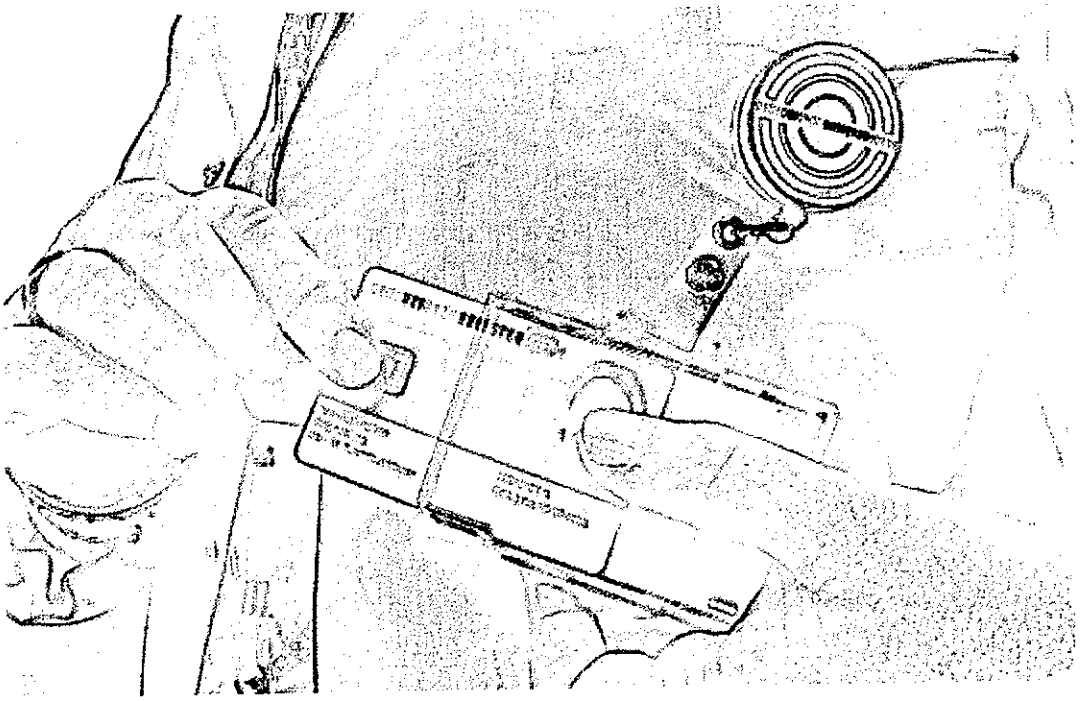
28.

0101UZI0100REGISTER1011

Certification Practice Statement (CPS)

agentschap CIBG
versie 4.1, definitief
Den Haag, 1 oktober 2008



Postadres
Postbus 16114
2500 BC DEN HAAG

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

Revisiehistorie

Versie	Datum	Status	Opmerking
1.0	17-01-2005	Definitief	Externe verspreiding
2.0	11-01-2006	Definitief	Wijziging conform adviesnota d.d. 1 december 2005 - Herstructurering van het Programma van Eisen van de PKI voor de overheid. - Juridische consultatie: verduidelijking verplichtingen, fusie en intellectuele eigendom. - Verlenging geldigheidsduur CRL.
3.0	01-03-2007	Definitief	Wijzigingen conform adviesnota d.d 9 februari 2007 - Werkwijze 'uitstervend' specialisme. - Beperking functienaam medewerker niet op naam - Wijziging UZI-nummer na wijziging unieke gegevens - Domeinnaam niet in eigendom - Verzoek intrekking ook via e-mail - Nieuwe gebruikersgroepen: indicatieorganen en aanvulling artikel 34 beroepsbeoefenaren. - Tekstuele aanpassingen Nieuwe indeling conform RFC 3647.
3.1	08-03-2007	Intern	Publiekrechtelijke versie. Deze is niet geldig geweest.
3.2	01-10-2007	Definitief	Wijziging conform adviesnota 9 februari 2007 (deel 1): - Toetsing apotheken op basis van apotheekregistratie. - Nieuw specialisme: apotheekhoudend huisarts. - Identiteitsvaststelling servercertificaat op basis van elektronische handtekening mogelijk. - Abonnee zorgverlener kan aanvragerrol delegeren. - Afkorting van te lange namen. - Tekstuele aanpassingen en update begrippenlijst.
3.3	6-12-2007	Definitief	Tweede generatie CA hiërarchie.
4.0	1-6-2008	Definitief	Wijziging conform adviesnota 9 februari 2007 (deel2): - Van kracht worden Wet gebruik BSN in de zorg - Verduidelijking betekenis begrip 'abonnee'. - Loskoppelen pashouder uit aanvraagproces. - Uitsluiting rijbewijs bij aanvraag pas. - Opvragen uittreksel KvK door UZI-register zelf. - Bewijsdocumenten wettelijk vertegenwoordiger. - Handelwijze UZI-register bij compromitatie algoritme - Nieuwe versie programma van eisen PKIoverheid - Tekstuele aanpassingen en update begrippenlijst.
4.1	1-10-2008	Definitief	Wijziging conform adviesnota d.d. 18-8-2008 - telefonisch intrekken; - verduidelijking beleid m.b.t. fusies - tekstuele aanpassingen en verduidelijkingen.

Tabel 1: Versiehistorie CPS UZI-register

Inhoudsopgave

Lijst met figuren

Lijst met tabellen

1 Introductie

1.1 UZI-register en producten

1.1.1 Introductie UZI-register

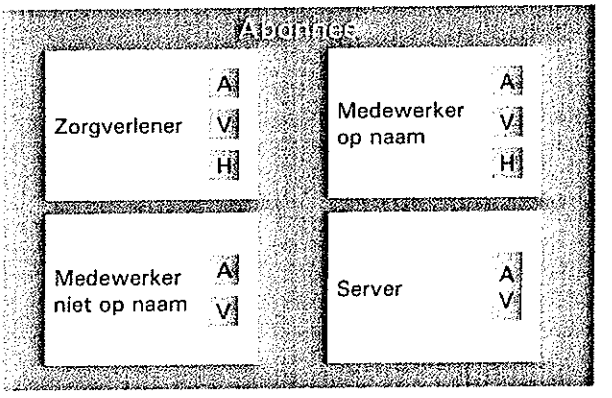
Om veilige communicatie en raadplegen van vertrouwelijk informatie in het zorgveld mogelijk te maken, worden drie domeinen onderscheiden: de zorgconsumenten, de zorgverzekeraars en de zorgaanbieders. Het Unieke Zorgverlener Identificatie register (kortweg UZI-register) is het door de Minister van VWS aangewezen register van zorgaanbieders zoals vermeld in artikel 14 van de Wet gebruik burgerservicenummer in de zorg (Wbsn-z). Het UZI-register is de certificatiedienstverlener (CSP)[1] die certificaten uitgeeft voor de unieke identificatie en authenticatie van zorgaanbieders en indicatieorganen in de zorg.

Het UZI-register heeft als doel zorgaanbieders en indicatieorganen bij elektronische communicatie en toegang tot gegevens uniek te identificeren. Het UZI-register koppelt hiertoe op unieke wijze de fysieke identiteit aan een elektronische identiteit en legt deze vast in certificaten. De certificaten en de hierbij behorende cryptografische sleutels bevinden zich op een smartcard. Het geheel wordt in dit Certification Practice Statement (CPS) aangeduid als UZI-pas[2].

Het UZI-register geeft UZI-passen uit voor door de minister van VWS bij wet en regelgeving aangewezen partijen. Een nadere beschrijving van de gebruikersgemeenschap van het UZI-register is opgenomen in paragraaf 1.3 'Betrokken partijen'. Het UZI-register geeft certificaten uit binnen het domein Overheid en Bedrijven van de hiërarchie van de PKI voor de overheid.

1.1.2 Soorten passen en certificaten

Het UZI-register geeft verschillende typen passen en certificaten uit. Figuur 1: Passenmodel en certificaten geeft een schematisch overzicht van de pastypen en de certificaten per pastype. De verschillende pastypen worden hierna kort toegelicht.



Figuur 1: Passenmodel en certificaten

[1] Voor een verklaring van de gebruikte begrippen en afkortingen wordt verwezen naar bijlage 1 'Definities en afkortingen'.

[2] Het begrip UZI-pas wordt gebruik om de certificaten, sleutels en de daarbij behorende drager aan te duiden. Ook als er sprake is van een andere drager dan de smartcard, wordt het begrip UZI-pas gebruikt.

