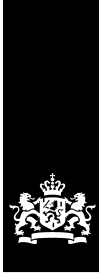


CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Certification Practice Statement (CPS)

UZI-register

Versie 9.5

Datum	01-08-2019
Status	Definitief (UZ52.01)

Inhoud

1 Introductie—12
1.1 UZI-register en producten—12
1.1.2 Introductie UZI-register—12
1.1.3 Soorten passen en certificaten—12
1.1.4 CA-model—14
1.2 Doel, naam en identificatie Certification Practice Statement (CPS)—15
1.2.1 Doel CPS—15
1.2.2 Verhouding CP en CPS—16
1.2.3 Naam en verwijzingen—16
1.3 Betrokken partijen—16
1.3.1 Certification Authority (CA) —16
1.3.2 Registration Authority (RA)—17
1.3.3 Dissemination Service (publicatiedienst)—17
1.3.4 Abonnees—17
1.3.5 Certificaathouders en certificaatbeheerders—17
1.3.6 Vertrouwende partijen—17
1.4 Certificaatgebruik—17
1.4.1 Toegestaan gebruik—17
1.4.2 Niet toegestaan gebruik—18
1.5 Organisatie beheer CPS—18
1.5.1 Contactgegevens—18
1.5.2 Wijziging en goedkeuring CPS—18
1.6 Definities en afkortingen—18

2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats—19
2.1 Elektronische opslagplaats—19
2.2 Publicatie van TSP informatie—19
2.3 Frequentie van publicatie—20
2.4 Toegang tot publicatie—20

3 Identificatie en authenticatie—21
3.1 Naamgeving—21
3.1.1 Soorten naamformaten—21
3.1.2 Noodzaak betekenisvolle benaming—21
3.1.3 Anonimiteit of pseudonimiteit van certificaathouders—21
3.1.4 Richtlijnen voor het interpreteren van de diverse naamvormen—22
3.1.5 Uniciteit van namen—23
3.1.6 Erkenning, authenticatie en de rol van handelsmerken—23
3.2 Initiële identiteitsvalidatie—23
3.2.1 Bewijs van bezit ‘private sleutel behorend bij het uit te geven certificaat’—23
3.2.2 Authenticatie van organisatorische identiteit—24
3.2.3 Authenticatie van persoonlijke identiteit—25
3.2.4 Niet geverifieerde gegevens—29
3.2.5 Autorisatie certificaathouder—29
3.3 Identificatie en authenticatie bij vernieuwing van het certificaat—29
3.3.1 Routinematige vernieuwing van het certificaat—29
3.3.2 Vernieuwing van sleutels na intrekking van het certificaat—30
3.4 Identificatie en authenticatie bij verzoeken tot intrekking—30

4 Operationele eisen certificaatlevenscyclus—32
4.1 Aanvraag van certificaten—32

4.2 Werkwijze met betrekking tot aanvraag van certificaten—32
4.3 Doorlooptijd—33
4.4 Uitgifte van certificaten—33
4.5 Acceptatie van certificaten—35
4.6 Sleutelpaar en certificaatgebruik—35
4.6.1 Verplichtingen van abonnee en certificaathouder—35
4.6.2 Verplichtingen van de vertrouwende partij—37
4.7 Vernieuwen van certificaten—37
4.8 Re-Key van certificaten—37
4.9 Aanpassing van certificaten—37
4.10 Intrekking en opschorting van certificaten—37
4.10.1 Omstandigheden die leiden tot intrekking—38
4.10.2 Wie mag verzoek tot intrekking indienen—39
4.10.3 Procedure voor verzoek tot intrekking—39
4.10.4 Uitstel van verzoek tot intrekking—40
4.10.5 Tijdsduur voor verwerking van verzoek tot intrekking—40
4.10.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie—41
4.10.7 CRL-uitgiftefrequentie—41
4.10.8 Tijd tussen generatie en publicatie—41
4.10.9 On line intrekking / statuscontrole—41
4.10.10 Vereisten online controle intrekkingstatus—42
4.11 Certificaat statusservice—42
4.12 Beëindiging abonnee relatie—42
4.12.1 Overgangstermijn voor een zorgverlener abonnee—42
4.12.2 Overgangstermijn voor een organisatie abonnee—42
4.13 Key escrow en recovery—43

5 Fysieke, procedurele en personele beveiliging—44
5.1 Fysieke beveiliging—44
5.2 Procedurele beveiliging—45
5.2.1 Vertrouwelijke functies—45
5.2.2 Aantal personen benodigd per taak—45
5.2.3 Identificatie en authenticatie met betrekking tot TSP functies—45
5.2.4 Functiescheiding—45
5.3 Personele beveiliging—45
5.3.1 Functie-eisen—45
5.3.2 Antecedentenonderzoek—45
5.3.3 Trainingseisen—46
5.3.4 Opleidingen—46
5.3.5 Frequentie van taak-roulatie en loopbaanplanning—46
5.3.6 Sancties van ongeautoriseerd handelen—46
5.3.7 Inhuur van personeel—46
5.3.8 Beschikbaar stellen documentatie medewerkers—46
5.4 Procedures ten behoeve van beveiligingsaudits—46
5.4.1 Vastleggen van gebeurtenissen—46
5.4.2 Interval uitvoeren loggingen—47
5.4.3 Bewaartermijn loggingen—47
5.4.4 Beveiliging audit logs—47
5.4.5 Bewaren van audit logs—47
5.4.6 Kennisgeving van logging gebeurtenis—47
5.4.7 Kwetsbaarheidsanalyse—47
5.5 Archivering van documenten—48
5.5.1 Gebeurtenissen—48
5.5.2 Bewaartermijn van het archief—48
5.5.3 Beveiliging van het archief—48

5.5.4 Archief back-up procedures—48
5.5.5 Voorwaarden en tijdsaanduiding van vastgelegde gebeurtenissen—48
5.5.6 Archiveringssysteem—49
5.5.7 Het verkrijgen en verifiëren van gearchiveerde informatie—49
5.6 Vernieuwen sleutels na re-key CA—49
5.7 Aantasting en continuïteit—49
5.8 TSP beëindiging—49

6 Technische beveiliging—51
6.1 Genereren en installeren van sleutelparen—51
6.1.1 Genereren van sleutelparen—51
6.1.2 Overdracht van publieke sleutels naar de CA—51
6.1.3 Overdracht van de publieke sleutel van de TSP naar eindgebruikers—52
6.1.4 Doelen van sleutelgebruik (zoals bedoeld in X.509 v3)—52
6.2 Private sleutel bescherming—52
6.2.1 Standaarden voor crytografische modulen—52
6.2.2 Functiescheiding beheer private sleutels—52
6.2.3 Escrow van private sleutels van certificaathouders—52
6.2.4 Back-up van de private sleutels van certificaathouders—52
6.2.5 Archivering van private sleutels van eindgebruikers en TSP—52
6.2.6 Toegang tot private sleutels in cryptografische module—52
6.2.7 Opslag private sleutels—52
6.2.8 Activeren private sleutels—53
6.2.9 Methode voor deactiveren private sleutels—53
6.2.10 Methode voor vernietigen van private sleutels—53
6.2.11 Veilige middelen voor het aanmaken van elektronische handtekeningen—53
6.3 Andere aspecten van sleutelpaar management—53
6.3.1 Archiveren van publieke sleutels—54
6.3.2 Gebruiksduur publieke/private sleutel—54
6.4 Activeringsgegevens—54
6.4.1 Generatie en installatie van activeringsgegevens—54
6.4.2 Bescherming activeringsgegevens—54
6.5 Toegangsbeveiliging van TSP-systemen—55
6.5.1 Algemene systeem beveiligingsmaatregelen—55
6.5.2 Specifieke systeem beveiligingsmaatregelen—55
6.5.3 Beheer en classificatie van middelen—55
6.6 Beheersingsmaatregelen technische levenscyclus—55
6.6.1 Beheersingsmaatregelen systeemontwikkeling—55
6.6.2 Beheersingsmaatregelen beveiligingsmanagement—55
6.6.3 Levenscyclus van beveiligingsclassificatie—56
6.7 Netwerkbeveiliging—56
6.8 Time-stamping—56

7 Certificaat-, CRL- en OCSP-profielen—57
7.1 Certificaatprofielen—57
7.1.1 Basis attributen—57
7.1.2 Extensies—59
7.1.3 E-mailadressen—61
7.1.4 UZI-nummer—61
7.1.5 SubjectAltName.otherName—61
7.2 CRL profielen—63
7.2.1 Attributen—63
7.2.2 Extensies—64
7.2.3 CRL Distribution Points—64
7.2.4 TSP en CA certificaten—64

7.3 OCSP profiel—64
7.3.1 OCSP responder certificaat—64
7.3.2 OCSP responses—65

8 Conformiteitbeoordeling—66
8.1 Auditcyclus—66
8.2 Certificerende instelling—67
8.3 Relatie met certificerende instelling—67
8.4 Onderwerp van audit—67
8.5 Resultaten audit—67
8.6 Beschikbaarheid conformiteitcertificaten—67

9 Algemene bepalingen en voorwaarden—68
9.1 Aanvraag, facturering en betaling van UZI-middelen—68
9.1.1 Tarief verbonden aan uitgifte UZI-middelen—68
9.1.2 *Wijziging tarieven*—68
9.1.3 Inschrijving in het UZI-register—68
9.1.4 Aanvragen UZI-middelen—68
9.1.5 Productie UZI-middel—68
9.1.6 Facturering en betaling—68
9.1.7 Betaaltermijn—69
9.1.8 Geldigheid UZI-middel—69
9.1.9 Levering en ingebruikname UZI-middelen—69
9.1.10 Vervangingsvoorwaarden—69
9.1.11 Risico, eigendom en zorgplicht—69
9.2 Vertrouwelijkheid bedrijfsgegevens—70
9.3 Vertrouwelijkheid persoonsgegevens—70
9.3.1 Vertrouwelijke informatie—70
9.3.2 Niet-vertrouwelijke informatie—70
9.3.3 Vrijgeven van informatie—71
9.4 Intellectuele eigendomsrechten—71
9.5 Aansprakelijkheid en garanties—71
9.5.1 Aansprakelijkheid van de TSP—71
9.5.2 Aansprakelijkheid van abonnees en certificaathouders—72
9.5.3 Aansprakelijkheid van vertrouwende partijen—74
9.6 Uitsluiting van garantie—74
9.7 Beperking van aansprakelijkheid—74
9.8 Schadeloosstelling—75
9.9 Geldigheidstermijn CPS—75
9.10 Communicatie binnen betrokken partijen—76
9.11 Wijzigingen—76
9.11.1 Wijzigingsprocedure—76
9.11.2 Verzoeken tot wijziging en classificatie—76
9.11.3 Publicatie van wijzigingen—76
9.12 Conflictoplossing—76
9.13 Toepasselijk recht—77
9.14 Naleving relevante wetgeving—77
9.15 Overige bepalingen—77

Bijlage 1: Definities en afkortingen—78

Bijlage 2: Toetsingscriteria organisaties en zorgverleners—85

Bijlage 3: Beroepstitels, opleidingstitels en specialismen—91

Lijst met tabellen

Tabel 1 Versiehistorie CPS UZI-register 11
Tabel 2 Toepassingsgebied certificaten 18
Tabel 3 Overzicht certificaten met OID van toepasselijke CP SHA-2 generatie (G21) 19
Tabel 4 Overzicht certificaten met OID van toepasselijke CP Public G3/Private G1 generatie 20
Tabel 5 Benaming certificaathouder in UZI-certificaten (subject.DistinguishedName) 21
Tabel 6 Levensduur CA certificaten SHA-2 generatie (G21). 54
Tabel 7 Levensduur CA certificaten Public G3/Private G1 hiërarchie 54
Tabel 8 Basisattributen certificaatprofielen 58
Tabel 9 Standaard extensies certificaatprofielen 60
Tabel 10 Private extensies certificaatprofielen 61
Tabel 11 <OID CA> productieomgeving UZI-register 62
Tabel 12 Velden <Subject ID> in SubjectAltName.otherName 62
Tabel 13 Toelichting gebruik AGB-code 63
Tabel 14 Attributen CRL
Tabel 15 Extensies CRL 64
Tabel 16 CRL Distribution points gebruikercertificaten UZI-register 64
Tabel 17 Relatie UZI-pas en bevoegdheid 89
Tabel 18 Relatie abonnee en bevoegdheid 89

Lijst met figuren

Figuur 1 Passenmodel en certificaten
Figuur 2 CA-model SHA-2 generatie (G21)
Figuur 3 CA-model generatie Public G3/Private G1

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	06-12-2007	Definitief	Tweede generatie CA hiërarchie.
4.0	01-06-2008	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	01-10-2008	Definitief	Wijziging conform adviesnota d.d. 18-8-2008: - telefonisch intrekken; - verduidelijking beleid m.b.t. fusies; - tekstuele aanpassingen en verduidelijkingen.
4.2	24-02-2011	Definitief	- SHA-2 release. - Einde levensduur eerste generatie CA's. - Tekstuele aanpassingen en verduidelijkingen.
5.0	18-01-2012	Definitief	- Toevoegen specialismen: - Verpl. spec. geestelijke gezondheidszorg (069) - Jeugdarts (070)

			- Spoedeisende hulp arts (071) - Toevoegen beroep: Klinisch fysicus (084). - Expliciet noemen telefonisch intrekken tijdens kantoortijden. - Wijziging wijzigingsprocedure hoofdstuk 9.12. - Tekstuele aanpassingen. - Beleid bij vernieuwing en intrekking nader gespecificeerd (par. 4.1, 4.6 en 4.9.1). - Wijziging aansprakelijkheid vertrouwende partijen.
5.1	28-06-2012	Definitief	- Clausule CAB-forum opgenomen (par. 1.1.1). - Randvoorwaarden routinematige vernieuwing certificaten (par. 3.3.1). - Wijze van aanlevering PKCS#10 bestanden (par. 4.1). - Omstandigheid tot intrekking op initiatief UZI-register toegevoegd (par. 4.9.1). - Tekstuele aanpassingen.
5.2	15-04-2013	Definitief	- WID moet bij de uitgifte UZI-pas geldig zijn (par. 3.2.3). - Toelichting niet toestaan telefonische intrekking van servercertificaat (par. 3.4). - CRL uitgiftefrequentie verhoogd naar elk uur. - Passage beslistermijn gewijzigd (par. 4.2). - Verplichting abonnee ten aanzien van een servercertificaat met een domeinnaam (FQDN) die via het internet adresseerbaar is (par. 4.6.1) . - Intrekken per post nader gedefinieerd (par 4.9.5). - Overgangstermijn bij naamswijziging of beëindiging abonnee organisatie (par. 4.11). - Basis attributen StateOrProvinceName en LocalityName toegevoegd (par. 7.1.1). - Indeling CPS conform RFC 3647. - Tekstuele aanpassingen.
5.3	27-06-2013	Definitief	- Alleen elektronische intrekkingen worden gegarandeerd binnen 4 uur ingetrokken (par. 4.9.5). - Tarifering UZI-middelen (par. 9.1).Tekstuele aanpassingen.
5.4	20-09-2013	Definitief	- Pasfoto geschrapt (par. 3.2.3). - Mobiele uitgifte certificaten (par. 4.3). - Rol certificaatbeheerder consistent gemaakt. - Tekstuele aanpassingen i.v.m. nieuwe leveranciers en gewijzigd uitgifteproces/identiteitsvaststelling.
5.5	24-01-2014	Definitief	- Einde levensduur tweede generatie CA's. - Beëindiging key escrow en recovery per 1-10-2013 (par. 4.12). - Benadrukken aansprakelijkheid abonnee (par. 9.1.6).
5.6	09-09-2014	Definitief	- Diverse kleine wijzigingen en spellingscorrecties (gehele CPS). - Publicatiedienst toegevoegd (par. 1.3.3). - Vereisten aan zorgverleners verduidelijkt (par. 3.2.3). - Validatie van functienaam en afdeling gelijkgetrokken (par. 3.1.4 en 3.2.4). - Certificaatvernieuwing verduidelijkt (par. 3.3.1-2). - Intrekkingsprocedure verduidelijkt, eis 'e-mail in niet-muteerbare vorm' geschrapt (par. 3.4 en 4.9.3).

			- Certificaataanvraag verduidelijkt, clausule over annulering van aanvraag toegevoegd (par. 4.1). - Acceptatieperiode van server certificaten verduidelijkt (par. 4.4). - Clausule 'defecte pas' geschrapt, verwezen naar par. 9.1.10 (par. 4.5.1). - Procedure kwetsbaarheidanalyse aangepast (par. 5.4.7). - Periode continueren certificaatstatusdienst bij CSP beëindiging aangepast (par. 5.8). - Het aanbieden van key escrow integraal geschrapt (par. 6.2.3-5, bijlage 1). - Onjuistheid in CRL uitgiftefrequentie aangepast (par. 7.2.1) - Juridische entiteit certificerende instelling gecorrigeerd (H8) - TTP.nl schema vermeld (par. 8.1). - Onderwerp van audit uitgebreid (par. 8.4). - Facturatieprocedure verduidelijkt (par. 9.1.6) - Garantieregeling toegevoegd (par. 9.1.10). - Onduidelijke clausule aansprakelijkheid geschrapt (par. 9.5.2) - Mogelijkheid tot inschrijving als abonnee toegevoegd voor organisatie die voldoen aan de gewijzigde Wbsn (bijlage 2). - Verduidelijkt dat publieke LDAP toegang alleen via zoekpagina op de website mogelijk is (par. 1.3.3, 2.4, 9.3.2).
5.7	23-02-2015	Definitief	- Diverse kleine wijzigingen (gehele CPS). - Niet-geverifieerde gegevens verduidelijkt (par. 3.2.4). - Procedure gemachtigd aanvrager verduidelijkt (par. 3.2.5). - Redenen voor intrekking verwijderd (par. 3.3), zie par. 4.9.1. - Annuleren van aanvragen verduidelijkt (par. 4.1). - Opgenomen dat geen Certification Authority Authorization DNS gegevens gecontroleerd worden (par. 4.2). - Verplichting voor abonnee opgenomen m.b.t. juistheid en volledigheid van gegevens (par. 4.6.1). - Abonnee is akkoord met intrekking bij misbruik (par. 4.10.1). - Sleutelgebruik moet stoppen na intrekking (par. 4.9.1). - Controle handtekening bij intrekking toegevoegd (par. 4.9.3). - Overgangstermijn abonneebeëindiging verduidelijkt (par. 4.11). - CRLs worden gearchiveerd bij CSP beëindiging (par 5.8). - Procedure herprinten van pincodebrief toegevoegd (par 6.4.2). - Nieuwe ETSI normeringen en PKIo PvE naamgeving doorgevoerd (par. 2.2, 7.1, 7.2, H8, 8.4). - Proefperiode verduidelijkt (par. 9.1.9 en 9.1.10). - Garanties van UZI-register verduidelijkt (par. 9.5.1). - Procedure voor schorsing verduidelijk (bijlage 2 deel D).
5.8	01-09-2015	Definitief	- Het separate document "Vertrouwende Partij Voorwaarden" is samengevoegd met dit CPS. Sectie 1.3 verwijst nu naar de verplichtingen voor alle betrokken partijen. - In een servercertificaat kan geen e-mailadres meer worden opgenomen (par. 3.2.3). - Beschrijving OCSP responder certificaat toegevoegd (par. 7.3). - Sportarts (rolcode 074) toegevoegd aan bijlage 3.

			- Bijlage 2 onderdeel C herzien i.v.m. wijziging BIG-register.
5.9	01-01-2016	Definitief	- Diverse kleine wijzigingen (gehele CPS). - Wijziging registreren functienaam op medewerkerpas niet op naam (par. 3.3.1 en 3.1.4). - Gebruik van BSN toegevoegd (par. 3.2.3). - Procedure voor digitaal aanvragen van UZI-passen toegevoegd (par. 3.2.3). - Procedure voor vernieuwen certificaten aangepast (par. 3.3.1.). - Paragraaf inzake doorlooptijd toegevoegd (par. 4.3). - Wijze van uitgifte certificaten verduidelijkt (par. 4.4). - Bewaartermijnen archief aangepast (par. 5.5.2). - Verduidelijking van het begrip productiedatum (par. 6.3.2 en 9.1.8).
6.0	01-04-2016	Definitief	- Diverse wijzigingen met betrekking tot de wetswijziging - Wet kwaliteit, klachten en geschillen zorg (gehele CPS). - Verwijzingen naar het opnemen van een (systeem)email adres in het servercertificaat verwijderd (par 7.1.3). - Wijziging contactgegevens UZI-register (par. 1.5.1). - Toetsingsregisters Kwaliteitsregister Apothekersassistenten (KAA) en het Kwaliteitsregister voor Apothekersassistenten in de Openbare Farmacie (KAOF) toegevoegd (par. 3.2.3 en bijlage 2). - Mogelijkheid tot het overleggen van een digitaal uittreksel (pdf met certificaat van DUO) toegevoegd. (par. 3.2.3 en bijlage 2). - Openbaar apotheker (rolcode 075) toegevoegd aan bijlage 3.
6.1	20-03-2017	Definitief	- Geldigheidsduur certificaten aangepast (gehele CPS).
7.0	01-06-2017	Definitief	- Nieuwe ETSI normering en de Verordening elektronische identiteiten en vertrouwensdiensten (de eIDAS-Verordening) - Begrip CSP (Certification Service Provider) vervangen door TSP (Trust Service Provider) - Beëindiging TSP verduidelijkt en de verwijzing gemaakt naar het CA Termination Plan CIBG (par. 5.8) - Opgenomen dat een nieuwe versie van het CPS wordt gemeld aan de Policy Authority (par. 9.11.1) - Verwijzing naar hoofdstuk 3.2.2.4.5 van de Baseline Requirements opgenomen (par. 3.2.3) - Intrekking UZI-middelen na uitblijven betaling (par. 4.10.1). Facturering van UZI- middelen per e-mail toegevoegd (par. 9.1.6) - Diverse kleine wijzigingen (gehele CPS)
7.1	01-08-2017	Definitief	- De wet gebruik burgerservicenummer in de zorg (Wbsn-z) vervangen door de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. - De ‘medewerkerpas niet op naam’ wordt tijdelijk niet uitgegeven (par. 1.1.2) - Diverse tekstuele aanpassingen

			- Zorgverlener Andere zorg (rolcode 99) toegevoegd aan bijlage 3 - Het Kwaliteitsregister voor Apothekersassistenten in de Openbare Farmacie (KAOF) verwijderd
8.0	04-01-2018	Definitief	- Uitgifte onder de Private G1 hierarchie van de Staat der Nederlanden. - Artikel 15 eIDAS verwerkt.
9.0	22-03-2018	Definitief	- Uitgifte pasgebonden certificaten onder de G3 hiërarchie Staat der Nederlanden.
9.1	10-09-2018	Definitief	- Diverse kleine wijzigingen (gehele CPS). - Tijdsduur voor verwerking van verzoek tot intrekking aangepast (par 4.10.5) - Physician Assistant toegevoegd aan artikel 3 Wet BIG. - Beperking aansprakelijkheid met betrekking tot de levering van de UZI-pas toegevoegd (par 9.7) - Definitie zorg aangepast. - De Algemene verordening gegevensbescherming verwerkt. - Bewaartermijnen opgenomen (par. 5.5.2) - Wijzigingsprocedure aangepast (par. 9.11)
9.2	05-11-2018	Definitief	- Uitgifte ‘medewerkerpas niet op naam’ wordt hervat
9.3	23-11-2018	Definitief	- Diverse kleine wijzigingen (gehele CPS) - G2 hiërarchie toegevoegd - Hoofdstuk 8 ‘Conformiteitbeoordeling geüpdate - Verwijzing naar hoofdstuk 3.2.2.4 van de Baseline Requirements opgenomen (par 3.2.3)
9.4	01-06-2019	Definitief	- Diverse kleine wijzigingen (gehele CPS) - Recht controle op compenserende maatregelen toegevoegd (par. 4.6.1.) - Update van CaIssuer URL’s als gevolg van resigning G3 CA’s (par. 7.1.2)
9.5	01-08-2019	Definitief	- Na uitgifte van de UZI-pas / servercertificaat wordt het oude certificaat niet meer ingetrokken (gehele CPS).

Tabel 1 Versiehistorie CPS UZI-register

Copyright CIBG 2019© te Den Haag
Niets uit deze uitgave mag verveelvoudigd en/of openbaar worden gemaakt (voor willekeurig welke doeleinden) door middel van druk, fotokopie, microfilm, geluidsband, elektronisch of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van CIBG.

Akkoord TSP Management
Versie: 9.5
Datum: 29-07-2019

1 Introductie

1.1 **UZI-register en producten**

1.1.2 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 aanvullende bepalingen verwerking persoonsgegevens in de zorg. Het UZI-register is de certificatiedienstverlener (TSP)[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[2]. Het geheel wordt in dit Certification Practice Statement (CPS) aangeduid als UZI-pas[3].

Het UZI-register geeft UZI-passen uit aan door de minister van VWS bij wet en regelgeving aangewezen partijen. Een nadere beschrijving van de gebruikers-gemeenschap van het UZI-register is opgenomen in paragraaf 1.3 ‘Betrokken partijen’. Het UZI-register geeft certificaten uit onder de hiërarchie van de PKI voor de overheid[4].

TSP UZI-register conformeert zich aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen dit CPS en de betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements.

Het UZI-register zal daar waar dat haalbaar is zijn onlinedienstverlening, zoals de content op de website, de intrekpagina en de digitale aanvraagfaciliteit toegankelijk maken voor personen met een functiebeperking[5]. Hierdoor zal bij de ontwikkeling van nieuwe applicaties en wijzigingen in de genoemde onlinedienstverlening aan ETSI EN 301 549 worden getoetst.

1.1.3 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.

---

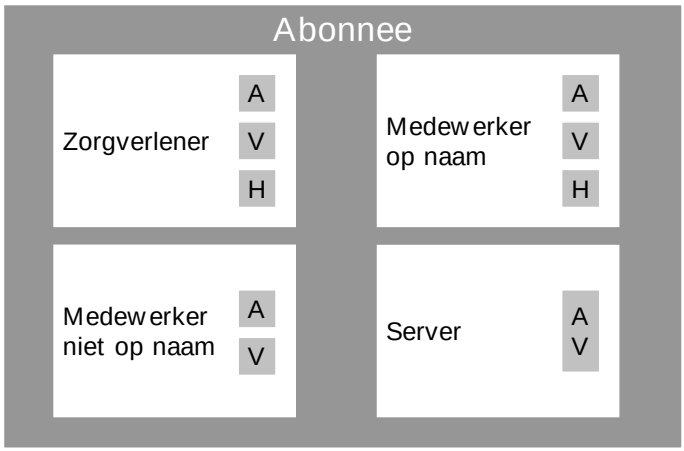
[1] Voor een verklaring van de gebruikte begrippen en afkortingen wordt verwezen naar bijlage 1 ‘Definities en afkortingen’.

[2] Dit betreft een zogenaamde Secure Signature Creation Device (SSCD)

[3] Het begrip UZI-pas wordt gebruik om de certificaten, sleutels en de daarbij behorende drager aan te duiden.

4 https://www.logius.nl/diensten/PKIoverheid/

5 Artikel 15 eIDAS



Figuur 1 Passenmodel en certificaten

Zorgverlenerpas
De zorgverlenerpas is voor een beroepsbeoefenaar als bedoeld in de artikelen 3, 34 en 36a 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 de beoogd pashouder werkelijk een zorgverlener is (zie bijlage 2). Het UZI-register garandeert naast de identiteit tevens de 'status zorgverlener' en de relatie naar de abonnee[6]. Zorgverleners krijgen een gepersonaliseerde pas 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 van de certificaathouder 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 en drie certificaten en sleutelparen (authenticatie, vertrouwelijkheid en onweerlegbaarheid).

