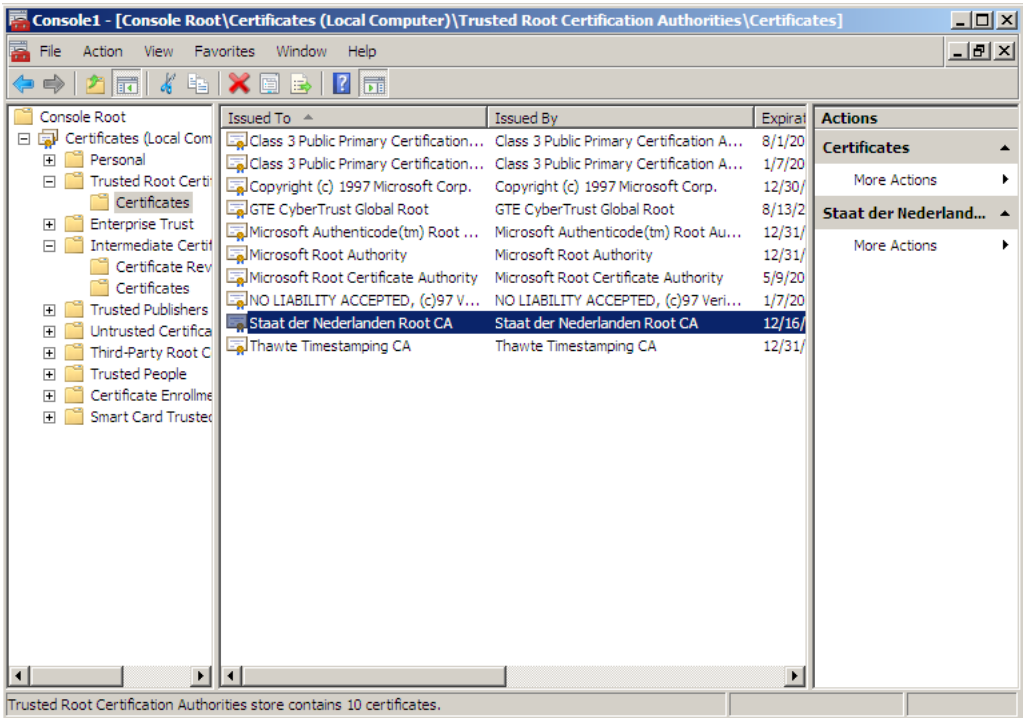
De complete CA keten moet u als vertrouwd aanmerken op de webserver.

Open een Microsoft Management Console (mmc.exe) en voeg de invoegtoepassing “Certificates” toe. Selecteer de “Local Computer”, niet de “Current User”.

Klap de Certificate Store (Local Computer) open en daarna de Trusted Root Certification Authorities.

Het Staat der Nederlanden Private Root CA –G1 certificaat importeert u in de ***Trusted Root Certification Authorities*** Certificate Store van de “Local Computer”.

De certificaten Staat der Nederlanden Private Services CA G1 en UZI-register Private Server CA G1 importeert u in de ***Intermediate Certification Authorities*** Certificate Store van de “Local Computer”.



5 Testen van de verbinding (optioneel)

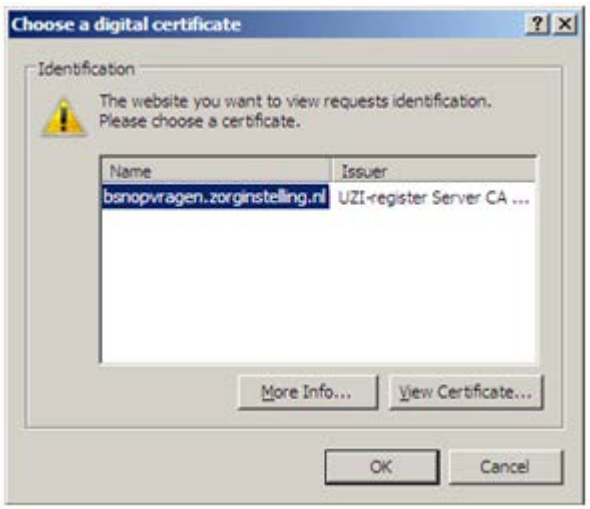
Om eventueel vast te stellen of het servercertificaat juist is geïnstalleerd kunt u inloggen op een link van de webservice van SBV-Z.

Let hierop dat het certificaat ook bij “Current User” staat in de Certificate Store naast dat het certificaat bij “Local Computer” staat (dit kan gedaan worden door het certificaat te kopiëren van “Local Computer” naar “Current User”).

