CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Certification Practice Statement (CPS)

ZOVAR

Versie 6.3

Datum	10-08-2022
Status	Definitief (ZV23.02)

Colofon

Organisatie	CIBG Bezoekadres: Rijnstraat 50 2515 XP Den Haag
Servicedesk	Postbus 16114 2500 BC Den Haag T 070 340 60 20 info@zovar.nl

Versie	6.3
Aantal pagina’s	67

Inhoud

Revisiehistorie

Versie	Datum	Status	Opmerking
1.0	01-10-2007	Definitief	
2.0	01-06-2008	Definitief	
3.0	01-09-2015	Definitief	
4.00	01/06/2017	Definitief	
5.0	04-01- 2018	Definitief	- Uitgifte onder de Private G1 hiërarchie van de Staat der Nederlanden.
5.1	10-09-2018	Definitief	- De Algemene verordening gegevensbescherming verwerkt. - Tijdsduur voor verwerking van verzoek tot intrekking aangepast (par 4.9.5) - Beperking aansprakelijkheid met betrekking tot de identificatie van de certificaatbeheerder toegevoegd (par 9.8) - Bewaartermijnen opgenomen (par. 5.5.2) Wijzigingsprocedure aangepast (par. 9.12)
5.2	01-11-2018	Definitief	- Diverse kleine wijzigingen (gehele CPS) - G2 hiërarchie toegevoegd. - Verwijzing naar hoofdstuk 3.2.2.4 van de Baseline Requirements opgenomen (par 3.2.3)
5.3	01-06-2019	Definitief	- Diverse kleine wijzigingen (gehele CPS) - Recht controle op compenserende maatregelen toegevoegd (par. 4.5.2.)
5.4	01-11-2019	Definitief	- Verwijzing naar hoofdstuk 3.2.2.4.2, 3.2.2.4.6 en 3.2.2.4.7 van de Baseline Requirements (3.2.3). - G2 hiërarchie verwijderd. - Diverse kleine wijzigingen (gehele CPS)
5.5	01-12-2019	Definitief	- Kantoortijden intrekkingen gewijzigd (par. 4.9.5).
5.6	01-04-2020	Definitief	- X-pact gewijzigd naar Cannock Outsourcing B.V. - Stopzetten ontvangstbevestigingen Servercertificaat. - Verwijzing naar RFC 2560 gewijzigd naar IETF RFC 6960. - Opmaak hoofdstuk 9 aangepast en tekstuele wijzigingen binnen het gehele CPS. - Verwijzing naar hoofdstuk 3.2.2.4.6 gewijzigd naar 3.2.2.4.18 van de Baseline Requirements (3.2.3).
5.7	01-05-2020	Definitief	- Contactgegevens gewijzigd [telefoonnummer]
5.8	01-11-2020	Definitief	- Ingetrokken certificaten blijven ook na verloop op CRL.
6.0	28-09-2021	Definitief	- Algemene actualisatie. - Subparagrafen nummering conform RFC3647. - Wijziging koeriersdienst Dynalogic → AMP Groep - Akkoord met voorwaarden CPS bij acceptatie

			certificaten expliciet opgenomen.
6.1	01-03-2022	Definitief	Specificering bewaartermijnen
6.2	02-06-2022	Definitief	Wijziging in aansprakelijkheid en garanties
6.3	10-08-2022	Definitief	Algemene actualisatie

Tabel 1 Versiehistorie CPS ZOVAR

Akkoord TSP Management
Versie: 6.3
Datum: 05-08-2022

1. Introductie

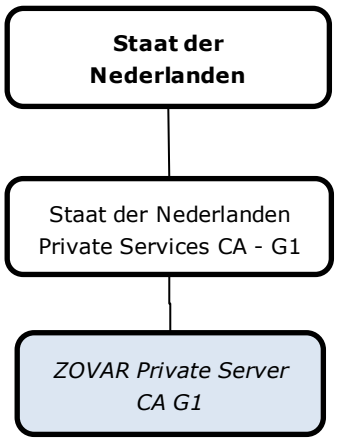
1.1 Overzicht

Om veilige communicatie en raadplegen van vertrouwelijke informatie in het zorgveld mogelijk te maken, worden drie domeinen te onderscheiden: de zorgconsumenten, de zorgverzekeraars en zorgkantoren, en de zorgaanbieders. Het Zorgverzekeraars identificatie en authenticatie register (kortweg ZOVAR) is het door de Minister van Volksgezondheid, Welzijn en Sport (VWS) aangewezen register van zorgverzekeraars zoals vermeld in artikel 14 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). ZOVAR is de certificatiedienstverlener (TSP)[1] die certificaten uitgeeft voor de unieke identificatie en authenticatie van zorgverzekeraars en zorgkantoren. ZOVAR geeft certificaten uit waarmee zorgverzekeraars en zorgkantoren het burgerservicenummer (BSN) bij de Sectorale Berichten Voorziening in de Zorg (SBV-Z) kunnen opvragen. In de servercertificaten van ZOVAR zijn de authenticiteit- en de vertrouwelijkheidfunctie gecombineerd.

1.1.1 CA model

ZOVAR geeft vanaf 4 januari 2018 certificaten uit onder de private Root CA G1 van PKIoverheid (Private G1). Met de invoering van G1 is het aantal niveaus in de CA-hiërarchie maximaal 3.

Onderstaande figuur geeft het CA model weer voor de generatie Private G1.



Figuur 1 CA-model Private G1 generatie

1.2 Doel, naam en identificatie

1.2.1 Doel CPS

Het CPS van ZOVAR 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

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

vertrouwen in de door ZOVAR 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 de facto standaard voor CPS'en.

1.2.2 Verhouding CP en CPS

ZOVAR geeft certificaten uit binnen het domein Overheid van de hiërarchie van de PKI voor de overheid (eerste en tweede generatie) en binnen het domein Organisatie (SHA-2 generatie). De eisen die worden gesteld aan uitgifte en gebruik van een ZOVAR certificaat zijn beschreven in het Programma van Eisen deel 3h Certificate Policy Server Certificaten – Domein Private Services.

1.2.3 Naam en verwijzingen

Formeel wordt dit document aangeduid als 'Certification Practice Statement ZOVAR (CPS)', kortweg CPS. Het CPS kan op papier worden opgevraagd bij het in paragraaf 1.5.2 opgenomen contactadres. De verwijzingen naar het CPS zijn opgenomen in de navolgende tabel.

CPS	**Omschrijving**
Naamgeving	Certification Practice Statement, ZOVAR vX.x
Link	https://www.zorgcsp.nl/cps/zovar.html
Object Identifier (OID)	2.16.528.1.1007.5.1.1

Tabel 2 Verwijzingen naar CPS ZOVAR

1.3 PKI Betrokken partijen

ZOVAR kent de navolgende betrokken partijen:

- uitvoerende organisatie van ZOVAR, inclusief leveranciers van producten en diensten;
- gebruikersgemeenschap bestaande uit:
  - abonnees;
  - certificaathouders;
  - 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 'ZOVAR'.

Clausules over aansprakelijkheid en garanties van de TSP zijn opgenomen in secties 9.6, 9.7 en 9.8.

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. Na intrekking publiceert de CA certificaatserienummers op de CRL's. Certificaten worden op een CRL gepubliceerd nadat de CA een bericht van intrekking van het certificaat heeft ontvangen van een hiertoe bevoegde persoon. Het CIBG heeft de rol van CA uitbesteed aan KPN B.V.

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 en het publiceren van certificaten. Het CIBG vervult de rol van RA. Het CIBG heeft het proces van vaststellen van de identiteit van de certificaathouder van een servercertificaat uitbesteed aan KPN B.V. AMP Groep stelt namens KPN B.V. de identiteit van de aanvrager/certificaatbeheerder vast.

1.3.3 Abonnees

De abonnee is de partij namens wie de certificaathouder (i.c. server/service) handelt bij gebruik van het certificaat. Een abonnee van ZOVAR is een zorgverzekeraar of zorgkantoor.

Met een zorgverzekeraar wordt bedoeld:

- Wlz-uitvoerder als bedoeld in artikel 1.1.1 van de Wet langdurige zorg;
- zorgverzekeraar als bedoeld in artikel 1 onder b van de Zorgverzekeringswet;
- verzekeringsonderneming als bedoeld in de richtlijn solvabiliteit II voor zover deze verzekeringen aanbiedt of uitvoert krachtens welke het verzekerde risico de behoefte aan zorg is waarop bij of krachtens de Wet langdurige zorg geen aanspraak bestaat en waarbij de verzekerde prestaties het bij of krachtens de Zorgverzekeringswet geregelde te boven gaat;

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

1.3.4 Vertrouwende partijen

Een vertrouwende partij is degene die handelt in vertrouwen op een certificaat.

De verplichtingen die van toepassing zijn op vertrouwende partijen zijn opgenomen in secties 4.5.2 en 9.6.4.

1.3.5 Andere deelnemers

De namens de zorgverzekeraar of zorgkantoor gemachtigd aanvrager van een servercertificaat heeft tevens de rol van certificaatbeheerder. Een certificaatbeheerder is een natuurlijke persoon die namens de abonnee handelingen uitvoert ten aanzien van het certificaat van de certificaathouder. De abonnee geeft de certificaatbeheerder opdracht de betreffende handelingen uit te voeren en legt dit vast in een bewijs van certificaatbeheer. Het CIBG garandeert als TSP 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/certificaatbeheerder. Voor servercertificaten zijn het authenticiteit- en vertrouwelijkheidcertificaat gecombineerd in één certificaat.

1.3.6 Dissemination Service (publicatiedienst)
ZOVAR 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.

1.4 Certificaatgebruik

1.4.1 Toegestaan certificaat gebruik
Het toepassingsgebied van door ZOVAR uitgegeven certificaten is beperkt tot de gebruikersgemeenschap zoals beschreven in paragraaf 1.3 deel 3h van het Programma van Eisen van de PKI voor de overheid.

ZOVAR geeft servercertificaten uit. In deze certificaten wordt de functie van een authenticiteitcertificaat en een vertrouwelijkheidcertificaat gecombineerd. Deze functies worden in Tabel 3: Toepassingsgebied servercertificaat nader toegelicht.

Toepassing	Doel
Authenticiteit en Vertrouwelijkheid	Dit certificaat wordt gebruikt voor het beveiligen van communicatie tussen machines

Tabel 3 Toepassingsgebied servercertificaat

1.4.2 Niet toegestaan certificaat gebruik
Certificaten worden uitgegeven voor het aangegeven doel. Er zijn geen verdere beperkingen aan het gebruik van de certificaten.

1.5 Beleidsadministratie

1.5.1 Organisatie die het document beheert
Het CIBG beheert het document.

1.5.2 Contactgegevens
Informatie over dit CPS of de dienstverlening van ZOVAR kan worden verkregen via onderstaande contactgegevens. Commentaar op het voorliggend CPS kan worden gericht aan hetzelfde adres:

ZOVAR
Rijnstraat 50 Postbus 16114
2515 XP Den Haag 2500 BC Den Haag
Tel: 070 340 60 20
info@zovar.nl www.zovar.nl

Een vermoeden van inbreuk op de private sleutel, misbruik van certificaten of andere vormen van fraude, compromitteren, misbruik, ongepast gedrag of enige andere kwestie met betrekking tot certificaten kan worden gemeld per e-mail via info@zovar.nl

1.5.3 Persoon die CPS-geschiktheid voor het beleid bepaalt
Het bepalen van de geschiktheid van het CPS beleid is onderdeel van de CPS goedkeuringsprocedure en wordt getoetst door een onafhankelijke auditor.