Medewerkerpas niet op naam
Voor een groep medewerkers met een bepaalde functie van een abonneeorganisatie van het UZI-register kan een medewerkerpas niet op naam worden verkregen. De certificaten van deze UZI-pas geven aan dat de certificaathouder een functionaris is van de abonnee die in de certificaten wordt genoemd maar zijn niet direct herleidbaar tot een persoon. Het UZI-register garandeert de relatie naar de abonnee en reikt de pas uit na een face-to-face controle en controle van de wettelijke identiteit van de geautoriseerde aanvrager. De aanvrager vervult voor 'Medewerkerpas niet op naam' ook de rol van certificaatbeheerder en is onder andere verantwoordelijk voor registratie van de relatie naar de specifieke medewerker(s) die de pas gebruiken. De 'Medewerkerpas niet op naam' is een niet-persoonsgebonden UZI-pas met twee certificaten en sleutelparen (authenticatie en

6 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.

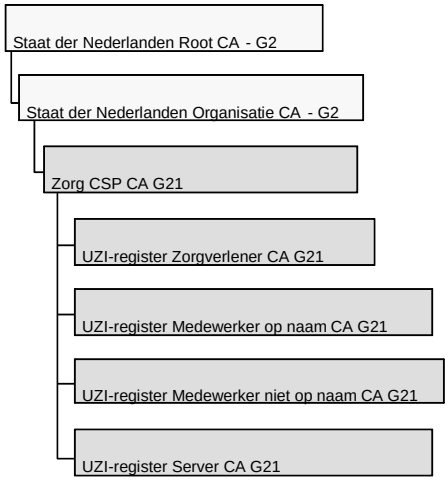
vertrouwelijkheid). Deze UZI-pas kan niet worden uitgegeven onder een abonneezorgverlener registratie.

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 en geeft het servercertificaat uit na een face-to-face controle en controle van de wettelijke identiteit van de aanvrager. De aanvrager vervult voor een servercertificaat ook de rol van certificaatbeheerder en is daarmee namens de abonnee verantwoordelijk voor het operationele beheer van het certificaat. Voor servercertificaten zijn het authenticiteit- en vertrouwelijkheidcertificaat gecombineerd in één certificaat.

1.1.4 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 in Figuur 2 en 3.

SHA-2 generatie (G21)
De einddatum van de SHA-2 (G21) hiërarchie is 22 maart 2020. Deze hiërarchie maakt gebruik van een cryptografisch algoritme SHA-2 bij ondertekening van certificaten en CRL's. Deze structuur is weergegeven in ***Figuur 2 CA-model SHA-2 generatie (G21)***



Figuur 2 CA-model SHA-2 generatie (G21)

Public G3 / Private G1 generatie
Vanaf 4 januari 2018 en 22 maart 2018 geeft het UZI-register servercertificaten respectievelijk UZI-passen uit onder de nieuwe CA's. Bij uitfasering van de SHA-2 (G21) hiërarchie is besloten om:

1. passen uit te gaan geven onder de publiek vertrouwde G3 Root van PKIoverheid (Public G3);
2. servercertificaten uit te geven onder de private Root CA G1 van PKIoverheid (Private G1).

Door het besluit om passen en servercertificaten onder verschillende nieuwe Root CA certificaten uit te gaan geven, zijn er twee volledig nieuwe CA hiërarchieën die los van elkaar staan.

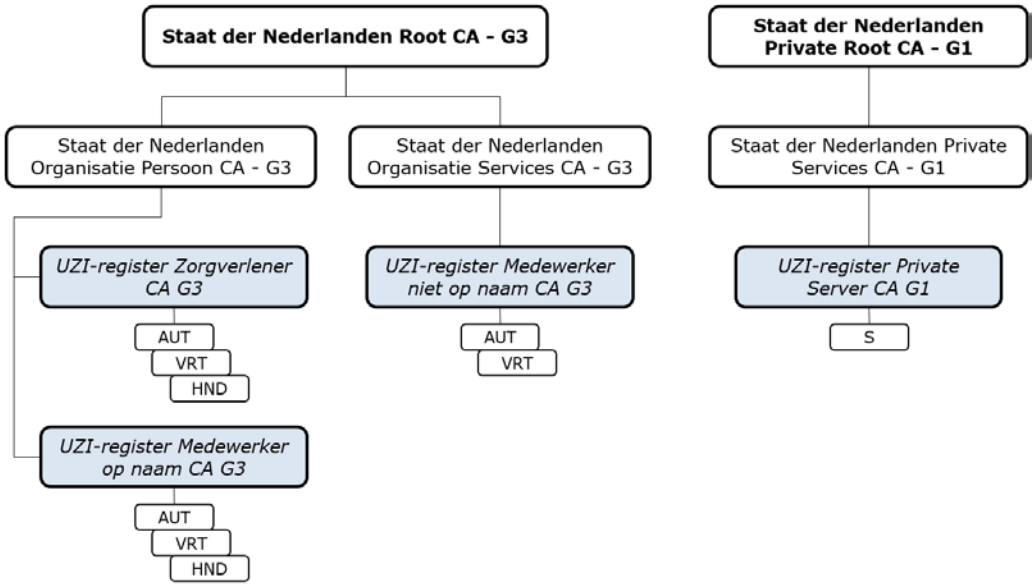
Bij invoering van deze G3 omgeving heeft Logius besloten om aparte domein CA's te creëren voor persoonsgebonden en services certificaten. Daarnaast heeft Logius een Private Root CA gecreëerd. Deze heeft als generatie aanduiding 'G1' aangezien het de eerste private omgeving is.

Met de invoering van de Public G3/Private G1 generatie is het aantal niveaus in de CA-hiërarchie maximaal 3.

Onderstaande figuur geeft het CA model weer voor de generatie Public G3/Private G1. Cursief en gearceerd zijn de CA's weergegeven die de eindgebruikercertificaten ondertekenen.

Voor de volledigheid zijn ook de verschillende typen eindgebruikercertificaten opgenomen:

- AUT: Authenticiteitcertificaat;
- VRT: Vertrouwelijkheidcertificaat;
- HND: Handtekeningcertificaat;
- S: Servercertificaat.



Figuur 3 CA-model generatie Public G3/Private G1

Er zijn geen cryptografische verschillen bij de overgang naar de Public G3/Private G1 hiërarchie. Dezelfde algoritmen en sleutellengten blijven in gebruik als in de SHA-2 generatie (G21).

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.
Tabel 3 en **Tabel 4** geven aan in welk PKIoverheid domein de verschillende soorten passen en certificaten worden uitgeven en welk deel van het Programma van Eisen van PKIoverheid het CP bevat.

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.xx
Link	https://www.zorgcsp.nl/cps/uzi-register.html
Object Identifier (OID)	2.16.528.1.1007.1.1

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 CIBG vervult de rol van **TSP** en heeft de eindverantwoordelijkheid voor het leveren van de certificatiediensten. Het CIBG is een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport. Het CIBG in de rol van TSP wordt in voorliggend CPS verder aangeduid als 'het UZI-register'.

Clausules over aansprakelijkheid en garanties van de TSP zijn opgenomen in secties 9.5, 9.5.1, 9.5.2 en 9.5.3.

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. Certificaten worden op een CRL gepubliceerd nadat de CA een bericht van intrekking van het certificaat heeft ontvangen van een hiertoe bevoegde persoon. Na intrekking publiceert de CA de unieke certificaatserienummers op de betreffende CRL. Het CIBG heeft de rol van CA uitbesteed aan KPN Corporate Market B.V. die samen met ATOS Nederland B.V. (het Consortium) het fysieke productieproces verzorgt. Multipost Services B.V.

produceert namens het Consortium de UZI-passen.

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 het Consortium. Dynalogic geeft namens het Consortium, na verificatie van de identiteit van de certificaathouder, de UZI-pas uit. Dynalogic controleert daarnaast de identiteit van certificaatbeheerders.

1.3.3 Dissemination Service (publicatiedienst)
Het UZI-register draagt verantwoordelijkheid voor de website waarop onder andere dit CPS is gepubliceerd. Ook is op deze website de CRL geplaatst (gegenereerd door de CA). Daarnaast bevat deze website de online intrekkingspagina en biedt deze website een publieke zoekfunctie voor certificaten.

1.3.4 Abonnees
De abonnee is de partij namens wie de certificaathouder handelt bij gebruik van de certificaten.

Het UZI-register kent twee typen abonnees, te weten personen (solistisch werkende zorgverlener) en organisaties (instellingen 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 solistisch werkende zorgverlener is en de pas voor zichzelf aanvraagt, geldt deze zorgverlener tevens als certificaathouder.

1.3.5 Certificaathouders en certificaatbeheerders
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 vervult ook de rol van 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.

1.3.6 Vertrouwende partijen
Een vertrouwende partij is degene die handelt in vertrouwen op een certificaat met als mogelijke doelen het authenticeren van de zorgaanbieders, verifiëren van een elektronische handtekening of het versleutelen van communicatie met die betreffende partij.

De verplichtingen die van toepassing zijn op certificaathouders en certificaatbeheerders zijn opgenomen in CPS secties 4.6.1

1.4 Certificaatgebruik

1.4.1 Toegestaan gebruik
Het toepassingsgebied van door het UZI-register uitgegeven certificaten is beperkt tot de gebruikersgemeenschap zoals beschreven in paragraaf 2.3 deel 3a van het Programma van Eisen van de PKI voor de overheid. Deze gebruikersgemeenschap

bestaat uit abonnees van het UZI-register, certificaathouders die bij deze abonnees behoren en vertrouwende partijen.

De producten van het UZI-register zijn bedoeld voor zorgaanbieders en indicatieorganen bij elektronische communicatie en toegang tot gegevens. De toepasbaarheid van de certificaten staat in *Tabel 2 Toepassingsgebied certificaten*.

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 2 Toepassingsgebied certificaten

1.4.2 Niet toegestaan gebruik

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:

Rijnstraat 50 Postbus 16114
2515 XP Den Haag 2500 BC Den Haag
Tel: 0900 - 232 4342
info@uzi-register.nl www.uziregister.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 TSP management is verantwoordelijk voor een juiste navolging van de procedure zoals beschreven in paragraaf 9.11 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 online 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 TSP informatie

Het UZI-register publiceert TSP informatie op www.uzi-register.nl en www.zorgcsp.nl. Deze locatie's bieden onder meer toegang tot de volgende documenten en diensten:

- CPS,
- Certificate Revocation Lists (CRL's),
- TSP en CA certificaten,
- Directory dienst.

Voor de Certificate Policies (CP) wordt verwezen naar www.logius.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/Servercertificaat	**Certificaat (functie)**		
Zorgverlener Medewerker op naam	authenticiteit	PvE deel 3a, Certificate Policy – Domein Organisatie (g21)	2.16.528.1.1003.1.2.5.1
	handtekening (onweerlegbaarheid)	PvE deel 3a, Certificate Policy – Domein Organisatie (g21)	2.16.528.1.1003.1.2.5.2
	vertrouwelijkheid	PvE deel 3a, Certificate Policy – Domein Organisatie (g21)	2.16.528.1.1003.1.2.5.3
Medewerker niet op naam	authenticiteit	PvE, deel 3b, Certificate Policy – Services, Domein Organisatie (g21)	2.16.528.1.1003.1.2.5.4
	vertrouwelijkheid	PvE, deel 3b, Certificate Policy – Services, Domein Organisatie(g21)	2.16.528.1.1003.1.2.5.5
Server	authenticiteit en vertrouwelijkheid	PvE, deel 3e, Certificate Policy – Services, Domein Organisatie(g21)	2.16.528.1.1003.1.2.5.6

Tabel 3 Overzicht certificaten met OID van toepasselijke CP SHA-2 generatie (G21)

Type certificaat		Toepasselijke CP	OID CP
Pas/Servercertificaat	**Certificaat (functie)**		
Zorgverlener Medewerker op naam	authenticiteit	PvE deel 3a: Certificate Policy - Domein Organisatie Persoon (g3)	2.16.528.1.1003.1.2.5.1
	handtekening (onweerlegbaarheid)	PvE deel 3a: Certificate Policy - Domein Organisatie Persoon (g3)	2.16.528.1.1003.1.2.5.2
	vertrouwelijkheid	PvE deel 3a: Certificate Policy - Domein Organisatie Persoon (g3)	2.16.528.1.1003.1.2.5.3
Medewerker niet op naam	authenticiteit	PvE deel 3b: CP auth.- en vertr. certificaten - Organisatie Services (g3)	2.16.528.1.1003.1.2.5.4
	vertrouwelijkheid	PvE deel 3b: CP auth.- en vertr. certificaten - Organisatie Services (g3)	2.16.528.1.1003.1.2.5.5
Server	authenticiteit en vertrouwelijkheid	PvE deel 3h: Certificate Policy Server Certificaten – Domein Private Services (g1 private)	2.16.528.1.1003.1.2.8.6

Tabel 4 Overzicht certificaten met OID van toepasselijke CP Public G3/Private G1 generatie

2.3 Frequentie van publicatie

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

2.4 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.

De gepubliceerde certificaten zijn alleen publiek opvraagbaar via de zoekfunctie op de website.

3 Identificatie en authenticatie

3.1 Naamgeving

Deze paragraaf beschrijft op welke wijze de identificatie en authenticatie van certificaatbeheerders 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
givenName (G)	Voornamen	Voornamen	Niet van toepassing	Niet van toepassing
surname (SN)	Tussenvoegsel en geboortenaam zorgverlener	Tussenvoegsel en geboortenaam medewerker	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 en adellijke titulatuur, zoals opgenomen in het bij registratie voorgelegde identificatiedocument of de Basisregistratie Personen (BRP). In de commonName wordt de adellijke titulatuur vermeld conform het bij de registratie overlegde identificatiedocument. Als identificatiedocument gelden bij artikel 1 van de Wet op de identificatieplicht (WID) aangewezen geldige documenten. Op het overgelegde identiteitsdocument moeten alle voornamen voluit vermeld staan.
- In de commonName worden in principe alle voornamen volledig vermeld conform de Basisregistratie Personen (BRP) of 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, in het geval van een instelling, de naam zoals deze op het bij registratie overlegde document voor identificatie van de organisatie voorkomt. Als de abonnee een solistische werkende zorgverlener is, wordt de commonName van de solistisch werkende zorgverlener opgenomen.
- Functienaam medewerker mag geen benaming bevatten die (geheel of gedeeltelijk) gelijk is aan, lijkt op, of de indruk wekt van een beschermde beroepstitel, opleidingstitel of specialisme. Het UZI-register heeft een lijst met functienamen opgesteld, waaruit een keuze kan worden gemaakt. Dit zijn: administratief medewerk(st)er, assistent(e), doktersassistent(e), manager, medewerk(st)er, stagiair(e), tandartsassistent(e). Er kan geen zelf gekozen functienaam worden opgegeven.
- Afdeling bevat de door de abonnee opgegeven afdelingsnaam. Het UZI-register stelt hierbij als eis dat de afdelingsnaam 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. Toetsing vindt onder meer plaats op basis van dit overzicht. Er vindt geen toetsing plaats op spel- en schrijffouten.
- 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 Basisregistratie Personen (BRP) of uit het overlegde identificatiedocument. Het kan echter zijn dat in de naamgegevens bijzondere tekens voorkomen die geen deel uitmaken van de standaard tekenset conform ISO8859-1 (Latin-1)[7]. 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.

7 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.

3.1.5 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 geboortenaam inclusief voorvoegsels en/of voornamen van een persoon wijzigt, 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 TSP management na afweging van de betrokken belangen, voor zover hierin niet wordt voorzien door dwingend Nederlands recht of overige toepasselijke regelgeving.

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 oprichtingsdocument, een notariële akte, een instellingsbesluit, een vergunning of in de wet, wordt overgenomen bij registratie en gebruikt in de certificaten.
De certificaatbeheerders 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 private 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 wettelijk vertegenwoordiger van de registratie ondertekend aanvraagformulier met daarin
  - de volledige naam van de organisatie;
  - de adresgegevens van de organisatie;
  - de volledige naam (volledige voornamen, voorvoegsels geboortenaam, geboortenaam, voorvoegsels achternaam en achternaam) en contactgegevens van de wettelijk vertegenwoordiger van de organisatorische identiteit.
  - de volledige naam en contactgegevens van de gemachtigde aanvrager/aanvragers die namens de organisatie UZI-passen mogen aanvragen en intrekken.
  - (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;
- Bewijs dat de wettelijk vertegenwoordiger 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;
  - afschrift van de benoeming van de wettelijk vertegenwoordiger als zodanig. Alleen wanneer de wettelijk vertegenwoordiger niet uit het Handelsregister van de Kamer van Koophandel blijkt.
- 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). Op het overgelegde identificatiedocument moeten alle voornamen voluit vermeld staan. 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 oprichtingsdocument of notariële akte;
  - afschrift van een vergunning of beschikking;
  - zorgovereenkomst;
  - door alle betrokkenen ondertekende eigenverklaring (alleen te overleggen als de organisatie geen rechtspersoonlijkheid heeft).
  - Verklaring waarin wordt aangegeven welke zorgverleners er binnen de zorginstelling werkzaam zijn, van toepassing bij een eenmanszaak.

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 solistisch werkende 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 zorgverlener ondertekend aanvraagformulier met daarin:
  - de volledige naam van de zorgverlener (geboortenaam, inclusief voorvoegsels en voornamen);
  - de contactgegevens (e-mailadres en (mobiele) telefoonnummer) 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 UZI-register neemt de voornamen, voorvoegsels geboortenaam, de geboortenaam en het BSN 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, Kwaliteitsregister Mondhygiënisten, Kwaliteitsregister Apothekersassistenten (KAA) moeten als bewijs dat zij de opleidingstitel mogen voeren een origineel en geldig gewaarmerkte kopie van het betreffende diploma of een digitaal uittreksel (PDF met certificaat van DUO) overleggen.
- Beroepsbeoefenaren als bedoeld in artikel 36a van de Wet BIG moeten als bewijs dat zij de opleidingstitel mogen voeren een origineel en geldig gewaarmerkte kopie van het betreffende diploma of een digitaal uittreksel (PDF met certificaat van DUO) 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. Dit is de wettelijk vertegenwoordiger of een namens de abonnee financieel gemachtigd aanvrager. De aanvraag geschiedt digitaal via de applicatie op de website van het UZI-register (www.uziregister.nl/aanvragen) of via een papieren aanvraagformulier.

Het UZI-register biedt de digitale aanvraagfaciliteit aan voor de volgende pastypen:

- Zorgverlenerpas art. 3 Wet BIG (met uitzondering van de specialismen jeugdarts, apotheekhoudend huisarts en SEH-arts)
- Medewerkerpas op naam
- Medewerkerpas niet op naam

Voor de bovenvermelde pastypen kan op verzoek van de pasaanvrager een papieren aanvraagformulier (PDF-formaat) door het UZI-register worden verstrekt.

Voor de pastypen zorgverlenerpas art. 34 en 36a Wet BIG, servercertificaten en de uitzonderingen vermeld bij de zorgverlenerpas art. 3 Wet BIG biedt het UZI-register via de website een papieren aanvraagformulier aan.

Toegang tot de digitale aanvraagfaciliteit
De digitale aanvraagfaciliteit op de website van het UZI-register kan worden gebruikt door wettelijk vertegenwoordigers of financieel gemachtigd aanvragers met een of meer actieve abonneeregistraties bij het UZI-register. De persoon identificeert zich via DigiD of persoonlijke UZI-pas. Het UZI-register controleert vervolgens of deze persoon staat geregistreerd als wettelijk vertegenwoordiger of financieel gemachtigd aanvrager bij een of meer actieve abonnees. Als dit zo is, wordt toegang verleend tot de digitale aanvraagfaciliteit en kunnen een of meer UZI-passen worden aangevraagd.

De applicatie toont de volgende gegevens van de abonnee: de naam van de abonnee, het abonneenummer, de naam en contactgegevens van de pasaanvrager. Is de pasaanvrager voor verschillende abonnees gemachtigd dan selecteert de pasaanvrager eerst de gewenste abonnee.

Het doen van de aanvraag via de digitale aanvraagfaciliteit
Er wordt gebruik gemaakt van automatische koppelingen met de Basisregistratie Personen (BRP) en het BIG-register. Deze koppelingen worden gebruikt om tijdens het doen van de aanvraag ingevulde gegevens te valideren of op te halen uit het desbetreffende register.

Onderstaand wordt per pastype aangegeven welke gegevens nodig zijn voor de digitale aanvraag en welke documenten moeten worden overlegd voor de uitgifte van de UZI-pas.

Medewerkerpas op naam
- Digitale aanvraag via www.uziregister.nl/aanvragen
  - BSN en geboortedatum van de beoogd pashouder. Op basis van deze gegevens vindt verificatie plaats in de Basisregistratie Personen (BRP) en wordt de geboortenaam opgehaald en getoond.
  - Verklaring van de pasaanvrager dat de beoogd pashouder expliciet toestemming heeft verleend voor het verstrekken van zijn/haar persoonsgegevens voor de aanvraag van de UZI-pas.
  - De contactgegevens (e-mailadres en het mobiele telefoonnummer) van de beoogd pashouder. Deze gegevens zijn nodig van de uitgifte van de UZI-pas.
  - Voor de aflevering van de pincodebrief kiest de pasaanvrager het postadres van de abonnee of het thuisadres van de beoogd pashouder. Het thuisadres wordt overgenomen uit de Basisadministratie Personen (BRP) en wordt uit privacy overwegingen niet getoond.
  - Naamgebruik in correspondentie. De pasaanvrager kiest hierbij voor de in de Basisregistratie Personen (BRP) geregistreerde partnernaam of de in de

Basisregistratie Personen (BRP) vermelde geboortenaam van de beoogd pashouder.

- Het uitreiken van de pas gebeurt persoonlijk aan de beoogd pashouder, waarbij de beoogd pashouder een geldig wettelijk identiteitsdocument zoals genoemd in de Wet op de identificatieplicht (WID) dient te overleggen. Op het overgelegde identiteitsdocument moeten alle voornamen voluit vermeld staan. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren. Het fysiek vaststellen van de identiteit van de pashouder en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic.

Zorgverlenerpas art. 3 Wet BIG (met uitzondering van specialismen jeugdarts, apotheekhoudend huisarts en SEH-arts)
Beroepsbeoefenaren als bedoeld in artikel 3 van de Wet BIG dienen ingeschreven te staan in het BIG-register.

- Digitale aanvraag via www.uziregister.nl/aanvragen
  - BSN en geboortedatum van de beoogd pashouder. Op basis van deze gegevens vindt verificatie plaats in de Basisregistratie Personen (BRP) en wordt de geboortenaam opgehaald en getoond.
  - Verklaring van de pasaanvrager dat de beoogd pashouder expliciet toestemming heeft verleend voor het verstrekken van zijn/haar persoonsgegevens voor de aanvraag van de UZI-pas.
  - BIG-registratie. Op basis van het in te vullen BIG-nummer en een set aan eerder verkregen persoonsgegevens wordt de toetsing in het BIG-register uitgevoerd. De beroepstitel en het eventuele specialisme worden getoond conform de registratie in het BIG-register.
  - De contactgegevens (e-mailadres en het mobiele telefoonnummer) van de beoogd pashouder. Deze gegevens zijn nodig van de uitgifte van de UZI-pas.
  - Voor de aflevering van de pincodebrief kiest de pasaanvrager het postadres van de abonnee of het thuisadres van de zorgverlener. Het thuisadres word overgenomen uit de Basisregistratie Personen (BRP) en wordt uit privacy overwegingen niet getoond.
  - Naamgebruik in correspondentie. De pasaanvrager kiest hierbij voor de partnernaam of de geboortenaam van de beoogd pashouder, zoals geregistreerd in de Basisregistratie Personen (BRP).
  - Het uitreiken van de pas gebeurt persoonlijk aan de beoogd pashouder, waarbij de beoogd pashouder een geldig wettelijk identiteitsdocument zoals genoemd in de Wet op de identificatieplicht (WID) dient te overleggen. Op het overgelegde identiteitsdocument moeten alle voornamen voluit vermeld staan. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren. Het fysiek vaststellen van de identiteit van de pashouder en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic.

Medewerkerpas niet op naam

- Digitale aanvraag via www.uziregister.nl/aanvragen
  - Functienaam waarvoor de pas wordt aangevraagd. Keuze wordt gemaakt uit een vaste selectie van functienamen. Zie paragraaf 3.1.4.
- Het uitreiken van de pas gebeurt persoonlijk aan de pasaanvrager, waarbij de pasaanvrager een geldig wettelijk identiteitsdocument zoals genoemd in de Wet op de identificatieplicht (WID) dient te overleggen. Op het overgelegde identiteitsdocument moeten alle voornamen voluit vermeld staan. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren. Het fysiek vaststellen van de identiteit van de pasaanvrager en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic.

Onderstaand wordt per pastype aangegeven welke gegevens nodig zijn voor de aanvraag en welke documenten moeten worden overlegd voor de uitgifte van het UZI-middel.

Zorgverlenerpas art. 34 Wet BIG, art. 36a Wet BIG en art. 3 Wet BIG voor de specialismen apotheekhoudend huisarts, jeugdarts en SEH-arts)

- 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;
  - de volledige naam (geboortenaam, inclusief voorvoegsels en voornamen) van de beoogd pashouder;
  - de contactgegevens (e-mail adres en mobiel telefoonnummer) van de beoogd pashouder;
  - de beroepstitel of opleidingstitel en een eventueel specialisme van de beoogd pashouder en de referentie naar de te hanteren toetsingscriteria;
- 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 UZI-register neemt de voornamen, voorvoegsels geboortenaam, de geboortenaam en het BSN over uit het identificatiedocument en zal de kopie van het identificatiedocument archiveren.
- Beroepsbeoefenaren als bedoeld in artikel 34 van de Wet BIG dienen ofwel te zijn geregistreerd bij het Kwaliteitsregister Paramedici, Kwaliteitsregister Mondhygiënisten, Kwaliteitsregister Apothekersassistenten (KAA) ofwel moeten als bewijs dat zij de opleidingstitel mogen voeren een origineel gewaarmerkte kopie van het betreffende diploma of een digitaal uittreksel (pdf met certificaat van DUO) overleggen.
- Beroepsbeoefenaren als bedoeld in artikel 3 van de Wet BIG die het specialisme apotheekhoudend huisarts in het certificaat willen opnemen, moeten geregistreerd zijn in het overzicht ‘Geldige APG-vergunningen’. Dit overzicht wordt beheert door farmatec, https://www.farmatec.nl/.
- Het uitreiken van de pas gebeurt persoonlijk aan de beoogd pashouder, waarbij de beoogd pashouder een geldig wettelijk identiteitsdocument zoals genoemd in de Wet op de identificatieplicht (WID) dient te overleggen. Op het overgelegde identiteitsdocument moeten alle voornamen voluit vermeld staan. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren. Het fysiek vaststellen van de identiteit van de pashouder en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic.

Servercertificaat

- Een volledig ingevuld en door de aanvrager/certificaatbeheerder van de abonnee ondertekend aanvraagformulier met daarin:
  - de naam van de abonnee;
  - het abonneenummer;
  - de naam van de aanvrager/certificaatbeheerder;
  - contactgegevens (e-mail adres en mobiel telefoonnummer) van de aanvrager;
  - de volledige domeinnaam (FQDN) waarvan de abonnee eigenaar is of waarvan de houder toestemming geeft voor gebruik. De domeinnaam moet uniek zijn en mag niet gebruikt worden bij een andere organisatie. Als de

abonnee geen eigenaar is van de domeinnaam, toetst het UZI-register of de abonnee gebruik mag maken van de domeinnaam[8].