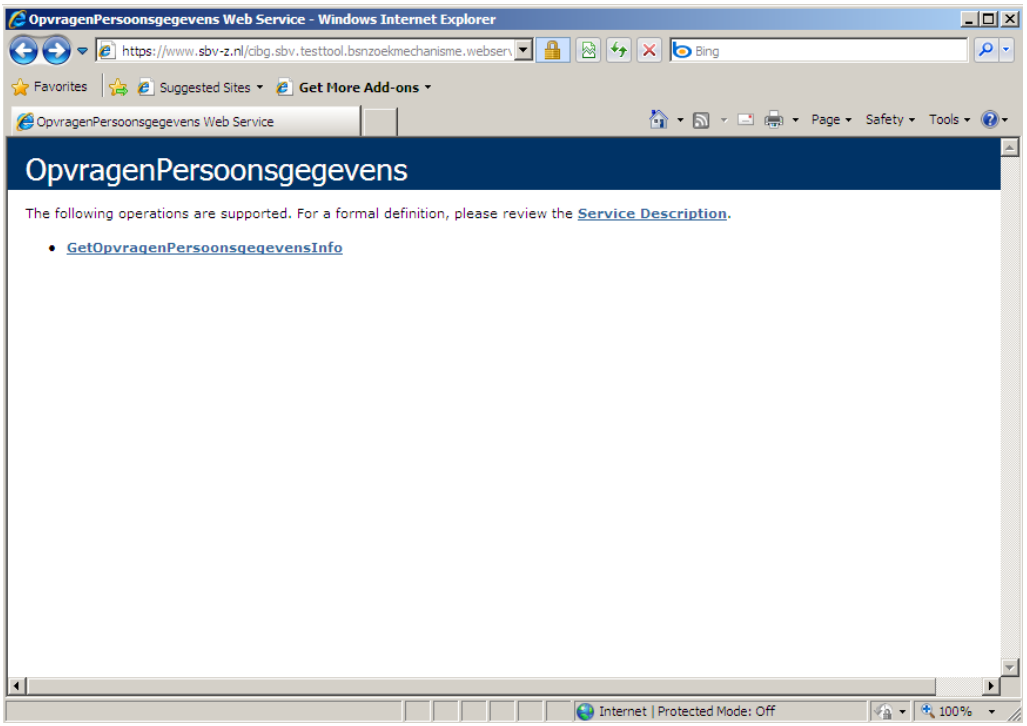
Bij het testen van een ‘productie’ servercertificaat gebruikt u deze link:
https://webservice.sbv-z.nl/cibg.sbv.interface.xis.webservice.dec14/opvragenpersoonsgegevens.asmx

Bij het testen van een ‘test’ servercertificaat gebruikt u deze link:
https://www.sbv-z.nl/cibg.sbv.testtool.bsnzoekmechanisme.webservice.dec14/opvragenpersoonsgegevens.asmx

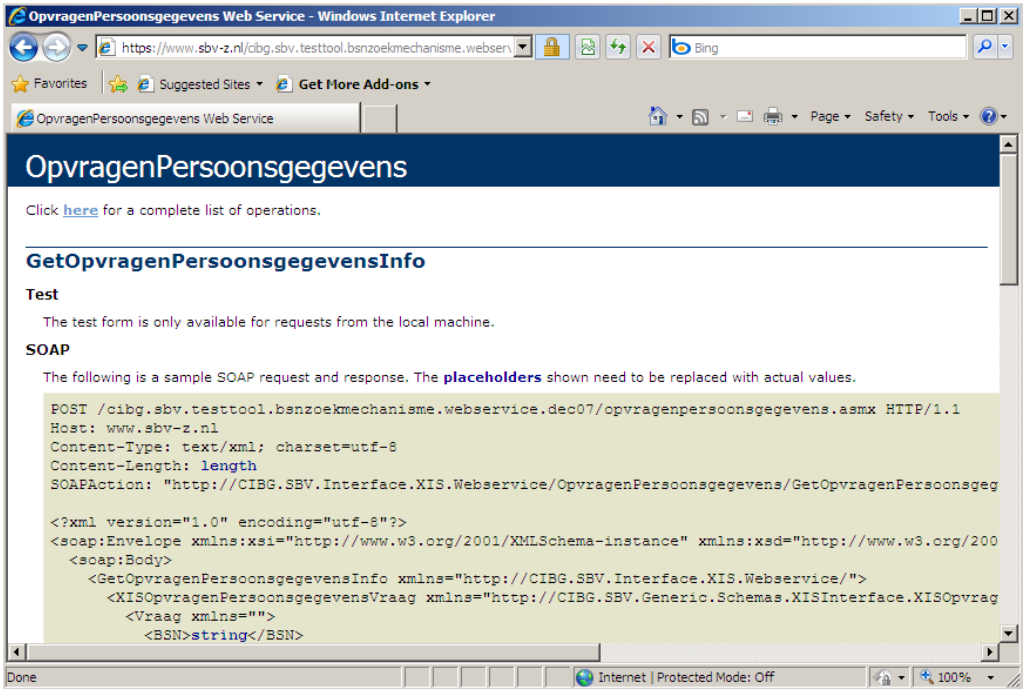
Selecteer in onderstaand scherm het gewenste servercertificaat om te testen (dit kan zowel test als productie zijn). Klik daarna op “OK”.



Als u onderstaand scherm krijgt te zien dan betekent dit dat connectie met de SBV-Z webservice gemaakt kan worden.



Als u klikt op de SOAP action dan krijgt u onderstaand scherm te zien.