1.5.4 CPS Goedkeuringsprocedure
Het CIBG heeft het recht het CPS te wijzigen of aan te vullen. Wijzigingen gelden vanaf het moment dat het nieuwe CPS ingaat en wordt gepubliceerd op de website www.zorgcsp.nl. Het TSP management is verantwoordelijk voor een juiste navolging van de procedure zoals beschreven in paragraaf 9.12 en voor de uiteindelijke goedkeuring van het CPS conform deze procedure.

1.6 Definities en afkortingen

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

2. Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

ZOVAR 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 certificeringsinformatie

ZOVAR publiceert TSP informatie op www.zovar.nl en www.zorgcsp.nl. Deze locatie biedt onder meer toegang tot de volgende documenten en diensten:

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

2.3 Frequentie van publicatie

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

2.4 Toegangscontrole tot elektronische opslagplaatsen

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 aanvrager/certificaatbeheerder plaatsvindt tijdens de initiële registratieprocedure en welke criteria ZOVAR stelt ten aanzien van de naamgeving.

3.1.1 Soorten naamformaten

In het servercertificaat is de benaming van de certificaathouder opgenomen. Dit veld is opgebouwd uit (X.500) attributen en als volgt gevuld:

Attribuut	**Server**
Country (C)	'NL'
Organization (O)	Naam abonnee
OrganizationalUnit (OU)	Afdeling (optioneel)
CommonName (CN)	Systeemnaam
SerialNumber	<UZOVI-nummer><ZOVAR-nummer>

Tabel 4 Benaming certificaathouder (subject.DistinguishedName)

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 abonnees

ZOVAR staat het gebruik van pseudoniemen in abonneeregistratie of in certificaataanvragen niet toe.

3.1.4 Richtlijnen voor het interpreteren van de diverse naamvormen

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

- Naam abonnee bevat de naam zoals deze tijdens de registratie in het Handelsregister van de Kamer van Koophandel voorkwam.
- Afdeling bevat de door de abonnee opgegeven afdelingsnaam. Deze wordt door ZOVAR niet getoetst.
- Systeemnaam bevat bijvoorbeeld de fully qualified domainname (fqdn) van het systeem.

Alle namen worden in principe exact overgenomen uit de overlegde identificatiedocumenten. Het kan echter zijn dat in de naamgegevens bijzondere tekens voorkomen die geen deel uitmaken van de standaard tekenset conform ISO8859-1 (Latin-1) . Als in de naam tekens voorkomen die geen deel uitmaken van deze tekenset, zal ZOVAR een transitie uitvoeren.

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

3.1.5 Uniciteit van namen

ZOVAR 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 ZOVAR-nummer dat voorafgegaan door het UZOVI-nummer is opgenomen in het subject.serialNumber.

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 zorgverzekeraar of zorgkantoor zoals genoemd in het gewaarmerkte uittreksel uit het Handelsregister van de Kamer van Koophandel wordt overgenomen bij registratie en gebruikt in de certificaten.

Aanvragers/certificaatbeheerders van certificaten dragen de volledige verantwoordelijkheid voor eventuele juridische gevolgen van het gebruik van de door hen opgegeven naam. ZOVAR 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. ZOVAR behoudt zich het recht voor om de aanvraag te weigeren of de aangevraagde naam aan te passen als deze in strijd zou kunnen zijn met het merkenrecht.

3.2 Initiële identiteitsvalidatie

3.2.1 Methode om het bezit van een private sleutel te bewijzen.
De sleutelparen worden 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 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, voervoegsels geboortenaam, geboortenaam, voorvoegsels achternaam en achternaam) en contactgegevens van de wettelijk vertegenwoordiger van de organisatie;
  - de volledige naam en contactgegevens van de medewerker of medewerkers die namens de organisatie certificaten mogen aanvragen en intrekken (de gemachtigde aanvrager);
  - het UZOVI-nummer.
- 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 identiteitsbewijs moeten alle voornamen voluit zijn vermeld. ZOVAR archiveert de kopieën van de overlegde identificatiedocumenten.
- Bewijs dat de naam van de organisatie actueel en correct is. Dit bewijs heeft de vorm van:
  - het registratienummer waaronder de organisatie 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 organisatie is geregistreerd in het Handelsregister van de Kamer van Koophandel en waaruit blijkt wie bevoegd is om de organisatie te vertegenwoordigen;
  - Indien de organisatie niet staat ingeschreven bij de Kamer van Koophandel kan een afschrift van de benoeming van de wettelijk vertegenwoordiger worden overgelegd.

Organisaties welke in het bezit zijn van een door de Nederlandsche Bank verleende vergunning behoren tot het domein van ZOVAR. Deze organisaties hoeven geen bewijsstukken te overleggen.
ZOVAR controleert de overlegde documenten en gegevens op echtheid, volledigheid en juistheid. ZOVAR controleert of een opgegeven UZOVI-nummer overeenkomt met het UZOVI-nummer in de registratie van Vektis. ZOVAR 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 de identiteitsvaststelling in het kader van de uitgifte van een servercertificaat.

Een aanvraag van certificaten dient te worden gedaan door (een gemachtigd aanvrager namens) de abonnee die tevens de rol van certificaatbeheerder heeft. Hierbij dient het volgende te worden overlegd:

- 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 van de abonnee;
  - de naam van het systeem of de server waarvoor certificaten worden aangevraagd.
- 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. ZOVAR toetst of de abonnee eigenaar is of gebruik mag maken van de domeinnaam. De door ZOVAR gebruikte toetsingsmethoden staan beschreven in hoofdstuk 3.2.2.4.2, 3.2.2.4.18 en 3.2.2.4.7 van de Baseline Requirements.
- 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 ZOVAR-servercertificaat wordt opgenomen. Het PKCS#10 bestand moet via een upload functionaliteit in het aanvraagformulier worden toegevoegd aan de aanvraag.

In alle gevallen controleert ZOVAR de overlegde documenten op echtheid, volledigheid en juistheid. ZOVAR controleert aan de hand van de overlegde documenten of de aanvrager daadwerkelijk gemachtigd is de certificaten aan te vragen. ZOVAR controleert 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. ZOVAR stelt de abonnee op de hoogte van de uitgifte van een certificaat of de afwijzing van de certificaataanvraag. Als de

certificaataanvraag wordt afgewezen, wordt de reden van afwijzing vermeld.

3.2.4 Niet geverifieerde abonnee gegevens
ZOVAR verifieert de naam van de abonnee aan de hand van erkende documenten (zie paragraaf 3.2.2 en 3.2.3).

ZOVAR verifieert alle gegevens die worden opgenomen in het certificaat, met uitzondering van het optionele veld 'afdeling'. Het veld 'afdeling' bevat optioneel de door de abonnee opgegeven afdelingsnaam. Deze wordt door ZOVAR niet getoetst. Gegevens die alleen voor correspondentiedoeleinden worden vastgelegd, zoals correspondentienaam en telefoonnummers worden niet geverifieerd. Gegevens die niet worden geverifieerd, neemt ZOVAR over uit het door een gemachtigde aanvrager namens de abonnee ondertekend aanvraagformulier.

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. ZOVAR controleert de authenticiteit van deze aanvraag van de wettelijk vertegenwoordiger. ZOVAR archiveert dit bewijs.

Alleen een wettelijk vertegenwoordiger kan aangeven wie namens de abonnee certificaten mag aanvragen. De wijze van authenticatie van de wettelijk vertegenwoordiger is beschreven in paragraaf 3.2.2. Bij een servercertificaataanvraag controleert ZOVAR aan de hand van een kopie van een identiteitsbewijs of de aanvraag is ondertekend door een geautoriseerd aanvrager.

3.2.6 Criteria voor interoperabiliteit
Geen nadere bepaling.

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

3.3.1 Identificatie en authenticatie voor routinematige vernieuwing.
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 vernieuwingsverzoek wordt altijd een nieuw sleutelpaar gegenereerd.
Voor vernieuwing van het certificaat kan gebruik gemaakt worden van een aanvraagformulier voor certificaatvernieuwing. Deze aanvraagformulieren worden door ZOVAR tijdig samen met de vernieuwingsbrief toegezonden. Alleen originele, door ZOVAR toegezonden, aanvraagformulieren voor certificaatvernieuwing worden in behandeling genomen. De vernieuwingsbrief en het aanvraagformulier wordt maximaal 3 maanden voor de verloopdatum toegezonden. 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 Identificatie en authenticatie na intrekking van het certificaat
Het vernieuwen van sleutels na intrekking van het certificaat vindt plaats conform een eerste aanvraag. Bij de uitvoering van een vernieuwingsverzoek wordt altijd een nieuw sleutelpaar gegenereerd. Zie de procedure in sectie 3.3.1.

3.4 Identificatie en authenticatie bij verzoeken tot intrekking

De wettelijk vertegenwoordiger of een gemachtigd aanvrager kan namens de abonnee verzoeken tot intrekking indienen. Verzoeken tot intrekking van

certificaten kunnen elektronisch worden gedaan, per e-mail of per post. Het telefonisch verzoeken tot het intrekken van een servercertificaat is niet mogelijk [2].

Bij elektronisch verzoek tot intrekking vindt identificatie en authenticatie plaats op basis van een nummer en intrekkingscode. Het nummer en de intrekkingscode wordt bij uitgifte van het certificaat schriftelijk ter beschikking gesteld aan de abonnee.

Bij verzoek tot intrekking via **niet-elektronisch ondertekende e-mail of per post** vindt identificatie en authenticatie plaats op basis van een door de tot intrekking bevoegde persoon ondertekend verzoek. ZOVAR 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 ZOVAR het intrekkingsverzoek uit.
- Indien de handtekening niet overeenkomt, neemt ZOVAR telefonisch contact op met de abonnee via de bij ZOVAR geregistreerde contactgegevens. De aanvrager wordt hierbij verzocht om de handtekening conform het bij ZOVAR gearchiveerde WID te zetten. Als de handtekening op het WID is gewijzigd wordt de aanvrager verzocht een geldige kopie van het WID aan ZOVAR toe te sturen. Na herhaalde controle van de handtekening voert ZOVAR het intrekkingsverzoek uit. ZOVAR archiveert de nieuwe kopie van het WID.

Bij verzoek tot intrekking via **elektronische ondertekende e-mail** geldt als eis dat de e-mail is ondertekend door de tot intrekking bevoegde persoon met een gekwalificeerd onweerlegbaarheidcertificaat (zoals op een PKI overheidspas).

2 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 ZOVAR telefonische intrekking niet aan.

4. Operationele eisen certificaatlevenscyclus

4.1 Certificaat aanvraag

4.1.1 Wie kan een certificaataanvraag indienen
Aanvragen voor certificaten kunnen alleen worden gedaan door een aanvrager en wettelijke vertegenwoordigers. Deze aanvragers zijn door de abonnee gemachtigd om aanvragen te doen.

4.1.2 Inschrijvingsproces en verantwoordelijkheden
Aanvragen worden altijd schriftelijk gedaan. PKCS#10 bestanden kunnen alleen via de website of via elektronisch ondertekende mail worden verstuurd.

Voordat certificaten kunnen worden aangevraagd, dient de abonnee geregistreerd te worden bij ZOVAR. 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 ZOVAR invullen of kan deze aanvragen bij ZOVAR. De abonnee neemt voor het invullen van het aanvraagformulier kennis van alle toepasbare voorwaarden in het CPS. ZOVAR neemt eventuele onvolledige aanvragen niet in behandeling.
- ZOVAR voert de in paragraaf 3.2 aangegeven controles uit en stelt de abonnee op de hoogte van het resultaat. Wanneer ZOVAR schriftelijk aan de abonnee kenbaar heeft gemaakt dat hij niet geregistreerd kan worden, heeft de abonnee zes weken de tijd om een bezwaarschrift in te dienen.