- Het PKCS#10 bestand (Certificate Signing Request (CSR)). PKCS#10 is de gangbare standaard voor een certificaataanvraag en bevat de publieke sleutel die in het UZI-servercertificaat wordt opgenomen. Het PKCS#10 bestand moet via een upload functionaliteit in het aanvraagformulier worden toegevoegd aan de aanvraag.

Bij een digitale aanvraag verifieert en haalt het UZI-register persoonsgegevens op in de Basisregistratie Personen (BRP). In de andere gevallen controleert het UZI-register de overlegde documenten op echtheid, volledigheid en juistheid. 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). 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, of wanneer deze geen eigenaar is of de abonnee toestemming heeft van de domeineigenaar om de domeinnaam te gebruiken. 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 alle gegevens die worden opgenomen in het certificaat, met de volgende uitzonderingen:

- in medewerkerpassen niet op naam het veld ‘afdeling’
- in servercertificaten het veld ‘afdeling’.

Gegevens die voor correspondentiedoeleinden door de pasaanvrager worden verstrekt, zoals correspondentienaam, e-mailadressen en telefoonnummers worden niet geverifieerd.

3.2.5 Autorisatie certificaathouder

De wettelijk vertegenwoordiger van de abonnee kan bij registratie vastleggen welke personen certificaten mogen aanvragen voor de abonnee. Deze aanvragers zijn tevens certificaatbeheerders en gerechtigd om voor een certificaathouder een certificaat te ontvangen namens de abonnee. Het UZI-register controleert de authenticiteit van deze aanvraag van de wettelijk vertegenwoordiger.
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 digitale aanvraag controleert het UZI-register aan de hand van de authenticatie via DigiD of de UZI-pas of de aanvraag wordt gedaan door een geautoriseerd pasaanvrager. Bij een papieren aanvraag gebeurt dit aan de hand van een kopie van een identiteitsbewijs of de ‘natte’ handtekening op het aanvraagformulier.

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. Bij de uitvoering van een

[8] *De door het UZI-register gebruikte methoden worden voorgeschreven vanuit hoofdstuk 3.2.2.4 van de Baseline Requirements*.

vernieuwingsverzoek wordt altijd een nieuw sleutelpaar gegenereerd. Indien van toepassing wordt tevens een nieuwe smartcard uitgegeven.

Het UZI-register stuurt de abonnee 70 dagen voor de verloopdatum van het UZI-middel een brief met informatie over het vernieuwen van het certificaat. Op de website van het UZI-register kunnen de UZI-passen vernieuwd worden. Gegevens die al bekend zijn bij het UZI-register, waaronder persoonsgegevens en beroepen zoals bedoeld in de Wet BIG, hoeven, niet opnieuw te worden aangeleverd. Het nieuwe certificaat gaat in op het moment dat de nieuwe UZI-pas is geproduceerd.

Let op: Alle typen UZI-passen, met uitzondering van de onder vermelde specialismen, kunnen op de site van het UZI-register worden vernieuwd. Op verzoek van de pasaanvrager kan een papieren aanvraagformulier (PDF-formaat) door het UZI-register worden verstrekt. In dit formulier worden gegevens die al bekend zijn bij het UZI-register niet voorbedrukt.

Voor de art. 3 Wet BIG beroepen waarvan het specialisme, zoals jeugdarts en apotheekhoudend huisarts, niet onder het BIG-nummer van de pashouder staat geregistreerd, kan geen vernieuwing worden gedaan via de digitale aanvraagfaciliteit. Hiervoor is een volledig ingevuld en door de pasaanvrager van de abonnee ondertekend aanvraagformulier nodig.

Voor vernieuwen van een UZI-servercertificaat kan gebruik gemaakt worden van een aanvraagformulier voor certificaatvernieuwing. Dit aanvraagformulier wordt door het UZI-register samen met de vernieuwingsbrief toegezonden. Alleen originele, door het UZI-register toegezonden, aanvraagformulieren voor certificaatvernieuwing worden in behandeling genomen. In dit formulier worden gegevens die al bekend zijn bij het UZI-register voorgedrukt.

Bij het vernieuwen van certificaten wordt altijd vooraf een controle uitgevoerd of is voldaan aan alle eisen uit paragraaf 3.1 en 3.2.

3.3.2 Vernieuwing van sleutels na intrekking van het certificaat

De procedures en controles rondom het vernieuwen van sleutels na intrekking van het certificaat zijn gelijk aan die bij initiële registratie. Bij de uitvoering van een vernieuwingsverzoek wordt altijd een nieuw sleutelpaar gegenereerd. Indien van toepassing wordt tevens een nieuwe smartcard uitgegeven. Zie de procedure in sectie 3.3.1 ‘Routinematige vernieuwing van het certificaat’.

3.4 Identificatie en authenticatie bij verzoeken tot intrekking

De pashouder/certificaathouder of een pasaanvrager/certificaatbeheerder kunnen namens de abonnee verzoeken tot intrekking indienen. Verzoeken tot intrekking kunnen worden gedaan elektronisch, telefonisch, per e-mail of per post. Het telefonisch intrekken van servercertificaten is niet mogelijk[9].

- 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

9 Dit besluit volgt op een risicoanalyse. Een intrekking van een servercertificaat kan gevolgen hebben voor de aansluiting van een abonnee op de zorginfrastructuur. Omdat de kans op een onterechte intrekking bij een telefonisch verzoek groter is dan bij de andere kanalen, biedt het UZI-register telefonische intrekking niet aan voor servercertificaten.

pashouder en de betrokken pas kunnen verstrekken. Telefonisch intrekken van servercertificaten is niet mogelijk.

- Bij intrekking per normale e-mail 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 Wet op de Identificatieplicht (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 elektronische ondertekende e-mail geldt onderstaande eis:
  - De e-mail is ondertekend door de tot intrekking bevoegde persoon met een gekwalificeerd onweerlegbaarheidcertificaat (zoals op de UZI-pas voor zorgverleners en medewerkers op naam of een andere PKI overheidspas).
- Bij intrekking via de post gelden dezelfde eisen als bij intrekking per normale e-mail.

Het UZI-register controleert of de indiener van het intrekkingsverzoek bevoegd is de aanvraag te doen. Tevens controleert het UZI-register bij intrekkingsverzoeken per normale e-mail en post de identiteit van de indiener van het intrekkingsverzoek 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 alleen via de website of via elektronisch ondertekende mail worden verstuurd.

Onder een abonneeregistratie is het niet mogelijk om voor een zorgverlener meerdere actieve passen te verkrijgen met hetzelfde basisberoep of specialisme. Bij vernieuwing van certificaten is vanwege de continuïteit een beperkte periode toegestaan dat beide certificaten actief zijn. Deze periode is vastgesteld op 70 dagen. 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 afgeleverd.

Het annuleren van een aanvraag is na indienen bij het UZI-register niet mogelijk. Uitzonderingen hierop zijn mogelijk, ter beoordeling van het TSP management. Hierbij kan bijvoorbeeld worden gedacht aan de situatie waarin de aanvrager onmiddellijk na het indienen een onjuistheid in de aanvraag aantreft, en de aanvraag nog niet in behandeling is genomen door het UZI-register.

4.2 Werkwijze met betrekking tot aanvraag van certificaten

Voordat certificaten kunnen worden aangevraagd, dient de zorgaanbieder als 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. 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 certificaten aanvragen. Hiervoor worden de volgende stappen doorlopen:

- Voor het aanvragen van een van een zorgverlenerpas art. 3 Wet BIG(*met uitzondering van specialismen jeugdarts, apotheekhoudend huisarts en SEH-arts,* medewerkerpas op naam en de medewerkerpas niet op naam logt de pasaanvrager in op de digitale aanvraagfaciliteit op de website. De pasaanvrager kiest vervolgens het gewenste pastype en vult het aanvraagformulier in en verstuurt deze digitaal.
- Voor de bovenvermelde pastypen kan op verzoek van de pasaanvrager een papieren aanvraagformulier (PDF-formaat) door het UZI-register worden verstrekt.
- Voor de overige UZI-middelen overlegt de pasaanvrager 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 pasaanvrager en de beoogd pashouder nemen via het CPS 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.

Voor servercertificaten controleert het UZI-register geen Certification Authority Authorization DNS gegevens ten behoeve van eventuele 'certificate pinning' door de abonnee.

4.3 Doorlooptijd

Bij een digitale aanvraag via de webapplicatie bedraagt de doorlooptijd van het versturen van de aanvraag tot aan het beschikbaar stellen van de UZI-pas voor uitlevering maximaal drie weken. Voor de afhandeling van een compleet en juist ingevuld papieren aanvraagformulier hanteert het UZI-register een doorlooptijd van maximaal acht weken. In geval van extreme drukte kan het UZI-register hiervan afwijken.

4.4 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 pashouder dient persoonlijk te verschijnen bij het door de pasaanvrager opgegeven adres.
- De beoogd pashouder overlegt een geldig identificatiedocument waarop de volledige voorna(a)m(en) en geboortenaam staan vermeld. Als identificatiedocument gelden de bij artikel 1 van de Wet op de identificatieplicht (WID) aangewezen geldige documenten. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren.
- Het fysiek vaststellen van de identiteit van de beoogd pashouder en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic. Dynalogic is hiervoor volledig gecertificeerd (conform ETSI EN 319411-2.). Dynalogic controleert de geldigheid en echtheid van het overlegde identiteitsdocument. Aan de hand van dit document en de fysieke verschijning van de beoogd pashouder voert Dynalogic de identiteitscontrole uit en controleert of de persoon de bevoegde persoon is om de betreffende UZI-pas aan te overhandigen.
- Bij een positief resultaat op alle controles ondertekent de beoogd pashouder de ontvangstbevestiging. Dynalogic 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 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 certificaatbeheerder van de abonnee die de aanvraag heeft gedaan.

- De pasaanvrager/certificaatbeheerder dient persoonlijk te verschijnen bij het door de pasaanvrager opgegeven adres.
- De pasaanvrager/certificaatbeheerder overlegt een geldig identificatiedocument waarop alle voornamen voluit en de volledige geboortenaam staat vermeld. Als identificatiedocument gelden de bij artikel 1 van de Wet op de identificatieplicht (WID) aangewezen geldige documenten. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren.
- Het fysiek vaststellen van de identiteit van de pasaanvrager/certificaatbeheerder en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic. Dynalogic is hiervoor volledig gecertificeerd (conform ETSI EN 319411-2). Dynalogic controleert de geldigheid en echtheid van het overlegde identiteitsdocument. Aan de hand van dit document en de fysieke verschijning van de pasaanvrager/certificaatbeheerder voert Dynalogic de identiteitscontrole uit en controleert of de persoon de bevoegde persoon is om de betreffende UZI-pas aan te overhandigen.
- Bij een positief resultaat op alle controles ondertekent de pasaanvrager/certificaatbeheerder de ontvangstbevestiging. Dynalogic 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 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 pasaanvrager/certificaatbeheerder met een elektronische handtekening ondertekend verzoek:

- De pasaanvrager/certificaatbeheerder stuurt het UZI-register een e-mail met daarin het volledig ingevulde aanvraagformulier. De pasaanvrager/certificaat-beheerder 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 elektronische 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/certificaatbeheerder. Daarnaast verstuurt het UZI-register een intrekkingcode naar het correspondentieadres van de abonnee ter attentie van aanvrager/certificaatbeheerder.

De servercertificaten worden uitgereikt na persoonlijk verschijnen van de aanvrager/certificaatbeheerder van de abonnee:

- De pasaanvrager/certificaatbeheerder dient persoonlijk te verschijnen bij het opgegeven adres. De pasaanvrager/certificaatbeheerder overlegt een geldig identificatiedocument zoals genoemd in de Wet op de Identificatieplicht (WID). Op het overgelegde identiteitsdocument moeten alle voornamen voluit vermeld

staan. Het UZI-register is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren.
- Het fysiek vaststellen van de identiteit van de pasaanvrager/certificaatbeheerder en het maken van de kopie worden in opdracht van het UZI-register uitgevoerd door koeriersbedrijf Dynalogic. Dynalogic is hiervoor volledig gecertificeerd (conform ETSI EN 319411-2).
- De aanvrager/certificaatbeheerder 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 het servercertificaat.
- Nadat het certificaat is geproduceerd, verstuurt het UZI-register het certificaat per e-mail naar de pasaanvrager/certificaatbeheerder. Daarnaast verstuurt het UZI-register een intrekkingcode naar het correspondentieadres van de abonnee ter attentie van de aanvrager.

4.5 Acceptatie van certificaten

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

Door het ondertekenen van de ontvangstbevestiging bevestigt de certificaathouder de ontvangst van de pas aan het UZI-register. Het UZI-register legt het moment van verstrekking conform de ontvangstbevestiging 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 en akkoord te gaan met de inhoud van het certificaat.

Het UZI-register vraagt de certificaatbeheerder 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 en akkoord te gaan met de inhoud van het certificaat. Indien UZI-register de bevestiging van de certificaatbeheerder niet ontvangt, zal het UZI-register per e-mail een herinnering sturen aan de certificaatbeheerder. Indien het UZI-register geen ontvangstbevestiging heeft ontvangen, dan zal het servercertificaat na 8 weken worden ingetrokken. De kosten van een eventueel nieuw servercertificaat zijn voor rekening van de abonnee.

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

4.6 Sleutelpaar en certificaatgebruik

4.6.1 Verplichtingen van abonnee en certificaathouder

- De abonnee garandeert dat alle aangeleverde gegevens juist en volledig zijn. Dit betreft de gegevens gerelateerd aan de abonneeregistratie, de certificaataanvraag en overige gegevens.
- De abonnee garandeert expliciet dat de certificaathouders behorend bij de abonnee de door hem aangevraagde certificaten binnen het toepassingsgebied zoals beschreven in hoofdstuk 1.4 van het CPS gebruiken en dat de certificaathouders het juiste certificaat gebruiken voor de juiste toepassing. De abonnee en de certificaathouder zijn verplicht om op aanwijzing van het UZI-register het gebruik van de certificaten en de bijbehorende private sleutels 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, aan de abonnee te overleggen. De abonnee en de certificaathouder 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 pincode, pukcode en de intrekkingscode door de certificaathouders binnen de organisatie altijd apart van de UZI-pas bewaard worden.

- De abonnee bevestigt dat het UZI-register gerechtigd is om de UZI-middelen in te trekken indien de abonnee de toepasselijke voorwaarden schendt, of wanneer CIBG vaststelt dat het certificaat gebruikt wordt bij criminele activiteiten, bijvoorbeeld phishing aanvallen, fraude, of de distributie van kwaadaardige software.
- De abonnee en aanvrager van UZI-middelen bevestigt dat het UZI-register gerechtigd is om persoonsgegevens, waaronder naam, adres, e-mail en telefoonnummer aan X-pact B.V. en Dynalogic te verstrekken.

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 en de inhoud hiervan juist is.
- 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[10].
- 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.
- Indien de domeinnaam (FQDN) zoals vermeld in een servercertificaat identificeerbaar en adresseerbaar is via het internet, garandeert de abonnee dat het servercertificaat alleen op een server wordt gezet die ten minste bereikbaar is met één van de FQDN's in dit servercertificaat.

10 Het UZI-register heeft het recht om de compenserende maatregelen te controleren.

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.

4.6.2 Verplichtingen van de vertrouwende partij

De verplichtingen van de vertrouwende partij zijn van toepassing wanneer er vertrouwd wordt op een certificaat uitgegeven door het UZI-register. De vertrouwende partij is verplicht om:

- per individueel geval zelfstandig te beoordelen of het gerechtvaardig is om op het certificaat te vertrouwen;
- de geldigheid en authenticiteit van de hiërarchie te controleren waarbinnen het certificaat is uitgegeven, inhoudende de geldigheid van certificaten van bovenliggende CA's alsmede van het stamcertificaat van de Staat der Nederlanden;
- de geldigheid van het certificaat door middel van de meest recent gepubliceerde Certificaten Revocatie Lijst (CRL) of via het Online Certificate Status Protocol (OCSP) te verifiëren;
- bij calamiteiten en/of incidenten waarbij het Online Certificate Status Protocol (OCSP) onbereikbaar is altijd de meest recent gepubliceerde Certificaten Revocatie Lijst (CRL) te gebruiken;
- kennis te nemen van alle verplichtingen over het gebruik van het certificaat zoals vermeld in voorliggend CPS en de vertrouwende partij voorwaarden, hieronder uitdrukkelijk mede begrepen alle beperkingen over het gebruik van het certificaat;
- alle overige voorzorgsmaatregelen te nemen die in redelijkheid door vertrouwende partijen genomen kunnen worden;
- zich ervan bewust te zijn dat voorgaande controles slechts de integriteit van de gegevens en de identiteit van de certificaathouder authenticeren, wat uitdrukkelijk geen oordeel inhoudt over de inhoud van de gegevens.

4.7 Vernieuwen van certificaten

Sleutels van certificaathouders zullen niet opnieuw worden gebruikt na het verstrijken van de geldigheidsduur of na het intrekken van de bijbehorende certificaten. Met het vernieuwen van certificaten wordt ook het sleutelpaar vernieuwd.

4.8 Re-Key van certificaten

Als na het (dreigend) verstrijken van de geldigheidsduur of na het intrekken een nieuwe UZI-pas wordt aangevraagd, dan worden hiervoor nieuwe sleutelparen en nieuwe certificaten aangemaakt. De procedures, controles en werkwijze die met betrekking tot aanvraag, productie en verstrekking worden gehanteerd zijn gelijk aan de procedures, controles en werkwijze rondom de eerste uitgifte.

4.9 Aanpassing van certificaten

Als aanpassing van certificaten noodzakelijk is, moeten de certificaten worden ingetrokken en moeten nieuwe certificaten met gewijzigde gegevens worden aangevraagd.

4.10 Intrekking en opschorting van certificaten

Verzoeken tot het intrekken van certificaten kunnen worden ingediend zoals hierna beschreven. Het UZI-register zorgt ervoor dat datum en tijdstip van intrekking van

certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door het UZI-register vastgestelde tijdstip als moment van intrekking. Als een certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

Het UZI-register staat (tijdelijke) opschorting van certificaten niet toe.

4.10.1 Omstandigheden die leiden tot intrekking

De certificaathouder of de abonnee zijn verplicht een verzoek tot intrekking in te dienen bij het UZI-register en het gebruik van het certificaat inclusief de bijbehorende sleutels te stoppen 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 pukcode is ingevoerd).
- Beëindiging bestaan abonnee.
- Beëindiging van de relatie tussen abonnee en certificaathouder.
- Onjuistheden in of wijziging van de gegevens die op de certificaten vermeld staan.
- Niet meer voldoen aan toetsingscriteria zoals beschreven in bijlage 2.
- Systeem / server niet meer in gebruik bij de zorginstelling.
- Toestemming om de domeinnaam te gebruiken is ingetrokken.

Intrekking op initiatief van het UZI-register vindt plaats in de volgende omstandigheden:

- De certificaten van een abonnee of certificaathouder kunnen worden ingetrokken als de abonnee of certificaathouder zich niet houdt aan de verplichtingen in het CPS.
- De certificaten van een abonnee worden ingetrokken als deze niet meer voldoet aan de toetsingscriteria in bijlage 2.
- Een zorgverlenerpas wordt ingetrokken als de houder de beroepstitel, opleidingstitel of het specialisme dat in het certificaat is opgenomen niet meer mag gebruiken. Hierbij kan het UZI-register een overgangstermijn van een maand hanteren voor ‘uitstervende’ specialismen. Een verdere toelichting is opgenomen in bijlage 2.
- Een servercertificaat wordt ingetrokken als de eigenaar van de domeinnaam aan het UZI-register meldt dat de toestemming tot gebruik van de domeinnaam wordt ingetrokken.
- Een servercertificaat wordt ingetrokken als de eigenaar ook na herhaald verzoek van het UZI-register de correcte ontvangst niet bevestigt.
- Een servercertificaat wordt ingetrokken indien deze niet binnen de gestelde termijn is betaald[11].
- De certificaten van een UZI-pas worden ingetrokken wanneer de uitgifte van de pas niet binnen de gestelde termijn van 6 weken heeft plaatsgevonden.
- De certificaten van een UZI-pas worden ingetrokken indien deze niet binnen de gestelde termijn is betaald[9].
- De certificaten van een abonnee of certificaathouder worden ingetrokken als het UZI-register onjuistheden constateert in de gegevens die zijn opgenomen in het certificaat, bijvoorbeeld bij een naamswijziging.
- De certificaten van een abonnee of certificaathouder worden ingetrokken wanneer de private sleutel behorende bij de certificaten, of de sleutel van de TSP of PKIoverheid is aangetast.
- De certificaten van een abonnee of certificaathouder worden ingetrokken als de technische inhoud van het certificaat een onverantwoord risico met zich mee

11 Zoals gesteld in sectie 9.1.7 is de termijn gesteld op zes weken na de ontvangst van de aanmaning.

brengt voor abonnees, vertrouwende partijen en derden (bijvoorbeeld browserpartijen).

De beweegreden voor elke intrekking geïnitieerd door het UZI-register wordt gedocumenteerd en gearchiveerd.

4.10.2 Wie mag verzoek tot intrekking indienen

Een verzoek tot intrekking van certificaten mag worden ingediend door:

- de certificaathouder zelf of de certificaatbeheerder;
- de wettelijk vertegenwoordiger of een geautoriseerde pasaanvrager van de abonnee;
- de curator die optreedt wanneer de abonnee of certificaathouder zelf niet langer bevoegd is rechtshandelingen met beoogd rechtsgevolg te verrichten;
- het UZI-register.

Een vertrouwende partij kan geen verzoek tot intrekking doen, maar kan wel melding maken van het vermoeden van een omstandigheid die aanleiding kan zijn tot het intrekken van een certificaat. Het UZI-register zal een dergelijk geval de melding onderzoeken en zal indien nodig het certificaat intrekken.

4.10.3 Procedure voor verzoek tot intrekking

Verzoeken tot intrekking van certificaten kunnen door een daartoe bevoegd persoon van de abonnee of door de certificaathouder elektronisch worden gedaan, of telefonisch, per e-mail, of per post. Nadrukkelijk wordt erop gewezen dat, in geval met de intrekking een spoedeisend belang gediend is, dit elektronisch via de website van het UZI-register (www.zorgcsp.nl) dient te geschieden. Deze vorm van intrekking is vierentwintig uur per dag, zeven dagen per week beschikbaar.

Bij **elektronische** intrekking vult de aanvrager het smartcardnummer van de intrekken pas en de bijbehorende intrekkingscode op de website van het UZI-register. Als intrekkingcode en smartcardnummer correct zijn, wordt de pas ingetrokken. De aanvrager krijgt hiervan op website een melding. Als de intrekkingcode en smartcardnummer niet correct zijn, wordt teruggemeld dat de intrekking niet wordt uitgevoerd. Het UZI-register heeft maatregelen genomen om te voorkomen dat onbeperkt (foutieve) intrekkingverzoeken kunnen worden gedaan.

Bij **telefonische**[12] intrekking worden geen documenten overlegd. De indiener van het intrekkingverzoek dient een aantal vooraf vastgestelde vragen te beantwoorden. Aan de hand van deze vragen dient het UZI-register voldoende zekerheid te verkrijgen over de identiteit van de aanvrager van de intrekking en de pas waarvoor intrekking wordt aangevraagd. Na het vaststellen van de identiteit van de indiener van het intrekkingverzoek en van de pas, controleert het UZI-register of de indiener bevoegd is de aanvraag tot intrekking te doen. Na uitvoering van de controles trekt het UZI-register de certificaten in. Een bevestiging van de afhandeling of melding van de afwijzing van het verzoek tot intrekking wordt schriftelijk aan de certificaathouder gemeld.

Bij intrekking **per niet-elektronisch ondertekende e-mail, of per post** moeten de volgende bewijzen worden overlegd:

- Een door de tot intrekking bevoegde persoon ondertekend verzoek tot intrekken met daarin:
  - de naam van de abonnee;
  - de naam van de persoon die het verzoek tot intrekking doet;

12 Zoals gesteld in sectie 3.4 is het telefonisch intrekken van servercertificaten niet mogelijk

de aanduiding van de pas of passen waarvoor het verzoek geldt. Het UZI-register controleert of de handtekening op het intrekkingsverzoek overeenkomt met de gearchiveerde kopie van een identificatiedocument zoals genoemd in de WID.

- Indien de handtekening overeenkomt, voert het UZI-register het intrekkingverzoek uit.
- Indien de handtekening niet overeenkomt, neemt het UZI-register telefonisch contact op met de abonnee via de bij het UZI-register geregistreerde contactgegevens. De aanvrager wordt hierbij verzocht om de handtekening conform het bij het UZI-register gearchiveerde WID te zetten. Als de handtekening op het WID is gewijzigd wordt de aanvrager verzocht een geldige kopie van het WID aan het UZI-register toe te sturen. Na herhaalde controle van de handtekening voert het UZI-register het intrekkingverzoek uit. Het UZI-register archiveert de nieuwe kopie van het WID.
- Indien er geen identificatiedocument bekend is bij het UZI-register moet deze met de aanvraag worden meegestuurd.

Bij intrekking via **elektronische ondertekende e-mail** geldt onderstaande eis:

- De e-mail is ondertekend door de tot intrekking bevoegde persoon met een gekwalificeerd onweerlegbaarheidcertificaat (zoals op de UZI-pas voor zorgverleners en medewerkers op naam of een andere PKI overheidspas).

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 of een reeds eerder gearchiveerde kopie van het identiteitsbewijs. Na uitvoering van de controles trekt het UZI-register de certificaten in en plaatst deze daarmee op de Certificate Revocation List (CRL). Een bevestiging van de afhandeling of melding van de afwijzing van het verzoek tot intrekking wordt schriftelijk aan de certificaathouder gemeld.

4.10.4 Uitstel van verzoek tot intrekking

De certificaathouder of de abonnee zijn verplicht om per direct en zonder vertraging een verzoek tot intrekking in te dienen bij het UZI-register in situaties zoals vermeld in paragraaf 4.9.1.

4.10.5 Tijdsduur voor verwerking van verzoek tot intrekking

Elektronische verzoeken worden direct online afgehandeld. Het UZI-register adviseert partijen om gebruik te maken van de faciliteiten ten behoeve van elektronische intrekking op de website van het UZI-register. Deze faciliteiten zijn vierentwintig uur per dag en zeven dagen per week beschikbaar. Bij elektronische en telefonische intrekking is de maximale vertraging tussen de ontvangst van het verzoek en wijziging van de revocation status information (CRL) vier uur.

Verzoeken tot intrekking welke per e-mail of post binnenkomen worden alleen binnen vier uur afgehandeld als het verzoek op werkdagen tijdens kantoortijden is ontvangen.

Verzoeken buiten kantoortijden worden op zijn vroegst de volgende werkdag binnen vier uur na ontvangst in behandeling genomen. Indien de intrekking een spoedeisend belang heeft, dient dit elektronisch (24 uur per dag en zeven dagen per week) of telefonisch (alleen mogelijk tijdens kantooruren 9:00 tot 17:00) te geschieden.

4.10.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie

Vertrouwende partijen zijn verplicht de actuele status (ingetrokken/niet ingetrokken) van een certificaat te controleren door raadpleging van de meest recent gepubliceerde CRL of via de faciliteit OCSP. Tevens zijn vertrouwende partijen gehouden om de elektronische handtekening waarmee de CRL is getekend, inclusief het bijbehorende certificatiepad, te controleren.