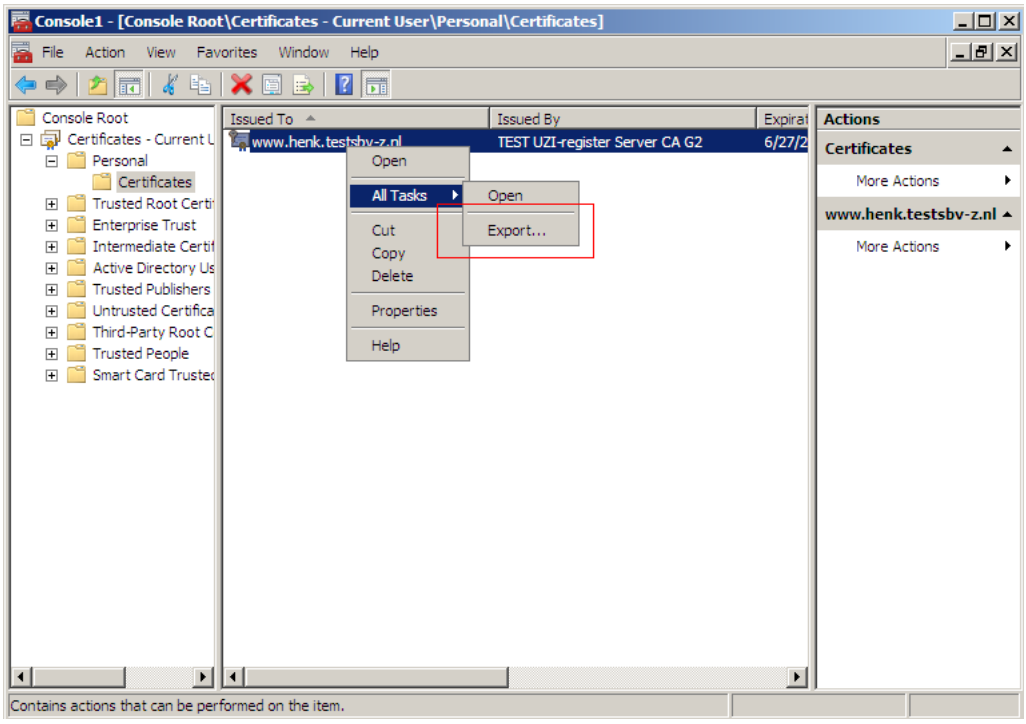


6 Het exporteren van het servercertificaat naar PFX

Het servercertificaat is nu geïnstalleerd. Dit servercertificaat bevat zowel de publieke als de private sleutel. U kunt dit exporteren naar PFX. In dit hoofdstuk staat beschreven hoe dit moet. Voorwaarde hierbij is wel dat het servercertificaat correct is geïnstalleerd.

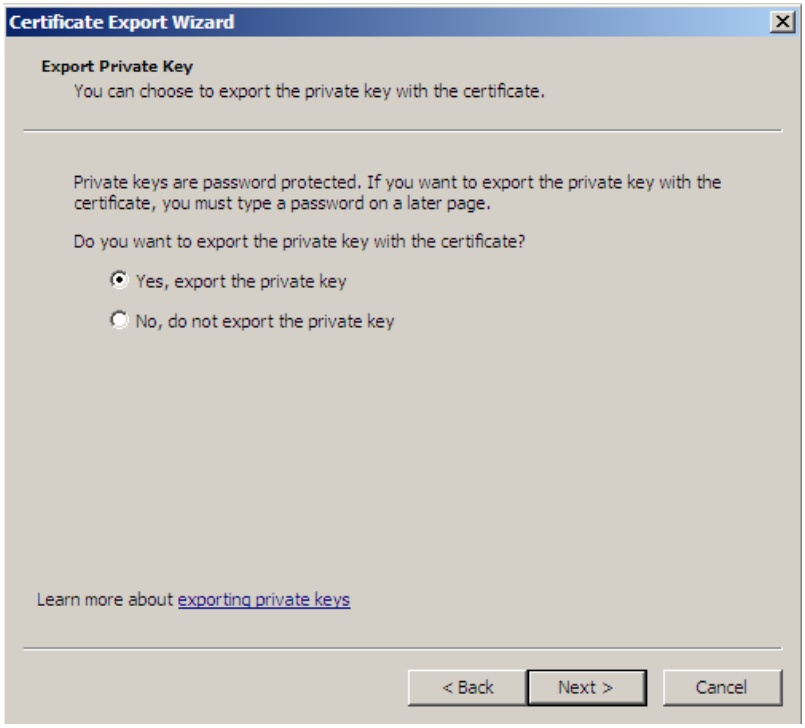
Start de MMC op en ga naar de map in Certificates (Local Computer) -> Personal -> Certificates.

Klik met de rechtermuisknop op het betreffende certificaat en kies voor All Tasks -> Export…



De Export Wizard verschijnt. Klik op “Next”.

