



# Aanvragen van een UZI-servercertificaat

.....  
**In deze factsheet krijgt u informatie over:**

Aanmaken sleutelpaar en  
PKCS#10 request

Aanvragen servercertificaat

Controle aanvraaggegevens

Identiteitsvaststelling

Uitgifteproces

Terugmelding  
.....

Elektronische communicatie is niet meer weg te denken uit onze samenleving. Ook in de zorg. Omdat zorginformatie over het algemeen privacy gevoelige gegevens bevat, staat zorgvuldige bescherming van die gegevens voorop. De patiënt moet daarop kunnen vertrouwen. Het moet duidelijk zijn wie gegevens leest, verstuurt of ontvangt. Om hierover zekerheid te kunnen geven is het Unieke Zorgverlener Identificatie register, kortweg UZI-register, ontwikkeld.

Dit is één van de factsheets van het UZI-register. Een overzicht van alle factsheets vindt u op onze website [www.uzi-register.nl](http://www.uzi-register.nl)

Naast de UZI-pas in de vorm van een smartcard geeft het UZI-register ook servercertificaten uit. Uw website, applicatie of server kan met een servercertificaat aantonen dat deze bij u als abonnee hoort. Met zowel een pas als een servercertificaat kunnen beveiligde verbindingen worden gemaakt waarop niemand kan mee kijken en kan zien welke gevoelige gegevens worden uitgewisseld. De UZI-pas is bedoeld voor personen, het servercertificaat voor beveiligde systemen.

Deze factsheet neemt u mee langs de stappen die u moet nemen bij het aanvragen van een servercertificaat bij het UZI-register. U kunt deze servercertificaten alleen aanvragen als u abonnee van het UZI-register bent. Een aanvraag kan alleen worden gedaan door een bij het UZI-register bekende aanvrager. Door het technische karakter is specifieke deskundigheid nodig. Vraagt u daarom uw leverancier of ICT-deskundige u hierbij te helpen of deze taak van u over te nemen. De hierna volgende informatie is bedoeld voor uw leverancier of ICT-deskundige.

### **Stap 1: Aanmaken sleutelbaar en PKCS#10 request**

Het systeem waarvoor u een servercertificaat aanvraagt, moet u bij het UZI-register bekend maken. U doet dit door als eerste technische stap een sleutelbaar te laten genereren. Het sleutelbaar bestaat uit twee wiskundig verbonden sleutels: een private en een publieke sleutel. De publieke sleutel wordt onderdeel van uw servercertificaat, de private sleutel houdt u te allen tijde geheim. Met het sleutelbaar kan het systeem bewijzen dat het bij u hoort.

Het aanmaken van het sleutelbaar is een technische activiteit die meestal uitgevoerd zal worden door de beheerder van het systeem waarvoor het servercertificaat wordt aangevraagd. Voor aanvragen die ingediend worden vóór 1 december 2010 moet het sleutelbaar een 1024 bits lang RSA sleutelbaar zijn. Voor alle aanvragen die ingediend worden vanaf 1 december 2010 moet het sleutelbaar een 2048 bits RSA sleutel bevatten. Deze aanvragen zullen na 1 januari 2011 geproduceerd worden onder de SHA-2 hiërarchie en vereisen daarom een langere RSA sleutel.

Het is van groot belang om dit sleutelbaar aan te maken in een veilige omgeving. Dat is het veiligst in een gecertificeerde Secure User Device (SUD), in de praktijk beter bekend onder de naam HSM (Hardware Security Module). Het is toegestaan om de private sleutel softwarematig te beschermen. Voorwaarde is dat u dan aanvullende beveiligingsmaatregelen treft van dusdanige kwaliteit dat het onmogelijk is deze sleutel ongemerkt te stelen of te kopiëren. Let op: het is heel moeilijk om een gewone werkplek aan deze beveiligingsmaatregelen te laten voldoen.