Zorgverlenerpas
De zorgverlenerpas is voor een beroepsbeoefenaar als bedoeld in de artikelen 3 en 34 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Uitreiking van de pas vindt plaats op basis van een face-to-face controle en controle van de wettelijke identiteit, nadat getoetst is of het daadwerkelijk om een zorgverlener gaat (zie bijlage 2). Het UZI-register garandeert naast de identiteit tevens de 'status zorgverlener' en de relatie naar de abonnee[3]. Zorgverleners krijgen een gepersonaliseerde pas met pasfoto en drie certificaten en sleutelparen (authenticatie, vertrouwelijkheid en onweerlegbaarheid).

Medewerkerpas op naam
Een medewerker van een abonnee van het UZI-register kan de beschikking krijgen over een 'Medewerkerpas op naam'. Uitreiking van de pas vindt plaats op basis van een face-to-face controle en controle van de wettelijke identiteit na een verzoek van een geautoriseerde aanvrager. Het UZI-register garandeert naast de identiteit tevens de relatie naar de abonnee. Medewerkers op naam krijgen een gepersonaliseerde pas met pasfoto en drie certificaten en sleutelparen (authenticatie, vertrouwelijkheid en onweerlegbaarheid).

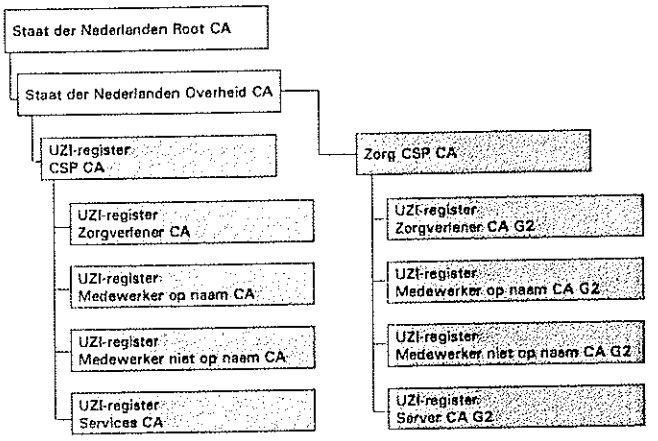
Medewerkerpas niet op naam
Voor medewerkers van een abonnee van het UZI-register kan een medewerkerpas niet op naam worden verkregen. De certificaten van deze UZI-pas geven aan dat de certificaathouder een medewerker is van de abonnee die in de certificaten wordt genoemd. Het UZI-register garandeert de relatie naar de abonnee. De abonnee registreert de relatie naar de specifieke medewerker. Medewerkers niet op naam krijgen een niet-gepersonaliseerde UZI-pas met twee certificaten en sleutelparen (authenticatie en vertrouwelijkheid).

Servercertificaten
Voor systemen van een abonnee kunnen servercertificaten verkregen worden. Deze certificaten geven aan dat een systeem namens de abonnee gegevens uitwisselt en/of services biedt. De abonnee is verantwoordelijk voor de juistheid van de gegevens in de servercertificaten van zijn systemen. Het UZI-register garandeert de relatie naar de abonnee. Voor servercertificaten zijn het authenticiteit- en vertrouwelijkheidcertificaat gecombineerd in één certificaat.

1.1.3 CA-model
Certificaten die door het UZI-register worden uitgegeven zijn ondertekend door het UZI-register. Hiervoor wordt de handtekening van de Certification Authority (CA) van het UZI-register gebruikt. Het UZI-register heeft een aantal CA's. De samenhang tussen deze CA's is geschetst Figuur 2: CA-model'.

De CA van de UZI-register CSP wordt opgenomen onder het Domein Overheid van de hiërarchie van de PKI voor de overheid. Het hoogste vertrouwenspunt is de Root CA van de Staat der Nederlanden. Beide laatstgenoemde CA's vallen onder de verantwoordelijkheid van de Policy Authority van de PKI voor de overheid.

[3] Het UZI-register garandeert de relatie naar de abonnee door vast te stellen dat wettelijk vertegenwoordiger of een door de wettelijk vertegenwoordiger gemachtigd persoon de pas voor de pashouder of certificaathouder heeft aangevraagd.



Figuur 2: CA-model

Vanaf 6 december 2007 zijn er onder het domein Staat der Nederlanden Overheid twee takken in de hiërarchie. De 'oude' tak kent een geldigheid tot december 2010. Na 6 december 2007 worden door deze CA's geen eindgebruikercertificaten meer ondertekend. Certificaten die door het UZI-register na die datum worden uitgegeven, zijn ondertekend door de 'nieuwe' tak (die aan de linkerkant in figuur 2 is weergegeven en die wordt gekenmerkt door G2 (generatie 2) in de naam). Uiteraard worden CRL's met certificaten die onder de 'oude' hiërarchie zijn uitgegeven, ondertekend door de CA's uit 'oude' hiërarchie.

1.2 Doel, naam en identificatie Certification Practice Statement (CPS)

1.2.1 Doel CPS

Het CPS van het UZI-register beschrijft op welke wijze invulling wordt gegeven aan de dienstverlening. Het CPS beschrijft de processen, procedures en beheersingsmaatregelen voor het aanvragen, produceren, verstrekken, beheren en intrekken van de certificaten. Met behulp van dit CPS kunnen betrokkenen hun vertrouwen in de door het UZI-register geleverde diensten bepalen. De algemene indeling van dit CPS volgt het model zoals gepresenteerd in Request for Comments 3647. De RFC 3647 geldt internationaal als een de facto standaard.

1.2.2 Verhouding CP en CPS

Voorliggend CPS beschrijft op welke wijze invulling is gegeven aan de eisen in de Certificate Policy's (CP's). In de CP's staat beschreven welke eisen worden gesteld aan de dienstverlening. Het CPS beschrijft hoe deze eisen zijn ingevuld. Het UZI-register geeft certificaten uit binnen het domein Overheid van de hiërarchie van de PKI voor de overheid. De eisen die worden gesteld aan uitgifte en gebruik van een certificaat binnen dit domein zijn beschreven in het Programma van Eisen deel 3a Certificate Policy – Domein Overheid en Bedrijven. Voor 'medewerkerpassen niet op naam' en voor 'servercertificaten' zijn de eisen zoals beschreven in het Programma van Eisen deel 3b Certificate Policy – Services van toepassing.

1.2.3 Naam en verwijzingen

Formeel wordt dit document aangeduid als 'Certification Practice Statement (CPS)', kortweg CPS. Het CPS kan op papier worden opgevraagd bij het in paragraaf 1.5.1 opgenomen contactadres.

De verwijzingen naar het CPS zijn opgenomen in de navolgende tabel.

CPS	Omschrijving
Naamgeving	Certification Practice Statement, UZI-register vX.x
Link	https://www.UZI-register.nl/cps/cps.html
Object Identifier (OID)	2.16.528.1.1007.1.1

Tabel 2: Verwijzingen naar CPS

1.3 Betrokken partijen

Het UZI-register kent de navolgende betrokken partijen:

- uitvoerende organisatie van het UZI-register, inclusief leveranciers van producten en diensten;
- gebruikersgemeenschap bestaande uit:
  - abonnees;
  - certificaathouders / certificaatbeheerders;
  - vertrouwende partijen.

Het agentschap Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) vervult de rol van **CSP** en heeft de eindverantwoordelijkheid voor het leveren van de certificatiediensten. Het CIBG is een agentschap van het ministerie van Volksgezondheid, Welzijn en Sport. Het CIBG in de rol van CSP wordt in voorliggend CPS verder aangeduid als 'het UZI-register'.

1.3.1 Certification Authority (CA)

De CA produceert en publiceert certificaten en certificaat revocatie lijsten (CRL's). De CA verzorgt de productie en publicatie van aangevraagde certificaten op basis van een geauthenticeerd verzoek van de RA. Certificaten worden gepubliceerd direct nadat zij door de CA zijn aangemaakt. De CA publiceert certificaten na intrekking op de CRL's. Certificaten worden op een CRL gepubliceerd nadat de CA een bericht van intrekking van het certificaat heeft ontvangen van een hiertoe bevoegde persoon. Het CIBG heeft de rol van CA uitbesteed aan Getronics PinkRoccade die samen met SDU Identification het fysieke productieproces verzorgt.