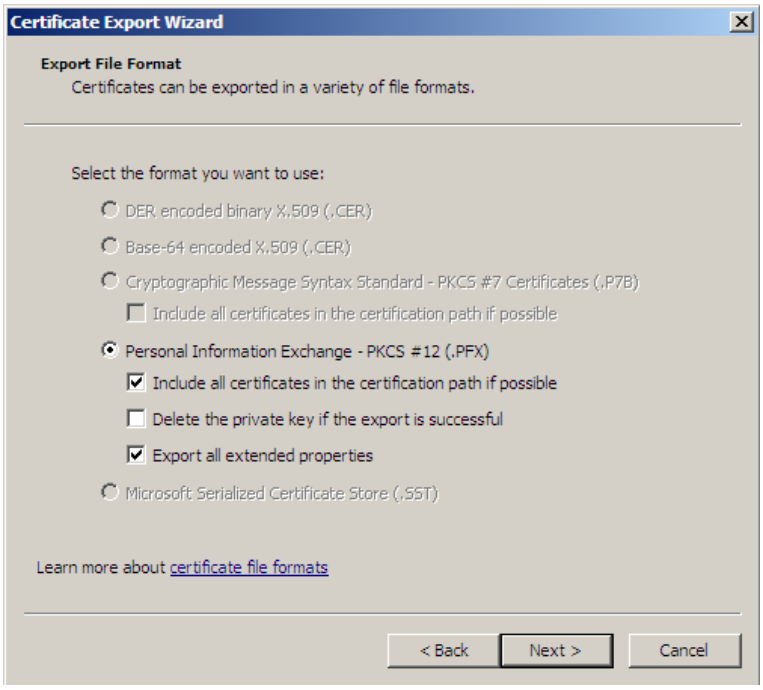
Selecteer “Yes, export the private key”. Dit betekent dat de private sleutel wordt meegenomen in het export bestand.
LET OP! Zonder de private sleutel kan het servercertificaat niet gebruikt worden.
Klik daarna op “Next”.



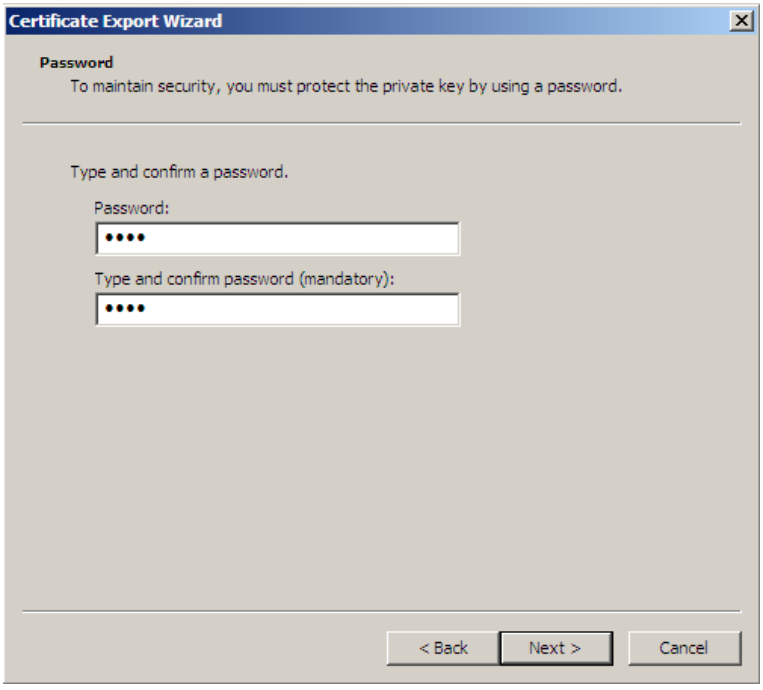
Selecteer de hieronder getoonde opties.

LET OP! Haal het vinkje weg dat staat bij “Delete the private key if the export is successful”. De private key moet u straks nogmaals exporteren voor archivering op de server.

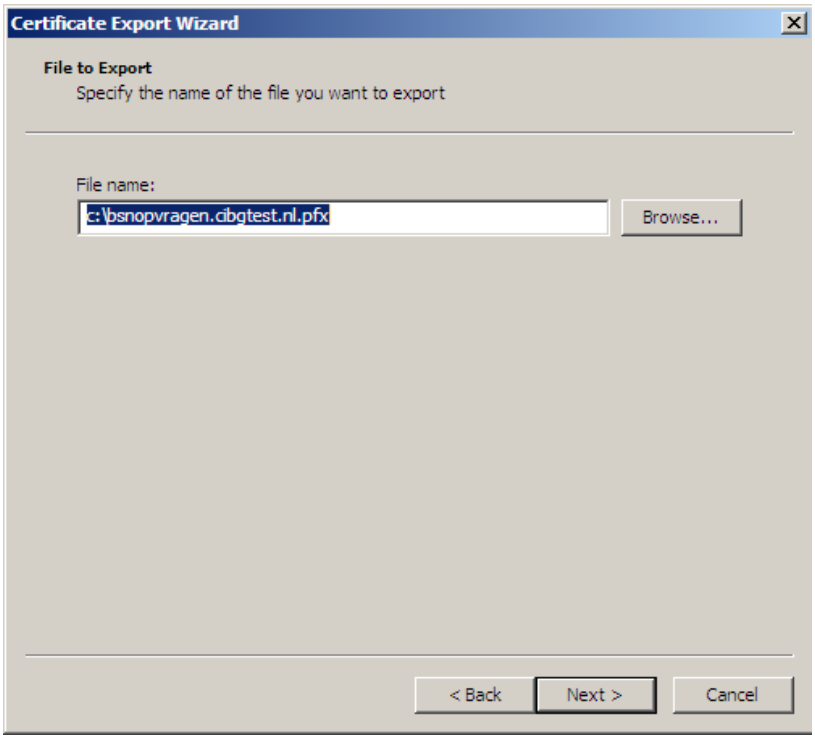
Klik vervolgens op “Next”.