4.2 Werkwijze met betrekking tot het aanvragen van certificaten

Een abonnee kan na registratie servercertificaten aanvragen. Hiervoor worden de volgende stappen doorlopen:

- De aanvrager overlegt een volledig ingevuld en ondertekend aanvraagformulier inclusief de in paragraaf 3.2.3 aangegeven documenten. De aanvrager kan formulieren verkrijgen via de website (www.zovar.nl). De aanvrager neemt voor het invullen van het aanvraagformulier kennis van alle toepasbare voorwaarden in het CPS. ZOVAR neemt eventuele onvolledige aanvragen niet in behandeling.
- ZOVAR archiveert de overlegde documenten voor eventuele bewijsvoering bij reconstructie conform de vigerende wet- en regelgeving.

Het annuleren van een aanvraag is in beginsel niet mogelijk. Uitzonderingen hierop zijn mogelijk in uitzonderlijke gevallen, 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 ZOVAR.

ZOVAR controleert geen Certification Authority Authorization DNS gegevens ten behoeve van eventuele 'certificate pinning' door de abonnee.

4.2.1 Uitvoering identificatie en authenticatie functies
ZOVAR voert de controles uit zoals beschreven in paragraaf 3.2 en paragraaf 4.3.

4.2.2 Goedkeuring of afwijzing van certificaataanvragen
ZOVAR voert de in paragraaf 3.2 aangegeven controles uit en stelt de abonnee op de hoogte van de uitgifte van het certificaat of de afwijzing van de aanvraag. Als de aanvraag wordt afgewezen, wordt de reden van afwijzing vermeld en heeft de

abonnee zes weken de tijd om een bezwaarschrift in te dienen.

4.2.3 Tijd om certificaataanvragen te verwerken
ZOVAR hanteert voor de maximale doorlooptijd vanaf ontvangst van de complete aanvraag tot aan het beschikbaar zijn van het ZOVAR-servercertificaat een termijn van maximaal acht weken. In geval van extreme drukte kan ZOVAR hiervan afwijken. Informatie hierover zal op de website www.zovar.nl verstrekt worden.

4.3 Uitgifte van certificaten

4.3.1 CA acties tijdens de uitgifte van certificaten
Servercertificaat
De uitgifte van een servercertificaat kent twee varianten. Beide worden toegelicht.

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

- De aanvrager ondertekent het PDF-aanvraagformulier met een gekwalificeerd onweerlegbaarheidcertificaat (zoals op de UZI-pas voor zorgverleners en medewerkers op naam). Óf;
- De aanvrager stuurt ZOVAR een e-mail met daarin het volledig ingevulde aanvraagformulier. De aanvrager ondertekent deze e-mail met een gekwalificeerd onweerlegbaarheidcertificaat (zoals op de UZI-pas voor zorgverleners en medewerkers op naam).
- De medewerker van het ZOVAR 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.

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

- De aanvrager dient persoonlijk te verschijnen bij het opgegeven adres in Nederland. De identiteitsvaststelling kan enkel binnen Nederland plaatsvinden. De aanvrager overlegt een geldig identificatiedocument waarop de eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing)en de volledige geboortenaam, evenals de geboortedatum en -plaats staan vermeld. Als identificatiedocument gelden de bij artikel 1 van de Wet op de identificatieplicht (WID) aangewezen geldige documenten. ZOVAR is verplicht een kopie van het document waarmee de identiteit wordt aangetoond te archiveren. De gegevens op de kopie die niet relevant zijn voor ZOVAR worden afgeschermd met behulp van automatische herkenningsoftware.
- Het fysiek vaststellen van de identiteit van de aanvrager en het maken van de kopie worden in opdracht van ZOVAR uitgevoerd door koeriersbedrijf AMP Groep. AMP Groep is hiervoor volledig gecertificeerd (conform ETSI EN 319411-1).
- De aanvrager ondertekent het bewijs van identiteitsvaststelling. De aanvrager gaat hierbij akkoord met de voorwaarden zoals gesteld in dit CPS, zie 4.4. Na een succesvolle identiteitsvaststelling ontvangt de aanvrager een bevestiging per e-mail van AMP Groep.
- Nadat het ondertekende bewijs van identiteitsvaststelling is verwerkt bij het ZOVAR wordt opdracht gegeven tot productie van het servercertificaat.

4.3.2 Kennisgeving aan de abonnee door de CA van de afgifte van een certificaat
Nadat het certificaat is geproduceerd, verstuurt ZOVAR het certificaat per e-mail naar de aanvrager. Daarnaast verstuurt ZOVAR een intrekkingscode naar het correspondentieadres van de abonnee ter attentie van de aanvrager.

4.4 Acceptatie van certificaten

De voorwaarden voor het gebruik van certificaten van ZOVAR staan vermeld in onderhavig CPS.

4.4.1 Gedrag dat certificaatacceptatie vormt

De certificaatbeheerder dient het certificaat op inhoud en volledigheid te controleren alvorens deze te gebruiken. Door het in gebruik nemen van het certificaat 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. Zie ook paragraaf 9.1.10.

4.4.2 Publicatie van het certificaat door de CA

Publicatie van de certificaten vindt plaats in de directory dienst direct na ondertekening van het certificaat door de CA gedurende het productieproces. Abonnee en pashouder/certificaathouder gaan akkoord met publicatie van de publieke certificaten en de daarin opgenomen informatie, zie hoofdstuk 7 en paragraaf 9.1.10.

4.4.3 Kennisgeving van de afgifte van certificaten door de CA aan andere entiteiten

Geen nadere bepaling.

4.5 Sleutelpaar en certificaatgebruik

4.5.1 Private sleutel en certificaatgebruik abonnee

Verplichtingen van abonnee en certificaathouder

- De abonnee is verplicht ZOVAR onmiddellijk op de hoogte te brengen en de certificaten in te trekken als zich een onregelmatigheid voordoet zoals aangegeven in paragraaf 4.9.1.
- De abonnee en de certificaathouder zijn verplicht om op aanwijzing van ZOVAR het gebruik van de certificaten en de bijbehorende private sleutels te staken. ZOVAR kan een dergelijke aanwijzing geven in het geval dat een CA-sleutel is gecompromitteerd.
- 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 dat alle aangeleverde gegevens, en daarmee de in het certificaat opgenomen gegevens, juist en volledig zijn. Dit betreft de gegevens gerelateerd aan de abonneeregistratie, de certificaataanvraag en overige gegevens. De abonnee dient ervoor te zorgen dat het sleutelmateriaal uitsluitend gegenereerd wordt in een veilig middel dat voldoet aan EAL 4+ of aan gelijkwaardige beveiligingscriteria.
- 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[3].
- De abonnee is verplicht de activeringsgegevens, die worden gebruikt om toegang te krijgen tot de private sleutel 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 een van de FQDN's in dit servercertificaat.
- De abonnee bevestigt dat CIBG gerechtigd is om het certificaat in te trekken indien de abonnee de toepasselijke voorwaarden schendt1F[4] 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 ZOVAR bevestigt dat het ZOVAR gerechtigd is om persoonsgegevens, waaronder naam, adres, e-mail en telefoonnummer aan Cannock Outsourcing B.V. en AMP Groep te verstrekken.
- Voorgaande verplichtingen voor de abonnee zullen voor zover zij als te onbepaald kunnen worden aangemerkt, nader worden uitgewerkt in richtlijnen van ZOVAR en/of nadere regelgeving.

4.5.2 Vertrouwende partij, openbare sleutel en certificaatgebruik

De verplichtingen van de vertrouwende partij zijn van toepassing wanneer er vertrouwd wordt op een certificaat uitgegeven door ZOVAR. De vertrouwende partij is verplicht om:
- per individueel geval zelfstandig te beoordelen of het gerechtvaardigd 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 server of service authenticeren, wat uitdrukkelijk geen oordeel inhoudt over de inhoud van de gegevens.

4.6 Vernieuwen van certificaten

Als na het (dreigend) verstrijken van de geldigheidsduur of na het intrekken een ZOVAR-servercertificaat 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.

Sleutels van certificaathouders zullen niet opnieuw worden gebruikt na het

3 ZOVAR heeft het recht om de compenserende maatregelen te controleren

4 De voorwaarden voor de abonnees zijn opgenomen in CPS secties 4.5.1 en 9.6.2.

verstrijken van de geldigheidsduur of na het intrekken van de bijbehorende certificaten. Met het vernieuwen van certificaten wordt ook het sleutelpaar vernieuwd.

4.6.1 Omstandigheid voor certificaatvernieuwing
Geen nadere bepaling.

4.6.2 Wie kan verlenging aanvragen
Geen nadere bepaling.

4.6.3 Het verwerken van aanvragen voor een vernieuwing van een certificaat
Geen nadere bepaling.

4.6.4 Kennisgeving van nieuwe certificaatuitgifte aan abonnee
Geen nadere bepaling.

4.6.5 Gedrag dat de aanvaarding van een verlengingscertificaat inhoudt
Geen nadere bepaling.

4.6.6 Publicatie van het verlengingscertificaat door de CA
Geen nadere bepaling.

4.6.7 Kennisgeving van de afgifte van certificaten door de CA aan andere entiteiten
Geen nadere bepaling.

4.7 Re-Key van certificaten

Als na het (dreigend) verstrijken van de geldigheidsduur of na het intrekken nieuwe servercertificaten worden 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.

4.7.1 Omstandigheid voor het opnieuw sleutelen van certificaten
Geen nadere bepaling.

4.7.2 Wie kan certificering van een nieuwe openbare sleutel aanvragen
Geen nadere bepaling.

4.7.3 Aanvragen voor het opnieuw sleutelen van certificaten verwerken
Geen nadere bepaling.

4.7.4 Kennisgeving van nieuwe certificaatuitgifte aan abonnee
Geen nadere bepaling.

4.7.5 Gedrag dat de aanvaarding van een opnieuw gesleuteld certificaat vormt
Geen nadere bepaling.

4.7.6 Publicatie van het opnieuw gesleutelde certificaat door de CA
Geen nadere bepaling.

4.7.7 Kennisgeving van de afgifte van certificaten door de CA aan andere entiteiten
Geen nadere bepaling.

4.8 Aanpassing van certificaten

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

4.8.1 Omstandigheid voor certificaatwijziging
Geen nadere bepaling.

4.8.2 Wie kan certificaatwijziging aanvragen
Geen nadere bepaling.

4.8.3 Aanvragen voor certificaatwijzigingen verwerken
Geen nadere bepaling.

4.8.4 Kennisgeving van nieuwe certificaatuitgifte aan abonnee
Geen nadere bepaling.

4.8.5 Gedrag dat de aanvaarding van een gewijzigd certificaat inhoudt
Geen nadere bepaling.

4.8.6 Publicatie van het gewijzigde certificaat door de CA
Geen nadere bepaling.

4.8.7 Kennisgeving van de afgifte van certificaten door de CA aan andere entiteiten
Geen nadere bepaling.

4.9 Intrekking en opschorting van certificaten

Verzoeken tot het intrekken van certificaten kunnen worden ingediend zoals hierna beschreven. ZOVAR zorgt ervoor dat datum en tijdstip van intrekking van certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door ZOVAR vastgestelde tijdstip als moment van intrekking. Als een certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

ZOVAR staat (tijdelijke) opschorting van certificaten niet toe.

4.9.1 Omstandigheden die leiden tot intrekking
De abonnee is verplicht een verzoek tot intrekking in te dienen bij ZOVAR en het gebruik van het certificaat te stoppen in de volgende omstandigheden:

- geconstateerd of vermoeden van misbruik of compromittatie;
- beëindiging bestaan abonnee;
- onjuistheden in of wijziging van de gegevens die op de certificaten vermeld staan;
- systeem / server niet meer in gebruik;
- toestemming om de domeinnaam te gebruiken is ingetrokken.