1.3.2 Registration Authority (RA)

De RA zorgt voor de verwerking van certificaataanvragen en alle daarbij behorende taken. De RA verzamelt fysiek de identificatiegegevens, controleert en registreert deze en voert de beschreven toetsingscontroles uit. De RA geeft, na de controles, opdracht aan de CA voor het produceren van de UZI-passen en het publiceren van certificaten. Het CIBG vervult de rol van RA. Het CIBG heeft de distributie en uitgifte van de UZI-passen uitbesteed aan Postkantoren BV. Deze organisatie geeft, na verificatie van de identiteit van de certificaathouder, de UZI-pas uit.

1.3.3 Abonnees en certificaathouders

De abonnee is de partij namens wie de certificaathouder handelt bij gebruik van de certificaten. Een abonnee van het UZI-register is een zorgaanbieder of een organisatie die valt onder artikel 9a eerste lid of 9b vierde lid van de Algemene Wet Bijzondere Ziektekosten (AWBZ). In de Wbsn-z worden deze organisaties gedefinieerd als 'indicatieorgaan' In voorliggend CPS worden zij daarom verder aangeduid als 'indicatieorganen'. Het UZI-register kent twee typen abonnees, te weten personen (individuele zorgverleners) en organisaties (zorginstellingen en indicatieorganen). Organisaties en personen die voldoen aan de in bijlage 2 beschreven criteria kunnen zich laten registreren als abonnee van het UZI-register. Alleen abonnees kunnen passen aanvragen. Als een abonnee een individuele zorgverlener is en de pas voor zichzelf aanvraagt, geldt deze zorgverlener tevens als certificaathouder.

Een certificaathouder is een natuurlijk persoon die in het certificaat is gekenmerkt als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is opgenomen. Voor servercertificaten is er feitelijk geen certificaathouder die in het certificaat is opgenomen. De aanvrager van het servercertificaat wordt aangeduid als certificaatbeheerder. De certificaatbeheerder is gerelateerd aan de in het certificaat opgenomen abonnee en voert namens de abonnee handelingen uit ten aanzien van het servercertificaat. De abonnee geeft de certificaatbeheerder opdracht de betreffende handelingen uit te voeren en legt dit vast in een bewijs van certificaatbeheer.

1.3.4 Vertrouwende partijen

Een vertrouwende partij is degene die handelt in vertrouwen op een certificaat. De categorie vertrouwende partijen bestaat uit iedereen die handelt in vertrouwen op certificaten van het UZI-register, met als mogelijke doelen het authenticeren van de zorgaanbieders, verifiëren van een elektronische handtekening of het versleutelen van communicatie met die betreffende partij.

1.4 Certificaatgebruik

Het toepassingsgebied van door het UZI-register uitgegeven certificaten is beperkt tot de gebruikersgemeenschap zoals beschreven in paragraaf 1.3 deel 3a van het Programma van Eisen van de PKI voor de overheid. Deze gebruikersgemeenschap bestaat uit abonnees van het UZI-register en certificaathouders die bij deze abonnees behoren. Daarnaast zijn er vertrouwende partijen, die handelen in vertrouwen op certificaten van de betreffende certificaathouders.

De producten van het UZI-register zijn bedoeld voor zorgaanbieders en indicatieorganen bij elektronische communicatie en toegang tot gegevens. De toepasbaarheid van de certificaten wordt in Tabel 3: Toepassingsgebied certificaten nader toegelicht.

Type certificaat	Doel
Authenticiteitcertificaat	Dit certificaat wordt gebruikt om de certificaathouder en / of abonnee te authenticeren.
Vertrouwelijkheidcertificaat	Dit certificaat wordt gebruikt voor het versleutelen van de communicatie met de certificaathouder of de zorginstelling.
Handtekeningcertificaat (onweerlegbaarheidcertificaat)	Dit certificaat wordt gebruikt om een elektronische handtekening te verifiëren die door de certificaathouder is gezet.
Servercertificaat (gecombineerde authenticatie en vertrouwelijkheid)	Dit certificaat wordt gebruikt voor authenticatie van systemen en het beveiligen van communicatie.

Tabel 3: Toepassingsgebied certificaten

Certificaten mogen alleen voor het aangegeven doel worden gebruikt. Er zijn geen verdere beperkingen aan het gebruik van de certificaten.

1.5 Organisatie beheer CPS

1.5.1 Contactgegevens

Informatie over dit CPS of de dienstverlening van het UZI-register kan worden verkregen via onderstaande contactgegevens. Commentaar op het voorliggend CPS kan worden gericht aan hetzelfde adres.

Contactgegevens UZI-register:

Wijnhaven 16	Postbus 16114
2511 GA Den Haag	2500 BC Den Haag
Tel: 0900-232 4342	Fax: 070 - 340 52 52
info@uzi-register.nl	www.uzi-register.nl

1.5.2 Wijziging en goedkeuring CPS

Het UZI-register heeft het recht het CPS te wijzigen of aan te vullen. Wijzigingen gelden vanaf het moment dat het nieuwe CPS gepubliceerd is. Het management van het UZI-register is verantwoordelijk voor een juiste navolging van de procedure zoals beschreven in paragraaf 9.12 en voor de uiteindelijke goedkeuring van het CPS conform deze procedure.

1.6 Definities en afkortingen

Voor een overzicht van de gebruikte definities en afkortingen wordt verwezen naar bijlage 1.

2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

Het UZI-register publiceert certificaten, als onderdeel van de uitgifteprocedure. Vertrouwende partijen, certificaathouders en abonnees kunnen certificaten raadplegen via de directory dienst.

De directory dienst is op adequate wijze beveiligd tegen manipulatie en is on line toegankelijk. Informatie over de status van een certificaat is door middel van een Certificate Revocation List (CRL) vierentwintig uur per dag en zeven dagen per week te raadplegen.

2.2 Publicatie van CSP informatie

Het UZI-register publiceert CSP informatie op www.uzi-register.nl. Deze locatie biedt onder meer toegang tot de volgende documenten en diensten:

- CPS.
- Consultatienotities en adviesnota's voor wijziging van de CPS.
- Vertrouwende partij voorwaarden.
- Certificate Revocation Lists (CRL's).
- CSP en CA certificaten.
- Directory dienst.

Voor de Certificate Policies (CP) verwijst deze site door naar www.pkioverheid.nl. Om de juiste CP te kunnen identificeren geeft de navolgende tabel de samenhang tussen de passen, de functies van de certificaten, de toepasselijke CP en de Object Identifier (OID) van de CP.

Type certificaat		Toepasselijke CP	OID CP
Pas	Certificaat (functie)		
Zorgverlener	authenticiteit	PvE deel 3a, Certificate Policy – Domein Overheid en Bedrijven	2.16.528.1.1003.1.2.2.1
	handtekening (onweerlegbaarheid)	PvE deel 3a, Certificate Policy – Domein Overheid en Bedrijven	2.16.528.1.1003.1.2.2.2
	vertrouwelijkheid	PvE deel 3a, Certificate Policy – Domein Overheid en Bedrijven	2.16.528.1.1003.1.2.2.3
Medewerker op naam	authenticiteit	PvE deel 3a, Certificate Policy - Domein Overheid en Bedrijven	2.16.528.1.1003.1.2.2.1
	handtekening (onweerlegbaarheid)	PvE deel 3a, Certificate Policy - Domein Overheid en Bedrijven	2.16.528.1.1003.1.2.2.2
	vertrouwelijkheid	PvE deel 3a, Certificate Policy - Domein Overheid en Bedrijven	2.16.528.1.1003.1.2.2.3
Medewerker niet op naam	authenticiteit	PvE, deel 3b, Certificate Policy - Services	2.16.528.1.1003.1.2.2.4
	vertrouwelijkheid	PvE, deel 3b, Certificate Policy - Services	2.16.528.1.1003.1.2.2.5
Server	authenticiteit en vertrouwelijkheid	PvE, deel 3b, Certificate Policy - Services	2.16.528.1.1003.1.2.2.6

Tabel 4: Overzicht certificaten met OID van toepasselijke CP

2.3 Publicatie van certificaat

Certificaten worden gepubliceerd zoals bepaald in de Wbsn-z en nadere regelgeving.

2.4 Frequentie van publicatie

Certificaten worden gepubliceerd als onderdeel van het uitgifteproces. De CRL-uitgiftefrequentie is drie uur.

2.5 Toegang tot publicatie

Gepubliceerde informatie is publiek van aard en vrij toegankelijk. De gepubliceerde informatie kan vierentwintig uur per dag en zeven dagen per week worden geraadpleegd.