Nadat het sleutelbaar is gemaakt, kunt u een zogenaamd certificate signing request genereren in de vorm van een PKCS#10 bestand. PKCS#10 is het gangbare technische bestandsformaat voor een certificaataanvraag en wordt ook wel 'certificate signing request (csr)' genoemd. Het PKCS#10 bestand dient vanwege interoperabiliteit vooralsnog ondertekend te zijn op basis van het Sha-1WithRSAEncryption algoritme. Dit is de standaard instelling van de meest gangbare tools om een PKCS#10 bestand te genereren.

Het PKCS#10 bestand kan naast de publieke sleutel allerlei gegevens bevatten die het systeem identificeren. Het UZI-register neemt enkel de publieke sleutel over in het UZI-servercertificaat.

Veel systemen ondersteunen het genereren van een PKCS#10 bestand. Het UZI-register verwijst daarom naar de documentatie die de leverancier van de server meevert. Enkele voorbeelden zijn Microsoft Internet Information Server ([www.microsoft.com](http://www.microsoft.com)), apache webserver en openssl ([www.openssl.org](http://www.openssl.org)), IBM Websphere server ([www.ibm.com](http://www.ibm.com)) en BEA Weblogic ([www.bea.com](http://www.bea.com)).

## Stap 2: Aanvragen servercertificaat

Levert u samen met het PKCS#10 bestand en het formulier 'Een servercertificaat aanvragen' de volgende gegevens aan:

### Gegevens die de aanvraag koppelen aan de abonnee:

- Naam zorgaanbieder volgens abonnee registratie.
- Abonneenummer dat u bij de bevestiging van uw abonnee registratie heeft ontvangen.
- Geboortenaam van de bij het UZI-register geregistreerde aanvrager.

### Gegevens over het systeem en de certificaataanvraag:

- Systeemnaam. Om het systeem uniek te identificeren heeft het UZI-register de fully qualified domain name (FQDN) nodig. Dit is de naam van het systeem inclusief domeinnaam.
- Het UZI-register toetst bij SIDN (Stichting Internet Domeinregistratie Nederland) of IANA (Internet Assigned Names Authority) of u als abonnee eigenaar bent van de domeinnaam. Bent u niet de eigenaar, dan vragen wij de eigenaar om toestemming. Het UZI-register neemt de domeinnaam op in het certificaat (zie CA model pasmodel Certificaatprofielen op [www.uzi-register.nl](http://www.uzi-register.nl)).
- Als u bij het landelijk schakelpunt (LSP) wilt kunnen aansluiten, stelt de beheerder aanvullende eisen: de volledige domeinnaam moet bij een zorgserviceprovider (ZSP) zijn vastgelegd. De volledige domeinnaam moet vallen onder het domein '.aorta-zorg.nl'
- Als de volledige domeinnaam eindigt op .aorta-zorg.nl dan moet deze zijn geregistreerd bij het landelijk schakelpunt. Neem hiervoor contact op met uw zorgserviceprovider (ZSP).

### Gegevens over de afdeling (niet verplicht):

- Als u een afdeling opgeeft, neemt het UZI-register dit op in het certificaat.

### Gegevens over het e-mailadres van het systeem (niet verplicht):

- Als u een e-mailadres opgeeft, wordt het opgenomen in het certificaat.

## Postkantoor voor de identiteitsvaststelling

Hier kan de aanvrager aangeven op welk postkantoor hij/zij zich wil melden om formeel de identiteit vast te laten stellen (zie stap 4). Heeft u een pas met een gekwalificeerd handtekeningcertificaat (=PKIoverheid certificaat), bijvoorbeeld een UZI-pas? Dan kan het UZI-register de identiteit aan de hand hiervan vaststellen. De aanvrager hoeft dan niet naar het postkantoor en hij hoeft geen postkantoor aan te geven.

## Handtekening op papier

Na handmatige ondertekening van het formulier 'Een servercertificaat aanvragen' kunt u het formulier met de aanvullende zaken sturen naar:

### UZI-register

**Antwoordnummer 10600**  
**2501 WB Den Haag**

Een postzegel is niet nodig. Het PKCS#10 bestand stuurt u per e-mail naar [info@uzi-register.nl](mailto:info@uzi-register.nl).