Intrekking op initiatief van ZOVAR vindt plaats in de volgende omstandigheden:

- Alle certificaten van een abonnee kunnen worden ingetrokken als de abonnee zich niet houdt aan de verplichtingen in het CPS[5].
- Alle certificaten van een abonnee worden ingetrokken als deze door De Nederlandsche Bank niet meer wordt aangemerkt als zorgverzekeraar of door het Ministerie van VWS niet meer wordt aangemerkt als zorgkantoor.

- Een servercertificaat wordt ingetrokken als de eigenaar van de domeinnaam aan

5 De voorwaarden voor de abonnees zijn opgenomen in CPS secties 4.5.1 en 9.6.2.

ZOVAR meldt dat de toestemming tot gebruik van de domeinnaam wordt ingetrokken.
- Een of meer certificaten van een abonnee worden ingetrokken als ZOVAR constateert in de gegevens die zijn opgenomen in het certificaat, bijvoorbeeld door een naamswijziging.
- Certificaten van een abonnee kunnen 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 brengt voor abonnees, vertrouwende partijen en derden (bijvoorbeeld browserpartijen).
- Een servercertificaat wordt ingetrokken indien de factuur niet binnen de gestelde termijn is voldaan[6].

De beweegreden voor elke intrekking geïnitieerd door ZOVAR wordt gedocumenteerd, gearchiveerd en getekend door het TSP management.

4.9.2 Wie mag verzoek tot intrekking indienen

Een verzoek tot intrekking van certificaten mag worden ingediend door:
- een geautoriseerde aanvrager namens de abonnee in de rol van certificaatbeheerder;
- de wettelijk vertegenwoordiger van de abonnee
- de curator die optreedt wanneer de abonnee zelf niet langer bevoegd is rechtshandelingen met beoogd rechtsgevolg te verrichten
- Daarnaast is ZOVAR bevoegd om op eigen initiatief intrekkingen te verrichten.

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. ZOVAR zal een dergelijk geval de melding onderzoeken en zal indien nodig het certificaat intrekken.

4.9.3 Procedure voor verzoek tot intrekking

Verzoeken tot intrekking van certificaten kunnen door certificaatbeheerder, een daartoe bevoegde persoon van de abonnee of door de certificaathouder elektronisch worden gedaan, 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 ZOVAR (www.zovar.nl) dient te geschieden. Deze vorm van intrekking is vierentwintig uur per dag beschikbaar, zeven dagen per week beschikbaar.

Bij een **elektronisch** verzoek tot intrekking vult de aanvrager/certificaatbeheerder een pasnummer met de bijbehorende intrekkingscode in op de website (www.zorgcsp.nl). Als intrekkingscode en pasnummer correct zijn, wordt het certificaat ingetrokken. De aanvrager krijgt hiervan op de website een melding. Als de intrekkingscode en pasnummer niet correct zijn, wordt teruggemeld dat de intrekking niet wordt uitgevoerd. ZOVAR heeft maatregelen genomen om te voorkomen dat onbeperkt foutieve intrekkingsverzoeken kunnen worden gedaan.

Bij een verzoek tot intrekking **per niet-elektronisch ondertekende e-mail of per post** dient het volgende te worden overlegd:
- Een door de tot intrekking bevoegde persoon ondertekend verzoek tot intrekken met daarin:
  - de naam van de abonnee;

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

- de naam van de persoon die het verzoek tot intrekking doet;
- de aanduiding van het certificaat of de certificaten waarvoor het verzoek geldt.

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

Bij een verzoek tot 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 een PKI overheidspas).

ZOVAR controleert of de indiener van het intrekkingsverzoek bevoegd is de aanvraag te doen. Tevens controleert ZOVAR de identiteit van de indiener van het intrekkingsverzoek aan de hand van het overlegde identiteitsbewijs of een eerder gearchiveerde kopie van het identiteitsbewijs. Na uitvoering van de controles trekt ZOVAR de certificaten in en plaatst deze 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 abonnee gemeld.

4.9.4 Uitstel van verzoek tot intrekking

De certificaatbeheerder of de abonnee zijn verplicht om per direct en zonder vertraging een verzoek tot intrekking in te dienen in situaties zoals vermeld in paragraaf 4.9.1.

4.9.5 Tijdsduur voor verwerking van verzoek tot intrekking

Elektronische verzoeken worden direct online afgehandeld. ZOVAR adviseert partijen om gebruik te maken van de faciliteiten ten behoeve van elektronische intrekking op de website van ZOVAR. Deze faciliteiten zijn vierentwintig uur per dag en zeven dagen per week beschikbaar. Bij elektronische intrekking is de maximale vertraging tussen de ontvangst van het verzoek en de 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 tussen 7:30 en 16:00 uur is ontvangen. Verzoeken ontvangen ná 16:00 uur worden de eerstvolgende werkdag in behandeling genomen.

Indien de intrekking een spoedeisend belang heeft, dient dit elektronisch (24 uur per dag en zeven dagen per week m.b.v. de intrekcode) te geschieden.

4.9.6 Controlevoorwaarden vertrouwende partijen 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.

4.9.7 CRL-uitgiftefrequentie

De CRL-uitgiftefrequentie is elk uur en de CRL is 48 uur geldig. Ook in geval van systeemdefecten, service-activiteiten of andere factoren die buiten het bereik van ZOVAR liggen, zorgt ZOVAR er voor dat intrekkingsverzoeken die via de website 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 ZOVAR-certificaten een hogere actualiteit van de certificaatstatus vereisen, wordt dringend geadviseerd om gebruik te maken van de faciliteit voor online controle van de intrekkingsstatus (zie paragraaf 4.9.9).

Ingetrokken certificaten blijven op de CRL staan, ook nadat de oorspronkelijke geldigheidsdatum is verstreken.

4.9.8 Tijd tussen generatie en publicatie

De CRL wordt direct na generatie gepubliceerd.

4.9.9 Online intrekking / statuscontrole

Naast de publicatie van CRL's biedt ZOVAR ook certificaat statusinformatie via de faciliteit Online Certificate Status Protocol (OCSP). De inrichting van OCSP is in overeenstemming met IETF RFC 6960. Op het moment dat een CA cetificaat de verloopdatum bereikt stopt de OCSP-dienst voor de betreffende CA.

OCSP validatie is een online validatie methode waarbij ZOVAR 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 ZOVAR. 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 intrekkingsstatus 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.

4.9.10 Vereisten online controle intrekkingsstatus

Deze dienst is onbeperkt toegankelijk voor alle vertrouwende partijen die de intrekking status van een door het ZOVAR uitgegeven certificaat willen valideren.

4.9.11 Andere beschikbare vormen van publicaties van intrekkingen

Geen nadere bepaling.

4.9.12 Speciale vereisten met betrekking tot gecompromitteerde sleutels

Intrekking van een domein of een TSP-certificaat zal worden overwogen als de ondertekeningssleutel die bij het certificaat hoort gecompromitteerd is of als vermoed wordt dat deze is gecompromitteerd. Indicatoren van inbreuk op de private sleutel kunnen zijn:

- diefstal of verlies van een apparaat met een private sleutel;
- Auditbevindingen die wijzen op een inbreuk op de private sleutel;
- CT-logboekbevindingen die duiden op ongeoorloofde ondertekening van certificaten;
- Incidenten die door derden aan CIBG zijn gemeld en die kunnen wijzen op gecompromitteerde sleutels.

4.9.13 Omstandigheden voor schorsing

ZOVAR staat de (tijdelijke) schorsing van certificaten niet toe.

4.9.14 Wie kan schorsing aanvragen

ZOVAR staat de (tijdelijke) schorsing van certificaten niet toe.

4.9.15 Procedure voor schorsingsverzoek

ZOVAR staat de (tijdelijke) schorsing van certificaten niet toe.

4.9.16 Beperkingen schorsingsperiode

ZOVAR staat de (tijdelijke) schorsing van certificaten niet toe.

4.10 Certificaat statusservice

4.10.1 Operationele kenmerken

ZOVAR geeft elk uur een nieuwe CRL uit. Met behulp van OCSP kan de actuele statusinformatie worden opgevraagd.

4.10.2 Beschikbaarheid van de service

In geval van verstoring van deze diensten, zorgt ZOVAR 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.

4.10.3 Optionele functies
Geen nadere bepaling.

4.11 Beëindiging abonnee relatie

De registratie als abonnee kent in beginsel geen einddatum. De registratie kan worden doorgehaald op verzoek van de abonnee dan wel indien de geregistreerde niet meer kan worden aangemerkt als zorgkantoor of zorgverzekeraar.

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

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

- de servercertificaten blijven actief,
- de abonneeregistratie blijft actief.

Na de overgangstermijn worden alle servercertificaten ingetrokken en wordt de abonneeregistratie doorgehaald.

4.12 Key escrow en recovery

ZOVAR ondersteunt geen key escrow en key recovery.

4.12.1 Key escrow and recovery beleid en praktijken
Geen nadere bepaling.

4.12.2 Session key encapsulation recovery beleid en praktijken
Geen nadere bepaling.

5. Facilitaire, beheers- en operationele maatregelen

5.1 Fysieke maatregelen

5.1.1 Locatie en constructie

De dienstverlening van ZOVAR vindt plaats vanuit verschillende locaties. De registratiewerkzaamheden worden verricht op de vestigingslocatie van het CIBG. De certificatie vindt plaats op het rekencentrum van de leverancier van CA-diensten De werkzaamheden met betrekking tot de mobiele identificatie van de certificaatbeheerder vinden plaats op locatie.

5.1.2 Fysieke toegang

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-, certificatie-, uitgifte en intrekking proces, 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 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.

ZOVAR 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 ZOVAR testen uit op basis van vooraf vastgestelde testplannen.

ZOVAR 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.

5.1.3 Stroom en airconditioning

Zie paragraaf 5.1.2

5.1.4 Blootstelling aan water

Zie paragraaf 5.1.2

5.1.5 Brandpreventie en –bescherming

Zie paragraaf 5.1.2

5.1.6 Mediaopslag

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.

5.1.7 Afvalverwijdering
CIBG personeel is verplicht om vertrouwelijke informatie weg te gooien in de daarvoor aangewezen afgesloten papierbakken of shredders. Voor de vernietiging van deze vertrouwelijke gegevens is een contract afgesloten met een datavernietigingsbedrijf.

5.1.8 Off-site backup
CIBG heeft maatregelen getroffen om de beschikbaarheid van bedrijfskritieke diensten te waarborgen. Deze maatregelen, alsmede de gehanteerde Recovery Point Objective en Recovery Time Objective staat beschreven in een continuiteïtsplan.

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.

5.2 Procedurele maatregelen

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. Al het personeel in vertrouwelijke functies is gescreend op het aanwezig zijn van tegengestelde belangen die de onpartijdigheid van de activiteiten van ZOVAR zouden kunnen beïnvloeden.

5.2.2 Aantal personen benodigd per taak
De dienstverlening van ZOVAR 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 functies
Geen nadere bepaling.

5.2.4 Functiescheiding
ZOVAR 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), TSP Manager(s), Systeem auditor(s), Chief Information Security Officer (CISO), systeembeheerder(s) en TSP operator(s).

5.3 Personele maatregelen

5.3.1 Vereisten inzake kwalificaties, ervaring en goedkeuring.
Alle bij de dienstverlening van ZOVAR 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 certificatie werkzaamheden zijn onderwerp van antecedentenonderzoek. ZOVAR vraagt van alle medewerkers die betrokken zijn bij registratie en identiteitsvaststelling een Verklaring omtrent Gedrag.

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

5.3.3 Trainingseisen

ZOVAR 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 en 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 bepaling.

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 ZOVAR 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

ZOVAR 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.