4.10.7 CRL-uitgiftefrequentie

De CRL-uitgiftefrequentie is elk uur. Ook in geval van systeemdefecten, service-activiteiten of andere factoren die buiten het bereik van het UZI-register liggen, zorgt het UZI-register er voor dat intrekkingverzoeken die via de registratiewebsite worden ingediend binnen vier uur na indiening zijn uitgevoerd. Daartoe is een uitwijkscenario ontworpen, dat regelmatig wordt getest.

Als de processen die vertrouwen op de UZI-certificaten een hogere actualiteit van de certificaatstatus vereisen, wordt dringend geadviseerd om gebruik te maken van de faciliteit voor online controle van de intrekkingstatus (zie paragraaf 4.9.9).

Ingetrokken certificaten blijven op de CRL staan zolang hun oorspronkelijke geldigheidsdatum niet is verstreken.

4.10.8 Tijd tussen generatie en publicatie

De CRL wordt direct na generatie gepubliceerd.

4.10.9 On line intrekking / statuscontrole

Naast de publicatie van CRL's biedt het UZI-register ook certificaat statusinformatie via de faciliteit Online Certificate Status Protocol (OCSP). De inrichting van OCSP is in overeenstemming met IETF RFC 2560.

OCSP validatie is een online validatie methode waarbij het UZI-register aan de vertrouwende partij een elektronisch ondertekend bericht (OCSP response) verstuurt nadat de vertrouwende partij een specifiek verzoek om statusinformatie (OCSP request) heeft verstuurd naar de OCSP dienst (OCSP responder) van het UZI-register. In de OCSP response staat de opgevraagde status van het betreffende certificaat. De status kan de volgende waarden aannemen: goed, ingetrokken of onbekend. Als een OCSP response om enigerlei reden uitblijft, kan daaruit geen conclusie worden getrokken met betrekking tot de status van het certificaat. De URL van de OCSP responder waarmee de intrekkingstatus van een certificaat gevalideerd kan worden, staat in het AuthorityInfoAccess.uniformResourceIndicator attribuut van het certificaat.

Een OCSP respons is altijd door de OCSP responder verzonden en ondertekend. Een vertrouwende partij dient de handtekening onder de OCSP respons te verifiëren met het systeemcertificaat dat meegestuurd wordt in de OCSP respons. Dit systeemcertificaat is uitgegeven door dezelfde Certification Authority (CA) als de CA die het certificaat heeft uitgegeven waarvan de status wordt opgevraagd.

De informatie die via de OCSP responder wordt verstrekt, kan actueler zijn dan de informatie die via de CRL wordt gecommuniceerd. Dit is alleen het geval als een intrekking heeft plaatsgevonden en de reguliere vernieuwing van de CRL nog niet heeft plaatsgevonden.

4.10.10 Vereisten online controle intrekkingstatus

Deze dienst is onbeperkt toegankelijk voor alle vertrouwende partijen die de intrekkingstatus van een door het UZI-register uitgegeven certificaat willen valideren.

4.11 Certificaat statusservice

Het UZI-register geeft elk uur een nieuwe CRL uit. Met behulp van OCSP kan de actuele statusinformatie worden opgevraagd.

In geval van verstoring van deze diensten, zorgt het UZI-register er voor dat deze diensten binnen vier uur na constatering van de verstoring weer beschikbaar zijn. Dit geldt alleen voor de CRL. In geval van verstoringen is het verplicht om altijd gebruik te maken van de CRL en dus niet van OCSP.

4.12 Beëindiging abonnee relatie

De registratie als abonnee kent geen einddatum. Als de relatie tussen de abonnee en het UZI-register wordt beëindigd, wordt de abonnee in het UZI-register doorgehaald.

Met een verzoek tot doorhalen van de registratie geeft de abonnee aan geen gebruik meer te willen maken van de dienstverlening van het UZI-register. De abonnee wordt dan uitgeschreven uit het UZI-register. Een verzoek tot doorhalen van een registratie van een abonnee (en daarmee tot intrekking van de certificaten die onder de abonnee zijn uitgegeven) dient schriftelijk te worden ingediend bij het UZI-register. Het UZI-register authenticeert de aanvrager van het verzoek conform de authenticatie bij aanvraag tot registratie.

4.12.1 Overgangstermijn voor een zorgverlener abonnee

Bij overlijden,onvoorwaardelijke schorsing of na doorhaling in het BIG-register van een zorgverlener die abonnee is, treedt een overgangstermijn van drie maanden in werking. Deze overgangstermijn houdt het volgende in:

- alle passen op naam (zorgverlenerpas en medewerkerpassen op naam) worden volgens de geldende regels ingetrokken. Dit geldt ook voor de passen op naam die vlak voor of tijdens de overgangstermijn zijn aangevraagd en/of verstrekt.
- medewerkerpassen niet op naam en servercertificaten blijven actief.
- de abonneeregistratie blijft actief.
- geen nieuwe producten mogen meer worden aangevraagd.

Na de overgangstermijn worden de medewerkerpassen niet op naam en servercertificaten ingetrokken en wordt de abonneeregistratie doorgehaald. Indien onder de abonneeregistratie geen of alleen UZI-passen op naam (de zorgverlenerpas en medewerkerpas op naam) actief zijn wordt de abonneeregistratie direct ingetrokken. Het UZI-register geeft geen restitutie voor de resterende geldigheidstermijn van de ingetrokken UZI-middelen.

4.12.2 Overgangstermijn voor een organisatie abonnee

Bij een naamswijziging of beëindiging van een instelling die abonnee is, treedt een overgangstermijn van drie maanden in werking. Deze overgangstermijn houdt het volgende in:

- Alle passen op naam (zorgverlenerpassen en medewerkerpassen op naam), medewerkerpassen niet op naam en servercertificaten blijven actief.
- de abonneeregistratie blijft actief.
- geen nieuwe producten mogen meer worden aangevraagd.

Na de overgangstermijn worden alle passen en servercertificaten ingetrokken en wordt de abonneeregistratie doorgehaald. Het UZI-register geeft geen restitutie voor de resterende geldigheidstermijn van de ingetrokken UZI-middelen.

4.13 Key escrow en recovery

Het UZI-register ondersteunt geen key escrow en key recovery.

5 Fysieke, procedurele en personele beveiliging

5.1 Fysieke beveiliging

De dienstverlening van het UZI-register vindt plaats vanuit verschillende locaties. De registratiewerkzaamheden worden verricht op de vestigingslocatie van het CIBG. De personalisatiewerkzaamheden vinden plaats op de vestigingslocatie van de leverancier van personalisatiediensten. De certificatie vindt plaats op het rekencentrum van de leverancier van CA-diensten. De werkzaamheden met betrekking tot de mobiele identificatie en uitgifte vinden plaats op locatie.

Voor alle locaties zijn de benodigde fysieke beveiligingsmaatregelen getroffen. Deze maatregelen zijn genomen op basis van risicoanalyses en beveiligingsplannen. De genomen maatregelen waarborgen een afgeschermd en goed beveiligd registratie-, personalisatie-, certificatie-, uitgifte en intrekkingproces, waarbij ongeautoriseerde toegang tot of inbreuk op deze processen of de locaties waar deze processen worden uitgevoerd, wordt tegengegaan. Zo vinden de werkzaamheden met betrekking tot de certificatie plaats in de zwaar beveiligde omgeving binnen een rekencentrum. Deze omgeving voldoet aan de voor de overheid in deze geldende wet- en regelgeving, waaronder onder meer begrepen de Wet Bescherming Staatsgeheimen 1951. In alle locaties zijn tal van maatregelen getroffen om noodsituaties te voorkomen en om eventuele schade bij noodsituaties te beperken. Voorbeelden daarvan zijn bliksemafleiding, energie voorziening, bouwkundige maatregelen en toegangsprocedures.

Het UZI-register beschikt over gescheiden test/acceptatie- en productiesystemen. Het overbrengen van programmatuur van de ene omgeving naar de andere vindt beheerst plaats via een change management procedure. Deze change management procedure omvat onder andere het bijhouden en vastleggen van versies, wijzigingen en noodreparaties van alle operationele software. Voordat programmatuur in productie wordt genomen, voert het UZI-register testen uit op basis van vooraf vastgestelde testplannen.

De integriteit van TSP-systemen en -informatie wordt beschermd tegen virussen, schadelijke en niet-geautoriseerde software en andere mogelijk bronnen die kunnen leiden tot verstoring van de dienstverlening, door middel van een samenstel van passende fysieke, logische en organisatorische maatregelen. Deze maatregelen zijn preventief, repressief en correctief van aard. Voorbeelden van maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen.

Opslagmedia van systemen die worden gebruikt worden veilig behandeld om de opslagmedia tegen schade, diefstal en niet-geautoriseerde toegang te beschermen. Opslagmedia worden zorgvuldig verwijderd wanneer zij niet meer nodig zijn.

Het capaciteitsgebruik wordt bijgehouden en voorspellingen van de in de toekomst vereiste capaciteit worden gemaakt om te voorzien in voldoende verwerkingsvermogen en opslagcapaciteit in de toekomst.

Het UZI-register onderneemt op tijdige en gecoördineerde wijze actie om snel te reageren op incidenten en om de invloed van inbreuk op de beveiliging te beperken. Alle relevante incidenten worden onmiddellijk gemeld aan door wet- en regelgeving vastgestelde organisaties nadat zij zich hebben voorgedaan. Incidenten van een

tevoren door de Policy Authority van de PKI voor de overheid te bepalen categorie, worden aan die Policy Authority gerapporteerd.

5.2 Procedurele beveiliging

5.2.1 Vertrouwelijke functies

Personeel met toegang tot cryptografisch materiaal, of personen die daarbij in een vertrouwensrol opereren, hebben een functie die als vertrouwelijk wordt gekwalificeerd. Hierdoor is het al het personeel in vertrouwelijke functies gescreend op het aanwezig zijn van tegengestelde belangen die de onpartijdigheid van de activiteiten van het UZI-register zouden kunnen beïnvloeden.

5.2.2 Aantal personen benodigd per taak

De dienstverlening van het UZI-register is zodanig ingericht dat het niet mogelijk is dat één persoon het betrouwbaarheidsniveau van de dienstverlening kan aantasten. Registratie, personalisatie, certificatie en uitgifte zijn organisatorisch gescheiden taken. Voor registratietaken wordt het ‘vier-ogen’ principe en/of functiescheiding toegepast.

5.2.3 Identificatie en authenticatie met betrekking tot TSP functies

Geen nadere bepalingen.

5.2.4 Functiescheiding

Het UZI-register hanteert functiescheiding tussen uitvoerende, beslissende en controlerende taken. Daarnaast is er sprake van functiescheiding tussen systeembeheer en bediening van de TSP systemen, alsmede tussen Security Officer(s), Systeem auditor(s), systeembeheerder(s) en TSP operator(s).

5.3 Personele beveiliging

5.3.1 Functie-eisen

Alle bij de dienstverlening van UZI-register betrokken medewerkers bezitten ruime kennis en ervaring op gebied van certificatiedienstverlening. Medewerkers die belast zijn met de controle van identificatiedocumenten bezitten de benodigde kennis om de echtheidskenmerken van deze documenten te controleren.

Beveiligingstaken en verantwoordelijkheden, waaronder vertrouwelijke functies, zijn gedocumenteerd in functieomschrijvingen. Deze zijn opgesteld op basis van de scheiding van taken en bevoegdheden en waarin de gevoeligheid van de functie is vastgesteld.

Autorisatie van alle medewerkers vindt plaats op basis van het ‘need-to-know’ principe. Voor alle vertrouwelijke en administratieve taken, die invloed hebben op de levering van certificatiediensten, zijn procedures opgesteld en geïmplementeerd.

5.3.2 Antecedentenonderzoek

Alle medewerkers die betrokken zijn bij personalisatie en certificatie werkzaamheden zijn onderwerp van antecedentenonderzoek. Het UZI-register vraagt van alle medewerkers die betrokken zijn bij registratie en uitgifte een Verklaring omtrent Gedrag.

Met betrekking tot alle medewerkers die taken uitvoeren voor het UZI-register worden activiteiten uitgevoerd in het kader van training en bewustwording voor de uitvoering van hun taak.

5.3.3 Trainingseisen

Het UZI-register zet voldoende personeel in dat beschikt over voldoende vakkennis, ervaring en kwalificaties die noodzakelijk zijn voor de TSP dienstverlening. Managers zijn doordrongen van de aard van de certificatiedienstverlening en bijbehorende kwaliteitsniveau.

5.3.4 Opleidingen

Voor alle functies is het volgen van specifieke trainingen verplicht. Om het volgen van deze opleidingen te bewaken, wordt gebruik gemaakt van een jaarlijks te actualiseren opleidingsplan.

5.3.5 Frequentie van taak-roulatie en loopbaanplanning

Geen nadere bepalingen.

5.3.6 Sancties van ongeautoriseerd handelen

Een medewerker die een ongeautoriseerde actie onderneemt, wordt terstond de toegang tot alle systemen ontnomen. Het TSP management beslist over de duur en de voorwaarden van de ontzegging en de verder te nemen acties en sancties.

5.3.7 Inhuur van personeel

Voor ingehuurd personeel gelden de hiervoor genoemde eisen. Inhuur van personeel gebeurt op basis van mantelcontracten.

5.3.8 Beschikbaar stellen documentatie medewerkers

Aan medewerkers van het UZI-register wordt aantoonbaar de documentatie ter beschikking gesteld die nodig is voor de goede vervulling van de hun opgedragen taak.

5.4 Procedures ten behoeve van beveiligingsaudits

5.4.1 Vastleggen van gebeurtenissen

Het UZI-register houdt overzichten bij van:

- Aanmaken van accounts.
- Installatie van nieuwe software of software updates.
- Datum en tijd en andere beschrijvende informatie betreffende back-ups.
- Datum en tijd van alle hardware wijzigingen.
- Datum en tijd van audit-log dumps.
- Afsluiten en (her)starten van systemen.
- Alle registratiehandelingen met betrekking tot aanvraag en intrekking van certificaten en eventuele wijzigingen van registratiegegevens.

Het UZI-register houdt de volgende gebeurtenissen handmatig of automatisch bij:

- Levenscyclus gebeurtenissen ten aanzien van de CA sleutel, waaronder:
  - genereren van sleutels, back-up, opslag, herstel, archivering en vernietiging;
  - levenscyclus gebeurtenissen ten aanzien van de cryptografische apparatuur.
- Levenscyclus gebeurtenissen ten aanzien van het beheer van certificaten, waaronder:
  - certificaataanvragen, heruitgifte en intrekking;
  - geslaagde of niet-geslaagde verwerking van aanvragen;
  - genereren en het uitgeven van certificaten en CRL's.
- Beveiligingsincidenten, waaronder:
  - geslaagde en niet-geslaagde pogingen om toegang tot het systeem te verkrijgen;
  - PKI en beveiligingsactiviteiten ondernomen door personeel;
  - lezen, schrijven of verwijderen van beveiligingsgevoelige bestanden of records;
  - veranderingen in het beveiligingsprofiel;
  - systeem crashes, hardware uitval, en andere onregelmatigheden.

De onderdelen van de loggingen bevatten de volgende elementen:

- Datum en tijd.
- Volgnummer.
- Identiteit invoerder.
- Soort.

5.4.2 Interval uitvoeren loggingen

Loggingen worden steekproefsgewijs en als onderdeel van interne kwaliteitsprocessen onderzocht.

5.4.3 Bewaartermijn loggingen

De geconsolideerde loggingen worden voor een periode van tenminste zeven jaar bewaard.

5.4.4 Beveiliging audit logs

Gebeurtenissen die op elektronische- en handmatige wijze worden opgenomen in audit log files worden beschermd tegen niet geautoriseerde inzage, wijziging, verwijdering, of andere ongewenste aanpassingen door middel van fysieke en logische toegangscontrole middelen.

5.4.5 Bewaren van audit logs

Alle audit logs worden intern op de systemen bewaard. Daarnaast wordt logging off-site gearchiveerd. De belangrijkste loggegevens worden per kwartaal ook gearchiveerd bij het CIBG.

5.4.6 Kennisgeving van logging gebeurtenis

Het UZI-register stelt een nader onderzoek in wanneer uit de logging kwaadwillende acties zijn af te leiden.

5.4.7 Kwetsbaarheidsanalyse

Minimaal jaarlijks voert het UZI-register een risicoanalyse uit, met als onderdeel hiervan een kwetsbaarheidsanalyse. Op basis van de uitkomsten van deze analyses treft het UZI-register indien nodig passende maatregelen.

5.5 Archivering van documenten

5.5.1 Gebeurtenissen

Het UZI-register archiveert alle relevante informatie met betrekking tot gebeurtenissen, gegevens, bestanden en formulieren. Tenminste worden vastgelegd:

- Aanvragen tot registratie en aanvragen tot certificatie (aanvraagformulieren).
- Overlegde documenten in de aanvraagprocedure (waaronder kopie identiteitsbewijs, uittreksel uit het Handelsregister van de Kamer van Koophandel, oprichtingsdocument en origineel gewaarmerkte kopie van een diploma).
- Opslaglocatie van kopieën van aanvragen en identiteitsdocumenten.
- Informatie die relevant is voor de identificatie van een abonnee of certificaathouder.
- Informatie betreffende de uitgevoerde controles.
- Correspondentie met betrekking tot registratieaanvraag of pasaanvraag.
- Bewijs van datum en tijdstip van uitgifte van de certificaten.
- Informatie betreffende verzoeken tot intrekking van certificaten of doorhalen van de registratie.
- Ontvangen klachten en correspondentie met betrekking tot klachten.
- Schriftelijk ontvangen informatieverzoeken.

5.5.2 Bewaartermijn van het archief

Alle gearchiveerde gebeurtenissen worden conform hoofdstuk 10.4 van de selectielijst[13] gedurende een periode van zeven jaar na de datum waarop de geldigheid van het gekwalificeerde certificaat is verlopen bewaard

Alle gearchiveerde gebeurtenissen met betrekking tot de abonneeregistratie worden gedurende een periode van zeven jaar na de datum waarop de abonneeregistratie is doorgehaald bewaard.

5.5.3 Beveiliging van het archief

Het UZI-register zorgt voor de integriteit en toegankelijkheid van de gearchiveerde gegevens. Het UZI-register zorgt voor een zorgvuldige en beveiligde wijze van opslag en archivering.

5.5.4 Archief back-up procedures

Incrementele back-ups van het registratiesysteem en van digitale documenten worden op dagelijkse basis gecreëerd, volledige back-ups worden op wekelijkse basis uitgevoerd en worden ook gearchiveerd op een externe locatie. Van het papieren archief wordt geen back-up gemaakt.

5.5.5 Voorwaarden en tijdsaanduiding van vastgelegde gebeurtenissen

Alle informatie op papier is voorzien van een dagtekening en/of een datum van binnenkomst.

Elektronisch opgeslagen informatie is voorzien van de datum en tijd van het verwerkend systeem waarop de handeling is verricht. De verwerkende systemen

---

13 Generieke Selectielijst voor de archiefbescheiden van het CIBG Dienst voor registers vanaf 1995- vallend onder het zorgdragerschap van het Ministerie van Volksgezondheid, Welzijn en Sport en Stichting Donorgegevens Kunstmatige Bevruchting vanaf 1995

worden volgens het Network Time Protocol gesynchroniseerd met een betrouwbare tijdsbron, die is gebaseerd op de atoomklok in Frankfurt.

De datum en tijd van de uitgifte van een pas wordt bij uitgifte vastgelegd en door beide partijen ondertekend.

5.5.6 Archiveringssysteem
Elektronische archivering vindt op fysiek gescheiden locaties plaats (online data synchronisatie). Papieren dossiers worden op één fysieke locatie bewaard.

5.5.7 Het verkrijgen en verifiëren van gearchiveerde informatie
Geen nadere bepalingen.

5.6 Vernieuwen sleutels na re-key CA

Als de CA een nieuw sleutelpaar in gebruik neemt worden de nieuwe CA certificaten op de UZI-pas geplaatst. Daarnaast worden de CA certificaten beschikbaar gemaakt in de directory en op de website.

5.7 Aantasting en continuïteit

Het UZI-register heeft een calamiteitenplan opgesteld om, in geval van een calamiteit, de gevolgen hiervan te minimaliseren. In het Business Continuity Plan zijn procedures en werkwijze rondom uitwijk van dienstverlening beschreven.

Het UZI-register kan bij eventuele compromittatie van sleutels of in geval van calamiteiten een onderzoek instellen, maar is hiertoe niet verplicht. Bij compromittatie van (een van) de private sleutel(s) van het UZI-register neemt het UZI-register minimaal de volgende acties:

- Het UZI-register stelt vertrouwende partijen, abonnees en certificaathouders hiervan zo spoedig mogelijk op de hoogte door de informatie te publiceren op https://www.uzi-register.nl
- Het UZI-register stelt de betrokken abonnees hiervan op de hoogte via een e-mail op het bij registratie opgegeven e-mail adres.
- Als dit noodzakelijk is, zal het UZI-register de betrokken certificaten direct intrekken en publiceren op de toepasselijke CRL.
- Het UZI-register stelt de Policy Authority van de PKI voor de overheid, Agentschap Telecom, NCSC, certificerende instantie en eventueel Autoriteit Persoonsgegevens onmiddellijk op de hoogte van de calamiteit.

Bij compromittatie van een van de door het UZI-register gebruikte algoritmen treedt het UZI-register in overleg met de Policy Authority van de PKI voor de overheid. In principe zal het UZI-register de richtlijnen van de Policy Authority volgen. Voordat wordt overgegaan tot grootschalige revocatie als gevolg van compromittatie van een algoritme vindt afstemming plaats met VWS.

5.8 TSP beëindiging

In geval het UZI-register de certificatiedienstverlening beëindigt, zal dit plaatsvinden conform een gecontroleerd proces zoals nader beschreven in het UZI-register CA Termination Plan. Deze beëindiging kan zowel van vrijwillige of onvrijwillige aard zijn, de uit te voeren activiteiten zijn hiervan afhankelijk.

Onderdelen van het plan bij beëindiging zijn onder andere het:

- Communicatie met abonnees, vertrouwende partijen en andere TSP's waarmee relaties bestaan of andere vormen van reguliere samenwerking;
- Buiten gebruik stellen van de relevante private CA keys;

- De publicatiedienst dient minimaal zes maanden na beëindiging actief te blijven;
- Aan Consortium zal opdracht gegeven worden tot de LunaCA Zeroization and Destruction Key Ceremony op nader te bepalen datum. Consortium zal ter bevestiging een procesverbaal aan CIBG overhandigen van de venietiging.
- Aan Doc-Direkt zal opdracht gegeven worden tot vernietigen van dossiers. Conform Doc-Direkt PDC (zie Rijksportaal).

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

Bij het genereren van sleutelparen maakt het UZI-register gebruik van veilige middelen en betrouwbare systemen. Het UZI-register zorgt ervoor dat de betrouwbaarheid en de veiligheid van de systemen in ieder geval voldoen aan internationaal erkende standaards en nationale wetgeving.

Het genereren van de sleutels geschiedt in apparatuur die voldoet aan Common Criteria EAL 4+ of hoger in overeenstemming met ISO 15408 (‘Cryptographic module for TSP Signing Operations’).

6.1.1 Genereren van sleutelparen

Bij het genereren van sleutelparen maakt het UZI-register gebruik van betrouwbare procedures in een beveiligde omgeving, die voldoet aan objectieve en internationaal erkende standaards.

De sleutelgeneratie van de CA’s van het UZI-register heeft plaats gevonden in een FIPS 140-2 level 3 gecertificeerde Hardware Security Module (HSM). De sleutels van de CA’s zijn 4096 bits RSA.

De sleutelgeneratie van de (beoogde) certificaathouders vindt plaats in een FIPS 140-2 level 3 gecertificeerde HSM. Hierbij wordt gebruik gemaakt van het signature algoritme ‘.. De sleutels worden via een beveiligd communicatiekanaal in de smartcard (Secure Signature Creating Device - SSCD) geïnjecteerd. Overdracht van private sleutels en SSCD naar de gebruiker

De UZI-pas (smartcard met sleutels en certificaten) wordt:

- Persoonlijk overhandigd aan de certificaathouder in geval van een ‘zorgverlener’ of een ‘medewerker op naam’. De pincode, pukcode en intrekkingcode worden in de vorm van een pincodebrief separaat naar de beoogd certificaathouder gestuurd.
- Persoonlijk overhandigd aan de aanvrager/certificaatbeheerder namens de abonnee in geval van een ‘medewerker niet op naam’. De pincode, pukcode en intrekkingcode worden in de vorm van een pincodebrief separaat naar de aanvrager gestuurd.

Bij servercertificaten is er geen sprake van overdracht van de private sleutel. Het certificaat en de gecertificeerde publieke sleutel worden na persoonlijk verschijnen van de aanvrager/certificaatbeheerder namens de abonnee per e-mail verstuurd naar een bij aanvraag opgegeven e-mailadres.

6.1.2 Overdracht van publieke sleutels naar de CA

De sleutelparen voor UZI-passen worden door de personalisator gegenereerd. De publieke sleutels worden via beveiligde verbindingen in ondertekende berichten naar de CA verstuurd ter ondertekening.

Voor servercertificaten wordt het sleutelpaar gegenereerd door de abonnee/aanvrager. Ook hier wordt de publieke sleutel in een ondertekend bericht via een beveiligde verbinding aan de CA aangeboden.

6.1.3 Overdracht van de publieke sleutel van de TSP naar eindgebruikers
De publieke sleutel van de CA's van het UZI-register, zijn door een Domein CA van PKIoverheid getekend, waardoor tevens de integriteit en herkomst van de publieke sleutel wordt gewaarborgd. Deze publieke sleutels worden in de vorm van CA certificaten van het UZI-register aan vertrouwende partijen beschikbaar gesteld via www.zorgcsp.nl/

Sleutellengten
De sleutellengte van een Certificaat is minstens 2048 bits RSA. De sleutellengte van een CA-Certificaat is 4096 bits RSA.

Het UZI-register genereert sleutels in smartcards of HSM's die voldoen aan de FIPS 140-2 level 3 normering.

6.1.4 Doelen van sleutelgebruik (zoals bedoeld in X.509 v3)
De certificaten, inclusief de daarbij behorende sleutelparen, zijn uitsluitend bedoeld voor de doeleinden die beschreven zijn in dit CPS. De doelen waarvoor een sleutel gebruikt mag worden zijn opgenomen in het certificaat (veld: KeyUsage).

6.2 Private sleutel bescherming

6.2.1 Standaarden voor crytografische modulen
Voor operationeel gebruik worden de cryptografische gegevens opgeslagen in een Hardware Security Module (HSM). De HSM voldoet aan de eisen zoals beschreven FIPS 140-2 niveau 3 of hoger.

6.2.2 Functiescheiding beheer private sleutels
De private sleutels van de CA's van het UZI-register zijn niet in één stuk leesbaar.

Er wordt een back-up gemaakt van de private sleutels van de CA's van het UZI-register. De back-up wordt in meerdere versleutelde delen bewaard in cryptografische modules. De back-up kan alleen in gebruik genomen worden als meerdere partijen aanwezig zijn met hun deel van de sleutel.

6.2.3 Escrow van private sleutels van certificaathouders
Het UZI-register biedt vanaf 1 oktober 2013 geen key escrow en key recovery. Deze beëindiging geldt ook voor alle passen die voor die datum zijn uitgegeven.

6.2.4 Back-up van de private sleutels van certificaathouders
Het UZI-register maakt geen back-up van de private sleutels van certificaathouders.

