

# Programma van Eisen voor een zorgserviceprovider (ZSP)



Betere zorg door betere informatie

postadres: Postbus 19121, 2500 CC Den Haag  
bezoekadres: Oude Middenweg 55, 2491 AC Den Haag  
telefoon: (070) 317 34 50; fax: (070) 320 74 37; e-mail: [servicedesk@infoEPD.nl](mailto:servicedesk@infoEPD.nl)  
[www.nictiz.nl](http://www.nictiz.nl)

Versie : 6.0.1.0  
Datum : 16 april 2009

# Inhoudsopgave

|       |   |    |
|-------|---|----|
| 1     | Inleiding .....                                   | 3  |
| 1.1   | Doel en doelgroep .....                           | 3  |
| 1.1.1 | Doel .....  | 3  |
| 1.1.2 | Doelgroep .....                                   | 3  |
| 1.2   | Versie, status en wijzigingshistorie .....        | 4  |
| 1.2.1 | Versie.....                                       | 4  |
| 1.2.2 | Status .....                                      | 4  |
| 1.2.3 | Wijzigingshistorie .....                          | 4  |
| 1.3   | Achtergrond.....                                  | 5  |
| 1.4   | Reikwijdte .....                                  | 6  |
| 1.5   | Structuur.....                                    | 7  |
| 1.6   | Samenhang met andere documenten .....             | 7  |
| 2     | Uitgangspunten .....                              | 8  |
| 2.1   | Normatieve referenties.....                       | 8  |
| 2.2   | Informatieve referenties.....                     | 8  |
| 2.3   | Afkortingen en begrippen .....                    | 9  |
| 3     | Overzicht van een ZSP .....                       | 10 |
| 3.1   | Wat is een ZSP? .....                             | 10 |
| 3.2   | Categorieën van eisen aan een ZSP .....           | 12 |
| 3.3   | Omgeving van een ZSP .....                        | 13 |
| 3.4   | Grenzen van een ZSP.....                          | 18 |
| 3.5   | ZSP-kwalificatie.....                             | 19 |
| 3.6   | Aansluitvoorwaarden versus gebruikerswensen ..... | 19 |
| 3.7   | Specificatie van eisen en wensen.....             | 20 |
| 4     | Functionaliteits-eisen.....                       | 21 |
| 4.1   | Inleiding.....                                    | 21 |
| 4.2   | Datacommunicatiefuncties.....                     | 21 |
| 4.2.1 | Connectiviteitsfuncties (CON) .....               | 21 |
| 4.2.2 | Domain Name System functies (DNS) .....           | 24 |
| 5     | Implementatie-eisen .....                         | 27 |
| 5.1   | Inleiding.....                                    | 27 |
| 5.2   | Beveiliging (BVL).....                            | 27 |
| 5.3   | Beschikbaarheid (BSC).....                        | 30 |
| 5.4   | Responstijden (RSP) .....                         | 32 |
| 6     | Exploitatie-eisen .....                           | 33 |
| 6.1   | Organisatie (ORG) .....                           | 33 |
| 6.2   | Beheerfuncties (BEH).....                         | 35 |
| 6.3   | Gebruikerondersteuning (GBO) .....                | 37 |
| 7     | Voorbeelden van een ZSP .....                     | 38 |
| 7.1   | Inleiding.....                                    | 38 |
| 7.2   | Voorbeeld 1 .....                                 | 38 |
| 7.3   | Voorbeeld 2 .....                                 | 38 |
| 7.4   | Voorbeeld 3 .....                                 | 39 |
| 7.5   | Voorbeeld 4 .....                                 | 39 |
| 7.6   | Voorbeeld 5 .....                                 | 40 |

# 1 Inleiding

## 1.1 Doel en doelgroep

### 1.1.1 Doel

Dit document specificereert de eisen waaraan een zorgserviceprovider (ZSP) moet voldoen, opdat deze de verbinding mag vormen tussen een goed beheerd zorgsysteem (GBZ) en het landelijk schakelpunt (LSP). De eisen in dit document omvatten zowel organisatorische, procedurele, functionele als technische aspecten. Een datacommunicatiedienstverlener die voldoet aan deze eisen kan zich laten kwalificeren als zorgserviceprovider.