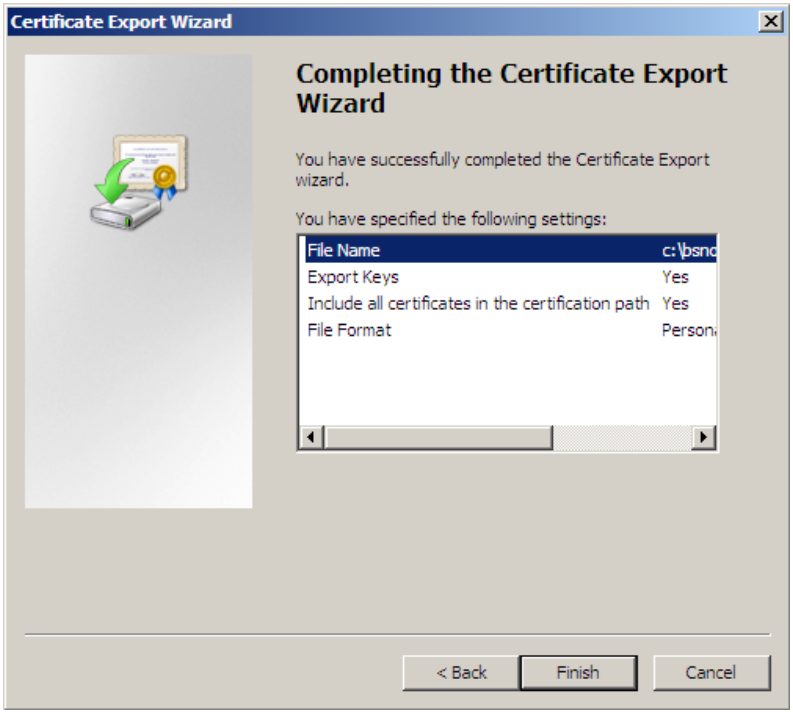
Voer hier het wachtwoord in om het servercertificaat te beveiligen. Dit wachtwoord moet u bij het importen van het servercertificaat invoeren.



Kies bij 'Browse' de locatie waar het PFX bestand opgeslagen moet worden. Zorg dat in de bestandsnaam de volledige FQDN staat. Klik daarna op “Next”.



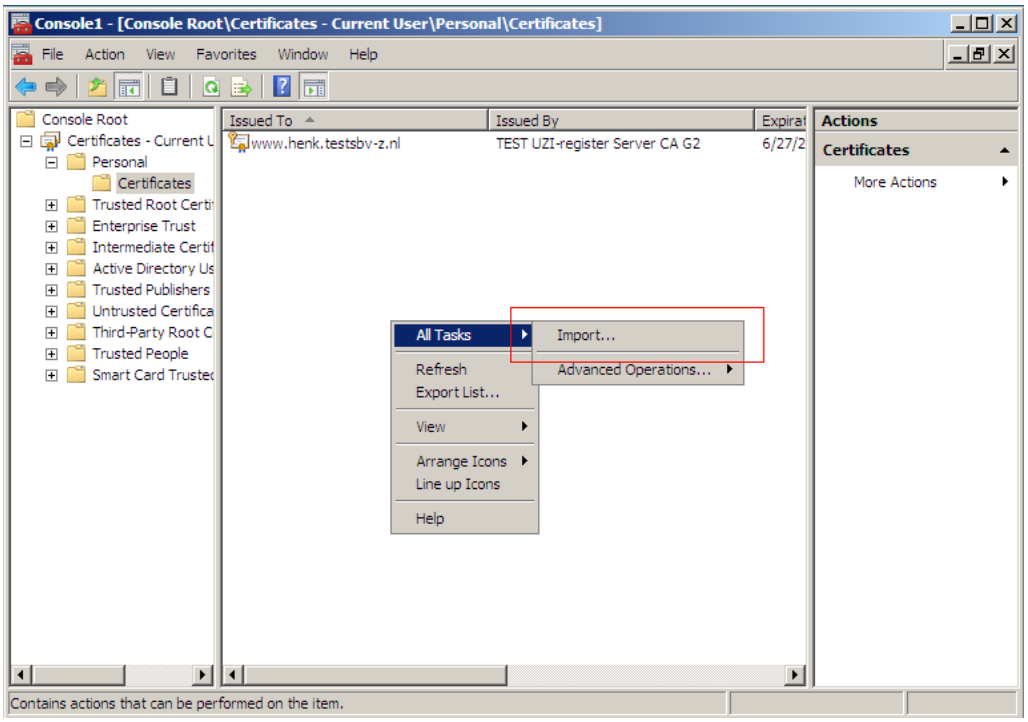
Controleer of alle settings correct zijn gekozen en klik op “Finish”.