3 Identificatie en authenticatie

3.1 Naamgeving

Deze paragraaf beschrijft op welke wijze de identificatie en authenticatie van certificaataanvragers plaatsvindt tijdens de initiële registratieprocedure en welke criteria het UZI-register stelt ten aanzien van de naamgeving.

3.1.1 Soorten naamformaten

Alle certificaten die door het UZI-register worden uitgegeven, bezitten een 'subject'-veld (DistinguishedName) waarin de benaming van de houder is opgenomen. Dit veld is opgebouwd uit (X.500) attributen en als volgt gevuld:

Attribuut	Zorgverlener	Medewerker op naam	Medewerker niet op naam	Server
Country (C)	'NL'	'NL'	'NL'	'NL'
Organization (O)	Naam abonnee	Naam abonnee	Naam abonnee	Naam abonnee
OrganizationalUnit (OU)	(veld ontbreekt voor dit pastype)	(veld ontbreekt voor dit pastype)	Afdeling	Afdeling (optioneel)
Title (T)	Aanspreektitel zorgverlener (beroepstitel, opleidingstitel of specialisme)	Niet van toepassing	Niet van toepassing	Niet van toepassing
CommonName (CN)	Voornamen, tussenvoegsel en geboortenaam zorgverlener	Voornamen, tussenvoegsel en geboortenaam medewerker	Functienaam medewerker	Systeemnaam
SerialNumber	UZI-nummer	UZI-nummer	UZI-nummer	UZI-nummer

Tabel 5: Benaming certificaathouder in UZI-certificaten (subject.DistinguishedName)

Namen van personen opgenomen in het Certificaat voldoen aan het naamformaat zoals gedefinieerd in 'NEN 1888:2002 (nl), Algemene persoonsgegevens; Definities, tekensets en uitwisselingsformats' van het NEN.

Naast de hiervoor aangegeven attributen worden geen andere attributen gebruikt. Een toelichting op de overige onderdelen van de certificaten is opgenomen in hoofdstuk 7.

3.1.2 Noodzaak betekenisvolle benaming

Naamgeving die in de uitgegeven certificaten wordt gehanteerd is ondubbelzinnig, zodanig dat het voor de vertrouwende partij mogelijk is de identiteit van de certificaathouder of abonnee onomstotelijk vast te stellen.

3.1.3 Anonimiteit of pseudonimiteit van certificaathouders

Het UZI-register staat het gebruik van pseudoniemen in abonneeregistratie of in pasaanvragen niet toe.

3.1.4 Richtlijnen voor het interpreteren van de diverse naamvormen

Voor de interpretatie van de benaming zijn de volgende punten relevant:

- Voor zorgverleners en medewerkers op naam bevat de commonName de geboortenaam inclusief voorvoegsels en voornamen, zoals opgenomen in het bij registratie voorgelegde identificatiedocument. Als identificatiedocument gelden bij artikel 1 van de Wet op de identificatieplicht (WID) aangewezen geldige documenten. Het rijbewijs is hierbij uitgesloten omdat dit in de meeste gevallen niet alle volledige voornamen bevat.

- In de commonName worden in principe alle voornamen volledig vermeld conform het bij registratie overlegde identificatiedocument. Als de zo ontstane commonName meer karakters bevat dan technisch mogelijk is, zullen één of meer voornamen worden vervangen door voorletters, te beginnen bij de laatste volledig voornaam, net zo lang tot de op deze wijze ontstane commonName wel past.
- Naam abonnee bevat de naam zoals deze op het bij registratie overlegde document voor identificatie van de organisatie voorkomt. Als de abonnee een individuele zorgverlener is, wordt de commonName van de individuele zorgverlener opgenomen.
- Afdeling bevat de door de abonnee opgegeven afdelingsnaam. Deze wordt door het UZI-register niet getoetst.
- Functienaam medewerker bevat een door de abonnee opgegeven functienaam. Het UZI-register stelt hierbij als eis dat de functienaam geen benaming mag bevatten die (geheel of gedeeltelijk) gelijk is aan, lijkt op, of de indruk wekt van een beschermde beroepstitel, opleidingstitel of specialisme. Een lijst van beschermde beroepstitels, opleidingstitels en specialismen is opgenomen in bijlage 3 van het CPS.
- Systeemnaam (ook wel aangeduid als volledige domeinnaam) bevat de fully qualified domainname (fqdn) van het systeem.

Alle namen worden in principe exact overgenomen uit de overlegde identificatiedocumenten. Het kan echter zijn dat in de naamgegevens bijzondere tekens voorkomen die geen deel uitmaken van de standaard tekenset conform ISO8859-1 (Latin-1)[4]. Als in de naam tekens voorkomen die geen deel uitmaken van deze tekenset, zal het UZI-register een transitie uitvoeren. Als namen langer zijn dan in de certificaten is toegestaan, maakt het UZI-register gebruik van de afbreekregels conform 'NEN 1888:2002 (nl), 'Algemene persoonsgegevens; Definities, tekensets en uitwisselingsformats' van het NEN. Dit betekent dat de laatste positie van een veld wordt vervangen door een koppelteken. Het UZI-register behoudt zich het recht voor om bij registratie de aangevraagde naam aan te passen als dit juridisch of technisch noodzakelijk is.

3.1.5 Uniciteit van namen

Het UZI-register garandeert dat de uniciteit van het 'subject'-veld wordt gewaarborgd. Hetgeen betekent dat de onderscheidende naam die is gebruikt in een uitgegeven certificaat, nooit kan worden toegewezen aan een ander subject. Dit gebeurt door middel van het UZI-nummer dat is opgenomen in het subject.serialNumber (zie hoofdstuk 7 voor een verdere toelichting).

Voor de 'zorgverlener' en de 'medewerker op naam' is het UZI-nummer uniek gekoppeld aan de natuurlijk persoon. Een eventuele nieuwe pasaanvraag voor dezelfde natuurlijke persoon, zal hetzelfde UZI-nummer bevatten. Als een 'zorgverlener' of 'medewerker op naam' voor verschillende instellingen passen aanvraagt, zullen deze hetzelfde UZI-nummer bevatten. Alleen als de voornamen, (voorvoegsels) geboortenaam, geboortedatum of geboorteplaats van een persoon wijzigen, krijgt deze persoon een nieuw UZI-nummer. In de pas voor de 'medewerker niet op naam' en in de servercertificaten is het UZI-nummer gekoppeld aan de UZI-pas. Bij elke nieuwe pasaanvraag wordt een nieuw UZI-nummer gegenereerd. Het UZI-register genereert voor alle pastypen het UZI-nummer uit dezelfde nummerreeks.

In gevallen waarin partijen het oneens zijn over het gebruik van namen, beslist het management van het UZI-register na afweging van de betrokken belangen, voor zover hierin niet wordt voorzien door dwingend Nederlands recht of overige toepasselijke regelgeving.

Het UZI-register behoudt zich het recht voor om bij registratie de aangevraagde naam aan te passen als dit juridisch of technisch noodzakelijk is.

[4] De door het UZI-register gebruikte tekenset kent de meeste diakritische tekens. Alleen bijzondere tekens bijvoorbeeld een Y met trema maken geen deel uit van deze set.

3.1.6 Erkenning, authenticatie en de rol van handelsmerken
De naam van een organisatorisch verband zoals genoemd in het uittreksel van een erkend register, een oprichtingsakte, een notariële akte, een instellingsbesluit, een vergunning of in de wet, wordt overgenomen bij registratie en gebruikt in de certificaten. Organisatorische verbanden die geen rechtspersoon zijn, leggen hun naam vast in een eigenverklaring.

Aanvragers dragen de volledige verantwoordelijkheid voor eventuele juridische gevolgen van het gebruik van de door hen opgegeven naam. Het UZI-register neemt bij het gebruik van merknamen de nodige zorgvuldigheid in acht maar is niet gehouden een onderzoek in te stellen naar mogelijke inbreuken op handelsmerken als gevolg van het gebruik van een naam die deel uitmaakt van de in het certificaat opgenomen gegevens. Het UZI-register behoudt zich het recht voor om de aangevraagde naam aan te passen als deze in strijd zou kunnen zijn met het merkenrecht.

3.2 Initiële identiteitsvalidatie

3.2.1 Bewijs van bezit 'private sleutel behorend bij het uit te geven certificaat'
De sleutelparen worden in een gecontroleerde en afgeschermde ruimte, als onderdeel van de personalisatieprocedure in een cryptografische module gegenereerd en vervolgens via een beveiligde communicatiesessie in de smartcard geïnjecteerd. De persoonlijke sleutel kan de smartcard niet verlaten.