ZOVAR 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 met betrekking tot certificaat life cycle management worden voor een periode van tenminste zeven jaar bewaard en daarna verwijderd. De logbestanden met betrekking tot technische bedreigingen en risico's worden 24 maanden bewaard en daarna verwijderd

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 Back-upprocedures voor controlelogboeken
Geen nadere bepaling.

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

5.4.7 Kennisgeving van logging gebeurtenis
ZOVAR stelt een nader onderzoek in wanneer uit de logging kwaadwillende acties zijn af te leiden.

5.4.8 Kwetsbaarheidsanalyse

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

5.5 Archivering van documenten

5.5.1 Soorten gearchiveerde documenten

ZOVAR 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 en uittreksel uit het Handelsregister van de Kamer van Koophandel).
- Opslaglocatie van kopieën van aanvragen en identiteitsdocumenten.
- Informatie die relevant is voor de identificatie van een abonnee.
- Informatie betreffende de uitgevoerde controles.
- Correspondentie met betrekking tot registratieaanvraag of certificaataanvraag.
- 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 bezwaarschriften en correspondentie met betrekking tot klachten en bezwaarschriften.
- Schriftelijk ontvangen informatieverzoeken en overige correspondentie die gerelateerd is aan de Wet bescherming persoonsgegevens of de Wet openbaarheid van bestuur.

5.5.2 Bewaartermijn van het archief

Alle gearchiveerde gebeurtenissen worden conform hoofdstuk 10.4 van de selectielijst[7] 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

ZOVAR zorgt voor de integriteit en toegankelijkheid van de gearchiveerde gegevens. ZOVAR 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.

7 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

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

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 bepaling.

5.6 Vernieuwen sleutels na re-key CA

Als de CA een nieuw sleutelpaar in gebruik neemt worden de nieuwe CA certificaten beschikbaar gemaakt in de directory en op de website.

5.7 Aantasting en continuïteit

5.7.1 Procedures voor incident- en compromittatie afhandeling
ZOVAR heeft een calamiteitenplan opgesteld om, in geval van een calamiteit, de gevolgen hiervan te minimaliseren. In het Business Continuity Plan ZorgCSP zijn procedures en werkwijze rondom uitwijk van dienstverlening beschreven.

ZOVAR 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 ZOVAR neemt ZOVAR minimaal de volgende acties:

- ZOVAR stelt vertrouwende partijen, abonnees en certificaathouders hiervan zo spoedig mogelijk op de hoogte door de informatie te publiceren op https://www.zovar.nl.
- ZOVAR 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 ZOVAR de betrokken certificaten direct intrekken en publiceren op de toepasselijke CRL.
- ZOVAR stelt de Policy Authority van de PKI voor de overheid, NCSC , Certificerende Instantie en eventueel Autoriteit Persoonsgegevens onmiddellijk op de hoogte van de calamiteit.

Bij compromittatie van een van de door ZOVAR gebruikte algoritmen treedt ZOVAR in overleg met de Policy Authority van de PKI voor de overheid. In principe zal ZOVAR 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.

5.7.2 Computerbronnen, software en/of gegevens zijn beschadigd
Zie paragraaf 5.7.1

5.7.3 Entiteit private key compromise procedures
Zie paragraaf 5.7.1

5.7.4 Mogelijkheden voor bedrijfscontinuïteit na een ramp
Zie paragraaf 5.7.1

5.8 CA of RA beëindiging

In het geval ZOVAR de certificatiedienstverlening beëindigt, zal dit plaatsvinden conform een gecontroleerd proces zoals nader beschreven in het ZOVAR 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 KPN B.V. zal opdracht gegeven worden tot de vernietiging van het sleutelmateriaal op nader te bepalen datum. KPN B.V. zal ter bevestiging een procesverbaal aan CIBG overhandigen van de vernietiging.
- Aan Doc-Direkt zal opdracht gegeven worden tot vernietigen van dossiers. Conform Doc-Direkt PDC (zie Rijksportaal).

6. Technische beveiligingsmaatregelen

6.1 Genereren en installeren van sleutelparen

6.1.1 Genereren van sleutelparen
Bij het genereren van sleutelparen maakt ZOVAR gebruik van betrouwbare procedures in een beveiligde omgeving, die voldoet aan objectieve en internationaal erkende standaards. De sleutelgeneratie van de CA's van ZOVAR 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. Hierbij wordt gebruik gemaakt van het ondertekeningalgoritme 'SHA256RSA'.

Voor gebruikerscertificaten wordt de publieke sleutel door de abonnee aangeleverd aan de RA via een Public Key Certificate Signing request (PKCS#10).

6.1.2 Overdracht van private sleutels naar abonnee.
Er is geen sprake van overdracht van de private sleutel. Het certificaat en de gecertificeerde publieke sleutel worden na persoonlijk verschijnen van de certificaatbeheerder namens de abonnee per e-mail verstuurd naar een bij aanvraag opgegeven e-mailadres.

6.1.3 Overdracht van publieke sleutels naar de CA
Voor servercertificaten wordt het sleutelpaar gegenereerd door de abonnee. De publieke sleutels worden via beveiligde verbindingen in ondertekende berichten naar de CA verstuurd ter ondertekening.

6.1.4 Overdracht van de publieke sleutel van de TSP naar eindgebruikers
De publieke sleutel van de ZOVAR CA, is door de Domein CA van de PA getekend, waardoor tevens de integriteit en herkomst van de publieke sleutel wordt gewaarborgd. Deze publieke sleutels worden in de vorm van CA certificaten aan vertrouwende partijen beschikbaar gesteld via www.zorgcsp.nl.

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

6.1.6 Openbare sleutelparameters genereren en kwaliteitscontrole
ZOVAR genereert sleutels in HSM's die voldoen aan de FIPS 140-2 level 3 normering.

6.1.7 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 en cryptografische module-engineering beheersmaatregelen

6.2.1 Standaarden voor crytografische modulen en controles
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 ZOVAR zijn niet in één stuk leesbaar. Er wordt een back-up gemaakt van de private sleutels van de CA's van ZOVAR. 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
ZOVAR neemt geen private sleutels van certificaathouders in escrow.

6.2.4 Back-up van de private sleutels
ZOVAR maakt geen back up van de private sleutels van certificaathouders.

6.2.5 Archivering van private sleutels
ZOVAR archiveert geen private sleutels van certificaathouders.

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

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

6.2.8 Methode voor activeren private sleutels
Slechts door middel van een sleutelceremonie en de daarvoor noodzakelijk aanwezige functionarissen worden de private sleutels van de CA's van ZOVAR geactiveerd. ZOVAR zorgt voor een zorgvuldige procedure in een beveiligde omgeving.

6.2.9 Methode voor deactiveren private sleutels
In de gevallen door ZOVAR te bepalen zullen de private sleutels worden gedeactiveerd met inachtneming van de daarop van toepassing zijnde zorgvuldigheidsprocedures.

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 kunnen worden gebruikt. ZOVAR zorgt voor een adequate vernietiging waarbij wordt voorkomen dat het mogelijk is de vernietigde sleutels te herleiden uit de restanten.

6.2.11 Cryptografische modulebeoordeling
Toegepaste Hardware Security Modules binnen de systemen van ZOVAR 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.

6.3 Andere aspecten van sleutelpaar management

Alle aspecten van het sleutelmanagement worden door ZOVAR 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 ZOVAR voor tenminste zeven jaar na het verstrijken van de oorspronkelijke geldigheidsduur van een certificaat, in een fysiek veilige omgeving.

6.3.2 Operationele periodes van certificaten en gebruiksperioden voor sleutelparen

De volgende tabel geeft een overzicht van de geldigheidsduur van de sleutelparen en CA certificaten van de Private G1 hiërarchie

Certificaat	Geldig tot
Stamcertificaat	14 november 2028
Stamcertificaat	14 november 2028
CSP certificaten	12 november 2028

Tabel 5 levensduur certificaten Public G3 / Private G1 hiërarchie

Voor de gebruikerscertificaten, wordt een maximale geldigheidsduur van drie jaar na de productiedatum gehanteerd.

6.4 Activeringsgegevens

6.4.1 Generatie en installatie van activeringsgegevens

ZOVAR geeft alleen servercertificaten uit. De abonnee dient zelf passende maatregelen te nemen conform de verplichtingen in paragraaf 4.5.

6.4.2 Bescherming activeringsgegevens

Geen nadere bepaling.

6.4.3 Andere aspecten van activeringsgegevens

Geen nadere bepaling.

6.5 Beveiligingsmaatregelen computersystemen

6.5.1 Specifieke technische vereisten aan computerbeveiliging

In de registratiesystemen van ZOVAR zijn passende controles en beveiligingsmaatregelen opgenomen. Mede hierdoor is het onmogelijk dat een aanvraag door één medewerker van ZOVAR wordt afgehandeld.

ZOVAR treft adequate maatregelen om de beschikbaarheid, integriteit en exclusiviteit te waarborgen. Computersystemen worden op passende wijze beveiligd tegen ongeautoriseerde toegang en andere bedreigingen. ZOVAR beschikt over een informatie beveiligingsplan waarin de maatregelen zijn uitgewerkt. Met de leverancier worden de maatregelen uitgewerkt in service level agreements. Beheerwerkzaamheden worden gelogd.

6.5.2 Beheer en classificatie van middelen

ZOVAR classificeert de gebruikte middelen op basis van een risicoanalyse.

6.6 Beheersingsmaatregelen technische levenscyclus

6.6.1 Systeemontwikkelingcontroles
Voor de door het ZOVAR gebruikte systemen is door een onafhankelijke EDP auditor een auditverklaring afgegeven op basis van CEN TS 419 261:2015 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 Beveiligingsmanagementcontroles
ZOVAR 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 mogelijke 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 Maatregelen 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 ZOVAR zijn voorzien van stringente veiligheidsmaatregelen (actuele firewall, virusscanners, proxy). Onderdeel van deze maatregelen is een maandelijkse security scan en een (minimaal) jaarlijkse penetratietest.

6.8 Timestamping

Geen nadere bepaling.

7. Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofiel

Deze paragraaf geeft een overzicht van het certificaatprofiel van ZOVAR. Met name de velden die voor certificaathouders relevante gegevens bevatten, komen aan de orde.

Een X.509 certificaat bestaat uit een verzameling informatie objecten. Ieder object heeft een naam, en ieder object bestaat uit een aantal attributen. Een attribuut kan diverse zaken bevatten: sleutels, algoritmen, namen, etc. Een certificaatprofiel beschrijft welke objecten worden gebruikt en welke waarden de attributen van deze objecten kunnen bevatten.

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 Versie nummers

De certificaten van ZOVAR voldoen aan de X.509 v3 standaard en aan deel 3h van het Programma van Eisen van de PKI voor de Overheid, (zie www.logius.nl);

7.1.2 Certificaat extensies

Basis attributen

De certificaten van ZOVAR kennen de navolgende basis attributen voor zover deze niet worden in andere paragrafen zijn beschreven:

Veld	Waarde
Certificate.SerialNumber	Bevat het unieke serienummer van het certificaat
Validity	De geldigheidsperiode van het certificaat is ingesteld op drie jaar.