Vervolgens krijgt u een melding betreft het succesvol exporteren en klikt u op “OK”.

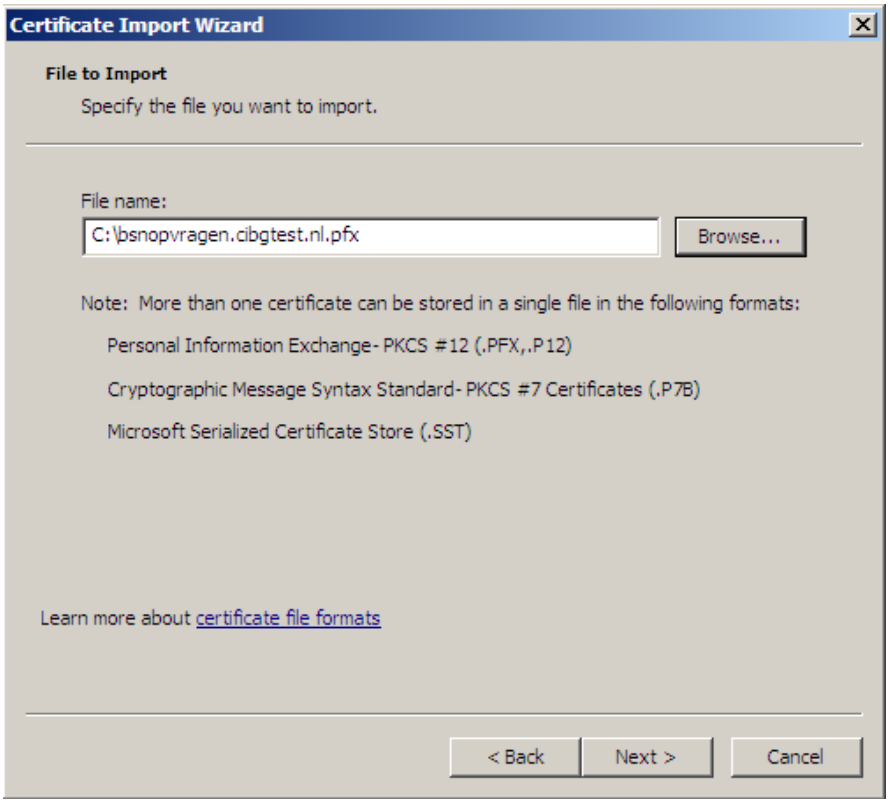
7 Het installeren van het servercertificaat in PFX formaat

Ga in de “MMC” naar “Certificates (Local Computer) -> Personal -> Certificates” en klik vervolgens met de rechtermuisknop op Certificates, selecteer “All Tasks” en vervolgens “Import…”.

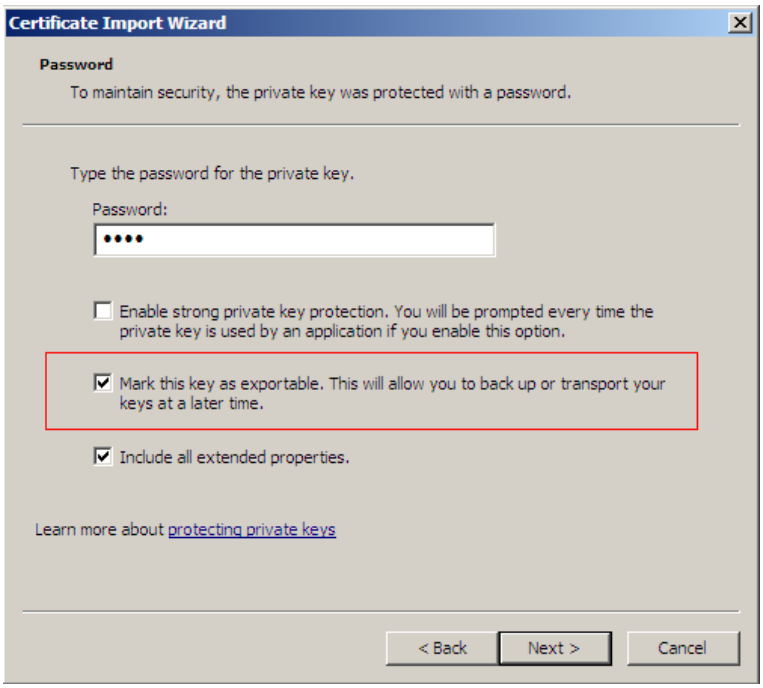


De Certificate Import Wizard wordt gestart. Klik op “Next”.