De sleutelparen voor servercertificaten worden niet centraal gegenereerd, maar gegenereerd door de certificaatbeheerder van de abonnee. Een aanvraag voor certificering van een publieke sleutel van een servercertificaat wordt ondertekend met de bijbehorende private sleutel. Hiermee toont de certificaatbeheerder het bezit van de private sleutel aan.

3.2.2 Authenticatie van organisatorische identiteit
Als een organisatie een aanvraag indient om als abonnee geregistreerd te worden in het UZI-register dient het volgende te worden overlegd:

- Een volledig ingevuld en door de aanvrager van de registratie ondertekend aanvraagformulier met daarin
  - de volledige naam en van de organisatie;
  - de adresgegevens van de organisatie;
  - de volledige naam (volledige voornamen, voorvoegsels geboortenaam, geboortenaam, voorvoegsels achternaam en achternaam) en contactgegevens van de aanvrager van de registratie[5];
  - de volledige naam en contactgegevens van de medewerker of medewerkers die namens de organisatie UZI-passen mogen aanvragen en intrekken (de pasaanvrager[6]);
  - (optioneel aan te leveren) de AGB-code (zorginstellingcode of praktijkcode).
- Bewijs dat de naam van de organisatorische entiteit actueel en correct is. Dit bewijs heeft de vorm van:
  - het registratienummer waaronder de organisatorische entiteit is geregistreerd in het Handelsregister van de Kamer van Koophandel en waaruit de juistheid van de naam blijkt;
  - kopie van een oprichtingsakte of notariële akte;
  - kopie van de overeenkomst gemeenschappelijk uitvoeringsorgaan (GUO);
  - door alle betrokkenen ondertekende eigenverklaring (alleen te overleggen als de organisatie geen rechtspersoonlijkheid heeft).

[5] Persoon wordt wel aangeduid met de term 'wettelijk vertegenwoordiger'.
[6] Persoon wordt ook wel aangeduid met de term 'aanvrager (gemachtigde)'.

- Bewijs dat de aanvrager bevoegd is de organisatie te vertegenwoordigen. Dit bewijs heeft de vorm van:
  - het registratienummer waaronder de organisatorische entiteit is geregistreerd in het Handelsregister van de Kamer van Koophandel en waaruit de bevoegdheid blijkt;
  - kopie van een oprichtingsakte of notariële akte;
  - afschrift van de benoeming van de wettelijk vertegenwoordiger als zodanig;
  - door alle betrokkenen ondertekende eigenverklaring (alleen te overleggen als de organisatie geen rechtspersoonlijkheid heeft).
- Bewijs dat de namen van de in het aanvraagformulier genoemde personen correct zijn. Dit bewijs dient te worden overlegd in de vorm van een kopie van een identificatiedocument zoals genoemd in de Wet op de identificatieplicht (WID). Het rijbewijs is hierbij uitgesloten omdat dit in de meeste gevallen niet alle volledige voornamen bevat. Het overlegde identificatiedocument moet op de datum van registratie geldig zijn. Het UZI-register archiveert de kopieën van de overlegde identificatiedocumenten.
- Bewijs dat de organisatorische entiteit behoort tot het domein van het UZI-register. Voor een nadere toelichting wordt verwezen naar bijlage 2. Organisaties die zijn opgenomen in het register van toegelaten instellingen in het kader van de Wet Toelating Zorginstellingen (WTZi) of in het Apothekenregister in het kader van de Geneesmiddelenwet behoren tot het domein en hoeven hiervoor geen bewijzen te overleggen. Als de organisatie niet is opgenomen in het register WTZi of het Apothekenregister, moet bewijs worden overlegd in de vorm van:
  - kopie van een oprichtingsakte of notariële akte;
  - afschrift van een vergunning of beschikking;
  - door alle betrokkenen ondertekende eigenverklaring (alleen te overleggen als de organisatie geen rechtspersoonlijkheid heeft).

Het UZI-register controleert de overlegde documenten op echtheid, volledigheid en juistheid. Het UZI-register controleert of een eventueel opgegeven AGB-code overeenkomt met de AGB-code in de registratie van Vektis. Het UZI-register controleert of de organisatie behoort tot het domein van het UZI-register (zie bijlage 2). Als het bewijs hiervan wordt overlegd in de vorm van een eigenverklaring, zal het UZI-register, voordat registratie plaatsvindt, steekproefsgewijs onderliggende bewijzen opvragen. Het UZI-register stelt de abonnee op de hoogte van de registratie of afwijzing van het verzoek tot registratie. Bij een afwijzing wordt de reden van afwijzing vermeld.

3.2.3 Authenticatie van persoonlijke identiteit

Authenticatie van de persoonlijke identiteit vindt plaats bij registratie als abonnee en bij uitgifte van een UZI-pas.

Registratie persoon als abonnee

Als een individuele zorgverlener een aanvraag indient om als abonnee geregistreerd te worden in het UZI-register dient het volgende te worden overlegd:

- Een volledig ingevuld en door de individuele zorgverlener ondertekend aanvraagformulier met daarin
  - de volledige naam (volledige voornamen, voorvoegsels geboortenaam, geboortenaam, voorvoegsels achternaam en achternaam) en contactgegevens (inclusief e-mail adres) van de zorgverlener;
  - de beroepstitel of opleidingstitel van de zorgverlener en de referentie naar de te hanteren toetsingscriteria (zie bijlage 2);
  - (optioneel aan te leveren) de AGB-code van de zorgverlener;
  - de adresgegevens van de zorgverlener.

- Bewijs dat de naamgegevens van de in het aanvraagformulier genoemde persoon correct zijn. Dit bewijs dient te worden overlegd in de vorm van een kopie van een identificatiedocument zoals genoemd in de WID. Op het overlegde identificatiedocument moeten alle voornamen voluit zijn opgenomen. Het rijbewijs is uitgesloten omdat dit in de meeste gevallen niet alle volledige voornamen bevat. Het identificatiedocument moet op de datum van registratie geldig zijn. Het UZI-register neemt de voornamen, voorvoegsels geboortenaam en de geboortenaam over uit het identificatiedocument en zal de kopie van het identificatiedocument archiveren.
- Beroepsbeoefenaren als bedoeld in artikel 34 van de Wet BIG die niet zijn geregistreerd bij de Stichting Kwaliteitsregister Paramedici moeten als bewijs dat zijn de opleidingstitel mogen voeren ook een origineel gewaarmerkte kopie van het betreffende diploma overleggen.

Het UZI-register controleert de overlegde documenten op echtheid, volledigheid en juistheid. Het UZI-register controleert of de aanvrager kan worden aangemerkt als zorgverlener (zie bijlage 2). Het UZI-register controleert of de eventueel opgegeven AGB-code overeenkomt met de AGB-code van de persoon in de registratie van Vektis. Het UZI-register stelt de abonnee op de hoogte van de registratie of afwijzing van het verzoek tot registratie. Bij een afwijzing wordt de reden van afwijzing vermeld.

Aanvraag en uitgifte van UZI-pas

Een aanvraag van UZI-passen dient te worden gedaan door (een pasaanvrager namens) de abonnee. De te overleggen documenten zijn afhankelijk van het type pas dat wordt aangevraagd en worden hierna weergegeven.

Zorgverlenerpas

- Een volledig ingevuld en door de pasaanvrager van de abonnee ondertekend aanvraagformulier met daarin:
  - de naam van de abonnee;
  - het abonneenummer;
  - de naam van de pasaanvrager namens de abonnee;
  - de volledige naam en contactgegevens (inclusief e-mail adres)van de zorgverlener waarvoor de pas wordt aangevraagd;
  - de beroepstitel of opleidingstitel en een eventueel specialisme van de zorgverlener waarvoor de pas wordt aangevraagd en de referentie naar de te hanteren toetsingscriteria;
  - (optioneel) de AGB-code van de zorgverlener waarvoor de pas wordt aangevraagd.
- Een recente pasfoto van de zorgverlener waarvoor de pas wordt aangevraagd. Deze pasfoto dient te voldoen aan de door het UZI-register gestelde kwaliteitseisen.
- Bewijs dat de naamgegevens van de beoogd pashouder correct zijn. Dit bewijs dient te worden overlegd in de vorm van een kopie van een identificatiedocument zoals genoemd in de WID. Op het overlegde identificatiedocument moeten alle voornamen voluit zijn opgenomen. Het rijbewijs is uitgesloten omdat dit in de meeste gevallen niet alle volledige voornamen bevat. Het identificatiedocument moet op de datum van registratie geldig zijn. Het UZI-register neemt de voornamen, voorvoegsels geboortenaam en de geboortenaam over uit het identificatiedocument en zal de kopie van het identificatiedocument archiveren.
- Beroepsbeoefenaren als bedoeld in artikel 34 van de Wet BIG die niet zijn geregistreerd bij de Stichting Kwaliteitsregister Paramedici moeten als bewijs dat zij de opleidingstitel mogen voeren ook een origineel gewaarmerkte kopie van het betreffende diploma overleggen.