6.2.5 Archivering van private sleutels van eindgebruikers en TSP
Private sleutels worden nooit gearchiveerd. Technische en organisatorische maatregelen zijn getroffen zodat de archivering van deze sleutels niet mogelijk is.

6.2.6 Toegang tot private sleutels in cryptografische module
Voor de private sleutels die zijn opgeslagen in een cryptografische hardwaremodule wordt toegangsbeveiliging gebruikt die zeker stelt dat de sleutels niet buiten de module kunnen worden gebruikt.

6.2.7 Opslag private sleutels
Private sleutels worden gedurende de gehele levensduur beveiligd opgeslagen.

6.2.8 Activeren private sleutels

Slechts door middel van een sleutelceremonie en de daarvoor noodzakelijk aanwezige functionarissen worden de private sleutels van de CA's van het UZI-register geactiveerd. Het UZI-register zorgt voor een zorgvuldige procedure in een beveiligde omgeving.

Voor activeren van private sleutels van eindgebruikers wordt een activeringscode verstrekt (zie paragraaf 6.4)

6.2.9 Methode voor deactiveren private sleutels

In de gevallen door UZI-register te bepalen zullen de private sleutels worden gedeactiveerd met inachtneming van de daarop van toepassing zijnde zorgvuldigheidsprocedures.

Als een door de certificaathouder verloren UZI-pas door de vinder aan het UZI-register wordt geretourneerd, zal het UZI-register de pas en de daarin opgenomen private sleutels vernietigen. Eventuele bij de pas behorende certificaten worden ingetrokken als deze nog actief zijn.

6.2.10 Methode voor vernietigen van private sleutels

De private sleutels waarmee certificaten worden ondertekend kunnen na het einde van hun levenscyclus niet meer worden gebruikt. Het UZI-register zorgt voor een adequate vernietiging waarbij wordt voorkomen dat het mogelijk is de vernietigde sleutels te herleiden uit de restanten.

6.2.11 Veilige middelen voor het aanmaken van elektronische handtekeningen

Toegepaste Hardware Security Modules binnen de systemen van het UZI-register zijn gecertificeerd conform FIPS 140-2 level 3. Hierdoor kan cryptografisch materiaal niet ongemerkt wordt gewijzigd tijdens opslag, gebruik en vervoer. De HSM's worden door de leverancier aangeleverd in tamper-evident bags, zijnde verpakking die elke vorm van corruptie daarvan toonbaar maken. Elke zending wordt direct na binnenkomst gecontroleerd aan de hand van de bijbehorende out-of-band list.

De smartcard (combinatie van microprocessor en operating system) is onafhankelijk gecertificeerd tegen de volgende standaarden:

- Common Criteria EAL4+(Common Criteria for Security Evaluation (Version 2.1, ISO/IEC 15408: 1999), Evaluation Assurance Level 4+ (EAL4+), http://www.commoncriteriaportal.org/)
- FIPS 140-2 level 3 (Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, http://csrc.nist.gov)

Verder voldoet de smartcard aan:

- ISO 7816 standaard (Information technology - Identification cards - Integrated circuit(s) cards with contacts)
- PKCS#15 (Cryptographic Token Information Syntax Standard (June 6th, 2000) , RSA Laboratories, www.rsasecurity.com.)

6.3 Andere aspecten van sleutelpaar management

Alle aspecten van het sleutelmanagement worden door het UZI-register uitgevoerd door toepassing van zorgvuldige procedures die in overeenstemming zijn met het beoogde doel.

6.3.1 Archiveren van publieke sleutels

Publieke sleutels worden gearchiveerd door het UZI-register voor tenminste zeven jaar na het verstrijken van de oorspronkelijke geldigheidsduur van een certificaat, in een fysiek veilige omgeving.

6.3.2 Gebruiksduur publieke/private sleutel

Tabel 6 geeft een overzicht van de geldigheidsduur van de SHA-2 generatie (G21).

Certificaat	Geldig tot
Stamcertificaat	23 maart 2020
Domeincertificaat	23 maart 2020
TSP certificaten	22 maart 2020

Tabel 6 Levensduur CA certificaten SHA-2 generatie (G21).

Tabel 7 geeft een overzicht van de geldigheidsduur van de Public G3/Private G1 hiërarchie.

Certificaat	Geldig tot
Stamcertificaat	14 november 2028
Domeincertificaat	13 november 2028
TSP certificaten	12 november 2028

Tabel 7 Levensduur CA certificaten Public G3/Private G1 hiërarchie

Voor de certificaten op de UZI-pas, inclusief de bijbehorende sleutelparen, wordt een maximale geldigheidsduur van drie jaar na de productiedatum gehanteerd. Voor certificaten in het servercertificaten wordt een maximale geldigheidsduur van drie jaar na de productiedatum gehanteerd. De productiedatum is de datum waarop de Certification Authority (CA) het certificaat heeft geproduceerd en gepubliceerd.

6.4 Activeringsgegevens

6.4.1 Generatie en installatie van activeringsgegevens

De toepassing van activeringsgegevens is verbonden aan het gebruik van een smartcard. Deze activeringsgegevens worden op veilige wijze voorbereid en gedistribueerd. Distributie gebeurt altijd gescheiden van de UZI-pas. De pincode en de pukcode bestaan in alle gevallen uit minimaal zes cijfers. De pincode en de pukcode worden alleen beschikbaar gesteld aan de certificaathouder en slechts eenmalig verstrekt.

6.4.2 Bescherming activeringsgegevens

De verspreiding van de activeringsgegevens vindt zodanig plaats dat het voor derden onmogelijk is ongezien kennis te nemen van deze gegevens. Na overdracht van de activeringsgegevens is de certificaathouder verantwoordelijk voor de bescherming van deze gegevens.

Indien de pashouder de eerste pincodebrief niet heeft ontvangen, dan biedt het UZI-register de mogelijkheid om deze nogmaals te verzenden. Herprinten van de pincodebrief is alleen mogelijk als de UZI-pas al is verstrekt. Herprinten van de pincodebrief is mogelijk tot en met 6 weken na afgifte van de pas. Aangezien de initiële activeringsgegevens mogelijk zijn verstrekt aan een andere persoon, dient de pashouder de pincode en pukcode direct na ontvangst te wijzigingen.

Na de termijn van 6 weken gaat het UZI-register er vanuit dat de activeringsgegevens juist zijn aangekomen. Het is de verantwoordelijkheid van de pashouder om deze termijn te bewaken. Voor een nieuwe pas met nieuwe codes rekent het UZI-register de normale kosten. Indien het de abonnee verwijtbaar is dat de pincodebrief naar een verkeerd adres is verzonden, bijvoorbeeld doordat een adreswijziging niet tijdig is doorgegeven aan het UZI-register of wanneer de pashouder/ abonnee de pincodebrief is verloren, ontvangt de abonnee een kostendekkende factuur voor het opnieuw afleveren van de pincodebrief.

Bij een herprint genereert het UZI-register om veiligheidsredenen een nieuwe intrekkingscode.

De UZI-pas blokkeert na de derde ingave van een foutieve pincode. Deblokkering kan gebeuren met behulp van een pukcode. Als de pukcode ook drie maal onjuist is ingevoerd, is de smartcard definitief geblokkeerd en daarmee onbruikbaar gemaakt. De pincode en de pukcode worden aan de certificaathouder kenbaar gemaakt in een pincodebrief. Bij verlies van de codes is de pas niet meer te gebruiken of te deblokkeren. Voor een nieuwe pas met nieuwe codes betaalt u de normale kosten.

6.5 Toegangsbeveiliging van TSP-systemen

6.5.1 Algemene systeem beveiligingsmaatregelen

Het UZI-register treft adequate maatregelen om de beschikbaarheid, integriteit en exclusiviteit te waarborgen. Computersystemen worden op passende wijze beveiligd tegen ongeautoriseerde toegang en andere bedreigingen. Het UZI-register beschikt over een informatiebeveiligingsplan waarin de maatregelen zijn uitgewerkt. Met leveranciers worden de maatregelen uitgewerkt in service level agreements. Beheerwerkzaamheden worden gelogd.

6.5.2 Specifieke systeem beveiligingsmaatregelen

In de registratiesystemen van het UZI-register zijn passende controles en beveiligingsmaatregelen opgenomen. Mede hierdoor is het onmogelijk dat een pasaanvraag door één medewerker van het UZI-register wordt afgehandeld.

6.5.3 Beheer en classificatie van middelen

Het UZI-register classificeert de gebruikte middelen op basis van een risicoanalyse.

6.6 Beheersingsmaatregelen technische levenscyclus

6.6.1 Beheersingsmaatregelen systeemontwikkeling

Voor de door het UZI-register gebruikte systemen is door een onafhankelijke EDP auditor een auditverklaring afgegeven op basis van CWA 14167-1 of EAL 4+ certificaat conform ISO/IEC 15408. Het UZI-register voert testen uit voordat systemen in gebruik worden genomen. Testen vinden plaats op basis van vooraf opgestelde testplannen.

6.6.2 Beheersingsmaatregelen beveiligingsmanagement

Het UZI-register beschikt over gescheiden test/acceptatie- en productiesystemen. Het overbrengen van programmatuur van de ene omgeving naar de andere vindt beheerst plaats via change management procedure. Deze change management procedure omvat onder andere het bijhouden en vastleggen van versies, wijzigingen en noodreparaties van alle operationele software.

De integriteit van TSP-systemen en -informatie wordt beschermd tegen virussen, schadelijke en niet-geautoriseerde software en andere mogelijk bronnen die kunnen

leiden tot verstoring van de dienstverlening, door middel van een samenstel van passende fysieke, logische en organisatorische maatregelen. Deze maatregelen zijn preventief, repressief en correctief van aard. Voorbeelden van maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen, systeemonderdelen en netwerkcomponenten.

Opslagmedia van systemen die worden gebruikt worden veilig behandeld om de opslagmedia tegen schade, diefstal en niet-geautoriseerde toegang te beschermen. Opslagmedia worden zorgvuldig verwijderd wanneer zij niet meer nodig zijn.

Het capaciteitsgebruik wordt bijgehouden en voorspellingen van de in de toekomst vereiste capaciteit worden gemaakt om te voorzien in voldoende verwerkingsvermogen en opslagcapaciteit in de toekomst.

6.6.3 Levenscyclus van beveiligingsclassificatie
De beveiligingsclassificatie wordt jaarlijks beoordeeld en zo nodig aangepast.

6.7 Netwerkbeveiliging

Er zijn maatregelen voor netwerkbeveiliging geïmplementeerd, zodanig dat de beschikbaarheid, integriteit en exclusiviteit van de gegevens wordt geborgd.

Communicatie over publieke netwerken tussen systemen van de TSP vindt in vertrouwelijke vorm plaats.

De koppeling tussen de publieke netwerken en de netwerken van het UZI-register zijn voorzien van stringente veiligheidsmaatregelen (actuele firewall, virusscanners, proxy).

6.8 Time-stamping

Geen nadere bepalingen.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

De certificaten van het UZI-register voldoen aan de volgende standaarden:

- X.509 v3 standaard.
- Deel 3a, 3b, 3e en 3h van het Programma van Eisen van de PKI voor de Overheid (zie http://www.logius.nl).
- Verder zijn de handtekeningcertificaten opgebouwd volgens het Qualified Certificate Profile van de relevante ETSI normen. De specifieke extensies in dat kader worden ook in de handtekeningcertificaten (onweerlegbaarheid) van het UZI-register opgenomen.

Een X.509 certificaat bestaat uit een verzameling objecten. Ieder object heeft een naam, en ieder object bestaat uit een aantal attributen. Een attribuut kan diverse zaken bevatten: sleutels, algoritmen, namen, types, etc. Een certificaatprofiel beschrijft welke objecten worden gebruikt en welke waarden de attributen van deze objecten kunnen bevatten. Voorliggend hoofdstuk geeft op hoofdlijnen een overzicht van de certificaatprofielen van het UZI-register. Met name de velden die voor certificaathouders relevante gegevens bevatten komen aan de orde.

De basis structuur van een certificaat bestaat uit een to-be-signed gedeelte (tbsCertificate) en een handtekening van de uitgever. Het tbsCertificate bestaat uit een aantal verplichte basisattributen gevolgd door extensies. De basis attributen en extensies zijn in de navolgende subparagrafen weergegeven.

7.1.1 Basis attributen

De certificaten van het UZI-register kennen de navolgende basis attributen:

Veld	**Waarde**
Version	2 (X.509v3)
Certificate. SerialNumber	Bevat het uniek serienummer van het certificaat
Signature	Het gebruikte algoritme is: • 'SHA256 with RSA Encryption'
Issuer	Bevat de naam van de betreffende UZI-register CA behorend bij het type UZI-pas en wordt weergegeven door de attributen OrganizationName, organizationIdentifier, CommonName en CountryName. De **OrganizationName** is 'CIBG'. De **organizationIdentifier** is 'NTRNL-50000535'. De **CommonName** bevat één van de onderstaande waarden afhankelijk van het pastype en generatie: - 'UZI-register Zorgverlener CA G21' - 'UZI-register Medewerker op naam CA G21' - 'UZI-register Medewerker niet op naam CA G21' - 'UZI-register Server CA G21' - 'UZI-register Zorgverlener CA G3' - 'UZI-register Medewerker op naam CA G3'

Veld	Waarde
	- 'UZI-register Medewerker niet op naam CA G3' - 'UZI-register Private Server CA G1' De **CountryName** is ingesteld op 'NL' volgens ISO 3166.
Validity	De geldigheidsperiode van het certificaat is ingesteld op drie jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door de volgende attributen die in alle certifcaten zijn opgenomen: CountryName, CommonName, OrganizationName, en SerialNumber. De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. De **CommonName** bevat: - voor de Zorgverlenerpas en Medewerkerpas op naam de volledige naam van de certificaathouder: <voornamen><spatie><indien gevuld: voorvoegsels geboortenaam+ spatie><geboortenaam>; - voor de Medewerkerpas niet op naam de functie van de medewerker zoals opgegeven door de abonnee; - voor de Servercertificaten de naam van het systeem, de zogenaamde qualified domainname (FQDN). De **OrganizationName** bevat de naam van de abonnee. Dit is de partij namens wie de certificaathouder handelt bij gebruik van het certificaat. De **CountryName** bevat het land van de abonneee volgens ISO 3166. Het **SerialNumber** bevat het UZI-nummer (Zie paragraaf 7.1.4). Naast bovenstaande attributen die altijd aanwezig zijn, zijn ook Title, Surname, GivenName, StateOrProvinceName, LocalityName en OrganizationalUnitName in gebruik maar niet voor alle typen certificaten. Het **Title** attribuut bevat voor de zorgverlenerpas de formele aanspreektitel (rol) van de zorgverlener (bijv. tandarts of cardioloog). Meer informatie over de invulling van dit veld is opgenomen in bijlage 3. Bij de Zorgverlenerpas en Medewerkerpas op naam zijn ook de **Surname** en **GivenName** in gebruik. Deze bevatten respectievelijk <indien gevuld: voorvoegsels geboortenaam+ spatie><geboortenaam> en de <voornamen>. De **OrganizationalUnitName** komt alleen optioneel voor bij de Medewerkerpas niet op naam en de servercertificaten en biedt ruimte voor het opnemen van de afdeling van de medewerker of de server. In Servercertificaten zijn opgenomen de **StateOrProvinceName** die de provincie van de abonnee bevat en de **LocalityName** die de vestigingsplaats van de abonnee bevat.
subjectPublicKeyInfo	Bevat de 2048 bits RSA PublicKey van de Subject

Tabel 8 Basisattributen certificaatprofielen

7.1.2 Extensies

Het certificaat bevat de navolgende standaard en private extensies:

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash van de publieke sleutel van de CA die het certificaat heeft uitgegeven.
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash van de publieke sleutel van het subject
KeyUsage	Ja	Verschilt per certificaattype: - In **authenticiteitcertificaten** is uitsluitend het digitalSignature bit opgenomen. - In **vertrouwelijkheidcertificaten** zijn uitsluitend de keyEncipherment en dataEncipherment bits opgenomen. - In **handtekeningcertificaten** is uitsluitend het non-Repudiation bit op unieke wijze zijn opgenomen. - In de **servercertificaten** (services) zijn uitsluitend de DigitalSignatureen KeyEncipherment bits opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op 'False' en pathLenConstraint op 'none'
CertificatePolicies	Nee	Bevat: - de Object Identifier (OID) voor de van toepassing zijnde Certificate Policy van de PKI voor de Overheid (zie *Tabel 4 Overzicht certificaten met OID van toepasselijke CP Public G3/Private G1 generatie)* - Een link naar de CPS van het UZI-register (zie par. 1.2.3); - een gebruikerstekst (UserNotice): 'Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Overheid zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie http://www.logius.nl.
AuthorityInfoAccess.accessMethod (OCSP)	Nee	In dit attribuut is de URL van de OCSP dienstverlening opgenomen: http://ocsp.uzi-register.nl.
AuthorityInfoAccess.accessMethod (CA Issuers)	Nee	In dit attribuut is de URL opgenomen naar CA certificaat van de uitgevende CA. Dit verschilt per product: - http://cert.pkioverheid.nl/UZI-register_Zorgverlener_CA_G3.cer - http://cert.pkioverheid.nl/UZI-register_Medewerker_op_naam_CA_G3.cer - http://cert.pkioverheid.nl/UZI-register_Medewerker_niet_op_naam_CA_G3.cer - http://cert.pkioverheid.nl/UZI-register_Private_Server_CA_G1.cer De TSP CA's onder de G3 root zijn 'resigned' op 18 april 2019 en per 1 juni 2019 in productie genomen. Vanaf dat moment zijn de opgenomen CaIssuers URL's in de eindgebruiker certificaten als volgt gewijzigd afhankelijk van het product: - http://cert.pkioverheid.nl/20190418_UZI-register_Zorgverlener_CA_G3.cer - http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_op_naam_CA_G3.cer - http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_niet_op_naam_CA_G3.cer

Veld	Essentieel	Waarde
ExtendedKeyUsage	Nee	In authenticiteitscertificaten is ExtendedKeyUsage noodzakelijk om het certificaat te kunnen gebruiken voor smartcard logon. De volgende waarden zijn opgenomen: - clientAuth: certificaat bruikbaar voor SSL client authenticatie - e-mail protection. Dit is nodig om het certificaat te kunnen gebruiken in gangbare e-mail clients - documentSigning zodat het certificaat bruikbaar is voor ondertekening documenten In de handtekeningscertificaten zijn de volgende ExtendedKeyUsages opgenomen: - e-mail protection. Dit is nodig om het certificaat te kunnen gebruiken in gangbare e-mail clients - documentSigning zodat het certificaat bruikbaar is voor ondertekening van documenten In de vertrouwelijkheidscertificaten zijn de volgende ExtendedKeyUsages opgenomen: - e-mail protection. Dit is nodig om het certificaat te kunnen gebruiken in gangbare e-mail clients - Encrypting File System. Dit is nodig voor encryptie van systeembestanden. In servercertificaten zijn de volgende ExtendedKeyUsages opgenomen: - ServerAuthenticatie - ClientAuthenticatie
SubjectAltName	Nee	In dit attribuut zijn in de subjectAltName.otherName diverse nummers opgenomen die binnen de zorgsector betekenis kunnen hebben en het subject als zorgverlener binnen een bepaalde zorginstelling uniek identificeren. Zie par. 7.1.5. In het authenticiteitcertificaat is een aparte subjectAltName.otherName opgenomen met een Microsoft User Principal Name (UPN) om het certificaat geschikt te maken voor smartcard logon. De UPN is gevuld met de volgende waarde: <UZI-nummer>@<abonneenummer>.
CrlDistributionPoints	Nee	Bevat het URI waar de betreffende CRL, die behoort bij het type certificaat, kan worden opgehaald. Zie par. 7.2.3.

Tabel 9 Standaard extensies certificaatprofielen

Private extensies
Onweerlegbaarheidscertificaten bevatten enkele qcStatements die aangeven dat het een gekwalificeerd certificaat betreft.

Veld	Essentieel	Waarde
etsiQcsCompliance	Nee	Geeft aan dat uitgifte van gekwalificeerd certificaat overeenstemt met annex I van EU Verordening 910/2014.
etsiQcsQcSSCD	Nee	Geeft aan dat de private sleutel behorende bij de publieke sleutel in het certificaat is opgeslagen op een qualified signature-creation device (QSCD) overeenstemmend met annex II van EU Verordening 910/2015.
etsiQcsQcType (Type1)	Nee	Geeft type gekwalificeerd certificaat overeenstemmend met annex I van EU Verordening 910/2014. Type 1: Certificate for electronic signatures (esign) as defined in Regulation (EU) No 910/2014

Veld	Essentieel	Waarde
etsiQcsQcPDS	Nee	Verwijzing naar PKI Dislosure Statement (PDS) met als URL: https://www.zorgcsp.nl/pds/pds.html en als taal Engels.

Tabel 10 Private extensies certificaatprofielen

7.1.3 E-mailadressen

In de certificaatprofielen voor het UZI-register is het e-mail adres niet opgenomen Om de UZI-pas in een Microsoft Windows/Outlook omgeving te gebruiken moeten de configuratie van een PC aangepast worden conform Microsoft Knowledge Base Article – 276597 (How to Turn Off E-mail Matching for Certificates).

7.1.4 UZI-nummer

In het certificaatprofiel van het UZI-register wordt het UZI-nummer opgenomen in het subject.SerialNumber van alle pastypen van het UZI-register. Op deze manier wordt gegarandeerd dat de subject Distinguished Name uniek is.

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.

Bij de Medewerkerpas niet op naam en de Servercertificaten wordt bij iedere (pas)aanvraag/(pas)uitgifte een nieuw uniek UZI-nummer gegenereerd. Het UZI-nummer op dit pastype biedt vertrouwende partijen de mogelijkheid om bij de betreffende abonnee na te gaan om welke medewerker of systeem het gaat. Bij iedere pasaanvraag zal een nieuw UZI-nummer worden gegenereerd omdat het UZI-register geen garantie kan afgeven dat het om dezelfde medewerker of service gaat. Dit wordt door de abonnee bijgehouden.

Het UZI-register zal voor alle pastypen het UZI-nummer genereren uit dezelfde negen-cijferige nummerreeks.

7.1.5 SubjectAltName.otherName

Deze paragraaf beschrijft hoe de subjectAltName.othername in de certificaten van het UZI-register wordt opgenomen.

PKIoverheid specificeert een subjectAltName.othername met een OID-achtige structuur, als volgt: **<OID CA>-<Subject ID>.** De <OID CA> en het <Subject ID> zijn gescheiden door een ‘-‘.

<OID CA>
staat voor de OID van de uitgevende CA, die een weergave is van **<PKIoverheid>.<Domein>.<TSP>.<CA>.**

<Subject ID>
is een specifieke identificatie binnen het domein van de TSP. Hierin is door het UZI-register een keuze gemaakt om diverse nummers op te nemen die binnen de zorgsector betekenis kunnen hebben en het subject als zorgverlener binnen een bepaalde abonnee uniek identificeren.

Waarden SubjectAltName.otherName: <OID CA>
De onderstaande tabel geeft de waarden van de <OID CA> in de productieomgeving.

CA type	OID
UZI-register Zorgverlener CA	2.16.528.1.1003.1.3.5.5.2
UZI-register Medewerker op naam CA	2.16.528.1.1003.1.3.5.5.3
UZI-register Medewerker niet op naam CA	2.16.528.1.1003.1.3.5.5.4
UZI-register Server CA	2.16.528.1.1003.1.3.5.5.5

Tabel 11 <OID CA> productieomgeving UZI-register

Waarden SubjectAltName.otherName: <Subject ID>
Het <Subject ID> in het UZI-register is een samengesteld veld, bestaande uit door een '-' gescheiden velden:

<Subject ID> = <versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>

De onderstaande tabel geeft een toelichting bij de velden:

Veld	Type	Waarde	Toelichting
versie-nr	1NUM	1	Versienummer van de <Subject ID> specificatie t.b.v. mogelijke toekomstige ontwikkelingen.
UZI-nr	9NUM	Zie par 7.1.4.	Een uniek nummer voor certificaathouders.
pastype	1CHAR	De volgende codering wordt toegepast: 'Z' : Zorgverlenerpas 'N' : Medewerkerpas op naam 'M' : Medewerkerpas niet op naam 'S' : Servercertificaten	Codering voor type UZI-middel.
Abonnee-nr	8NUM		Abonneenummer van de zorgaanbieder of indicatieorgaan.
Rol	6CHAR	Afhankelijk van pastypen Voor zorgverlenerpassen <code beroepstitel>.<code specialisme> De <code beroepstitel>=2NUM De <code specialisme>=3NUM **OF** '00.000' Voor Medewerkerpas op naam, Medewerkerpas niet op naam en Servercertificaten	Bij de Zorgverlenerpas heeft de <code beroepstitel> altijd een waarde ongelijk aan nul. De <code specialisme> kan wel nul zijn omdat veel beroepstitels geen specialisme kennen en het niet verplicht is om het specialisme op te nemen. Voor verdere toelichting op de invulling zie bijlage 3.
AGB-code	8NUM	AGB-code of 00000000 als geen AGB-code is opgegeven.	Zie tabel 11

Tabel 12 Velden <Subject ID> in SubjectAltName.otherName

Toelichting waarde AGB-code

Op verzoek kan in de pas of servercertificaten een AGB-code worden opgenomen. In overleg met Vektis is bepaald welke AGB-code per pas wordt opgenomen.

Pastype	Abonneetype: Zorgverlener	Abonneetype: Organisatie
Zorgverlener		
Medewerker op naam	AGB-zorgverlenercode abonnee	AGB-code praktijk of instelling
Medewerker niet op naam	AGB-zorgverlenercode abonnee	AGB-code praktijk of instelling
Server	AGB-zorgverlenercode abonnee	AGB-code praktijk of instelling

Tabel 13 Toelichting gebruik AGB-code

7.2 CRL profielen

De CRL profielen zijn opgemaakt conform deel 3a, 3b, 3e en 3h van het Programma van Eisen van de PKI voor de overheid (zie http://www.logius.nl). Het profiel van de CRL voor de certificaten bevat een aantal attributen en extensies. Deze zijn in de navolgende subparagrafen weergegeven.

7.2.1 Attributen

De CRL's voor certificaten van het UZI-register kennen de navolgende attributen:

Field	Value
Version	1 (X.509 versie 2)
signatureAlgorithm	SHA-256 WithRSAEncryption
Issuer	Bevat de naam van de betreffende UZI-register CA behorend bij het type certificaat en wordt weergegeven door de volgende attributen: OrganizationName, CommonName, organizationIdentifier en CountryName. De OrganizationName is ingesteld op ' CIBG De organizationIdentifier is 'NTRNL-50000535'. De CommonName bevat afhankelijk van de CA die de CRL ondertekent: 'Zorg CSP CA G21' 'UZI-register Zorgverlener CA G21' 'UZI-register Medewerker op naam CA G21' 'UZI-register Medewerker niet op naam CA G21' 'UZI-register Server CA G21' 'UZI-register Zorgverlener CA G3' 'UZI-register Medewerker op naam CA G3' 'UZI-register Medewerker niet op naam CA G3' 'UZI-register Private Server CA G1' De CountryName is ingesteld op 'NL' volgens ISO 3166.
thisUpdate	Datum/tijdstip van uitgifte.
nextUpdate	Dit is de datum/tijdstip waarop de geldigheid van de CRL eindigt. De waarde is 'thisUpdate' plus achtenveertig uur. Het UZI-register publiceert elk uur een update van de CRL.
revokedCertificates	De ingetrokken certificaten met certificaatserienummer en datum van intrekking.