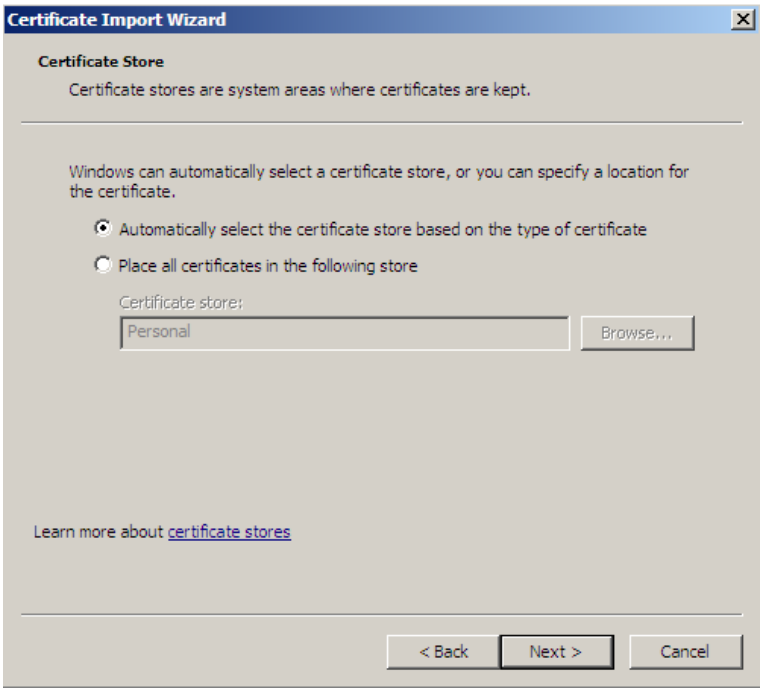
Selecteer bij “Browse” het PFX bestand en klik op “Next”.



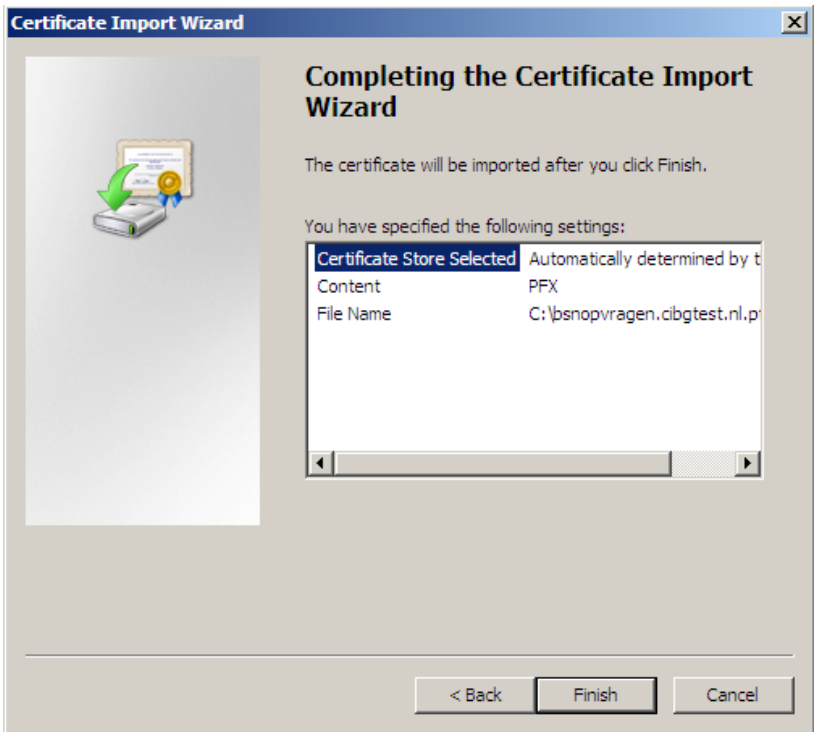
Voer het wachtwoord in wat u in hoofdstuk 6 heeft opgegeven.
LET OP! Indien er geen vinkje bij “Mark this key as exportable. This will allow you to back up or transport your keys at a later time.” staat kan het geïnstalleerde certificaat niet meer worden geëxporteerd naar een nieuw PFX bestand.



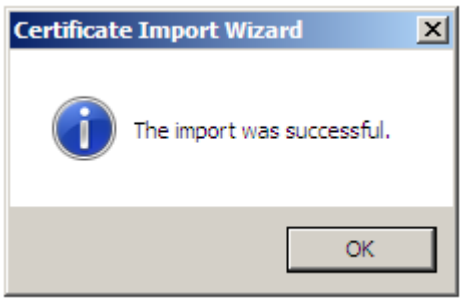
Kies voor: “Automatically select the certificate store based on the type of certificate.” Hiermee worden zowel de bovenliggende certificaatniveaus (bijv. Root CA) en het servercertificaat op de juiste plaats opgeslagen.



Controleer of de juiste instellingen zijn gekozen en klik daarna op “Finish”.



Het importeren is voltooid op de betreffende server.



Bijlage: Pending request binnen IIS is niet meer beschikbaar

Als het pending request binnen IIS niet meer beschikbaar is, dan is het niet meer mogelijk om het servercertificaat te installeren. IIS bewaart het private deel van het servercertificaat voor het pending request. Als deze verwijderd wordt binnen IIS dan wordt alleen de koppeling verwijderd. De private key is nog steeds aanwezig in de Certificate Store.
Met behulp van de Microsoft tool CertUtil kunt u alsnog het servercertificaat installeren, zonder dat het pending request beschikbaar is binnen IIS.
Meer informatie over CertUtil is te vinden op:
http://technet.microsoft.com/en-us/library/cc772898(WS.10).aspx

Werkwijze:

Stap 1
Open command prompt (Admin). Ga via het command prompt naar de installatie directory waar CertUtil.exe is opgeslagen. Standaard is dit C:\Windows\System32.

