



Controles installatie servercertificaat op een Windows server:

MMC

Open de MMC (Microsoft Management Console) en voeg vervolgens de volgende modules toe (via bestand → Module toevoegen/verwijderen): Certificaten (van zowel Lokale computer als Huidige gebruiker).

Ga naar Lokale computer → persoonlijk → certificaten. Hier zou men het servercertificaat moeten kunnen terugvinden.

Private Key

Als het pending request succesvol is gecompleteerd dan zou de private key gekoppeld moeten zijn aan het servercertificaat. Als u het servercertificaat 'opent' dan zou onderaan op het tabblad 'algemeen' moeten staan "u hebt een persoonlijke sleutel die overeenkomt met dit certificaat" (of uiteraard het Engelse equivalent). Staat vorengenoemde hier niet dan is de private key niet gekoppeld aan het servercertificaat. Het completeren van het pending request is dan niet goed gegaan of men heeft geprobeerd het servercertificaat op de verkeerde server te installeren (op een andere server dan waarop het PKCS#10-bestand is gegenereerd).

Doorloop alsnog de stappen om het certificaat te koppelen aan het 'pending request'. Indien het 'pending request' in IIS (Internet Information Server) niet meer zichtbaar is, kan het koppelen middels een workaround alsnog uitgevoerd worden. (Bijlage: Pending request binnen IIS is niet meer beschikbaar).

Let op, indien het 'pending request' handmatig is verwijderd, werkt deze workaround ook niet meer. Er zal dan opnieuw een certificaat aangevraagd moeten worden.

CA-certificaten en hiërarchie

Dubbelklik in de MMC op het certificaat en controleer of de hiërarchie compleet is op het tabblad 'certificeringspad'. Zie de installatiehandleiding, hoofdstuk 'installatie Root CA certificaten'. Laat waar nodig ook gelijk de benodigde CA certificaten voor SBV-z installeren: <https://www.sbv-z.nl/ondersteuning/documentatie>

Controleer in de MMC of de CA-certificaten in de juiste store zijn opgeslagen.

Het Staat der Nederlanden Private Root CA -G1 certificaat importeert u in de **Vertrouwde basiscertificeringsinstanties** Certificate Store (of het Engelse equivalent) van de "Lokale Computer"

De certificaten Staat der Nederlanden Private Services CA G1 en UZI-register Private Server CA G1 importeert u in de **Tussenliggende certificeringsinstanties** Certificate Store (of het Engelse equivalent) van de "Lokale Computer".

Controle werking certificaat

Is de private key aanwezig en de hiërarchie compleet dan is het servercertificaat in basis goed geïnstalleerd. U kunt middels uw zorgapplicatie controleren of het certificaat functioneert.

Ook kunt u op de volgende wijze vaststellen of het servercertificaat juist is geïnstalleerd:

Hiervoor is het benodigd 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/exporteren 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>

Mocht men nog steeds een 403 foutmelding krijgen dan moet mogelijk de server worden herstart om de wijzigingen ook in het register door te voeren.

Kan men nog steeds geen werkende situatie realiseren dan kan het zijn dat de Firewall de verbinding 'tegenhoudt'. De verbinding met SBV-z gaat over de gebruikelijke internet poorten.

Een enkele keer is het noodzakelijk dat er meer rechten aan de private key gegeven moeten worden. Dit kan in de MMC d.m.v. rechtermuisknop op het servercertificaat (in locale computer) en dan kiezen voor "manage private keys"