## Elektronische handtekening

Als u beschikt over een pas met een gekwalificeerd handtekening certificaat, dan heeft het de voorkeur dat u de aanvraag elektronisch ondertekent. U spaart dan de weg naar het postkantoor. U kunt uw aanvraag elektronisch ondertekenen door de e-mail, met als bijlagen het formulier 'Een servercertificaat aanvragen' en het PKCS#10 bestand, elektronisch te ondertekenen en te sturen naar [info@uzi-register.nl](mailto:info@uzi-register.nl). Vermeldt u bij het onderwerp uw abonneenaam en in uw mail de systeemnaam. Hoe u een e-mail met een UZI-pas kunt ondertekenen leest u op de website bij 'Vraag en Antwoord': 'Hoe ondertekenen ik een e-mail met mijn UZI-pas'.

### Stap 3: Controle aanvraaggegevens

Als de aanvraag is ontvangen, voert het UZI-register een aantal controles en toetsen uit. Het UZI-register stelt vast of:

- de bestanden correct zijn;
- de abonnee eigenaar is van de opgegeven domeinnaam;
- de opgegeven domeinnaam (URL) bij de Stichting Internet Domeinregistratie Nederland of IANA is geregistreerd.

Pas als uw aanvraag correct is binnengekomen kan het UZI-register starten met het verwerken van de aanvraag.

### Stap 4: Identiteitsvaststelling

Om op de certificaten te kunnen vertrouwen, worden hoge eisen gesteld aan het registratie-, productie- en uitgifteproces van de certificaten.

Het UZI-register moet altijd met zekerheid vaststellen wie de verantwoordelijke voor een servercertificaat is. Om die reden moet het UZI-register de identiteit van de aanvrager vaststellen. Hiervoor krijgt de aanvrager een meldverzoek toegestuurd waarmee de aanvrager zich kan melden bij het postkantoor. De medewerker op het postkantoor zal de aanvrager vragen zich te legitimeren en het meldverzoek te overleggen. Daarna meldt het postkantoor aan het UZI-register dat de identiteitsvaststelling succesvol heeft plaatsgevonden.

Is de aanvraag met een pas met een gekwalificeerde handtekening ondertekend, dan stelt het UZI-register de identiteit aan de hand hiervan vast. U kunt de stap identiteitsvaststelling door het postkantoor dan overslaan.

### Stap 5: Uitgifteproces

Als stap 3 (Controle aanvraaggegevens) en stap 4 (Identiteitsvaststelling) succesvol zijn uitgevoerd, produceert het UZI-register het servercertificaat.

Na productie ontvangt u instructies om het servercertificaat te ontvangen. Daarnaast ontvangt u van het UZI-register een brief met het pasnummer en de intrekingscode van het UZI-servercertificaat. **Bewaar deze brief zorgvuldig!**

Als het in de toekomst nodig is kunt u, met het pasnummer en de intrekingscode die op deze brief staan, het servercertificaat te allen tijde intrekken via de intrekingspagina op de website.

### Stap 6: Belangrijk: terugmelding

Na controle van het servercertificaat bevestigt u de ontvangst per e-mail. Om er zeker van te zijn dat het servercertificaat bij u is aangekomen, is het heel belangrijk dat u deze stap zo spoedig mogelijk doet. Alleen zo kan het UZI-register de betrouwbaarheid van het servercertificaat garanderen naar vertrouwende partijen.

#### Tip!

U heeft uw ICT-leverancier niet gemachtigd als aanvrager, maar hij heeft u wel met de aanvraag van dit servercertificaat geholpen? Zet uw ICT-leverancier dan op de 'cc' van uw mail als u de ontvangst van het servercertificaat aan het UZI-register bevestigt. Ook uw ICT-leverancier wil graag weten of u het UZI-servercertificaat heeft ontvangen.

#### Dit is een uitgave van het UZI-register.

Het UZI-register is een onderdeel van het CIBG, een uitvoeringsorganisatie van het Ministerie van Volksgezondheid, Welzijn en Sport.

Wijnhaven 16 | 2511 GA Den Haag  
Postbus 16114 | 2500 BC Den Haag  
T 0900 - 2324342 (1 cent per minuut) | F 070 - 340 5252  
info@uzi-register.nl | www.uzi-register.nl