Stap 2
Voer het volgende commando uit: certutil -addstore my certnew.cer
CertNew.cer is hier het servercertificaat dat u heeft ontvangen van het UZI-register.
Er komt een melding: CertUtil: -addstore command completed successfully.

Stap 3
Ga naar de locatie waar het servercertificaat (het deel dat door het UZI-register is opgestuurd) is opgeslagen. Klik met de rechtermuisknop op dit servercertificaat en kies voor “Eigenschappen”.

Stap 4
Ga naar het tabblad “Details” en selecteer bij “Weergeven:” in het dropdownmenu <Alle>.
Selecteer het veld Thumbprint (Vingerafdruk), zodat de waarde zichtbaar wordt in het scherm daaronder.

Stap 5
Selecteer de hele Thumbprint en druk op CTRL-C.

Stap 6
Voer in het command prompt het volgende commando in: certutil -repairstore my "Thumbprint" Thumbprint is de waarde die in stap 5 is gekopieerd.
Als het commando goed is uitgevoerd komt de volgende melding: "Encryption test passed CertUtil: = repairstore command completed successfully."

Het servercertificaat is nu op juiste wijze beschikbaar en kan worden geïnstalleerd op de webservice.
Als bovenstaand commando de volgende foutmelding geeft: "Certutil: -repairstore command FAILED: 0x80090011 (-2146893807) Certutil: Object was not found." betekent dit dat de koppeling niet te herstellen is.

In dit geval moet u een nieuw servercertificaat aan vragen bij het UZI-register.

Bijlage: Toelichting systeemnaam (FQDN)

Voor het aanvragen van een servercertificaat moet de aanvrager een systeemnaam opgeven. Deze komt in het servercertificaat te staan. Deze systeemnaam moet een 'Fully Qualified Domain Name' zijn en aan een aantal eisen voldoen.

Beleid
Als de aanvraag voor een servercertificaat is ontvangen voert het UZI-register een aantal controles uit. Het UZI-register stelt vast of de bestanden correct zijn en of de opgegeven systeemnaam (URL) bij de Stichting Internet Domeinregistratie Nederland (www.sidn.nl) is geregistreerd. De aanvrager kan via de website vaststellen welke gegevens SIDN heeft geregistreerd. Als deze gegevens niet overeenkomen met de aan het UZI-register geleverde gegevens dan is het nodig dat u eerst de informatie bij SIDN laat actualiseren, of ter alternatief, een verklaring/factuur van de houder van de domeinnaam kunt overleggen waaruit blijkt dat u gebruik mag maken van de opgegeven domeinnaam. Voor andere extensies kunt u gebruik maken van www.iana.org. Voorbeelden zijn: *.com & *.org.

De opgegeven domeinnaam moet uniek zijn en mag niet worden gebruikt bij een andere organisatie/UZI-abonnee.

Het UZI-register adviseert om in de systeemnaam voor de productieomgeving geen test te vermelden, het mag echter wel als de klant dit wenst. De systeemnaam die u in productie gebruikt, mag al gebruikt zijn in de testomgeving. Onze ervaring leert echter dat dit door gebruik van dezelfde systeemnaam lastiger te beheren is.

Systeemnamen die eindigen op .local zijn niet te toetsen voor het UZI-register: een aanvrager kan in principe iedere naam opgeven die hij wenst. Het UZI-register kan er nu niet zeker van zijn of het systeem onder het domein van de abonnee hangt. Het UZI-register accepteert dus geen systeemnamen die eindigen op .local.

Het gebruiken van een servercertificaat voor aansluiting op het Landelijk Schakel Punt (LSP) kan alleen als de systeemnaam eindigt op .aorta-zorg.nl.

Technisch
In een systeemnaam mogen alleen letters, cijfers en het minteken voorkomen, met de volgende beperkingen:
- de systeemnaam mag alleen uit kleine letters bestaan, tekens in de reeks van 0 t/m 9, a t/m z en het koppelteken: "–". Een underscore mag niet;
- de systeemnaam mag niet bestaand uit diakrieten;
- er moet tenminste één letter in de naam staan;
- een minteken mag alleen tussen twee letters en/of cijfers staan.

Voorbeelden van juiste systeemnamen
- webservice.zorginstelling.nl is een juiste systeemnaam.
- systeemnaam1.ziekenhuis.nl is een juiste systeemnaam.
- webmail.afdelinga.ziekenhuis.nl is een juiste systeemnaam.

Voorbeelden van onjuiste systeemnamen
- www.zorginstelling/.sbvzbevraging.nl is een onjuiste systeemnaam.
- www.intrekking.uzi-register.local is een onjuiste systeemnaam.
- ziekenhuis.nl is een onjuiste systeemnaam.
- *.ziekenhuis.nl is een onjuiste systeemnaam.