- Beroepsbeoefenaren die het specialisme apotheekhoudend huisarts in het certificaat willen opnemen, dienen een kopie van de vergunning voor het houden van de apotheek te overleggen.
- Bij het uitreiken van de pas dient de zorgverlener persoonlijk te verschijnen en een origineel identificatiedocument te overleggen. Bij het uitreiken controleert het UZI-register of de pasfoto op de UZI-pas en de pasfoto op het overlegde identificatiedocument overeenstemmen met de fysieke verschijning.

Medewerkerpas op naam

- Een volledig ingevuld en door de pasaanvrager van de abonnee ondertekend aanvraagformulier met daarin:
  - de naam van de abonnee;
  - het abonneenummer;
  - de naam van de pasaanvrager namens de abonnee;
  - de volledige naam en contactgegevens (inclusief e-mail adres)van de medewerker waarvoor de pas wordt aangevraagd.
- Een recente pasfoto van de medewerker waarvoor de pas wordt aangevraagd. Deze pasfoto dient te voldoen aan de door het UZI-register gestelde kwaliteitseisen.
- Bewijs dat de naamgegevens van de beoogd pashouder correct zijn. Dit bewijs dient te worden overlegd in de vorm van een kopie van een identificatiedocument zoals genoemd in de WID. Op het overlegde identificatiedocument moeten alle voornamen voluit zijn opgenomen. Het rijbewijs is uitgesloten omdat dit in de meeste gevallen niet alle volledige voornamen bevat. Het identificatiedocument moet op de datum van registratie geldig zijn. Het UZI-register neemt de voornamen, voorvoegsels geboortenaam en de geboortenaam over uit het identificatiedocument en zal de kopie van het identificatiedocument archiveren.
- Bij het uitreiken van de pas dient de medewerker persoonlijk te verschijnen en een origineel identificatiedocument te overleggen. Bij het uitreiken controleert het UZI-register of de pasfoto op de UZI-pas en de pasfoto op het overlegde identificatiedocument overeenstemmen met de fysieke verschijning.

Medewerkerpas niet op naam

- Een volledig ingevuld en door de pasaanvrager van de abonnee ondertekend aanvraagformulier met daarin:
  - de naam van de abonnee;
  - het abonneenummer;
  - de naam van de pasaanvrager namens de abonnee;
  - de functienaam waarvoor de pas wordt aangevraagd.
- Bij het uitreiken van de pas dient de pasaanvrager van de abonnee persoonlijk te verschijnen en een geldig identificatiedocument zoals genoemd in de WID te overleggen.

Servercertificaat

- Een volledig ingevuld en door de pasaanvrager van de abonnee ondertekend aanvraagformulier met daarin:
  - de naam van de abonnee;
  - het abonneenummer;
  - de naam van de pasaanvrager namens de abonnee;
  - de naam van het systeem of de server waarvoor certificaten worden aangevraagd.
- Als een abonnee zelf geen eigenaar is van een domeinnaam, kan hij deze wel gebruiken als er een verklaring wordt overlegd waaruit blijkt dat de eigenaar van de domeinnaam hiervoor toestemming verleent.

In alle gevallen controleert het UZI-register de overlegde documenten op echtheid, volledigheid en juistheid. Het UZI-register controleert aan de hand van de overlegde documenten of de aanvrager daadwerkelijk gemachtigd is de pas aan te vragen. Bij aanvraag van een UZI-pas voor een zorgverlener controleert het UZI-register bovendien of de beoogd certificaathouder kan worden aangemerkt als zorgverlener (zie bijlage 2) en of de eventueel opgegeven AGB-code overeenkomt met de AGB-code van de persoon in de registratie van Vektis. Bij aanvraag van servercertificaten voor een domeinnaam, controleert het UZI-register bij de erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) of de abonnee de eigenaar is van de domeinnaam. Het UZI-register stelt de abonnee op de hoogte van de uitgifte van de pas of de afwijzing van de pasaanvraag. Als de pasaanvraag wordt afgewezen, wordt de reden van afwijzing vermeld.

3.2.4 Niet geverifieerde gegevens
Het UZI-register verifieert de naam van de abonnee aan de hand van erkende documenten (zie paragraaf 3.2.2 en 3.2.3. Van organisatorische verbanden die geen rechtspersoon zijn, neemt het UZI-register de naam over uit de eigenverklaring.

Het UZI-register verifieert alle gegevens die worden opgenomen in het certificaat, met uitzondering van de velden 'functienaam' en 'afdeling'. Gegevens die alleen voor correspondentiedoeleinden worden vastgelegd, zoals correspondentienaam, academische titels en telefoonnummers worden niet geverifieerd. Gegevens die niet worden geverifieerd, neemt het UZI-register over uit het door een gemachtigd aanvrager namens de abonnee ondertekend aanvraagformulier.

3.2.5 Autorisatie certificaathouder
Bij registratie van de abonnee legt het UZI-register vast welke personen UZI-passen mogen aanvragen voor de abonnee. Alleen een wettelijk vertegenwoordiger kan aangeven wie namens de abonnee passen mag aanvragen. De wijze van authenticatie van de wettelijk vertegenwoordiger is beschreven in paragraaf 3.2.2. Bij een pasaanvraag controleert het UZI-register aan de hand van een kopie van een identiteitsbewijs of de aanvraag is ondertekend door een geautoriseerd pasaanvrager.

De certificaathouder of de pasaanvrager namens de abonnee zijn verplicht om per direct een verzoek tot intrekking in te dienen bij het UZI-register in de volgende omstandigheden:
- verlies, diefstal of onklaar raken van de drager van het certificaat (UZI-pas);
- geconstateerd of vermoeden van misbruik of compromitteren;
- definitieve blokkering van de smartcard (als driemaal een foutieve PUK-code is ingevoerd);
- beëindiging bestaan abonnee of beëindiging dienstverband of schorsing certificaathouder;
- onjuistheden in of wijziging van de gegevens die op de certificaten vermeld staan;
- niet meer voldoen aan toetsingscriteria conform bijlage 2;
- systeem / server niet meer in gebruik bij de zorginstelling;
- toestemming om de domeinnaam te gebruiken is ingetrokken.

Als de certificaathouder niet in staat is om de eigen certificaten in te trekken, dan dient hij of zij zich met het verzoek tot intrekking direct en zonder vertraging te wenden tot de aanvrager namens de abonnee.

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

3.3.1 Routinematige vernieuwing van het certificaat
De procedures en controles rondom identificatie en authenticatie bij vernieuwing van het certificaat zijn gelijk aan die bij initiële registratie. Voor vernieuwing van het certificaat kan gebruik gemaakt worden van een aanvraagformulier voor certificaatvernieuwing. In dit formulier

wordt naast het UZI-nummer van de pashouder een beperkte set gegevens is opgevraagd. Gegevens die al bekend zijn bij het UZI-register, hoeven niet opnieuw te worden aangeleverd. Als bij de aanvraag van vernieuwing een UZI-nummer wordt opgegeven, is het niet nodig bewijs te overleggen van de juistheid van de naamgegevens van de beoogd pashouder. Beroepsbeoefenaren als bedoeld in artikel 34 van de Wet BIG, hoeven niet opnieuw een kopie van hun diploma te overleggen. Bij de uitvoering van een vernieuwingsverzoek wordt altijd een nieuw sleutelpaar gegenereerd. Indien van toepassing wordt tevens een nieuwe smartcard uitgegeven. Bij het vernieuwen van certificaten wordt altijd vooraf een controle uitgevoerd of is voldaan aan alle eisen uit paragraaf 3.1 en 3.2. De uitgifte is gelijk aan de initiële uitgifte.