Tabel 14 CRL attributen

7.2.2 Extensies

De CRL's voor certificaten van het UZI-register kennen de navolgende extensies:

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	Bevat 160 bit SHA-1 hash van de publieke sleutel van de CA die de CRL heeft ondertekend.
CRLNumber	Nee	Volgnummer

Tabel 15 Extensies CRL

7.2.3 CRL Distribution Points

Bij de gebruikercertificaten verschilt het CRL Distribution Point per certificaattype afhankelijk van de CA die het certificaat uitgeeft. Onderstaande tabel geeft het overzicht van de CRL Distribution Points per pastype in de Productieomgeving:

Naam UZI-pastype	CRL Distribution Point
Zorgverlener	http://www.csp.uzi-register.nl/cdp/uzi-register_zorgverlener_ca_g21.crl
Medewerkerpas op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca_g21.crl
Medewerkerpas niet op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca_g21.crl
Servercertificaten	http://www.csp.uzi-register.nl/cdp/uzi-register_private_server_ca_g1.crl

Tabel 16 CRL Distribution points gebruikercertificaten UZI-register

7.2.4 TSP en CA certificaten

Een UZI-pas (smartcard) wordt geleverd met de volledige certificaat hiërarchie voor het betreffende gebruikerscertificaat. https://cert.pkioverheid.nl/. Alle CA certificaten van de TSP zijn beschikbaar via: https://cert.pkioverheid.nl/

7.3 OCSP profiel

7.3.1 OCSP responder certificaat

De OCSP responder certificaten volgen zoveel mogelijk het certificaatprofiel voor servercertificaten. Specifieke afwijkingen in de OCSP responder certificaatprofielen zijn:

- het ontbreken van Subject.StateOrProvinceName, Subject.Locality en Subject.Serialnumber
- het ontbreken van de Authority Information Access
- het ontbreken van de Subject.AltName
- de subject.CommonName is als volgt: OCSP responder [CN delegated CA]. Bijvoorbeeld voor de 'UZI-register Zorgverlener CA G3' is de CN van de bijbehorende OCSP responder: 'OCSP responder UZI-register Zorgverlener CA G3'het gebruik van KeyUsage=Digital Signature
- het gebruik van extendedKeyUsage=id-kp-OCSPSigning

het gebruik van een zogenaamd ocsp-nocheck extensie: (iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1) no-check(5)})

7.3.2 OCSP responses

De OCSP responses van het UZI-register zijn van het type ‘basic’ -zoals gespecificeerd in RFC 2560 OCSP- dat door alle OCSP clients ondersteund moet worden.

Dit houdt in dat:

- de response is ondertekend door een geautoriseerde CA Responder die een specifiek servercertificaat heeft dat is getekend door dezelfde CA als de CA die het certificaat heeft uitgegeven dat gevalideerd wordt. Op die manier wordt aangegeven dat de responder geautoriseerd is om request over de status van deze certificaten te beantwoorden. Dit certificaat wordt met iedere response meegestuurd, zodat de vertrouwende partij de response kan controleren.
- een (basic) OCSP response bestaat uit:
  - een versienummer van de response syntax;
  - de naam van de responder;
  - een response voor ieder van de certificaten in het request;
  - optionele extensies. Momenteel is dat alleen de OCSP Nonce;
  - een OID die het gebruikte signature algoritme aangeeft;
  - een handtekening van de response.

Voor ieder van de certificaten in een request bevat de response:

- een certificaat identifier;
- de certificaat status;
- de geldigheidsduur van de response;
- optionele extensies, momenteel is dat alleen de OCSP Nonce.

De certificaat status is één van de 3 onderstaande waarden:

- ‘Good’.
- ‘Revoked’.
- ‘Unknown’.

De status "good" geeft minimaal aan dat het certificaat niet is ingetrokken, maar garandeert niet dat het certificaat op dat moment nog geldig is. De "revoked" status geeft aan dat het certificaat is ingetrokken. De "unknown" status geeft aan de OCSP responder van het UZI-register de status van het certificaat niet kent. Dit is bijvoorbeeld het geval als de status van een testcertificaat wordt opgevraagd bij de OCSP responder van de productieomgeving.

8 Conformiteitbeoordeling

De TSP dienstverlening van het UZI-register is per 22-11-2004 gecertificeerd tegen 'Scheme for certification of Certification Authorities tegen ETSI EN 319 411-2 en ETSI TS 102 042 en voldoet daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners in ETSI EN 319 411-2 en daarmee aan de eisen uit de Wet elektronische handtekening (Weh). De norm ETSI TS 101 456 is opgevolgd door ETSI EN 319 411-2 (in combinatie met ETSI EN 319 401). ETSI 102 042 is per 1 juli 2016 opgevolgd door 319 411-1.
De laatste vernieuwing van deze certificering heeft plaatsgevonden op 22-11-2017 door BSI Group The Netherlands B.V. (hierna: BSI).

eIDAS
Op 1 juli 2016 is de Europese Verordening (verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG) van kracht geworden.
Deze verordening vervangt de Wet Elektronische Handtekening.
Omdat in deze verordening de eisen t.a.v. frequentie van de audit en de accreditatie zijn opgenomen is het TTP.NL Scheme per die datum vervallen.

Ook zijn de eerdere ETSI certificeringen in november 2016 ETSI TS 101 456 en ETSI TS 102 042 vervangen door resp. de ETSI certificeringen ETSI EN 319 411-2 en ETSI EN 319 411-1.

Het UZI-register voldoet tevens aan de relevante onderdelen van het Programma van Eisen van de PKIoverheid zoals gesteld in het Programma van Eisen. Dit is aantoonbaar met behulp van een door BSI Group The Netherlands B.V. afgegeven auditverklaring,

Een afschrift van het ETSI EN 319 411-1 en het ETSI EN 319 411-2-certificaat staan vermeld op de site van het UZI-register (zie certificeringsbeleid).
De door de betreffende auditors opgestelde auditrapporten zijn vanuit beveiligingsoogpunt geheim. Ze worden niet beschikbaar gesteld aan derden en zijn alleen op verzoek en onder strikte geheimhouding in te zien.

Met ingang van 10 maart 2017 is Agentschap Telecom (hierna AT) aangewezen als wettelijk toezichthouder op de eIDAS verordening. Het UZI-register is als Trust Service Provider (TSP), onder registratienummer 940473 geregistreerd bij de Agentschap Telecom, als getoetste uitgever van Gekwalificeerde Certificaten aan het publiek.

8.1 Auditcyclus

De auditcyclus wordt uitgevoerd volgens ETSI EN 319 403 certificatieschema. Het UZI-register ondergaat eenmaal per 2 jaar een certificatieaudit. In de tussenliggende jaren wordt jaarlijks een volledige controle audit uitgevoerd. Als op beleidsmatig of technisch vlak grotere wijzigingen worden doorgevoerd, kan een tussentijdse conformiteitsaudit worden uitgevoerd.

Naast deze audits voert het UZI-register zelf interne audits en self-assessments uit.

8.2 Certificerende instelling

Certificatieaudit en controle audits worden uitgevoerd door een door de Raad van Accreditatie geaccrediteerde organisatie.

8.3 Relatie met certificerende instelling

De auditoren die de audits uitvoeren zijn onafhankelijk. Er is geen verdere relatie tussen het UZI-register en de certificerende instelling.

8.4 Onderwerp van audit

Tijdens de audits wordt beoordeeld in hoeverre het managementsysteem voor het uitgeven van (gekwalificeerde) certificaten blijvend voldoet aan de eisen in de normen:

- ETSI EN 319 411-1, (ten behoeve van de medewerkerpas niet op naam en servercertificaten), inclusief de hierin verwezen normen in de CABforum Baseline Requirements en de Network Security Controls.
- ETSI EN 319 411-2, (ten behoeve van de zorgverlenerpas en medewerkerpas op naam)
- eisen uit de Verordening elektronische identiteiten en vertrouwensdiensten (de eIDAS-Verordening)
- het Programma van Eisen PKIoverheid delen 3a, 3b en 3h.

De audit is uitgevoerd op de volgende onderwerpen en processen:

- Registration Service.
- Certificate Generation Service.
- Dissemination Service.
- Revocation Management Service.
- Revocation Status Service.
- Subject Device Provision Service.

8.5 Resultaten audit

Als bij de audit tekortkomingen worden geconstateerd, stelt het UZI-register binnen 3 weken na ontvangst van het auditrapport een plan van aanpak op om de geconstateerde afwijkingen te analyseren en doeltreffende corrigerende maatregelen te nemen.

8.6 Beschikbaarheid conformiteitcertificaten

De conformiteitcertificaten van de meest recente audits zullen beschikbaar zijn op de website van het UZI-register en in de elektronische opslagplaats van de Policy Authority van de PKI voor de overheid. Het UZI-register voldoet tevens aan het normenkader van de PKI voor de overheid zoals gesteld in het Programma van Eisen (zie hiervoor www.logius.nl).

9 Algemene bepalingen en voorwaarden

9.1 Aanvraag, facturering en betaling van UZI-middelen

9.1.1 Tarief verbonden aan uitgifte UZI-middelen

Aan de aanvraag van UZI-middelen, te weten het servercertificaat en de UZI-pas, van een in het UZI-register geregistreerde zorgaanbieder (abonnee), is een kostendekkend tarief verbonden. Dit tarief is van toepassing op zowel de initiële aanvraag als de vervolgaanvraag, waaronder vernieuwing, van een UZI-middel. De tarieven voor de UZI-middelen staan vermeld op www.uziregister.nl.

9.1.2 *Wijziging tarieven*

Het tarief voor de UZI-middelen kan periodiek wijzigen. Indien het tarief wordt gewijzigd, wordt de Regeling gebruik burgerservicenummer in de zorg dienovereenkomstig gewijzigd en wordt dit bekendgemaakt op www.uziregister.nl.

9.1.3 Inschrijving in het UZI-register

Voordat UZI-middelen kunnen worden aangevraagd, dient de zorgaanbieder, als abonnee te zijn ingeschreven in het UZI-register. De wijze van inschrijving is beschreven in hoofdstuk 3 (‘Identificatie en authenticatie’).

9.1.4 Aanvragen UZI-middelen

Een aanvraag van UZI-middelen dient te worden gedaan door de pasaanvrager. Hiertoe moet een aanvraag via de applicatie op de website (www.uziregister.nl/aanvragen) of een door het UZI-register beschikbaar gesteld aanvraagformulier worden ingediend. De procedure rondom de aanvraag en uitgifte van UZI-middelen is gedetailleerd vastgelegd in hoofdstuk 3 (‘Identificatie en authenticatie’) en hoofdstuk 4 (‘Operationele eisen certificaatlevenscyclus’).

Voor afgewezen aanvragen worden geen kosten in rekening gebracht.

9.1.5 Productie UZI-middel

Nadat de identificatie en authenticatie (hoofdstuk 3 ‘Identificatie en authenticatie’) is uitgevoerd en is goedgekeurd door het UZI-register, wordt het aangevraagde UZI-middel geproduceerd.

9.1.6 Facturering en betaling

De abonnee ontvangt binnen drie weken na de productiedatum van de UZI-pas, op het bij het UZI-register geregistreerde postadres, een hieraan gerelateerde factuur Daarnaast wordt de factuur digitaal naar het e-mailadres van de aanvrager verzonden. Het UZI-register heeft voor de facturering onderaannemer X-Pact B.V. gecontracteerd. Voor het verzenden van de factuur worden de gegevens, zoals het postadres van de abonnee en het e-mailadres van de aanvrager van het betreffende UZI-middel, aan X-Pact B.V. verstrekt. Het UZI-register zal een verzoek tot aanpassing van een factuur niet honoreren.

De pasaanvrager is verantwoordelijk voor het kiezen van het juiste UZI-middel. Indien de pasaanvrager een UZI-middel aanvraagt dat niet juist blijkt te zijn, bijvoorbeeld een verkeerd type UZI-pas of verkeerd PKCS#10 bestand, dan worden hier de volledige kosten voor in rekening gebracht.

9.1.7 Betaaltermijn

De betaaltermijn na facturering bedraagt dertig dagen. Het UZI-register is gerechtigd bij niet-tijdige betaling incassomaatregelen te treffen en/of de vordering over te dragen aan een derde. Bij niet-tijdige betaling worden UZI-middelen door het UZI-register ingetrokken. Het intrekken van UZI-middelen vindt zes weken na dagtekening aanmaning plaats.

9.1.8 Geldigheid UZI-middel

De geldigheidsduur van een UZI-middel bedraagt drie jaar na de productiedatum. De productiedatum is de datum waarop de Certification Authority (CA) het certificaat heeft geproduceerd en gepubliceerd.

9.1.9 Levering en ingebruikname UZI-middelen

De UZI-middelen worden geleverd conform de in het Certification Practice Statement (CPS) genoemde technische en/of functionele specificaties. Indien bij ingebruikname blijkt dat het UZI-middel niet functioneert conform het CPS stelt de abonnee of diens gemachtigde het UZI-register binnen zes weken na levering van de UZI-pas of na verzending van het UZI-servercertificaat hiervan onverwijld op de hoogte.

9.1.10 Vervangingsvoorwaarden

Indien een UZI-middel niet conform de in het CPS beschreven technische en/of functionele specificaties werkt, vervangt het UZI-register dit UZI-middel kosteloos tijdens de genoemde 6 weken in paragraaf 9.1.9.

Alleen tijdens deze 6 weken kunnen de activeringsgegevens (de pincode en pukcode) nogmaals worden verzonden. Zie paragraaf 6.4.2 voor de voorwaarden en procedure.

Wanneer een certificaathouder vermoedt dat de UZI-pas defect is, dient de certificaathouder contact op te nemen met de supportdesk van Atos[14]. Indien na een telefonische controle door een medewerker van de supportdesk is vastgesteld dat de UZI-pas vermoedelijk defect is, kan de abonnee in aanmerking komen voor de garantieregeling. Onder de garantieregeling kan de abonnee kosteloos een nieuwe pas ontvangen. De garantieregeling is alleen van kracht bij de volgende voorwaarden:

- De supportdesk na een telefonische toets heeft vastgesteld dat de pas vermoedelijk defect is.
- De UZI-pas nog minimaal 3 maanden geldig is.
- De certificaten op de UZI-pas worden ingetrokken door de abonnee, conform de procedure in paragraaf 4.10.
- De abonnee of certificaathouder de UZI-pas retourneert aan het UZI-register met bijbehorende PIN- en PUK-codes. De abonnee is ervoor verantwoordelijk dat de zending juist wordt ontvangen door het UZI-register. Het wordt daarom aangeraden om deze middels aangetekende post te verzenden. Deze kosten kunnen niet worden gedeclareerd.
- Aan de hand van de melding en de ontvangen UZI-pas dient het UZI-register vast te kunnen stellen dat de pashouder zorgvuldig met de pas is omgegaan. De pas dient niet zichtbaar beschadigd te zijn bij ontvangst.

9.1.11 Risico, eigendom en zorgplicht

Het risico voor tenietgaan, verlies of diefstal, beschadiging of achteruitgaan van UZI-middelen gaat over op de abonnee op het moment van het in ontvangst nemen

14 De servicedesk van Atos is hiervoor door de TSP gemachtigd.

van een UZI-middel. De abonnee is niet gerechtigd om op het UZI-middel wijzigingen aan te brengen. De uitgegeven UZI-middelen blijven eigendom van het UZI-register. Het UZI-register is bevoegd om het gebruik van een UZI-middel door een abonnee in te trekken. UZI-middelen zijn niet overdraagbaar aan derden. De abonnee of diens gemachtigde, dient ervoor zorg te dragen dat de UZI-middelen op een zorgvuldige, veilig en behoedzame wijze gebruikt en bewaard worden.

9.2 Vertrouwelijkheid bedrijfsgegevens

Op basis van de Wet openbaarheid van bestuur (Wob) kan een ieder een verzoek doen aan het UZI-register om documenten te overleggen met betrekking tot een bestuurlijke aangelegenheid.

Als het UZI-register werkzaamheden uitbesteed aan derden, worden deze werkzaamheden uitgevoerd onder verantwoordelijkheid van het UZI-register. De afspraken tussen derden en het UZI-register zijn contractueel vastgelegd.

Wanneer het verstrekken van documenten of gegevens de dienstverlening van het UZI-register, de afnemers van haar diensten of van een door het UZI-register ingeschakelde derde kan schaden, worden deze niet aan anderen overlegd, behalve dan die partijen die vanuit hun functie toegang tot die documenten moeten hebben. Gedacht moet worden aan documenten die bedrijfsgevoelige informatie kan bevatten op het gebied van infrastructuur, beveiliging en financiën.

9.3 Vertrouwelijkheid persoonsgegevens

Alle uitgevoerde handelingen die van belang zijn in het registratieproces worden vastgelegd. Hierbij worden zo min mogelijk persoonsgegevens vastgelegd. In ieder geval worden geen (persoons)gegevens vastgelegd die niet van belang zijn voor het registratieproces of voor een van de faciliterende diensten van het UZI-register.

De gemachtigd aanvragers, certificaathouders en certificaatbeheerders hebben recht op inzage en correctie van hun persoonsgegevens.

9.3.1 Vertrouwelijke informatie

De informatie die door het UZI-register wordt verkregen over een persoon, zijnde een natuurlijk persoon of rechtspersoon, wordt vertrouwelijk behandeld. De eisen gesteld in de Algemene verordening gegevensbescherming (AVG) zijn hierop uitdrukkelijk van toepassing.
Tenminste de volgende documenten bevatten informatie die als vertrouwelijk worden beschouwd en zullen in beginsel dan ook niet aan derden worden verstrekt:

- informatie in het kader van de registratie en certificering van partijen;
- overeenkomsten met (toe)leveranciers en dienstverleners;
- beveiligingsprocedures en maatregelen;
- procedures Administratieve Organisatie (AO);
- audit rapporten.

9.3.2 Niet-vertrouwelijke informatie

De gepubliceerde gegevens van certificaten zijn alleen openbaar raadpleegbaar via de zoekfunctie op https://www.zorgcsp.nl/. De informatie die wordt verstrekt met betrekking tot gepubliceerde en ingetrokken certificaten is beperkt tot hetgeen in hoofdstuk 7 ‘Certificaat-, CRL- en OCSP-profielen’ van voorliggend CPS vermeld is.

Informatie met betrekking tot intrekking van certificaten is beschikbaar via de CRL. De daar gegeven informatie betreft slechts het certificaatnummer, het moment van intrekking en de status (geldig/ingetrokken) van het certificaat.

9.3.3 Vrijgeven van informatie

Als in het kader van een straf- of tuchtrechtelijk onderzoek niet-openbare informatie uit het UZI-register wordt opgevraagd door een bevoegde opsporingsambtenaar, dan wordt deze informatie door de directeur van het CIBG op basis van een gerechtelijk bevel vrijgegeven. De eisen gesteld in de AVG zijn hierop uitdrukkelijk van toepassing.

Als door een abonnee of certificaathouder in een civiele procedure niet-openbare informatie uit het UZI-register wordt opgevraagd ten behoeve voor het leveren van bewijs van certificatie, dan wordt deze informatie vrijgegeven door de directeur van het CIBG, als naar het oordeel van deze laatste er geen sprake is van een zwaarwegend belang dat zich verzet tegen de genoemde gegevensverstrekking. Als tot gegevensverstrekking zal worden overgegaan, wordt de betrokkene hiervan op de hoogte gesteld.

Vertrouwelijke gegevens zullen slechts ter bewijsvoering aan andere partijen dan de abonnee of certificaathouder worden verstrekt met voorafgaande schriftelijke toestemming van de abonnee of de certificaathouder.

Behoudens het hiervoor gestelde worden geen gegevens behorende bij certificaathouders of abonnees vrijgegeven aan derden, zonder dat dit uit nadere wet- en regelgeving blijkt of dat de abonnees of certificaathouders hier uitdrukkelijk toestemming voor hebben gegeven.

9.4 Intellectuele eigendomsrechten

Dit CPS is eigendom van het UZI-register. Ongewijzigde kopieën van dit CPS mogen zonder toestemming verspreid en gepubliceerd worden mits dit met bronvermelding geschiedt.

Door het UZI-register uitgegeven certificaten en dragers van de private en publieke sleutel (UZI-pas) blijven eigendom van het UZI-register. UZI-passen dienen op verzoek van het UZI-register te worden teruggegeven. Alle intellectuele eigendomsrechten in relatie tot de certificaten en de UZI-pas, waaronder begrepen de rechten met betrekking tot software, databanken en beeldmerken, berusten bij het UZI-register. De rechten zijn niet overdraagbaar aan derden.

Het UZI-register garandeert jegens haar abonnees en certificaathouders dat de door haar uitgegeven certificaten en dragers van de private en publieke sleutel, inclusief de daarbij behorende en geleverde apparatuur en documentatie, geen inbreuk maakt op intellectuele eigendomsrechten, waaronder auteursrechten, merkenrechten en gebruikte programmatuur waarvan deze berusten bij haar (toe)leveranciers.

9.5 Aansprakelijkheid en garanties

9.5.1 Aansprakelijkheid van de TSP

Het UZI-register is in haar functie van certificatiedienstverlener aansprakelijk voor schade die natuurlijke personen of rechtspersonen, die in redelijkheid op een door het UZI-register uitgegeven certificaat vertrouwen en op grond daarvan handelen, ondervinden in samenhang met:

- De juistheid, op het tijdstip van afgifte, van alle in het certificaat opgenomen gegevens en de opneming van alle voor dit certificaat voorgeschreven gegevens.
- Het feit dat, op het tijdstip van uitgifte, degene die in het certificaat is aangeduid als ondertekenaar de houder was van de gegevens voor het aanmaken van elektronische handtekeningen.

- Het feit dat de gegevens voor het aanmaken van elektronische handtekeningen en de gegevens voor het verifiëren van elektronische handtekeningen, als zij beide door het UZI-register zijn gegenereerd, complementair kunnen worden gebruikt.

Het UZI-register kan aansprakelijk worden gesteld, wanneer zij nalaat intrekking van het certificaat te registeren, met inbegrip van het bijwerken en publiceren van de CRL, en een persoon in redelijk vertrouwen daarop heeft gehandeld. Het UZI-register kan op basis van voorgaande gronden niet aansprakelijk worden gesteld, indien zij bewijzen kan overleggen dat het UZI-register niet onzorgvuldig heeft gehandeld.

Het UZI-register sluit alle aansprakelijkheid uit voor schade indien het certificaat niet conform het in paragraaf 1.4 beschreven certificaatgebruik wordt gebruikt.

Het UZI-register kan op aanwijzing van de Policy Authority van de PKI voor de overheid in een handtekeningencertificaat beperkingen ten aanzien van het gebruik opnemen, mits deze beperkingen voor derden duidelijk zijn. Het UZI-register is niet aansprakelijk voor schade die het gevolg is van het gebruik van een handtekeningencertificaat in strijd met de door de Policy Authority bepaalde beperkingen.

Het UZI-register garandeert dat procedures zijn ingericht en maatregelen zijn geïmplementeerd zodat voldaan wordt aan dit CPS.

Het UZI-register aanvaardt geen enkele aansprakelijkheid tegenover de vertrouwende partij voor door hem/haar geleden schade in welke vorm dan ook behoudens de hierna vermelde uitzonderingen:

- Het UZI-register is in beginsel aansprakelijk, in die gevallen waar een vertrouwende partij schade lijdt, overeenkomstig artikel 6:196b eerste tot en met het derde lid van het Burgerlijk Wetboek, met dien verstande dat:
  - voor ‘ondertekenaar’ gelezen wordt ‘certificaathouder’;
  - aanvullend voor authenticiteitscertificaten:
    - voor ‘een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet’ gelezen wordt ‘een authenticiteitscertificaat’;
    - voor ‘elektronische handtekeningen’ gelezen wordt ‘authenticiteitskenmerken’.
  - aanvullend voor vertrouwelijkheidscertificaten:
    - voor ‘een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet’ gelezen wordt ‘een vertrouwelijkheidscertificaat’;
    - voor ‘aanmaken van elektronische handtekeningen’ gelezen wordt ‘aanmaken van vercijferde data’;
    - voor ‘verifiëren van elektronische handtekeningen’ gelezen wordt ‘ontcijferen van vercijferde data’.

9.5.2 Aansprakelijkheid van abonnees en certificaathouders

Abonnees en certificaathouders zijn gehouden aan de bepalingen van het UZI-register met betrekking tot de afname van certificatiediensten zoals deze zijn vastgelegd in het CPS. Daarnaast dienen zij zich te houden aan aanwijzingen die hen door het UZI-register zijn meegedeeld bij de uitreiking van de UZI-passen en/of op een later tijdstip aan hen kenbaar zijn gemaakt.

Certificaathouders binnen een organisatie zijn daarnaast ook gehouden aan aanwijzingen die hen door de abonnee zijn kenbaar gemaakt. Als er sprake zou zijn

van eventuele tegenstrijdigheid in de aanwijzingen van beide partijen, gaan de aanwijzingen van het UZI-register in beginsel voor op de aanwijzingen van de abonnee.

Wanneer door abonnees of certificaathouders niet aan deze bepalingen wordt voldaan, kan er sprake zijn van schade voor het UZI-register, de abonnee, certificaathouders of derden. In dergelijke gevallen zal in beginsel de abonnee aansprakelijk worden gesteld voor het niet naleven van de bepalingen. Onderstaande bepalingen zijn aanvullend op paragraaf 4.6.1 van dit CPS.

- De abonnee zal enkel en alleen certificatiediensten van het UZI-register afnemen voor zijn systemen, databases en medewerkers.
- De wettelijk vertegenwoordiger garandeert dat hij in rechte bevoegd is om de abonnee aan het UZI-register te binden. Daarnaast kan de wettelijk vertegenwoordiger onder zijn of haar eindverantwoording binnen de organisatie een of meerdere gemachtigden aanwijzen: de aanvrager(s). Deze aanvrager(s) zal (zullen) namens de abonnee belast worden met de daadwerkelijke uitvoering van de aanvragen voor en intrekken van UZI-passen volgens de procedures van het CPS. Als er sprake is van doorhalen van de abonneeregistratie van (de organisatie van) de abonnee, dan is daartoe uitsluitend de wettelijk vertegenwoordiger zelf bevoegd.
- De abonnee is verplicht een procedure in te richten en uit te voeren aan de hand waarvan hijzelf of de aanvrager(s) kan (kunnen) controleren of de beoogde certificaathouders binnen de organisatie van de abonnee daadwerkelijk werkzaamheden voor de organisatie verrichten. Wanneer de abonnee zelf certificaathouder is volgt hij dezelfde procedure.
- De abonnee garandeert dat de beoogde certificaathouder werkzaam is binnen de organisatie voor wie UZI-passen worden aangevraagd en dat de pasvraag per individuele certificaathouder volledig, correct en bevoegd gegeven is. De eindverantwoordelijkheid voor een juiste aanvraag ligt te allen tijde bij de abonnee. Wanneer de abonnee zelf certificaathouder is volgt hij dezelfde procedure.
- De abonnee dient voordat hij een UZI-pas aanvraagt, de beoogde certificaathouder binnen de organisatie schriftelijk op de hoogte te brengen van de precieze voorwaarden voor het gebruik van de UZI-pas. Het gaat hier om eventuele beperkingen over dit gebruik, het bestaan van een vrijwillige accreditatie en de procedures voor klachtenbehandeling en de afhandeling van geschillen. Een en ander volgens het CPS. Deze informatie moet door de abonnee schriftelijk en in gemakkelijk te begrijpen taal worden opgesteld. Daarnaast dient de abonnee zich te verzekeren dat de beoogde certificaathouder daadwerkelijk kennis heeft genomen van de voor hem van toepassing zijnde verplichtingen en procedures uit het CPS voordat het UZI-register tot verstrekken van een UZI-pas overgaat. Hiertoe zal de abonnee de rechten en verplichtingen van de beoogde certificaathouders binnen de organisatie schriftelijk vastleggen en zal hij ervoor zorgen dat de certificaathouders binnen de organisatie zullen voldoen aan de procedures, rechten en verplichtingen die voortvloeien uit het CPS. Wanneer de abonnee zelf certificaathouder is volgt hij dezelfde procedure.
- De abonnee is altijd verantwoordelijk voor de keuze en (fysieke) beveiliging van zijn programmatuur, apparatuur en telecommunicatiefaciliteiten en de beschikbaarheid van zijn informatie- en communicatiesystemen, waarmee hij de elektronische communicatie voor zichzelf en de certificaathouders binnen de organisatie tot stand brengt. Zo zal de abonnee onder meer geschikte maatregelen nemen om zijn systeem te beschermen tegen virussen en overige programmatuur voorzien van oneigenlijke elementen.