Tabel 6 Basisattributen certificaatprofielen

Standaard extensies

ZOVAR certificaten bevatten de navolgende standaard extensies:

Veld	Essentiel	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	Bevat de DigitalSignature en KeyEncipherment bits.
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 par. 7.1.6);

Veld	Essentiel	Waarde
		• Een link naar de CPS van ZOVAR (zie tabel 1); • 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 www.logius.nl'
AuthorityInfoAccess.accessMethod (OCSP)	Nee	In dit attribuut is de URL van de OCSP dienstverlening opgenomen: http://ocsp.zovar.nl.
AuthorityInfoAccess.accessMethod (CA Issuers)	Nee	In dit attribuut is de URL opgenomen naar CA certificaat van de uitgevende CA: - http://cert.pkioverheid.nl/ZOVAR_Private_Server_CA_G1.cer
ExtendedKeyUsage	Nee	In ZOVAR certificaten zijn de volgende ExtendedKeyUsages opgenomen: - ServerAuthenticatie - ClientAuthenticatie
SubjectAltName	Nee	In dit attribuut zijn in de subjectAltName.otherName diverse nummers opgenomen, zie onderstaande toelichting.
CrlDistributionPoints	Nee	Bevat de URI waar de CRL, kan worden opgehaald: http://www.csp.zovar.nl/cdp/zovar_private_server_ca_g1.crl

Tabel 7 Standaard extensies certificaatprofiel ZOVAR

Toelichting SubjectAltName.otherName
Deze paragraaf beschrijft hoe de subjectAltName.othername in de certificaten van ZOVAR 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 '-'.

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

CA	OID
TSP CA	2.16.528.1.1003.1.3.5.5.1
ZOVAR Server CA	2.16.528.1.1003.1.3.5.5.6

Tabel 8 <OID CA> productieomgeving SHA-2 generatie

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

<Subject ID> = <versie-nr>-<subject-nr>-<pastype>-<UZOVI-nr>-<erkenning>

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.
subject-nr	13NUM	<UZOVI-mmer><ZOVAR-nummer>	Een uniek nummer voor ZOVAR rvercertificaat.
pastype	1CHAR	De volgende codering wordt toegepast: 'V' :Servercertificaten	
UZOVI-nr	4NUM	UZOVI-nummer	Het Vektis UZOVI-nummer
erkenning	2CHAR	Type erkenning: 'ZV' : Zorgverzekeraar	De erkenning zal in eerste instantie altijd gevuld zijn met 'ZV' omdat alleen zorgverzekeraars abonnee kunnen worden van ZOVAR

Tabel 9 Velden <Subject ID> in SubjectAltName.otherName

Private extensies
Het ZOVAR certificaat bevat geen private extensies.

7.1.3 Cryptografische algoritem identificaties
De certificaten van het ZOVAR zijn ondertekend met het algoritme sha256WithRSAEncryption (Object Identifier 1.2.840.113549.1.1.11).
De certificaten bevatten een RSA sleutel van minimaal 2048 bits.

7.1.4 Naamvormen
Certificaten uitgegeven door ZOVAR bevatten de naam van de CA die het certificaat ondertekent (issuer) en van de certificaathouder (subject) zoals weergegeven in de volgende tabel.

Veld	Waarde
Issuer	Bevat de naam van de CA en wordt weergegeven door de attributen de attributen OrganizationName, organizationIdentifier, CommonName en CountryName. Deze hebben de volgende vaste waarden: **OrganizationName** 'CIBG' **organizationIdentifier** 'NTRNL-50000535' **CommonName** 'ZOVAR Private Server CA G1' **CountryName** 'NL' (volgens ISO 3166).
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: CountryName, CommonName, OrganizationName, StateOrProvinceName, LocalityName en SerialNumber. Deze attributen worden als volgt gevuld: **CommonName** naam van het systeem, , de zogenaamde qualified domainname (FQDN). **OrganizationName** naam van de abonnee. **OrganizationalUnitName** (optionele) afdeling van de

Veld	Waarde	
	server.	
	StateOrProvinceName	provincie van de abonnee.
	LocalityName	plaatsnaam van de abonnee
	CountryName	land van de abonnee (volgens ISO 3166).
	SerialNumber	het UZOVI-nummer direct gevolgd door het ZOVAR-nummer.

7.1.5 Naambeperkingen
Voor de namen in certificaten gelden de randvoorwaarden die voortvloeien uit RFC 5280, ETSI EN 319 411-1 en ETSI EN 319 411-2 en het Programma van Eisen PKIoverheid.

7.1.6 Certificeringsbeleid Object Identifier
Voor de Certificate Policies (CP) wordt verwezen naar https://www.logius.nl. Om de juiste CP te kunnen identificeren geeft de navolgende tabel de samenhang tussen de certificaten, de toepasselijke CP en de Object Identifier (OID) van de CP. De kolom OID CP bevat de Object Identifier die in de certificaten is opgenomen en die eenduidig verwijst naar het Certificeringsbeleid (CP) dat van toepassing is op het betreffende certificaat.

Type certificaat		**Toepasselijke CP**	**OID CP**
Naam	**Certificaat inctie)**		
Server ivate G1)	authenticiteit en trouwelijkheid	PvE deel 3h: Certificate Policy Server Certificaten Domein Private Services	2.16.528.1.1003.1.2.8.6

Tabel 10 Overzicht certificaten met OID van toepasselijke CP

7.1.7 Gebruik van de beleidsbeperkings extensie
Geen nadere bepaling.

7.1.8 Syntax en semantiek van beleidskwalificaties
Zoals is weergegeven in par. 7.1.2 bevat de certificaat extensie 'CertificatePolicies' twee Policy Qualifiers:
- Een link naar de CPS van ZOVAR (zie par. 1.2.3);
- een gebruikerstekst (UserNotice (zie par. 7.1.2)

7.1.9 Semantiek voor het verwerken van kritieke certificaatbeleid extensie
Geen nadere bepaling.

7.2 CRL profiel

Het CRL profiel is opgemaakt conform deel 3h van het Programma van Eisen van de PKI voor de overheid (zie www.logius.nl). Het profiel van de CRL voor de certificaten bevat een aantal attributen en extensies. Deze zijn in de navolgende subparagrafen beschreven.

7.2.1 Versie nummers
ZOVAR geeft CRL's uit volgens het X.509 versie 2 formaat.

7.2.2 CRL en CRL lijst-item extensies

De CRL voor certificaten van ZOVAR kent de navolgende attributen:

Veld	Waarde
Version	1 (X.509 versie 2)
signatureAlgorithm	sha-256 WithRSAEncryption
Issuer	Bevat de naam van de CA en wordt weergegeven door de attributen OrganizationName, CommonName, organizationIdentifier en CountryName. OrganizationName 'CIBG' organizationIdentifier 'NTRNL-50000535' CommonName 'ZOVAR Private Server CA G1' CountryName 'NL' (volgens ISO 3166)
thisUpdate	Datum/tijdstip van uitgifte en ondertekening van de CRL.
nextUpdate	Dit is de datum/tijdstip waarop de geldigheid van de CRL eindigt. De waarde is 'thisUpdate' plus 48 uur. ZOVAR publiceert elk uur een update van de CRL.
revokedCertificates	Lijst van ingetrokken certificaten per lijst-item bestaande uit: - Certificaatserienummer - datum/tijdstip van intrekking

Tabel 11 Attributen CRL

De CRL voor certificaten van ZOVAR kent 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
ExpiredCertsOnCRL	Nee	Geeft aan dat ingetrokken certificaten na het verlopen van het certificaat op de CRL blijven staan conform ETSI EN 319 411-2: CSS-6.3.10-05

Tabel 12 Extensies CRL

7.3 OCSP profiel

7.3.1 Versie nummers

De OCSP dienst van ZOVAR is van het type 'pkix-basic', voldoet aan RFC 6960 en heeft verder de volgende specifieke kenmerken:

- De OCSP dienst maakt geen gebruik van pre-computed responses.
- Alle OCSP communicatie voor certificaten van ZOVAR verloopt via http://ocsp.zovar.nl
- Iedere CA van het ZOVAR die gebruikercertificaten uitgeeft, heeft een eigen OCSP responder die de OCSP responses ondertekent met een eigen private key;
- Iedere OCSP responder heeft een servercertificaat, waarmee een vertrouwende partij de respons kan valideren. Dit certificaat is uitgegeven door de CA waarvan de OCSP responder de status informatie geeft. 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 ZOVAR Private Server CA G1'
- het gebruik van KeyUsage=Digital Signature
- het gebruik van extendedKeyUsage=id-kp-OCSPSigning
- het gebruik van een zogenaamd ocsp-nocheck extensie (Object Identifier 1.3.6.1.5.5.7.48.1.5)

7.3.2 OCSP extensies

De OCSP responses van ZOVAR hebben de volgende kenmerken:

- een versienummer van de response syntax;
- het ID van de responder;
- een response voor ieder van de certificaten in het request zoals hieronder nader is toegelicht;
- de geldigheidsduur van de response;
- optionele extensies. Momenteel is dat alleen de OCSP Nonce;
- een OID die het gebruikte signature algoritme aangeeft: sha256WithRSAEncryption;
- een handtekening van de response;
- het certificaat om de handtekening onder de respons te kunnen valideren.

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

- een certificaat identifier;
- de certificaat status, die één van de 3 onderstaande waarden heeft:
  - '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 ZOVAR 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. Conformiteitsbeoordeling en andere beoordelingen

De TSP dienstverlening van ZOVAR is per 22-11-2004 gecertificeerd tegen 'Scheme for certification of Certification Authorities against ETSI TS 102 042 en voldoet daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners. De norm ETSI 102 042 is per 1 juli 2016 opgevolgd door 319 411-1.

Een afschrift van het EN 319 411-1 certificaat staat vermeld op de site van ZOVAR (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. ZOVAR 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 Frequentie of omstandigheden van de beoordeling

De auditcyclus wordt uitgevoerd volgens ETSI EN 319 403 certificatieschema. ZOVAR 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 ZOVAR zelf interne audits en self-assessments uit.

8.2 Identiteit/kwalificaties van beoordelaar

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

8.3 Relatie van de beoordelaar met beoordeelde entiteit.

De auditoren die de audits uitvoeren zijn onafhankelijk. Er is geen verdere relatie tussen CIBG als TSP en de certificerende instelling.

8.4 Onderwerpen die bij de audit worden behandeld

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

- ETSI EN 319 411-1, inclusief de hierin verwezen normen in de CABforum Network Security Controls.
- het Programma van Eisen PKIoverheid deel 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 Maatregelen die genomen zijn als gevolg van een tekort

Als bij de audit tekortkomingen worden geconstateerd, stelt het CIBG 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.

Mededeling van de resultatenDe conformiteitcertificaten van de meest recente audits zullen beschikbaar zijn op de website van ZOVAR en in de elektronische opslagplaats van de Policy Authority van de PKI voor de overheid. De TSP dienstverlening van het CIBG 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 voorwaarden en bepalingen

9.1 Vergoedingen

9.1.1 Kosten voor uitgifte of verlenging van certificaten
Aan de aanvraag van het ZOVAR-servercertificaat, van een in ZOVAR geregistreerde zorgverzekeraar (abonnee), is een kostendekkend tarief verbonden. Dit tarief is van toepassing op zowel de initiële aanvraag als de vervolgaanvraag, waaronder vernieuwing, van het ZOVAR-servercertificaat. De tarieven voor het ZOVAR-servercertificaat staat vermeld op www.zovar.nl.

9.1.2 Kosten voor toegang tot certificaten
ZOVAR rekent geen kosten voor toegang tot certificaten.

9.1.3 Kosten voor intrekking of toegang tot statusinformatie
ZOVAR rekent geen kosten voor intrekking of toegang tot statusinformatie.

9.1.4 Vergoedingen voor andere diensten
Geen nadere bepaling.

9.1.5 Restitutiebeleid
Conform artikel 6, lid 3 van de Regeling gebruik burgerservicenummer in de zorg is restitutie van betaalde vergoedingen niet mogelijk, tenzij naar het oordeel van de Minister van Volksgezondheid, Welzijn en Sport sprake is van een omstandigheid die niet kan worden toegerekend aan degene ten behoeve van wie de pas of het certificaat is geproduceerd

9.1.6 Wijziging tarieven
Het tarief voor het ZOVAR-servercertificaat kan periodiek wijzigen. Indien het tarief wordt gewijzigd, wordt de Regeling gebruik Burgerservicenummer in de zorg dienovereenkomstig gewijzigd en wordt dit bekendgemaakt op www.zovar.nl.