3.3.2 Vernieuwing van sleutels na intrekking van het certificaat

Het vernieuwen van sleutels na intrekking van het certificaat vindt plaats conform een eerste aanvraag. Voor vernieuwing van het certificaat kan gebruik gemaakt worden van een aanvraagformulier voor certificaatvernieuwing. In dit formulier wordt naast het UZI-nummer van de pashouder een beperkte set gegevens is opgevraagd. Gegevens die al bekend zijn bij het UZI-register, hoeven niet opnieuw te worden aangeleverd. Als bij de aanvraag van vernieuwing een UZI-nummer wordt opgegeven, is het niet nodig bewijs te overleggen van de juistheid van de naamgegevens van de beoogd pashouder. Beroepsbeoefenaren als bedoeld in artikel 34 van de Wet BIG die niet zijn geregistreerd bij de Stichting Kwaliteitsregister Paramedici, hoeven niet opnieuw een kopie van hun diploma te overleggen. Bij de uitvoering van een vernieuwingsverzoek wordt altijd een nieuw sleutelpaar gegenereerd. Indien van toepassing wordt tevens een nieuwe smartcard uitgegeven. Bij het vernieuwen van certificaten wordt altijd vooraf een controle uitgevoerd of is voldaan aan alle eisen uit paragraaf 3.1 en 3.2. De uitgifte van het certificaat is gelijk aan de initiële uitgifte.

3.4 Identificatie en authenticatie bij verzoeken tot intrekking

De certificaathouder of een gemachtigd aanvrager namens de abonnee kunnen verzoeken tot intrekking indienen. Verzoeken tot intrekking kunnen worden gedaan telefonisch, per post, per fax, per e-mail of elektronisch. Het telefonisch intrekken van servercertificaten is niet mogelijk.

- Bij **elektronische** intrekking vindt identificatie en authenticatie plaats op basis van smartcardnummer en intrekkingcode. De intrekkingcode wordt bij uitgifte van de pas schriftelijk ter beschikking gesteld aan de certificaathouder.
- Bij **telefonische** intrekking vindt identificatie en authenticatie plaats op basis van een toetsing van bij het UZI-register aanwezige gegevens. De aanvrager van de intrekking moet tenminste een aantal vooraf vastgestelde gegevens over de pashouder en de betrokken pas kunnen verstrekken. Telefonisch intrekken van servercertificaten is niet mogelijk.
- Bij intrekking per **post** of per **fax** vindt identificatie en authenticatie plaats op basis van:
    - Een door de tot intrekking bevoegde persoon ondertekend verzoek.
    - Bewijs van de identiteit van de indiener van het intrekkingverzoek. Dit bewijs dient te worden overlegd in de vorm van een kopie van een identificatiedocument zoals genoemd in de WID. Het identificatiedocument moet op de datum van het intrekkingsverzoek geldig zijn. Het UZI-register zal de kopie van het identificatiedocument archiveren.
- Bij intrekking via **e-mail** gelden dezelfde eisen als bij intrekking per post of per fax. Daarboven wordt als eis gesteld dat het verzoek moet worden ingediend in een niet-muteerbare vorm (zoals PDF of JPG).

Het UZI-register controleert of de indiener van het intrekkingverzoek bevoegd is de aanvraag te doen. Tevens controleert het UZI-register de identiteit van de indiener van het intrekkingverzoek aan de hand van het overlegde identiteitsbewijs en een reeds eerder gearchiveerde kopie van het identiteitsbewijs.

4 Operationele eisen certificaatlevenscyclus

4.1 Aanvraag van certificaten

Aanvragen voor certificaten kunnen alleen worden gedaan door geregistreerde aanvragers. Deze aanvragers zijn zelf abonnee van het UZI-register of zijn door de wettelijk vertegenwoordiger van de abonnee gemachtigd om aanvragen te doen. Aanvragen worden altijd schriftelijk gedaan. PKCS#10 bestanden kunnen via e-mail of op een elektronische gegevensdrager per post worden verstuurd.

Het UZI-register controleert de aanvragen en is verantwoordelijk voor de fysieke aanvraag en productie. Na afronding van de registratie van de aanvraag geeft de RA opdracht tot productie van de UZI-pas. De CA genereert de certificaten en publiceert deze. Het UZI-register informeert de beoogd certificaathouder dat, waar en hoe de UZI-pas kan worden afgehaald (afhaalbewijs). Het UZI-register verstuurt de UZI-pas naar het uitgiftepunt. Op het uitgiftepunt wordt de pas veilig bewaard.

4.2 Werkwijze met betrekking tot aanvraag van certificaten

Voordat certificaten kunnen worden aangevraagd, dient de abonnee geregistreerd te worden bij het UZI-register. Hiervoor worden de volgende stappen doorlopen:

- De beoogd abonnee overlegt een volledig ingevuld en ondertekend aanvraagformulier inclusief de in paragraaf 3.2 aangegeven documenten. De beoogd abonnee kan formulieren via de website van het UZI-register invullen of kan deze aanvragen bij het UZI-register. De abonnee neemt via het CPS kennis van alle toepasbare voorwaarden.
- Het UZI-register voert de in paragraaf 3.2 aangegeven controles uit en stelt de abonnee op de hoogte van het resultaat.

Een abonnee van het UZI-register kan UZI-passen aanvragen. Hiervoor worden de volgende stappen doorlopen:

- De gemachtigd aanvrager overlegt een volledig ingevuld en ondertekend aanvraagformulier inclusief de in paragraaf 3.2.3 aangegeven documenten. De aanvrager kan formulieren verkrijgen via de website van het UZI-register. De aanvrager en de beoogd certificaathouder nemen via het CPS en de vertrouwende partij voorwaarden kennis van alle relevante voorwaarden.
- Het UZI-register voert de in paragraaf 3.2 aangegeven controles uit en stelt de abonnee op de hoogte van de uitgifte van de pas of de afwijzing van de pasaanvraag. Als de pasaanvraag wordt afgewezen, wordt de reden van afwijzing vermeld.

Het UZI-register archiveert de overlegde documenten voor eventuele bewijsvoering bij reconstructie.

Het UZI-register hanteert voor de maximale doorlooptijd vanaf het ontvangst van de complete aanvraag tot aan het beschikbaar zijn van de pas voor uitgifte op het uitgiftepunt een termijn van maximaal acht weken, wat op grond van de Algemene wet bestuursrecht (Awb) aangemerkt wordt als een redelijke termijn.

4.3 Uitgifte van certificaten

De wijze van uitgifte verschilt voor de verschillende pastypen. Per pastype is hierna de werkwijze van het UZI-register beschreven.

Zorgverlenerpas en Medewerkerpas op naam
De pas voor de zorgverlener en de medewerker op naam wordt uitgereikt op basis van direct verschijnen door de beoogd certificaathouder.

- De beoogd certificaathouder dient persoonlijk te verschijnen bij het uitgiftepunt. De beoogd certificaathouder overlegt een afhaalbewijs en een geldig identificatiedocument zoals genoemd in de WID.
- De medewerker van het uitgiftepunt controleert de geldigheid en echtheid van de overlegde documenten. Aan de hand van de foto op de pas, de foto in het identificatiedocument en de fysieke verschijning voert de medewerker een identiteitscontrole van de beoogd houder uit. Tenslotte controleert de medewerker of de persoon op basis van het overlegde afhaalbewijs de bevoegde persoon is om de betreffende UZI-pas op te halen.
- Bij een positief resultaat op alle controles ondertekent de beoogd certificaathouder het afhaalbewijs. De medewerker van het uitgiftepunt controleert de handtekening aan de hand van het overlegde identificatiedocument.
- Na ondertekening wordt de UZI-pas overhandigd en wordt de datum en het tijdstip van overhandigen vastgelegd. Beide partijen ontvangen hiervan een bewijs.
- Bij een negatief resultaat op een van de controles of als de beoogd houder het afhaalbewijs niet ondertekent, wordt de UZI-pas niet uitgereikt.

Medewerkerpas niet op naam
De pas voor de medewerker niet op naam wordt uitgereikt op basis van indirect verschijnen. De certificaathouder wordt vertegenwoordigd door een gemachtigd pasaanvrager van de abonnee.

- De pasaanvrager van de abonnee dient persoonlijk te verschijnen bij het uitgiftepunt. De pasaanvrager van de abonnee overlegt een afhaalbewijs en een geldig identificatiedocument zoals genoemd in de WID.
- De medewerker van het uitgiftepunt controleert de geldigheid en echtheid van de overlegde documenten. Aan de hand van het identificatiedocument en de fysieke verschijning voert de medewerker een identiteitscontrole van de pasaanvrager uit. Tenslotte controleert de medewerker of de persoon op basis van het overlegde afhaalbewijs de bevoegde persoon is om de betreffende UZI-pas op te halen.
- Bij een positief resultaat op alle controles ondertekent de pasaanvrager het afhaalbewijs. De medewerker van het uitgiftepunt controleert de handtekening aan de hand van het overlegde identificatiedocument.
- Na ondertekening wordt de UZI-pas overhandigd en wordt de datum en het tijdstip van overhandigen vastgelegd. Beide partijen ontvangen hiervan een bewijs.
- Bij een negatief resultaat op een van de controles of als de pasaanvrager het afhaalbewijs niet ondertekent wordt de UZI-pas niet uitgereikt.