- De abonnee zal juiste, volledige en actuele gegevens verstrekken aan het UZI-register, met inbegrip van gegevens van de certificaathouders binnen de organisatie voor het genereren en de uitgifte van certificaten. Wijzigingen in adres, organisatie, organisatienaam, functies, contactpersonen of persoonsgegevens van de abonnee of de certificaathouders binnen de organisatie of andere relevante wijzigingen zullen door de abonnee niet later dan 24 uur nadat deze wijziging zich heeft voorgedaan aan het UZI-register gemeld worden.
- Als door de abonnee servercertificaten worden aangevraagd geldt aanvullend dat hij verplicht is een procedure in te richten en uit te voeren aan de hand waarvan hijzelf of de aanvrager(s) kan (kunnen) controleren of het systeem of database waarvoor een servercertificaat wordt aangevraagd daadwerkelijk wordt ingezet voor de organisatie.
- De abonnee en certificaathouder kunnen rechten en verplichtingen die uit de relatie met het UZI-register voortvloeien niet overdragen aan derden, tenzij door het UZI-register anders is bepaald.
- De abonnee draagt zelf zorg voor een tijdige vervanging in het geval van een naderende afloop van de geldigheid, en noodvervanging in geval van compromittatie en/of andere soorten van calamiteiten met betrekking tot het certificaat of van bovenliggende certificaten. Van de abonnee wordt verwacht dat hij zelf adequate maatregelen neemt om de continuïteit van het gebruik van certificaten te borgen.[15]

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.

9.5.3 Aansprakelijkheid van vertrouwende partijen
Geen nadere bepalingen.

9.6 **Uitsluiting van garantie**
In geval van systeemdefecten, serviceactiviteiten, of factoren die buiten het bereik van het UZI-register liggen, zal het UZI-register al het mogelijke doen om ervoor te zorgen dat de dienstverlening zo snel mogelijk weer bereikbaar is. Uiterlijk binnen 24 uur zal de publicatiedienst weer beschikbaar zijn. Hiervoor is een uitwijkscenario ontworpen, dat regelmatig wordt getest. Het UZI-register is niet verantwoordelijk voor de niet-beschikbaarheid van de dienstverlening vanwege natuurrampen of andere omstandigheden waar het UZI-register niet verantwoordelijk voor kan worden gehouden.

9.7 **Beperking van aansprakelijkheid**
Het UZI-register erkent geen aansprakelijkheid voor schade ontstaan bij natuurlijke personen of rechtspersonen in het geval van:
- Schade als het certificaat niet volgens het beschreven toepassingsgebied wordt gebruikt;
- Schade die voortvloeit uit gebruik van het certificaat, waarbij de op het certificaat aangegeven beperkingen worden overschreden;

15 In het geval van calamiteiten bij het UZI-register zal het Ministerie van VWS adequate maatregelen treffen.

- Schade die ontstaat doordat beperkingen in het gebruik van het handtekeningcertificaat zijn overschreden, met die voorwaarde dat de beperkingen van tevoren door het UZI-register aan derden kenbaar is gemaakt;
- Schade ten gevolge van niet-toerekenbare tekortkomingen in de nakoming (overmacht), onder meer inhoudende vertraging en gebreken in de uitvoering van werkzaamheden die te wijten zijn aan al dan niet technische storingen, zoals transmissiefouten, storingen aan apparatuur en systeemprogrammatuur, defecten in de apparatuur en programmatuur, opzet hieronder verstaan onder meer fraude, illegaal gebruik van programmatuur, sabotage, diefstal van gegevens en bedieningsfouten door derden, fouten van derden met als gevolg netwerkuitval, stroomuitval, brand, blikseminslag, aanzienlijke waterschade, een breuk in een telefoonkabel, oorlogsgeweld, terreurdaden, natuurrampen en meer in het algemeen oorzaken welke niet de redelijk in acht te nemen zorg van het UZI-register betreffen;
- Schade die ontstaat doordat abonnees, pashouders en/of vertrouwende partijen niet de verplichtingen zoals beschreven in voorliggend CPS nakomen;
- Schade ten gevolge van misbruik, verlies, diefstal of anderszins verdwijnen van het certificaat, de pincode, de pukcode, intrekkingcode, drager van de publieke en private sleutel en de private sleutel;
- Schade ontstaan door de afgifte van een certificaat op grond van door de abonnee of pashouder verkeerd verstrekte informatie, voor zover het UZI-register op basis van de in onderhavige CPS genoemde procedures en controles in redelijkheid niet had kunnen ontdekken dat de informatie niet correct was;
- Schade ten gevolge van het gebruik van een certificaat na het tijdstip van intrekking van het certificaat en publicatie op de CRL;
- Schade als gevolg van fouten die zijn veroorzaakt door de overdracht van gegevens door de abonnee en/of pashouder, de programmatuur, de apparatuur of telecommunicatie-faciliteiten gebruikt door abonnee en/of pashouder;
- Schade als gevolg van een gebrek en/of onjuiste informatie in het verzonden bericht of in de verzending of ontvangst daarvan, die ernstige schade zoals lichamelijk letsel, dood of milieuschade ten gevolge heeft, daaronder begrepen doch niet daartoe beperkt, in het kader van het gebruik van medische toepassingen.
- Schade ontstaan doordat het koeriersbedrijf het UZI-product of de identificatie van de certificaatbeheerder buiten het overeengekomen tijdvenster levert/uitvoert. Schade ontstaan doordat het koeriersbedrijf geen correcte identificatie van de certificaatbeheerder door toedoen van de certificaatbeheerder heeft kunnen uitvoeren.

In zoverre dat de met het vertrouwen gemoeide belangen disproportioneel zijn ten opzichte van het door het certificaat geboden niveau van betrouwbaarheid, wordt de vertrouwende partij geacht niet in redelijkheid op het certificaat te hebben vertrouwd, zelfs wanneer hij/zij aan alle overige verplichtingen heeft voldaan.

9.8 Schadeloosstelling

Schadeloosstelling geschiedt enkel nadat onomstotelijk is vastgesteld dat het UZI-register aansprakelijk kan worden gehouden voor de geleden schade.

9.9 Geldigheidstermijn CPS

Het CPS is geldig vanaf de datum van publicatie. Het CPS is geldig zolang de dienstverlening van het UZI-register voortduurt of totdat het CPS wordt vervangen door een nieuwere versie. Nieuwere versies worden aangeduid met een hoger versienummer (vX.xx). Bij ingrijpende wijzigingen wordt het versienummer opgehoogd met 1, bij redactionele aanpassingen wordt het versienummer

opgehoogd met 0.10. Nieuwere versies worden gepubliceerd op de website van het UZI-register.

Indien één of meerdere bepalingen van onderhavig CPS bij gerechtelijke uitspraak of anderszins niet van toepassing wordt verklaard, laat die de geldigheid en toepasselijkheid van alle overige bepalingen onverlet. Partijen zullen in dat geval gebonden zijn aan een bepaling van zoveel mogelijk overeenkomstige strekking die niet aan vernietiging blootstaat.

9.10 Communicatie binnen betrokken partijen

Geen nadere bepalingen.

9.11 Wijzigingen

9.11.1 Wijzigingsprocedure

De werking van het geldende CPS wordt ten minste jaarlijks beoordeeld en geüpdate door het UZI-register. Wijzigingen gelden vanaf het moment dat het nieuwe CPS wordt gepubliceerd. Het TSP management is verantwoordelijk voor de uiteindelijke goedkeuring van het CPS.

9.11.2 Verzoeken tot wijziging en classificatie

Abonnees, certificaathouders, vertrouwende partijen en eventuele andere belanghebbenden kunnen schriftelijk gemotiveerd een verzoek tot wijziging indienen. Het UZI-register kan zelf een verzoek tot wijziging indienen, bijvoorbeeld naar aanleiding van een interne review of audit, een wijziging in het programma van eisen van de PKI voor de overheid, veranderende wetgeving of dergelijke. Alle voorstellen tot wijziging worden direct vastgelegd. De indiener van het verzoek ontvangt van het UZI-register een ontvangstbevestiging.

De verzoeken tot wijziging worden door het TSP management en de staf van het UZI-register geclassificeerd. Waar dit nodig is, wordt hierbij specialistische juridische of technische kennis betrokken. Bij classificatie wordt tevens de urgentie van het verzoek tot wijziging bepaald. Wijzigingen op het CPS worden zo veel mogelijk gegroepeerd doorgevoerd.

9.11.3 Publicatie van wijzigingen

Het UZI-register publiceert het CPS op de website: www.zorgcsp.nl. Tevens kan het CPS worden opgevraagd via de in paragraaf 1.5.1 ‘Contactgegevens’ vermelde contactinformatie. Deze aanvraag kan zowel telefonisch als schriftelijk worden gedaan.

9.12 Conflictoplossing

Als er een conflict ontstaat over de interpretatie van de bepalingen van voorliggend CPS, geeft het CPS de interpretatie van de bepalingen van het UZI-register aan. Deze interpretatie dient de algemene doelstelling van het UZI-register in acht te nemen. Wanneer deze uitleg niet tot een voor betrokkene(n) bevredigd resultaat leidt, dan zal, alvorens andere al dan niet juridische stappen genomen worden, het conflict worden voorgelegd aan een voor alle betrokkenen acceptabele conflict-bemiddelaar. Over de bekostiging van deze conflictbemiddeling worden als dan afspraken gemaakt. Als voorgaande het geschil alsnog niet beslecht, wordt ze bij uitsluiting voorgelegd aan de bevoegde rechter te ’s-Gravenhage.

In geval van klachten betreffende diensten geleverd door het UZI-register, moet de klacht schriftelijk ingediend worden bij het UZI-register, ter attentie van het afdelingshoofd Registers & Knooppunten 1 onder vermelding van ‘Klacht’. Het UZI-

register zal de klacht vervolgens afhandelen conform de klachtenprocedure CIBG, welke voortvloeit uit hoofdstuk 9 van de Awb.

Ontstaat er een conflict tussen twee afnemers van diensten die het UZI-register biedt, dan kan het afdelingshoofd van het UZI-register bemiddelen of een onafhankelijke bemiddelaar aanwijzen, indien partijen niet in onderling overleg tot overeenstemming komen.

9.13 Toepasselijk recht

Op de diensten van het UZI-register, voorliggend CPS is het Nederlandse recht van toepassing.

9.14 Naleving relevante wetgeving

Het UZI-register is een certificatiedienstverlener in de zin van de Telecommunicatiewet. Hierdoor is zij gehouden aan alle Europese en nationale wet- en regelgeving die verband houdt met haar hoedanigheid van TSP en de diensten die zij levert. Een en ander met inachtneming van het feit dat het UZI-register als onderdeel van het CIBG een bestuursorgaan is in de zin van de Awb.

9.15 Overige bepalingen

Als één of meerdere bepalingen van het CPS bij gerechtelijke uitspraak ongeldig of anderszins niet van toepassing wordt verklaard, laat dit de geldigheid en toepasselijkheid van alle overige bepalingen onverlet.

Bijlage 1: Definities en afkortingen

Bij de samenstelling van de definities van de gehanteerde begrippen zijn de volgende uitgangspunten gehanteerd:

- Er is in een aantal gevallen gekozen voor het gebruik van Engelstalige termen. Reden hiervoor is, dat er vaak geen correcte Nederlandse vertaling voor die Engelstalige term bestaat. Als een Nederlandstalig begrip naast een Engelstalig begrip wordt gebruikt met dezelfde betekenis, staan beide begrippen in de lijst (het meest gangbare begrip is in de lijst opgenomen direct gevolgd door de vertaling die dan cursief is weergegeven);
- Waar het gaat om 'PKI-termen' (PKI = Public Key Infrastructure) is zoveel mogelijk aangesloten bij de algemeen gehanteerde definities van de PKI voor de overheid en in de vakliteratuur over dit onderwerp.

De begrippenlijst bestaat uit drie kolommen: Afkorting, Begrip en Definitie. De sortering is alfabetisch en op de kolom 'Begrip'. In een aantal gevallen is direct na de definitie een toelichting gegeven en, indien van toepassing, de bron van de informatie; als scheiding is een witregel opgenomen.

Afkorting	Begrip	Definitie
	Abonnee	Een in het UZI-register geregistreerde zorgaanbieder die certificatiediensten afneemt van het UZI-register. De abonnee is de partij namens wie een certificaathouder handelt bij gebruik van een certificaat. De naam en het abonneenummer van de abonnee zijn vermeld in het certificaat.
	Achternaam	De achternaam is de (correspondentie) naam zoals deze dagelijks wordt gebruikt door de persoon.
AT	Agentschap Telecom	Agentschap Telecom is zowel uitvoerder als toezichthouder van wet- en regelgeving op het gebied van telecommunicatie, Bron: www.agentschaptelecom.nl
AGB	Algemeen GegevensBeheer-zorgverleners	Een database waarin gegevens staan geregistreerd van zorgverleners. Deze registratie omvat, naast de algemene persoons- en praktijkinformatie, ook gegevens die van belang zijn voor de communicatie tussen zorgaanbieders en zorgverzekeraars, met name over declaraties. AGB wordt beheerd door Vektis.
	Asymmetrisch sleutelpaar	Een publieke - en persoonlijke sleutel die op zodanige manier wiskundig met elkaar verbonden zijn, zodat ze, in een cryptografische berekening, elkaars tegenhanger worden. Asymmetrische sleutelparen worden onder meer gebruikt voor het plaatsen en controleren van de elektronische handtekening. Zie ook 'Private sleutel' en 'Publieke sleutel'.
	Authenticatie	Een proces waarbij iemands identiteit bevestigd kan worden of waarmee de integriteit en de herkomst van aangeboden gegevens gecontroleerd kunnen worden. Zie ook 'Authenticatiecertificaat', 'Autorisatie' en 'Identificatie'.
	Authenticatie-certificaat	Een certificaat dat uitsluitend gebruikt dient te worden voor, authenticatie - of elektronische identificatie.
	Autorisatie	Iemand de bevoegdheid verlenen om bepaalde handelingen uit te voeren (voorbeelden van handelingen: inzien -, aanpassen - of bewerken van gegevens).
AP	Autoriteit Persoonsgegevens	Het AP zie er op toe dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd en dat privacy ook in de toekomst gewaarborgd blijft.

Afkorting	Begrip	Definitie
AVG	Algemene verordening gegevensbescherming (AVG)	Sinds 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Deze verordening zorgt ervoor dat in de hele EU dezelfde privacywetgeving geldt.
	BIG-register	Register van beroepsbeoefenaren in de individuele gezondheidszorg zoals bedoeld in artikel 3 en 34 van de Wet op de Beroepen in de Individuele Gezondheidszorg (Wet BIG). Zie ook: www.bigregister.nl
	BSN-diensten	BSN-diensten omvatten: - het opvragen en verifiëren van een burgerservicenummer, - het opvragen van persoonsgegevens - de WID controle.
BSN	Burgerservicenummer	Het als zodanig overeenkomstig de Wet algemene bepalingen burgerservicenummer aan een natuurlijk persoon toegekend uniek identificerend nummer.
	CA-certificaat	Een certificaat van een Certification Authority dat onder andere de publieke sleutel bevat en is uitgegeven en ondertekend door een hogere CA.
CIBG	CIBG	Het CIBG is een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport, dat belast is met een aantal wettelijke uitvoeringstaken. Zie ook: www.cibg.nl
	Certificaat	Elektronische bevestiging die gegevens voor het verifiëren van een bepaalde persoon verbindt met gegevens over de vertrouwelijkheid en authenticiteit en/of elektronische handtekening en daarmee de identiteit van de persoon bevestigt. Een certificaat is een publiekelijk toegankelijk document dat is uitgegeven door een TSP en dat een aantal door die TSP gecontroleerde gegevens bevat. Een certificaat, bevat tenminste: a) de vermelding dat het certificaat als gekwalificeerd certificaat wordt afgegeven; b) de identificatie en het land van vestiging van de afgevende certificatiedienstverlener; c) de naam van de ondertekenaar; d) ruimte voor een specifiek attribuut van de ondertekenaar, dat indien nodig, afhankelijk van het doel van het gekwalificeerde certificaat, wordt vermeld; e) gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening die onder controle van de ondertekenaar staan; f) vermelding van het tijdstippen van het begin en van het einde van de geldigheidsduur van het gekwalificeerde certificaat; g) de identiteitscode van het gekwalificeerde certificaat; h) de elektronische handtekening van de afgevende certificatiedienstverlener die voldoet aan de criteria van artikel 15a, tweede lid, onderdeel a tot en met d, van Boek 3 van het Burgerlijk Wetboek; i) eventuele beperkingen betreffende het gebruik van het gekwalificeerde certificaat, en j) eventuele grenzen met betrekking tot de waarde van de transacties waarvoor het gekwalificeerde certificaat kan worden gebruikt.
	Certificaathouder	Een natuurlijk persoon of rechtspersoon, voor wie een certificaat is afgegeven en wiens identiteit kan worden vastgesteld met behulp van het certificaat.
	Certificaatbeheerder	De rol van certificaatbeheer is alleen van belang voor producten waarbij de certificaathouder een systeem is of een groep/functie betreft, dus servercertificaten en de Medewerkerpas op naam. Het UZI-register heeft ervoor gekozen dat bij deze producten de aanvrager van deze producten namens een abonnee ook optreedt als certificaatbeheerder.
	Certificaatprofiel	Een beschrijving van de inhoud van een certificaat. Ieder soort certificaat (handtekening, vertrouwelijkheid, e.d.) heeft een eigen invulling en daarmee een eigen beschrijving. Hierin staan bijvoorbeeld afspraken omtrent naamgeving, e.d.

Afkorting	Begrip	Definitie
CP	Certificate Policy - *certificerings-beleid*	Een document met een benoemde verzameling eisen dat de kaders aangeeft waarbinnen het UZI-register certificaten uitgeeft. Het CP wordt opgesteld door de Policy Authority van de PKI voor de Overheid. Met behulp van onder andere het CP kunnen certificaathouders en vertrouwende partijen bepalen hoeveel vertrouwen zij stellen in het UZI-register.
CRL	Certificate Revocation List - *certificaat revocatie lijst*	Een lijst van ingetrokken (= gerevoceerde) certificaten. De Certificate Revocation List (CRL) is openbaar toegankelijk en raadpleegbaar. De lijst is beschikbaar gesteld door en onder verantwoordelijkheid van het UZI-register. De CRL is zelf ook elektronisch ondertekend door de CA van het UZI-register.
	Certificatiediensten	Het afgeven, beheren en intrekken van certificaten door certificatiedienstverleners, alsook andere diensten die samenhangen met het gebruik van elektronische handtekeningen, identiteit en vertrouwelijkheid.
CA	Certification Authority	Het onderdeel van het UZI-register dat de ondertekening van de certificaten verzorgt en dat door eindgebruikers wordt vertrouwd.
CPS	Certification Practice Statement	Een document dat de door het UZI-register gevolgde procedures en getroffen maatregelen over alle aspecten van de dienstverlening beschrijft. Het CPS beschrijft op welke wijze het UZI-register voldoet aan de eisen zoals gesteld in de Certificate Policy (CP).
	Compromittatie	Iedere aantasting van het vertrouwen in het exclusieve gebruik van een component door bevoegde personen. In het kader van de PKI voor de overheid wordt met die component meestal de private sleutel bedoeld. Een sleutel wordt als aangetast beschouwd in geval van: - Ongeautoriseerde toegang of vermeende ongeautoriseerde toegang; - Verloren of vermoedelijk verloren private sleutel of SSCD; - Gestolen of vermoedelijk gestolen private sleutel of SSCD; - Vernietigde private sleutel of SSCD. Compromittatie vormt aanleiding om een certificaat op de Certificate Revocation List te plaatsen.
	Consortium	Het consortium van KPN Corporate Market BV en ATOS Nederland BV met als penvoerder KPN Corporate Market BV.
DAF	Digitale aanvraagfaciliteit	
	Directory service	De directory service is een dienst van het UZI-register en heeft tot doel het op internet beschikbaar stellen en het toegankelijk maken van uitgegeven certificaten.
	Eindgebruiker	Zie certificaathouder

Afkorting	Begrip	Definitie
	Elektronische handtekening	Een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. De elektronische handtekening die gezet kan worden met de UZI-pas, heet formeel de 'geavanceerde elektronische handtekening'. Dit is een elektronische handtekening die dezelfde rechtskracht heeft als een handgeschreven handtekening op papier, mits zij voldoet aan de volgende eisen: - Zij is op unieke wijze aan de ondertekenaar verbonden; - Zij maakt het mogelijk de ondertekenaar te identificeren; - Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; - Zij is op zodanige wijze aan de elektronisch bestand waarop zij betrekking heeft verbonden, dat op elke wijziging achteraf van de gegevens kan worden opgespoord; - Zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet; Zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen, als bedoeld in artikel 1.1 onderdeel vv Telecommunicatiewet.
	Elektronische identiteit	Een unieke elektronische representatie van een identiteit, bijvoorbeeld in de vorm van een X.500 Distinguished Name structuur. Deze elektronische gegevens worden toegevoegd aan, of op logische wijze verbonden met andere elektronische gegevens. Ze fungeren als uniek kenmerk van de identiteit van de eigenaar.
	Escrow (Key-escrow)	'Sleutelborging'. Een methode van opslag voor een kopie van een private sleutel die bij een vertrouwde derde in bewaring gegeven wordt, een zogenoemde 'Key Escrow Agency' (KEA).
ETSI	European Telecommunication Standard Institute	De ETSI is een onafhankelijk instituut op het gebied van standaardisatie voor telecommunicatie.
	Geboortenaam	De geboortenaam is de naam zoals deze in het identiteitsbewijs is opgenomen (ook wel meisjesnaam of geslachtsnaam genoemd).
	Gekwalificeerd certificaat	Een certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een certificatiedienstverlener die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet.
	Gemachtigde aanvrager	Een zorgverlener of vertegenwoordiger van een (zorg)instelling die gemachtigd is door de wettelijk vertegenwoordiger van de (zorg)instelling om in naam van de (zorg)instelling aanvragen tot uitgifte van UZI-passen in te dienen bij het UZI-register.
	Handtekening-certificaat (onweerlegbaarheid certificaat)	Een certificaat dat gekoppeld is aan de sleutel die gebruikt moet worden bij het plaatsen van een elektronische handtekening.
HSM	Hardware Security Module	Een middel dat de private sleutel(s) van systemen bevat deze sleutel(s) tegen compromittatie beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert namens het systeem.
	Hiërarchie	Een gezagsketen van elkaar vertrouwende Certification Autorities (CA).
	Identificatie	Het proces waarbij de identiteit van een persoon of een organisatie vastgesteld wordt.
	Identiteitsbewijs of Identiteitsdocument	Een document zoals genoemd in de Wet op de Identificatieplicht (WID) om de identiteit van een natuurlijk persoon vast te stellen.
	Indicatieorgaan	Het CIZ, genoemd in artikel 7.1.1, eerste lid, van de Wet langdurige zorg.
	Instelling	Een rechtspersoon die bedrijfsmatig zorg verleent, een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen en de door de minister van Volksgezondheid, Welzijn en Sport aangewezen instellingen.
	Integriteit	De zekerheid dat gegevens volledig en niet gewijzigd zijn.

Afkorting	Begrip	Definitie
ISO	International Organization for Standardization.	Uitgevende organisatie van een aantal normen en richtlijnen voor Kwaliteitsmanagementsystemen. Het gaat daarbij om de kwaliteit van het hoofdproces van een organisatie. De ISO-normen en -richtlijnen zijn internationaal geaccepteerd en worden om de vijf jaar herzien.
	Intrekkingcode	Code waarmee de certificaathouder een intrekkingverzoek voor een UZI-pas kan indienen en autoriseren, bijvoorbeeld na verlies van de pas.
	Onweerlegbaarheid - *non-repudiation*	Onweerlegbaarheid bewijst de oorsprong of de ontvangst van gegevens zodat geen van beide partijen (ontvanger en verzender) de transactie of het bericht kan ontkennen. In de praktijk van het UZI-register is deze eigenschap verbonden aan het certificaat voor de elektronische handtekening. Zie ook: handtekeningcertificaat.
	Pasaanvrager	De wettelijk vertegenwoordiger of de persoon voor wie de wettelijk vertegenwoordiger een financiële machtiging heeft afgegeven aan het UZI-register voor het aanvragen van UZI-middelen.
	Pashouder	De natuurlijke persoon die gebruik maakt van de UZI-pas. (zie ook certificaathouder)
PIN	Personal Identification Number	Data die nodig is om de UZI-pas te kunnen gebruiken. Deze data is persoonsgebonden en dient te allen tijde geheim te blijven. Het UZI-register gebruikt als activeringsdata een pincode.
PUK	Personal Unblocking Key	De pukcode is nodig om de UZI-pas te deblokkeren.
	Persoonlijke sleutel	Zie 'Private sleutel'.
	PIN-mailer Pincodebrief	De pincodebrief bevat de pin-, puk- en intrekkingcode en wordt afhankelijk van het pastype verzonden naar de aanvrager of de certificaathouder. De codes zijn op een beveiligde manier geprint zodat alleen degene die de envelop opent de codes kent.
	PKCS#10 request	Dit is een door RSA laboratories gestandaardiseerd bestandsformaat (syntax) waarmee de benodigde informatie (public key, subject info rmatie) aan een CA systeem aangeleverd kan worden waarmee dit CA-systeem een certificaat kan genereren. Voor systeemcertificaten leveren aanvragers rechtstreeks een PKCS#10 request in ASCII formaat aan via de webregistratie.
PA	Policy Authority	Autoriteit onder de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties die het certificeringsbeleid (CP / Certificate Policy) van het UZI-register vaststelt. zie ook http://www.logius.nl
	Private sleutel	De sleutel van een asymmetrisch sleutelpaar die alleen bekend dient te zijn bij de houder ervan en strikt geheim moet worden gehouden .Soms wordt de term geheime of persoonlijke sleutel gebruikt. Zie ook: 'asymmetrisch sleutelpaar' en 'publieke sleutel'.
PKI	Public Key Infrastructure	Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op asymmetrische sleutelparen. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.
	Publieke sleutel	De sleutel van een asymmetrisch sleutelpaar die publiekelijk kan worden bekend gemaakt. Soms wordt de term openbare sleutel gebruikt. Zie ook: 'asymmetrisch sleutelpaar' en 'persoonlijke sleutel'.
RA	Registration Authority - *registratie autoriteit*	Het onderdeel van het UZI-register dat de registratie werkzaamheden uitvoert ter verwerking van de certificaataanvragen.
	Revocatie	Revocatie betreft het ongeldig maken (intrekken) van een certificaat. Een certificaat wordt gerevoceerd door het serienummer van het certificaat op de Certificate Revocation List (CRL) te zetten (revocatie = herroepen / intrekken).
	Root CA	Het hoogste vertrouwenspunt van de hiërarchie van een Public Key Infrastructure (PKI).