9.1.7 Facturering en betaling
De abonnee ontvangt drie weken na de productiedatum van het ZOVAR Certificaat, op het bij ZOVAR geregistreerde postadres, een hieraan gerelateerde factuur. Daarnaast wordt de factuur digitaal naar het e-mailadres van de aanvrager verzonden.

Het ZOVAR heeft voor de facturering onderaannemer Cannock Outsourcing B.V. gecontracteerd. Voor het verzenden van de factuur worden de gegevens, zoals het postadres van de abonnee en persoonsgegevens van de pasaanvrager zoals naam en e-mailadres van aan Cannock Outsourcing B.V. verstrekt. ZOVAR zal een verzoek tot aanpassing van een factuur niet honoreren.

De aanvrager is verantwoordelijk voor het kiezen van het juiste ZOVAR-certificaat. Indien de aanvrager een certificaat aanvraagt dat niet juist blijkt te zijn, bijvoorbeeld door een verkeerd PKCS#10 bestand, dan worden hier de volledige kosten voor in rekening gebracht.

9.1.8 Betaaltermijn

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

9.1.9 Geldigheid ZOVAR-servercertificaat

Conform artikel 7 van de Regeling gebruik Burgerservicenummer in de zorg bedraagt de geldigheidsduur van een ZOVAR-servercertificaat drie jaar na de productiedatum.

9.1.10 Levering en ingebruikname ZOVAR-servercertificaat

Het ZOVAR-servercertificaat wordt geleverd conform de in het Certification Practice Statement (CPS) genoemde technische en/of functionele specificaties. Binnen drie maanden na ontvangst van het ZOVAR-servercertificaat neemt de abonnee het ZOVAR-servercertificaat in gebruik. Indien bij ingebruikname blijkt dat het ZOVAR-servercertificaat niet optimaal functioneert stelt de abonnee of diens gemachtigde het ZOVAR hiervan onverwijld op de hoogte.

9.1.11 Vervangingsvoorwaarden

Indien het ZOVAR-servercertificaat niet conform de in het CPS beschreven technische en/of functionele specificaties werkt, vervangt ZOVAR dit certificaat kosteloos tijdens de eerste drie maanden na overdracht van het ZOVAR-servercertificaat.

9.1.12 Risico, eigendom en zorgplicht

Het risico voor tenietgaan, verlies of diefstal, beschadiging of achteruitgaan van het ZOVAR-servercertificaat gaat over op de abonnee op het moment van het in ontvangst nemen van het ZOVAR-servercertificaat. De abonnee is niet gerechtigd om op het ZOVAR-servercertificaat wijzigingen aan te brengen. Het uitgegeven ZOVAR-servercertificaat blijven eigendom van ZOVAR. ZOVAR is bevoegd om het gebruik van het ZOVAR-servercertificaat door een abonnee in te trekken. ZOVAR-servercertificaten zijn niet overdraagbaar aan derden. De abonnee of diens gemachtigde, dient ervoor zorg te dragen dat het ZOVAR-servercertificaat op een zorgvuldige, veilig en behoedzame wijze gebruikt en bewaard worden.

9.2 Financiële verantwoordelijkheid

9.2.1 Verzekeringsdekking

Als overheidsorganisatie kan het CIBG zich niet verzekeren en is zij derhalve eigen risicodrager. Met het ministerie zijn afspraken gemaakt over het risicobeleid. In onderhavige gevallen is het zo dat in gevallen van schadeclaims het CIBG aansprakelijk is tot het maximum van haar eigen (beperkt door agentschapvoorschriften) vermogen. Daarboven neemt het ministerie (i.c. de eigenaar/opdrachtgever) de aansprakelijkheid over.

9.2.2 Andere activa

Geen nadere bepaling.

9.2.3 Verzekering of garantiedekking voor eindentiteiten
Geen nadere bepaling.

9.3 Vertrouwelijkheid bedrijfsgegevens

9.3.1 Reikwijdte van vertrouwelijke informatie
Op basis van de Wet open overheid kan eenieder een verzoek doen om publieke informatie. Bij het verzoek dient de aangelegenheid of het daarop betrekking hebbende document waarover verzoeker informatie wenst te ontvangen, worden vermeld.
Als ZOVAR werkzaamheden uitbesteed aan derden, worden deze werkzaamheden uitgevoerd onder verantwoordelijkheid van ZOVAR. De afspraken tussen derden en ZOVAR zijn contractueel vastgelegd.

9.3.2 Informatie die niet onder vertrouwelijke informatie valt
Geen nadere bepaling.

9.3.3 Verantwoordelijkheid om vertrouwelijke informatie te beschermen
Wanneer het verstrekken van documenten of gegevens de dienstverlening van ZOVAR, de afnemers van haar diensten of van een door ZOVAR 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.

9.4 Vertrouwelijkheid van persoonsgegevens

9.4.1 Privacy plan
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 ZOVAR voor de gebruikers.

De certificaatbeheerders hebben recht op inzage en correctie van hun persoonsgegevens.

9.4.2 Vertrouwelijke informatie
De informatie die door ZOVAR 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.

9.4.3 Niet-vertrouwelijke informatie
De gepubliceerde gegevens van certificaten zijn alleen openbaar raadpleegbaar via de zoekfunctie op de website. 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.

9.4.4 Verantwoordelijkheid om privé-informatie te beschermen
CIBG heeft de verantwoordelijkheid om privé-informatie te beschermen.

9.4.5 Kennisgeving en toestemming voor het gebruik van privégegevens
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.

9.4.6 Openbaarmaking op grond van een gerechtelijke of administratieve procedure
Als in het kader van een straf- of tuchtrechtelijk onderzoek niet-openbare informatie uit het ZOVAR 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 ZOVAR 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.

9.4.7 Andere omstandigheden openbaarmaking van informatie
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.

9.5 Intellectuele eigendomsrechten

Dit CPS is eigendom van ZOVAR. Ongewijzigde kopieën van deze CPS mogen zonder toestemming verspreid en gepubliceerd worden mits dit met bronvermelding geschiedt.

Door ZOVAR uitgegeven certificaten blijven eigendom van ZOVAR. Alle intellectuele eigendomsrechten in relatie tot de certificaten, waaronder begrepen de rechten met betrekking tot software, databanken en beeldmerken, berusten bij ZOVAR. De rechten zijn niet overdraagbaar aan derden.

ZOVAR garandeert jegens haar abonnees dat de door haar uitgegeven certificaten, inclusief de daarbij behorende en geleverde documentatie, geen inbreuk maakt op intellectuele eigendomsrechten, waaronder auteursrechten, merkenrechten en gebruikte programmatuur waarvan deze berusten bij haar (toe)leveranciers.

9.6 Aansprakelijkheid en garanties

9.6.1 CA aansprakelijkheid en garanties
Met de invoering van de Wet elektronisch bestuurlijk verkeer heeft de wetgever voor wat betreft de aansprakelijkheid bepaalt dat er aansluiting moet worden

gezocht bij de aansprakelijkheidsbepalingen betreffende de aansprakelijkheid in het elektronisch rechtsverkeer, in het bijzonder op de aansprakelijkheid van de certificatiedienstverlener die gekwalificeerde certificaten uitgeeft, zoals vastgelegd in boek 6 Burgerlijk wetboek.

Het CIBG is in haar functie van certificatiedienstverlener aansprakelijk voor schade die natuurlijke personen of rechtspersonen, die in redelijkheid op een uitgegeven ZOVAR-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 CIBG kan aansprakelijk worden gesteld, wanneer zij nalaat intrekking van een ZOVAR-certificaat te registeren, met inbegrip van het bijwerken en publiceren van de CRL, en een persoon in redelijk vertrouwen daarop heeft gehandeld.

Het CIBG kan op basis van voorgaande gronden niet aansprakelijk worden gesteld, als zij bewijzen kan overleggen dat ZOVAR niet onzorgvuldig heeft gehandeld.

ZOVAR sluit alle aansprakelijkheid uit voor schade indien het certificaat niet conform het in paragraaf 1.4 beschreven certificaatgebruik wordt gebruikt.

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

ZOVAR is aansprakelijk in geval van opzettelijk of uit onachtzaamheid toegebrachte schade aan een natuurlijk persoon of rechtspersoon die is te wijten aan een verzuim de verplichtingen uit hoofd van EU-verordening nr. 910/2014 (eIDAS) na te leven. ZOVAR is niet aansprakelijk voor schade die ontstaat door gebruikmaking van diensten die de aangegeven beperkingen overschrijden.

RA aansprakelijkheid en garanties.
Zie 9.6.1.

9.6.2 Abonnee aansprakelijkheid en garanties.
Abonnees en certificaathouders zijn gehouden aan de bepalingen van ZOVAR 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 ZOVAR zijn meegedeeld bij de uitreiking van de certificaten en/of op een later tijdstip aan hen kenbaar zijn gemaakt.

Wanneer door abonnees of certificaathouders niet aan deze bepalingen wordt voldaan, kan er sprake zijn van schade voor ZOVAR, 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 4.5.1 van dit CPS.

- De abonnee zal enkel en alleen certificatiediensten van ZOVAR afnemen voor haar systemen en databases.
- De abonnee garandeert dat hij in rechte bevoegd is om de organisatie aan ZOVAR te binden. Daarnaast kan de abonnee onder zijn eindverantwoording binnen de organisatie een of meerdere gemachtigden aanwijzen: de aanvrager/certificaatbeheerder(s). Deze aanvrager/certificaatbeheerder(s) zal (zullen) namens de abonnee belast worden met de daadwerkelijke uitvoering van de aanvragen voor en intrekken ZOVAR certificaten 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 abonnee zelf bevoegd.

- 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 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 ZOVAR, met inbegrip van gegevens van de systemen voor het genereren en de uitgifte van certificaten. Wijzigingen in adres, organisatie, organisatienaam, functies, contactpersonen of persoonsgegevens van de abonnee of andere relevante wijzigingen zullen door de abonnee niet later dan 24 uur nadat deze wijziging zich heeft voorgedaan aan ZOVAR gemeld worden.
- De abonnee is verplicht een procedure in te richten en uit te voeren aan de hand waarvan hijzelf of de aanvrager/certificaatbeheerder(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 ZOVAR voortvloeien niet overdragen aan derden, tenzij door ZOVAR 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. [8]

Voorgaande verplichtingen voor de abonnee zullen voor zover zij als te onbepaald kunnen worden aangemerkt, nader worden uitgewerkt in richtlijnen van ZOVAR en/of nadere regelgeving.

9.6.3 Aansprakelijkheid en garanties van vertrouwende partijen
Geen nadere bepaling.

9.6.4 Aansprakelijkheid en garanties van andere deelnemers
Voor de aansprakelijkheid en garanties t.a.v. certificaathouders zie paragraaf 9.6.3.

9.7 Beperkingen van garantie

In geval van systeemdefecten, serviceactiviteiten, of factoren die buiten het bereik van ZOVAR liggen, zal ZOVAR 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. ZOVAR is niet verantwoordelijk voor de niet-beschikbaarheid van de dienstverlening vanwege natuurrampen of andere omstandigheden waar ZOVAR niet verantwoordelijk voor kan worden gehouden.