Dit document is geschreven in het kader van het AORTA-programma van Nictiz.

### 1.1.2 Doelgroep

Dit document is primair geschreven voor netwerkdienstverleners en secundair voor overige partijen die zich bezighouden met de ontwikkeling en implementatie van ICT-toepassingen in de zorg, zoals zorgaanbieders en ontwikkelaars, leveranciers, onderzoekers.

De lezer wordt verondersteld een ICT-achtergrond te hebben. Voor een goed begrip van dit document is het raadzaam kennis te nemen van:

- het [\[Documentatieoverzicht\]](#);
- de [\[Verklarende woordenlijst\]](#);
- de [\[Architectuurvisie\]](#);
- de [\[Bedrijfsarchitectuur\]](#);
- de [\[Informatiesysteemarchitectuur\]](#);
- de [\[Technische architectuur\]](#).

Het maakt deel uit van de documentatieset van de AORTA-basisinfrastructuur. De lezer wordt verondersteld hiervan basiskennis te hebben. De samenstelling van die documentatieverzameling en de samenhang met overige documenten binnen die documentatieverzameling is opgenomen in [\[Documentatieoverzicht\]](#).

## 1.2 Versie, status en wijzigingshistorie

### 1.2.1 Versie

Dit is versie 6.0.1.0 van het document "Programma van Eisen voor een zorgserviceprovider (ZSP)". Het correspondeert met PvE LSP versie 6.0.1.0.

### 1.2.2 Status

De status van dit document is: "Definitief".

### 1.2.3 Wijzigingshistorie

Ten opzicht van de vorige versie zijn de volgende wijzigingen in dit document doorgevoerd.

|                 |  |
|-----------------|--|
| Wijziging #1994 | Redundante verbinding met tweede operationele locatie als eis opgenomen.   |
| Wijziging #1993 | Naar aanleiding van het reviewcommentaar op de kwalificatiecriteria ZSP door BDO is een groot aantal wijzigingen in de kwalificatiecriteria doorgevoerd.<br>De aanpassingen hebben tevens een aantal aanpassingen in het 'Programma van Eisen' tot gevolg gehad. |
| Wijziging #1824 | Aanscherping opzet, bestaan en werking. Verder LSP verantwoordelijkheden verwijderd omdat dit geen ZSP eisen zijn.   |
| Wijziging #1729 | Aanpassen ORG.04. Afsluiten SLA wordt een {wens}.  |
| Wijziging #1635 | Wijzigingen eisen ivm verhoging beschikbaarheid en DNS-resolving<br>Wijziging paragraaf 4.2.1, DNS-01, DNS-05, DNS-06 (toegevoegd)   |
| Wijziging #1633 | Toegevoegd: Eis, dat een ZSP buiten de kantooruren van werkdagen voor noodgevallen voor diens GBZ'en op een noodnummer bereikbaar moet zijn.   |
| Wijziging #1632 | Par. 7.6 toegevoegd: GBZ via meerdere ZSP naar het LSP --> 3.1 aangepast.  |
| Wijziging #1631 | FE.CON.03 aangepast : 1 IP adres per GBZ applicatie.   |
| Wijziging #1585 | Door de aanpassing van de frequentie van optreden van storingen als functie van hun reparatietijd en hun omvang zijn BSC.02 en BSC.03 vervallen en opgenomen in BSC.04.  |
| Wijziging #1562 | Verwijdering van het gebruik van de termen MTBF en MTTR in eis BSC.02, BSC.03 en BSC.04  |
| Wijziging #1512 | Correctie van de gemiddelde reparatietijd voor grote storingen in eis BSC.04 van 1 uur naar 12 uur.  |
| Wijziging #1472 | Het is nu een {wens} en niet langer een eis dat een ZSP datacommunicatie verzorgt met andere ZSP's die niet via het LSP verloopt. Hiervoor is CON.04 aangepast.  |
| Wijziging #1309 | Het onderhoudsvenster is verlengd tot 0700 uur in eis BSC.07.  |
| Wijziging #1947 | 1947 Invoering Zorgadresboek: wijziging tekst van paragraaf 3.3.   |
| Wijziging #2232 | Bepaling servicedesk, waarvoor een aanpassing van paragraaf 3.3.<br>Aanpassing eisen: EE.GBO.01 en EE.GBO.02. Nieuwe eis {wens}  |