Afkorting	Begrip	Definitie
SSCD	Secure Signature Creation Device	Een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld in artikel 18.17, eerste lid van de Telecommunicatiewet.
SUD	Secure User Device	Een middel dat de private sleutel(s) van gebruikers bevat deze sleutel(s) tegen compromittatie beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert in naam van de gebruiker.
	Servercertificaat	Naast de UZI-pas in de vorm van een smartcard geeft het UZI-register ook servercertificaten uit. Met behulp van deze servercertificaten wordt aangetoond dat een service, bv. applicatie of server daadwerkelijk bij een zorgaanbieder hoort. Daarnaast kan met een servercertificaat een beveiligde verbinding tussen services worden gemaakt.
	Sleutel(s)	Zie respectievelijk: - Asymmetrisch sleutelpaar - Private sleutel - Publieke sleutel
	Sleutelpaar	Zie ook asymmetrisch sleutelpaar.
	Smartcard	Een plastic pasje ter grootte van een creditcard die in een chip elektronica bevat, inclusief een microprocessor, geheugenruimte en een voedingsbron. De kaarten kunnen worden gebruikt om informatie op te slaan en zijn eenvoudig mee te nemen.
	Stamcertificaat	Dit is het certificaat behorend bij de plek waar het vertrouwen in alle PKI voor de overheid uitgegeven certificaten zijn oorsprong vindt. Er is geen hoger liggende CA waaraan het vertrouwen wordt ontleend. Dit certificaat wordt door de houder, de beleidsverantwoordelijke van het hoogste vertrouwenspunt, zelf ondertekend. Alle onderliggende certificaten worden uitgegeven door de houder van het stamcertificaat.
	Toetsingsregister	Een door de beleidsverantwoordelijke van het UZI-register erkend register. Het UZI-register kan voor een zorgverlener of instelling die in een dergelijk register is opgenomen de garantie zorgverlener of instelling afgeven.
TSP	Trusted Service Provider *certificatiedienst verlener*	Een natuurlijk persoon of rechtspersoon die de certificaten afgeeft en/of andere diensten in verband met de elektronische handtekeningen, waaronder identiteit en vertrouwelijkheid, verleent. Het UZI-register is een TSP.
UZI	Unieke Zorgverleners Identificatie	Unieke Identificatie van zorgaanbieders.
	UZI-pas	De drager van de elektronische identiteit van een zorgaanbieder.
	UZI-register	Register van zorgaanbieders. Het UZI-register zorgt voor de unieke identificatie van zorgaanbieders. Het is gebaseerd op een PKI die de wettelijke en fysieke identiteit koppelt aan een elektronische identiteit en deze vastlegt in certificaten. Zie ook: www.uzi-register.nl
	Verantwoordelijke	Voor het registratieproces van zorginstellingen wordt met de verantwoordelijke degene bedoeld die de zorginstelling mag inschrijven in het UZI-register.
	Vertrouwelijkheid	De garantie dat gegevens daadwerkelijk en uitsluitend terechtkomen bij degene voor wie zij zijn bedoeld, zonder dat iemand anders ze kan ontcijferen. Buiten de private sector wordt hiervoor ook wel de term exclusiviteit gebruikt.
	Vertrouwelijkheids-certificaat	Een certificaat dat hoort bij het sleutelpaar dat gebruikt moet worden bij toepassingen ten behoeve van vertrouwelijkheid.
	Vertrouwende partij	De natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat.
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.	De wet regelt dat binnen de zorgsector gebruikt gemaakt wordt van het burgerservicenummer. Het gebruik van het burgerservicenummer in de zorg is nodig om eenduidig vast te kunnen stellen welke gegevens bij welke client horen. Daarnaast zijn regels opgenomen over elektronische uitwisselingssystemen in de zorg.

Afkorting	Begrip	Definitie
WID	Wet op de Identificatieplicht	De Wet op de identificatieplicht noemt het paspoort en de identiteitskaart als geldige identificatiemiddelen. Een aantal documenten is aan het paspoort en identiteitskaart gelijkgesteld: rijbewijs, diplomatiek paspoort, dienstpaspoort, reisdocument voor vluchtelingen- of vreemdelingen en overige reisdocumenten die door de minister vastgesteld zijn, zoals de Nederlandse identiteitskaart. Het noodpaspoort en de laissez passer zijn geen geldige identificatiemiddelen.
Wkkgz	Wet Kwaliteit, klachten en geschillen zorg	De Wet kwaliteit, klachten en geschillen zorg (Wkkgz) gaat over kwaliteit en klachtrecht van cliënten in de zorgsector en is sinds 1 januari 2016 van kracht. De Wet kwaliteit, klachten en geschillen zorg geldt voor alle zorgaanbieders. Zowel voor zorginstellingen als zelfstandige beroepsbeoefenaren, zoals zzp'ers.
WTZi	Wet Toelating Zorginstellingen	Zorginstellingen hebben een toelating nodig wanneer zij zorg willen aanbieden die op grond van de Zorgverzekeringswet of Wet langdurige zorg voor vergoeding in aanmerking komt. De Wet toelating zorginstellingen (WTZi) regelt deze toelatingen.
	Wettelijk vertegenwoordiger	De persoon die conform het uittreksel KvK of oprichtingsdocument bevoegd is om de organisatie juridisch te binden aan het UZI-register.
X.509	X.509	Dit is een elektronisch certificaat dat volgens een gestandaardiseerde structuur is opgebouwd.
	Zorg	zorg: **1°.** zorg of dienst als omschreven bij of krachtens de Zorgverzekeringswet en de Wet langdurige zorg; **2°.** vorm van hulp voor de kosten waarvan een subsidie wordt verstrekt op grond van artikel 3.3.3 van de Wet langdurige zorg of artikel 68 van de Zorgverzekeringswet; **3°.** zorg als bedoeld in de artikelen 5, 6b en 12a van de Wet publieke gezondheid; **4°.** handelingen op het gebied van de individuele gezondheidszorg als bedoeld in artikel 1 van de Wet op de beroepen in de individuele gezondheidszorg; één en ander met inbegrip van de financiële afwikkeling; Bron: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.
	Zorgaanbieders	Zorgaanbieder als bedoeld in de Wet kwaliteit, klachten en geschillen zorg. De Wkkgz bepaalt dat een *zorgaanbieder* een instelling dan wel een solistisch werkende zorgverlener is.
	Zorgverlener	een natuurlijke persoon die beroepsmatig zorg verleent

Bijlage 2: Toetsingscriteria organisaties en zorgverleners

Het UZI-register garandeert dat alleen partijen die behoren tot het door de minister van VWS aangegeven domein, abonnee kunnen worden van het UZI-register. Het UZI-register kent twee typen abonnees, te weten organisaties (zorginstellingen en indicatieorganen) en personen (solistisch werkende zorgverlener). Beide typen abonnees kunnen UZI-passen aanvragen voor zorgverleners, andere medewerkers en services. Voor zorgverlenerpassen garandeert het UZI-register dat deze zijn uitgegeven aan een zorgverlener. Als de zorgverlener niet meer voldoet aan de toetsingscriteria, trekt het UZI-register de zorgverlenerpas in.

Deze bijlage geeft een toelichting op de criteria op basis waarvan de genoemde garanties worden afgegeven.

A. Toetsingscriteria organisaties
Organisaties die tot het domein van het UZI-register behoren zijn:

- Zorgaanbieders die onder de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg vallen. Voor het begrip zorgaanbieder wordt verwezen naar de Wet kwaliteit, klachten en geschillen zorg.
- Indicatieorgaan: het CIZ, genoemd in artikel 7.1.1, eerste lid, van de Wet langdurige zorg;
- Jeugdhulpaanbieder: jeugdhulpaanbieder als bedoeld in artikel 1.1 van de Jeugdwet.

Voordat een organisatie wordt ingeschreven als abonnee, toetst het UZI-register of de organisatie behoort tot het domein. Hierbij worden de volgende criteria gehanteerd:

- Organisaties die in het bezit zijn van een toelating in de zin van de Wet toelating zorginstellingen (WTZi) behoren tot het domein. Deze organisaties hoeven geen verdere bewijsstukken te overleggen.
- Organisaties die zijn opgenomen in het Apothekenregister in het kader van de Geneesmiddelenwet behoren tot het domein. Deze organisaties hoeven geen verdere bewijsstukken te overleggen. Als de organisatie niet is opgenomen in bovengenoemde registers, moet de organisatie bewijsstukken overleggen. Dit bewijs kan worden overlegd in de vorm van:
-
  - Kopie van een oprichtingsdocument of notariële akte, ondertekend door de notatris:
    De organisatie kan aan de hand van de doelstelling van de organisatie zoals beschreven in het oprichtingsdocument of de notariële akte aantonen tot het hierboven aangegeven domein te behoren.
  - Afschrift van een vergunning of beschikking:
    De organisatie kan aan de hand van een verleende vergunning of toegekende beschikking aantonen tot het hierboven aangegeven domein te behoren.
  - Eigenverklaring:
    Een samenwerkingsverband van zorgverleners zonder rechtspersoonlijkheid kan aan de hand van een door alle betrokkenen ondertekende eigenverklaring ingeschreven worden in het UZI-register. Uit deze eigenverklaring moet blijken dat er sprake is van een zorgaanbieder in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Deze verklaring dient te zijn ondertekend door de betreffende zorgaanbieders binnen het samenwerkingsverband.

- Zorgovereenkomst met een zorgverzekeraar.
  De zorgaanbieder kan hiermee aantonen dat deze zorg verleent in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.
- Verklaring waaruit blijkt welke zorgverleners er binnen de eenmanszaak werkzaam zijn.
  De zorgaanbieder kan hiermee aantonen dat hij geen solistisch werkende zorgverlener is maar met meerder zorgverleners zorg doet verlenen.

B. Toetsingscriteria Zorgverleners
Personen die in het UZI-register als zorgverlener (abonnee of certificaathouder) worden aangemerkt zijn:

- Beroepsbeoefenaren zoals bedoeld in artikel 3 van de Wet BIG
- Beroepsbeoefenaren zoals bedoeld in artikel 34 van de Wet BIG.
- Beroepsbeoefenaren zoals bedoeld in artikel 36a van de Wet BIG

Beroepsbeoefenaren die zorg verlenen in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, maar geen beroepsbeoefenaar is zoals bedoeld in artikel 3, 34 of 36a van de Wet BIG. Deze groep kan niet in het bezit worden gesteld van een zorgverlenerpas. Voordat een zorgverlener wordt ingeschreven als abonnee of certificaathouder toetst het UZI-register of is voldaan aan de toetsingscriteria. De volgende criteria worden gehanteerd:

- Het UZI-register toetst of de beroepsbeoefenaar is geregistreerd in het BIG-register en of er eventueel sprake is van een situatie waarin de beroepsbeoefenaar de opgegeven beroepstitel of specialisme niet mag gebruiken (zie C Criteria registratie en intrekking pas bij schorsing). In deze toetsing wordt ook een eventueel opgegeven specialisme meegenomen. Als de beroepsbeoefenaar in het BIG-register is geregistreerd en de beroepstitel mag voeren, kan deze in het UZI-register worden ingeschreven als abonnee of houder van een zorgverlenerpas. Beroepsgroepen waarvoor deze toetsing geldt zijn:
  Apothekers
  Artsen[16]
  Fysiotherapeuten
  Gezondheidszorgpsychologen
  Psychotherapeuten
  Tandartsen
  Verloskundigen
  Verpleegkundigen
  Physician assistant
  Klinisch technoloog

- Beroepsbeoefenaren die zijn opgenomen in het Kwaliteitsregister Paramedici hoeven geen verdere bewijzen te overleggen. Het UZI-register toetst bij Stichting Kwaliteitsregister Paramedici of de beroepsbeoefenaar daadwerkelijk is geregistreerd. Beroepsgroepen waarvoor deze toetsing geldt zijn:
  Diëtisten
  Ergotherapeuten
  Huidtherapeuten
  Logopedisten
  Mondhygiënisten
  Oefentherapeuten Cesar

16 Het specialisme apotheekhoudend huisarts wordt in de certificaten opgenomen nadat in het BIG-register is gecontroleerd dat de beroepsbeoefenaar het specialisme huisarts mag voeren en nadat de certificaathouder een kopie van de vergunning voor het houden van de apotheek heeft overlegd.

Oefentherapeuten Mensendieck
Optometristen
Orthoptisten
Podotherapeuten
Radiodiagnostisch laboranten
Radiotherapeutisch laboranten

- Beroepsbeoefenaren die zijn opgenomen in het Kwaliteitsregister Mondhygiënisten hoeven geen verdere bewijzen te overleggen. Het UZI-register toetst bij Kwaliteitsregister Mondhygiënisten of de beroepsbeoefenaar daadwerkelijk is geregistreerd. Beroepsgroepen waarvoor deze toetsing geldt zijn:
  Mondhygiënisten

- Beroepsbeoefenaren die zijn opgenomen in het Kwaliteitsregister Apothekersassistenten (KAA) hoeven geen verdere bewijzen te overleggen. Het UZI-register toets bij dit register of de beroepsbeoefenaar daadwerkelijk is geregistreerd. De beroepsgroepen waarvoor deze toetsing geldt is:
  Apothekersassistenten

- Beroepsbeoefenaren zoals bedoeld in artikel 34 van de Wet BIG die niet zijn opgenomen in het Kwaliteitsregister Paramedici of het Kwaliteitsregister Mondhygiënisten, Kwaliteitsregister Apothekersassistenten (KAA) moeten bij hun aanvraag tot registratie als abonnee of bij de aanvraag van een zorgverlenerpas een origineel gewaarmerkte kopie van het relevante diploma of een digitaal uittreksel (pdf met certificaat van DUO) overleggen. Het UZI-register besluit op basis van een diplomatoets of de betrokkene kan worden ingeschreven als abonnee of houder van een zorgverlenerpas. Beroepsgroepen waarvoor deze toetsing geldt zijn:
  Apothekersassistenten
  Diëtisten
  Ergotherapeuten
  Huidtherapeuten
  Logopedisten
  Mondhygiënisten
  Oefentherapeuten Cesar
  Oefentherapeuten Mensendieck
  Optometristen
  Orthoptisten
  Podotherapeuten
  Radiodiagnostisch laboranten
  Radiotherapeutisch laboranten
  Tandprothetici
  Verzorgenden in de individuele gezondheidszorg (VIG-ers)

    - Beroepsbeoefenaren zoals bedoeld in artikel 36a van de Wet BIG die niet zijn opgenomen in het BIG-register moeten bij hun aanvraag tot registratie als abonnee een origineel gewaarmerkte kopie van het relevante diploma of een digitaal uittreksel (PDF met certificaat van DUO) overleggen. Het UZI-register besluit op basis van een diplomatoets of de betrokkene kan worden ingeschreven als abonnee. Beroepsgroepen waarvoor deze toetsing geldt zijn:
    - Klinisch technoloog
    - Bachelor Medisch Hulpverlener

- Beroepsbeoefenaar die zorg verleent in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, maar geen beroepsbeoefenaar is zoals bedoeld in artikel 3, 34 of 36a van de Wet BIG moeten bij hun aanvraag tot registratie als abonnee stukken overleggen waaruit blijkt dat er zorg wordt verleent, zoals genoemd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.
  Hierdoor moet deze groep zorgverleners bij hun aanvraag tot registratie als abonnee de volgende stukken overleggen:
  - Een origineel gewaarmerkte kopie van het relevante diploma of een digitaal uittreksel (pdf met certificaat van DUO) overleggen.
  - Een zorgovereenkomst op naam van de zorgverlener (indien de zorgverlener in het bezit is van een zorgovereenkomst)
  - Verklaring waaruit blijkt welke zorg er door de zorgverlener wordt verleent.

Het UZI-register besluit op basis van bovenstaande stukken of de zorgverlener kan worden ingeschreven als abonnee.

C. Gevolgen van een bevoegdheidsbeperking

Het UZI-register kan alleen de garantie zorgverlener afgeven als het gaat om een zorgverlener die het recht heeft de beschermde beroepstitel of opleidingstitel te voeren. Voor de beroepsbeoefenaren conform artikel 3 van de Wet BIG, geldt dat een inschrijving in het BIG-register een eerste vereiste is om in aanmerking te komen voor de garantie zorgverlener. Het kan voorkomen dat er sprake is van een beperking in de bevoegdheid. Met betrekking tot bevoegdheid om de beroepstitel te voeren in relatie tot de inschrijving in het BIG-register zijn de volgende situaties mogelijk:

1 De zorgverlener is ingeschreven in het BIG-register en is volledig bevoegd. Eventueel kan er sprake zijn van een voorwaardelijke maatregel. Door het voorwaardelijke karakter heeft deze maatregel geen effect op de bevoegdheid.
2 De zorgverlener is ingeschreven in het BIG-register en is gedeeltelijk onbevoegd. Dit betekent dat bepaalde handelingen niet mogen worden verricht. De zorgverlener mag nog wel de beroepstitel voeren.
3 De zorgverlener is ingeschreven in het BIG-register en is tijdelijk onbevoegd (dit is het geval bij een schorsing of voorlopige voorziening). De zorgverlener mag op het moment van de schorsing de beroepstitel niet voeren en heeft de bijbehorende rechten verloren.
4 De zorgverlener is doorgehaald in het BIG-register. De zorgverlener is onbevoegd.

Omdat inschrijving in het BIG-register een vereiste is om in aanmerking te komen voor de garantie zorgverlener, kunnen de geschetste situaties als volgt worden vertaald naar het UZI-register:

1 Als een zorgverlener volledig bevoegd is, kan het UZI-register zonder meer de garantie zorgverlener afgeven.
2 Als een zorgverlener gedeeltelijk onbevoegd is, mag de zorgverlener de beroepstitel blijven voeren. Het UZI-register zal dan in principe de garantie zorgverlener afgeven. Als de gedeeltelijke ontzegging gevolgen zou moeten hebben voor de garantie zorgverlener in de UZI-pas, zou dit bij de tuchtrechtelijke uitspraak vermeld moeten worden.
3 Hoewel er bij een schorsing of voorlopige voorziening situaties zijn die mogelijk in hoger beroep nog kunnen worden herroepen, is de zorgverlener op het moment van de schorsing of voorlopige voorziening onbevoegd. Het UZI-register kan daarom feitelijk de garantie zorgverlener niet afgeven.

4 Wanneer de inschrijving van de zorgverlener is doorgehaald, kan het UZI-register de garantie zorgverlener niet afgeven.

Relatie UZI-pas en bevoegdheid

De mate van bevoegd zijn, laat zich vertalen naar het al dan niet kunnen verkrijgen of behouden van een UZI-pas met garantie zorgverlener. In kolom (I) van onderstaande tabel is aangegeven wat de gevolgen zijn bij de aanvraag van een pas. In kolom (II) is aangegeven wat de gevolgen zijn als de zorgverlener al in het bezit is van een zorgverlenerpas.

Bevoegd?	(I) Aanvraag UZI-pas	(II) UZI-pas in bezit
Volledig bevoegd	pas toekennen	geen actie
Deels onbevoegd	pas toekennen	geen actie
Tijdelijk onbevoegd	aanvraag afwijzen	UZI-pas intrekken
Onbevoegd	aanvraag afwijzen	UZI-pas intrekken

Tabel 17 Relatie UZI-pas en bevoegdheid

Door de geschetste acties en handelwijze, kunnen het zorgveld en alle vertrouwende partijen er van uitgaan dat de houder van een zorgverlenerpas ook daadwerkelijk zorgverlener is.

Relatie abonnee en bevoegdheid

Een abonnee kan passen aanvragen voor zorgverleners, medewerkers (hulppersonen) en systemen. In deze passen is de relatie naar de abonnee opgenomen. Ook voor abonnees geldt dat het UZI-register de garantie zorgaanbieder afgeeft. Dat betekent dat een zorgverlener die (tijdelijk) onbevoegd is, geen abonnee kan worden bij het UZI-register.

Als deze zorgverlener al abonnee is, moeten alle voor deze abonnee uitgegeven passen worden ingetrokken. Dat wil zeggen dat ook de passen van andere zorgverleners onder de abonnee zullen worden ingetrokken. Bij een tijdelijke schorsing kan de abonnee na afloop van de schorsing opnieuw passen aanvragen.

De navolgende tabel toont in een oogopslag de gevolgen.

Bevoegd?	Aanvraag registratie abonnee	Bestaande abonnee
Volledig bevoegd	aanvraag abonnee toekennen	geen actie
Deels onbevoegd	aanvraag abonnee toekennen	geen actie
Tijdelijk onbevoegd	aanvraag abonnee afwijzen	alle passen abonnee intrekken
Onbevoegd	aanvraag abonnee afwijzen	alle passen abonnee intrekken

Tabel 18 Relatie abonnee en bevoegdheid

Als er sprake is van een schorsing als voorlopige voorziening, zal er meestal sprake zijn van een hoger beroep. Er bestaat in dat geval de kans dat de tijdelijke onbevoegdheid als onterecht wordt aangemerkt. In die situatie kan overwogen worden om nieuwe passen zonder kosten voor de abonnee uit te geven.

Bij onvoorwaardelijke schorsing van een zorgverlener die abonnee is, treedt een overgangstermijn van drie maanden in werking. Deze overgangstermijn houdt het volgende in:

- alle passen op naam (zorgverlenerpas en medewerkerpassen op naam) worden volgens de geldende regels ingetrokken.

- medewerkerpassen niet op naam en servercertificaten blijven actief.
- de abonneeregistratie blijft actief.
- onder deze abonnee mogen geen nieuwe UZI-middelen worden verstrekt.

Na de overgangstermijn worden de medewerkerpassen niet op naam en servercertificaten ingetrokken en wordt de abonneeregistratie doorgehaald. Het UZI-register verstrekt geen restitutie voor de eventueel resterende geldigheidsduur van de UZI-middelen.

D. Overgangstermijn 'uitstervend specialisme'
In de zorgverlenerpas is altijd een wettelijk beschermde beroepstitel of wettelijke beschermde opleidingstitel opgenomen. Als dit van toepassing is, bevat de zorgverlenerpas ook het wettelijk beschermde specialisme van de zorgverlener. Een specialisme kan alleen in de zorgverlenerpas worden opgenomen als dit in het BIG-register is geregistreerd. Als een specialisme in het BIG-register wordt uitgeschreven, moet een eventuele zorgverlenerpas waarop dit specialisme is vermeld worden ingetrokken. Deze pas mag niet meer worden gebruikt.
De betrokken zorgverlener kan uiteraard wel een nieuwe UZI-pas aanvragen zonder specialisme of met een ander, in het BIG-register vastgelegde, specialisme. Het UZI-register toetst periodiek bij het BIG-register of de registraties van beroepstitels en specialisme nog steeds actueel zijn. Op basis van de uitkomsten van deze toets neemt het UZI-register passende maatregelen. Waar nodig neemt het UZI-register het initiatief tot intrekking van passen.

Op dit beleid maakt het UZI-register een uitzondering als het gaat om een 'uitstervend' specialisme. Dit is een specialisme waarvoor geen herregistratie meer kan plaatsvinden. De registratie van het nieuwe specialisme vindt soms later plaats dan het uitschrijven van het oude specialisme. In die gevallen kan de zorgverlener onmogelijk tijdig een nieuwe UZI-pas met het correcte specialisme aanvragen.

Zodra het UZI-register een melding krijgt dat het specialisme in het BIG-register is uitgeschreven, zal het UZI-register pas na één kalendermaand over gaan tot intrekking van de pas. Het UZI-register informeert de abonnee hierover en adviseert abonnee en zorgverlener om deze maand te gebruiken om er voor te zorgen dat een eventueel nieuw specialisme in het BIG-register wordt geregistreerd en om een nieuwe pasaanvraag te doen.

Specialismen waarvoor deze werkwijze geldt:
- zenuw- en zielsziekten

Bijlage 3: Beroepstitels, opleidingstitels en specialismen

De bijlage bevat de beroepstitels, opleidingstitels en specialismen en de daarbij bijbehorende codes zoals deze door het UZI-register worden gehanteerd. De genoemde codes worden – na toetsing – in de certificaten opgenomen conform de beschrijving in paragraaf 7.1.5 van voorliggend CPS. De genoemde codes zijn vaste codes, de exacte tekst kan echter afwijken.

Artikel 3 Wet BIG

Beroepsgroepen die zijn opgenomen in het BIG-register zijn:

Aanspreektitel	Code
Apotheker	17
Arts	01
Fysiotherapeut	04
Gezondheidszorgpsycholoog	25
Psychotherapeut	16
Tandarts	02
Verloskundige	03
Verpleegkundige	30
Physician assistant	81

Specialismen bij art. 3 beroepen

Apotheker	Code
Ziekenhuisapotheker	060
Openbaar apotheker (Openbare Farmacie)	075

Arts	Code
Allergoloog (gesloten register)	002
Anesthesioloog	003
Apotheekhoudend huisarts	004
Arts klinische chemie (gesloten register)	020
Arts maatschappij en gezondheid	055
Arts v. maag-darm-leverziekten	013
Arts voor verstandelijk gehandicapten	056
Arts-microbioloog	024
Bedrijfsarts	008
Cardioloog	010
Cardiothoracaal chirurg	011
Chirurg	014
Dermatoloog	012
Gynaecoloog	046
Huisarts	015
Internist	016
Internist-allergoloog (gesloten register)	062
Jeugdarts	070
Keel- neus- oorarts	018
Kinderarts	019
Klinisch geneticus	021
Klinisch geriater	022
Longarts	023
Neurochirurg	025
Neuroloog	026

Arts	Code
Nucleair geneeskundige	030
Oogarts	031
Orthopedisch chirurg	032
Patholoog	033
Plastisch chirurg	034
Psychiater	035
Radioloog	039
Radiotherapeut	040
Reumatoloog	041
Revalidatiearts	042
Specialist ouderengeneeskunde	047
Spoedeisende hulp arts	071
Sportarts	074
Uroloog	045
Verzekeringsarts	048
Zenuwarts (gesloten register)	050

Gezondheidszorgpsycholoog	Code
Klinisch neuropsycholoog	063
Klinisch psycholoog	061

Tandarts	Code
Orthodontist	053
Kaakchirurg	054

Verpleegkundige	Code
Verpl. spec. acute zorg bij som. aandoeningen	066
Verpl. spec. chronische zorg bij som. aandoeningen	068
Verpl. spec. geestelijke gezondheidszorg	069
Verpl. spec. intensieve zorg bij som. aandoeningen	067
Verpl. spec. prev. zorg bij som. aandoeningen	065

Artikel 34 Wet BIG

Opleidingstitels conform artikel 34 Wet BIG zijn:

Aanspreektitel	Code
Apothekersassistent	83
Diëtist	89
Ergotherapeut	90
Huidtherapeut	88
Klinisch fysicus	84
Logopedist	91
Mondhygiënist	92
Oefentherapeut Cesar	94
Oefentherapeut Mensendieck	93
Optometrist	87
Orthoptist	95
Podotherapeut	96
Radiodiagnostisch laborant	97
Radiotherapeutisch laborant	98
Tandprotheticus	85
VIG-er[17]	86

17 Verzorgende in de individuele gezondheidszorg

Artikel 36a Wet BIG

Opleidingstitels conform artikel 36a Wet BIG zijn:

Aanspreektitel	Code
Klinisch technoloog	82
Bachelor medisch hulpverlener	80

Andere Zorg

Beroepsbeoefenaren die ‘zorg’ in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg verlenen.

Aanspreektitel	Code
Zorgverlener andere zorg	99