9.8 Beperking van aansprakelijkheid

ZOVAR erkent geen aansprakelijkheid voor schade ontstaan bij natuurlijke personen of rechtspersonen in het geval van:

8 In het geval van calamiteiten bij ZOVAR zal het Ministerie van VWS adequate maatregelen treffen.

- 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;
- 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 ZOVAR betreffen;
- Schade die ontstaat doordat abonnees, certificaathouders 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, intrekkingscode en de private sleutel;
- Schade ontstaan door de afgifte van een certificaat op grond van door de abonnee verkeerd verstrekte informatie, voor zover ZOVAR 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, de programmatuur, de apparatuur of telecommunicatiefaciliteiten gebruikt door abonnee;
- 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 de identificatie van de certificaatbeheerder buiten het overeengekomen tijdvenster 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.

9.9 Schadeloosstelling

Schadeloosstelling geschiedt enkel nadat onomstotelijk is vastgesteld dat ZOVAR aansprakelijk kan worden gehouden voor de geleden schade.

9.10 Termijn en afloop

9.10.1 Termijn

Het CPS is geldig vanaf de datum van publicatie op de website www.zorgcsp.nl. Het CPS is geldig zolang de dienstverlening van ZOVAR voortduurt of totdat het CPS

wordt vervangen door een nieuwere versie. Nieuwere versies worden aangeduid met een hoger versienummer (vX.x). Bij ingrijpende wijzigingen wordt het versienummer opgehoogd met 1, bij redactionele aanpassingen wordt het versienummer opgehoogd met 0.1. Nieuwere versies worden gepubliceerd op de website van ZOVAR

9.10.2 Afloop

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.

9.10.3 Effect van beëindiging en overleving

Geen nadere bepaling.

9.11 Communicatie binnen betrokken partijen

Geen nadere bepaling.

9.12 Wijzigingen

9.12.1 Wijzigingsprocedure

De werking van het geldende CPS wordt ten minste jaarlijks beoordeeld en geactualiseerd. Wijzigingen gelden vanaf het moment dat het nieuwe CPS wordt gepubliceerd. Het management van het CIBG is verantwoordelijk voor een juiste navolging van de procedure zoals beschreven in paragraaf 9.12 en voor de uiteindelijke goedkeuring van het CPS conform deze procedure.

9.12.2 Meldingsmechanisme en periode

Geen andere bepaling.

9.12.3 Omstandigheden waaronder OID moet worden gewijzigd

Geen andere bepaling.

9.12.4 Verzoeken tot wijziging en classificatie

Abonnees, certificaathouders, vertrouwende partijen en eventuele andere belanghebbenden kunnen schriftelijk gemotiveerd een verzoek tot wijziging indienen. ZOVAR 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 een ontvangstbevestiging.

De verzoeken tot wijziging worden door het TSP management en de staf van ZOVAR 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.

Wijzigingen op het CPS worden zo veel mogelijk gegroepeerd doorgevoerd.

9.12.5 Publicatie van wijzigingen

ZOVAR 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 alleen schriftelijk worden gedaan.

Zodra het CPS is gepubliceerd op www.zorgcsp.nl wordt dit aan de Policy Authority gerapporteerd.

9.13 Conflictoplossing

Het CPS geeft de interpretatie van de bepalingen van ZOVAR aan. Deze interpretatie dient de algemene doelstelling van ZOVAR 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 conflictbemiddelaar. Over de bekostiging van deze conflictbemiddeling worden alsdan 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 ZOVAR, moet de klacht schriftelijk ingediend worden bij het CIBG, ter attentie van het clusterhoofd verantwoordelijk voor ZOVAR onder vermelding van 'Klacht'. ZOVAR 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 ZOVAR biedt, dan kan het clusterhoofd van ZOVAR bemiddelen of een onafhankelijke bemiddelaar aanwijzen, indien partijen niet in onderling overleg tot overeenstemming komen.

9.14 Toepasselijk recht

Op de diensten van ZOVAR en het voorliggend CPS is het Nederlandse recht van toepassing.

9.15 Naleving relevante wetgeving

Het CIBG als uitvoerder van de dienstverlening van ZOVAR 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 ZOVAR als onderdeel van het Ministerie van Volksgezondheid, Welzijn en Sport een bestuursorgaan is in de zin van de Awb.

9.16 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.

9.16.1 Gehele overeenkomst

Geen nadere bepaling.

9.16.2 Toewijzing

Geen nadere bepaling.

9.16.3 Scheidbaarheid

Geen nadere bepaling.

9.16.4 Tenuitvoerlegging (honoraria van advocaten en afstand van rechten)

Geen nadere bepaling.

9.16.5 Overmacht

Geen nadere bepaling.

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	Zorgverzekeraar of zorgkantoor volgens de definitie die ZOVAR hanteert, die certificatendiensten afneemt van ZOVAR. De abonnee is de partij namens wij een server/service 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.
	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. Zie ook 'Private sleutel' en 'Publieke sleutel'.
AT	Agentschap Telecom	Agentschap Telecom is zowel uitvoerder als toezichthouder van wet- en regelgeving op het gebied van telecommunicatie, Bron: www.agentschaptelecom.nl
	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.

Afkorting	Begrip	Definitie
	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.
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.
	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 betreffende de vertrouwelijkheid en authenticiteit en/of elektronische handtekening en daarmee de identiteit van de persoon bevestigt. Een certificaat is vercijferd met de private sleutel van de Certification Authority die de publieke sleutel heeft uitgegeven, waardoor het certificaat onvervalsbaar is. Een certificaat, bevat tenminste: - de identificatie en het land van vestiging van de afgevende certificatiedienstverlener; - de naam van de ondertekenaar; - vermelding van het tijdstippen van het begin en van het einde van de geldigheidsduur van het certificaat; - de identiteitscode van het certificaat; - eventuele beperkingen betreffende het gebruik van het certificaat, en - eventuele grenzen met betrekking tot de waarde van de transacties waarvoor het certificaat kan worden gebruikt.
	Certificaathouder	Een natuurlijk persoon of rechtspersoon, ten behoeve van wie een certificaat is afgegeven en wiens identiteit kan worden vastgesteld met behulp van het certificaat. In het geval van servercertificaten zal de certificaathouder een machine of server zijn.

Afkorting	Begrip	Definitie
	Certificaatbeheerder	De rol van certificaatbeheer is alleen van belang voor producten waarbij de certificaathouder een systeem is of een groep/functie betreft, dus server-certificaten. ZOVAR 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.
CP	Certificate Policy - *certificerings-beleid*	Een document met een benoemde verzameling eisen dat de kaders aangeeft waarbinnen ZOVAR 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 ZOVAR.
CRL	Certificate Revocation List - *certificaat revocatie lijst*	Een lijst van ingetrokken (= gerevoceerde) certificaten. Deze lijst is openbaar toegankelijk en raadpleegbaar. De lijst is beschikbaar gesteld door en onder verantwoordelijkheid van ZOVAR. De CRL is zelf ook elektronisch ondertekend door de CA van ZOVAR.
	Certificatie-diensten	Het afgeven, beheren en intrekken van certificaten door certificatiedienstverleners, alsmede andere diensten die samenhangen met het gebruik van elektronische handtekeningen, identiteit en vertrouwelijkheid.
CA	Certification Authority	Het onderdeel van ZOVAR dat de ondertekening van de certificaten verzorgt en dat door eindgebruikers wordt vertrouwd.
CPS	Certification Practice Statement	Een document dat de door het CIBG gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de dienstverlening beschrijft. Het CPS beschrijft op welke wijze ZOVAR 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 drager; • Gestolen of vermoedelijk gestolen private sleutel of drager; • Vernietigde private sleutel of drager. Compromittatie vormt aanleiding om een certificaat op de Certificate Revocation List te plaatsen.

Afkorting	Begrip	Definitie
	Directory service	De directory service is een dienst van ZOVAR en heeft tot doel het op internet beschikbaar stellen en het toegankelijk maken van uitgegeven certificaten.
	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 paspoort of identiteitsbewijs is opgenomen (ook wel meisjesnaam of geslachtsnaam genoemd).
	Gemachtigde aanvrager	Een persoon die gemachtigd is door de wettelijk vertegenwoordiger van de abonnee om namens de abonnee aanvragen tot uitgifte van certificaten in te dienen.
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 gezag keten van elkaar vertrouwende Certification Autorities (CA).
	Identificatie	Het proces waarbij de identiteit van een persoon of een zaak 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.
	Integriteit	De zekerheid dat gegevens volledig en niet gewijzigd zijn.
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.
	Intrekkingscode	Code waarmee de certificaathouder een intrekkingsverzoek voor certificaten kan indienen en autoriseren.
	Persoonlijke sleutel	Zie 'Private sleutel'.
PA	Policy Authority	Autoriteit onder de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties die het certificeringsbeleid (CP / Certificate Policy) van ZOVAR vaststelt. Zie ook www.logius.nl

Afkorting	Begrip	Definitie
	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 ZOVAR 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).
	Sleutel(s)	Zie respectievelijk: • Asymmetrisch sleutelpaar • Private sleutel • Publieke sleutel
	Sleutelpaar	Zie ook asymmetrisch sleutelpaar.
	Servercertificaat	Een certificaat waarmee een dienst of apparaat, bijvoorbeeld een server wordt gekoppeld aan een rechtspersoon of andere organisatie. In het geval van een server wordt het certificaat aangeboden aan een browser, die toegang zoekt tot de server. Hierdoor kan een vertrouwende partij zekerheid krijgen omtrent de identiteit van de eigenaar va de server. Een servercertificaat is geen gekwalificeerd certificaat.
	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.

Afkorting	Begrip	Definitie
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 in de zin van artikel 1.1 sub tt van de Telecommunicatiewet.
UZOVI	Unieke Zorgverzekeraar identificatie	In het UZOVI register worden de adresgegevens en het unieke UZOVI-nummer geregistreerd en onderhouden. Sinds 1 januari 2006 bevat het register de gegevens van de zorgverzekeraars, gevolmachtigde assurantietussenpersonen, zorgkantoren, labelorganisaties en nevenvestigingen.
	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.
	Vertrouwelijk-heidscertificaat	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.
	Wettelijk vertegenwoordiger	De persoon die conform het uittreksel KvK of oprichtingsdocument bevoegd is om de organisatie juridisch te binden aan ZOVAR.
	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 cliënt horen. Daarnaast zijn regels opgenomen over elektronische uitwisselingssystemen in de zorg.
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.
X.509	X.509	Dit is een elektronisch certificaat dat volgens een gestandaardiseerde structuur is opgebouwd.
	Zorgkantoor	Een ingevolge artikel 4.2.4, tweede lid, voor een bepaalde regio aangewezen Wlz-uitvoerder;

Afkorting	Begrip	Definitie
	Zorgverzekeraar	Hiermee wordt bedoeld: **1°.** Wlz-uitvoerder als bedoeld in artikel 1.1.1 van de Wet langdurige zorg; **2°.** zorgverzekeraar als bedoeld in artikel 1, onder b, van de Zorgverzekeringswet; **3°.** verzekeringsonderneming als bedoeld in de richtlijn solvabiliteit II voor zover deze verzekeringen aanbiedt of uitvoert krachtens welke het verzekerde risico de behoefte aan zorg is waarop bij of krachtens deWet Langdurige zorg geen aanspraak bestaat en waarbij de verzekerde prestaties het bij of krachtens de Zorgverzekeringswet geregelde te boven gaat; 1. Solvency II Richtlijn 2009/138/EG is het nieuwe, risico gebaseerde toezichtraamwerk voor verzekeraars dat per 1 januari 2016 in werking is getreden. Het voornaamste doel van het raamwerk is de bescherming van de belangen van polishouders. Dit wordt bereikt via kwantitatieve kapitaaleisen, kwalitatieve eisen aan de kwaliteit van de bedrijfsvoering en transparantie naar publiek en toezichthouder. Solvency II geldt niet voor natura-uitvaartverzekeraars en de meeste kleine verzekeraars.