## 1.3 Achtergrond

Nictiz werkt onder meer aan de ontwikkeling van een landelijke basisinfrastructuur in de zorg, AORTA genaamd, die mogelijk moet maken dat zorgaanbieders en later ook zorgverzekeraars en patiënten, ten behoeve van verschillende zorgtoepassingen op landelijke schaal patiëntgegevens kunnen uitwisselen.

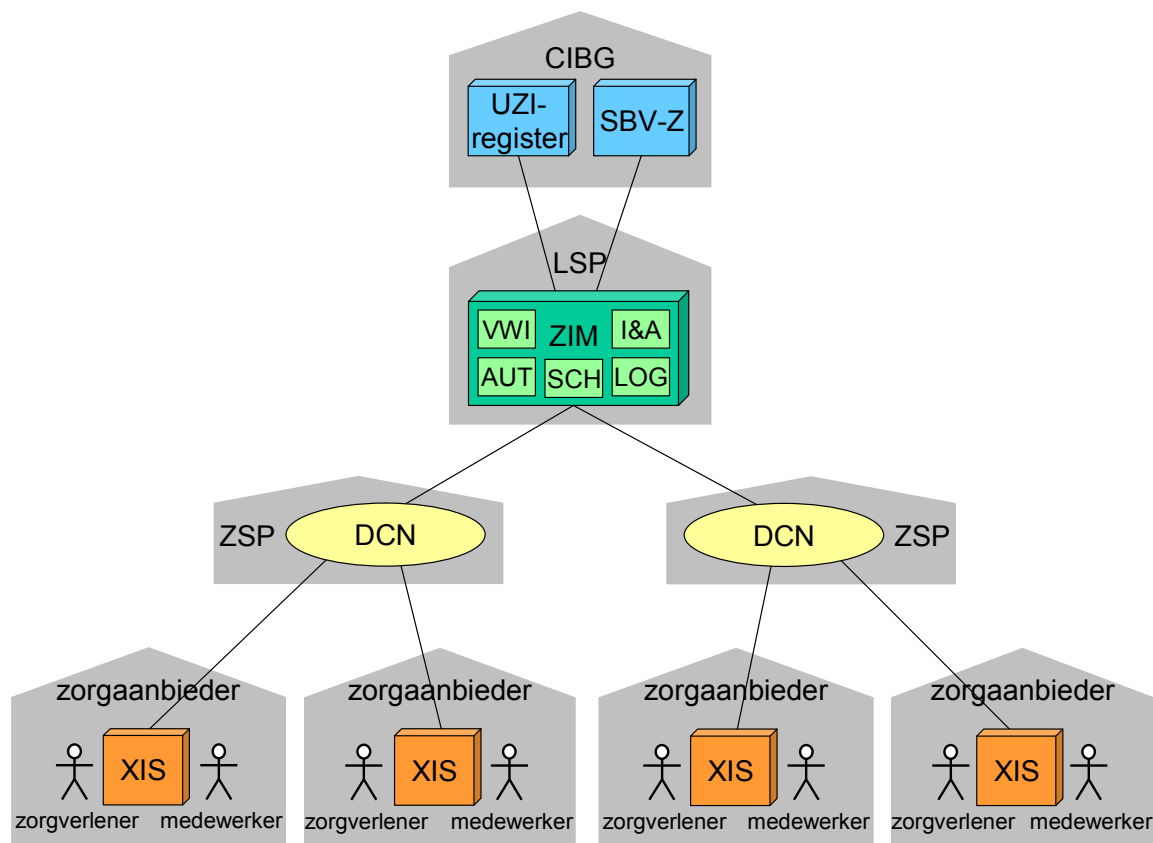
De volgende landelijke zorgtoepassingen zijn onder meer gepland of in productie voor AORTA:

- Medicatiegegevens , in productie
- Huisartswaarneemgegevens , in productie
- Spoedeisende-hulpdossier (SEH), gepland
- Elektronisch pathologiedossier (PAD), gepland.