Servercertificaat
De uitgifte van een servercertificaat kent twee varianten. Beide worden toegelicht.

De servercertificaten worden uitgereikt op basis van een door de gemachtigd pasaanvrager met een geavanceerde elektronische handtekening ondertekend verzoek:

- De pasaanvrager stuurt het UZI-register een e-mail met daarin het volledig ingevulde aanvraagformulier. De pasaanvrager ondertekent deze e-mail met een gekwalificeerd onweerlegbaarheidcertificaat (zoals op de UZI-pas voor zorgverleners en medewerkers op naam).
- De medewerker van het UZI-register controleert de overlegde gegevens en voert geldigheidscontroles uit op de handtekening. Na het uitvoeren van de controles en het vastleggen van de gegevens wordt opdracht gegeven tot productie van het servercertificaat.

- Nadat het certificaat is geproduceerd, verstuurt het UZI-register het certificaat per e-mail naar de aanvrager. Daarnaast verstuurt het UZI-register een intrekkingcode naar het correspondentieadres van de abonnee ter attentie van de aanvrager.

De servercertificaten worden uitgereikt na persoonlijk verschijnen van de gemachtigd pasaanvrager van de abonnee:

- De pasaanvrager ontvangt van het UZI-register een meldverzoek. Het UZI-register verstuurt dit meldverzoek na controle en vastlegging van de aanvraag.
- De pasaanvrager van de abonnee dient persoonlijk te verschijnen bij het uitgiftepunt. De pasaanvrager van de abonnee overlegt het meldverzoek en een geldig identificatiedocument zoals genoemd in de WID.
- De medewerker van het uitgiftepunt controleert de geldigheid en echtheid van het overlegde identificatiedocument. De medewerker van het uitgiftepunt legt de identiteitsvaststelling vast op het meldverzoek. De pasaanvrager van de abonnee ondertekent het bewijs van identiteitsvaststelling. Beide partijen ontvangen hiervan een getekend exemplaar.
- Nadat het ondertekende bewijs van identiteitsvaststelling is verwerkt bij het UZI-register wordt opdracht gegeven tot productie van de servercertificaten.
- Nadat het certificaat is geproduceerd, verstuurt het UZI-register het certificaat per e-mail naar de aanvrager. Daarnaast verstuurt het UZI-register een intrekkingcode naar het correspondentieadres van de abonnee ter attentie van de aanvrager.

4.4 Acceptatie van certificaten

De voorwaarden voor het gebruik van certificaten van het UZI-register zijn gepubliceerd in onderhavig CPS.

Door het ondertekenen van het afhaalbewijs bevestigt de certificaathouder de ontvangst van de pas aan het UZI-register. Het UZI-register legt het moment van verstrekking conform het afhaalbewijs vast. Door het in ontvangst nemen van de pas geeft de certificaathouder aan kennis te hebben genomen van en in te stemmen met de rechten en plichten zoals genoemd in het CPS.

Het UZI-register vraagt de aanvrager van een servercertificaat de ontvangst van het certificaat per e-mail te bevestigen. Door bevestiging van de ontvangst van het certificaat geeft de certificaatbeheerder aan kennis te hebben genomen van en in te stemmen met de rechten en plichten zoals genoemd in het CPS. Als een bevestiging van de ontvangst van een certificaat – ook na herhaald verzoek - achterwege blijft, zal het certificaat door het UZI-register worden ingetrokken.

Publicatie van de certificaten vindt plaats in de directory dienst direct na ondertekening van het certificaat door de CA gedurende het productieproces.

4.5 Sleutelpaar en certificaatgebruik

4.5.1 Verplichtingen van abonnee en certificaathouder

De abonnee garandeert expliciet dat de certificaathouders binnen de organisatie de door hem aangevraagde certificaten niet buiten het toepassingsgebied zoals beschreven in hoofdstuk 1.4 van het CPS gebruiken en dat de certificaathouders het juiste certificaat gebruiken voor de juiste toepassing. Wanneer de abonnee zelf certificaathouder is volgt hij dezelfde procedure.

De abonnee en de certificaathouder zijn verplicht om op aanwijzing van het UZI-register het gebruik van de certificaten te staken. Het UZI-register kan een dergelijke aanwijzing geven in het geval dat een CA-sleutel is gecompromitteerd.

De abonnee en de certificaathouder zijn verplicht het UZI-register onmiddellijk op de hoogte te brengen en vervolgens de UZI-pas in te trekken als zich een onregelmatigheid voordoet zoals aangegeven in paragraaf 4.9.1. Dit geldt zowel voor de omstandigheden die worden opgemerkt, of vermoed, door de abonnee, als de omstandigheden die door de certificaathouders binnen de organisatie zelf worden gemeld aan de abonnee.

Indien van toepassing dient de certificaathouder de intrekkingscode, op uitdrukkelijk verzoek van de abonnee, deze aan de abonnee te overleggen.

De abonnee en de pashouder zijn verplicht geschikte maatregelen te nemen om te voorkomen dat de private sleutels onbevoegd worden gebruikt. Hieronder wordt ten minste verstaan dat de UZI-passen worden beschermd tegen beschadiging, verlies en/of diefstal, niet worden uitgeleend aan derden en de UZI-passen in het algemeen worden beveiligd zoals men ook waardevolle persoonlijke eigendommen als creditcards of paspoorten beveiligt. Daarnaast draagt de abonnee er zorg voor dat de PIN-code, PUK-code en de intrekkingscode door de certificaathouders binnen de organisatie altijd apart van de UZI-pas bewaard worden.

Als er sprake is van een defect aan een van de UZI-passen, zal de abonnee direct de certificaathouder binnen de organisatie verzoeken de UZI-pas in te trekken via de website; door middel van de intrekkingcode, of op een andere door het UZI-register aangegeven wijze. Als de abonnee in het bezit is van de intrekkingscode van de certificaathouder binnen de organisatie, dan kan de abonnee zelf de UZI-pas intrekken. Vervolgens zal de abonnee de UZI-pas aan het UZI-register toezenden. Wanneer de abonnee zelf certificaathouder is volgt hij dezelfde procedure.

Verplichtingen met betrekking tot servercertificaten
Als door de abonnee servercertificaten worden aangevraagd gelden de volgende aanvullende verplichtingen:

- De abonnee moet het UZI-register direct schriftelijk bevestigen dat de servercertificaten door hem zijn ontvangen.
- De abonnee is verplicht de sleutels die behoren bij servercertificaten op te slaan in een Secure User Device (SUD). De abonnee dient het SUD waarop de private sleutels worden bewaard te beveiligen op een wijze waarop kritieke bedrijfsmiddelen zijn beveiligd. De abonnee kan hiervan afwijken als er compenserende maatregelen op het gebied van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging, audit en functiescheiding worden getroffen in de omgeving van het systeem dat de sleutels van de servercertificaten bevat. Het is daarbij toegestaan dat de sleutels softwarematig worden beschermd. De compenserende maatregelen moeten van dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren.
- De abonnee dient ervoor te zorgen dat het sleutelmateriaal van de certificaathouders binnen de organisatie van de abonnee uitsluitend gegenereerd wordt in een veilig middel dat voldoet aan EAL 4+ of aan gelijkwaardige beveiligingscriteria.
- De abonnee is verplicht de activeringsgegevens, die worden gebruikt om toegang te krijgen tot de private sleutel(s) van de certificaathouders binnen de organisatie, gescheiden van het SUD te bewaren.

Voorgaande verplichtingen voor de abonnee of certificaathouder zullen worden vastgelegd en, voor zover zij als te onbepaald kunnen worden aangemerkt, nader worden uitgewerkt in richtlijnen van het UZI-register en of nadere regelgeving. Voor zover de bepalingen betrekking hebben op UZI-passen die door een abonnee zijn aangevraagd ten behoeve van de certificaathouder binnen de organisatie van de abonnee, zullen de rechten en verplichtingen tussen de abonnee en de certificaathouder zelf onderling schriftelijk vastgelegd moeten worden.