Centraal in AORTA staat de zorginformatiemakelaar (ZIM), die wordt geëxploiteerd door het landelijke schakelpunt (LSP). Daarop kunnen zorgaanbieders hun bestaande zorginformatiesystemen (ook wel XIS'en genoemd) aansluiten, mits zij voldoen aan de eisen van een goed beheerd zorgsysteem (GBZ). Die aansluiting vindt plaats via datacommunicatienetwerken (DCN), die worden geëxploiteerd door zorgserviceproviders (ZSP).

Voor het uniek identificeren van patiënten, zorgaanbieders en zorgsystemen wordt gebruik gemaakt van landelijke registers: het UZI-register (Unieke Zorgverleners Identificatie) en de SBV-Z (Sectorale Berichten Voorziening in de Zorg van het BSN-stelsel).

De onderstaande figuur toont op vereenvoudigde wijze hoe zorgaanbieders met hun XIS via het DCN van een ZSP worden aangesloten op de ZIM van het LSP, opdat zorgverleners en hun medewerkers vanuit hun eigen XIS op landelijke schaal patiëntgegevens kunnen uitwisselen met andere zorgaanbieders.



Het LSP, de SBV-Z en het UZI-register zijn reeds operationeel

Om tot een betrouwbare gegevensuitwisseling te kunnen komen, worden aan de componenten LSP, ZSP en GBZ eisen gesteld, opgenomen in programma's van eisen.

Het voorliggende document is het programma van eisen voor de zorgserviceprovider (ZSP).

Omdat voldoen aan de gestelde eisen van groot belang is voor betrouwbare gegevensuitwisseling, is een vorm van toetsing nodig. Binnen AORTA wordt daarvoor de term 'kwalificatie' gebruikt.

Dit document dient gelezen te worden in samenhang met de overige AORTA documenten.

## 1.4 Reikwijdte

Dit document richt zich op de functionele, implementatie en organisatorische eisen waaraan een netwerkdienstverlener moet voldoen om zich als ZSP te laten kwalificeren en GBZ'en te kunnen aansluiten op het LSP ter ondersteuning van landelijke uitwisseling van patiëntgegevens.

In tegenstelling tot de overige programma's van eisen zijn er voor het programma van eisen voor een zorgserviceprovider geen addendums per zorgtoepassing. De eisen in dit document zijn onafhankelijk van toekomstige zorgtoepassingen. Ze gelden dus zonder uitzondering voor alle netwerkdienstverleners die zich willen laten kwalificeren. Wel

wordt in dit document op enkele plaatsen onderscheid gemaakt voor wat betreft het moment dat eisen van kracht worden:

- Indien in dit document eisen voorzien zijn van het predicaat {toekomst}, dan zijn die eisen vooralsnog in het geheel niet van kracht. Ze worden slechts genoemd zodat netwerkdienstverleners kunnen anticiperen op het eventueel ooit van kracht worden van de betreffende eis.
- Indien eisen niet voorzien zijn van bovengenoemd predicaat, dan zijn de eisen direct van kracht.

## 1.5 Structuur

Dit document heeft de volgende indeling:

- Hoofdstuk 1, geeft een inleiding voor dit document,
- Hoofdstuk 2, geeft de uitgangspunten en referenties voor dit document,
- Hoofdstuk 3, geeft een overzicht en afbakening van de architectuurcomponent ZSP,
- Hoofdstuk 4, licht de *functionaliteit*-eisen toe, die worden gesteld aan een ZSP,
- Hoofdstuk 5, licht de *implementatie*-eisen toe, die worden gesteld aan een ZSP,
- Hoofdstuk 6, licht de *organisatie*-eisen toe, die worden gesteld aan een ZSP,
- Hoofdstuk 7, geeft enkele voorbeelden van ZSP's.

## 1.6 Samenhang met andere documenten

Dit document maakt deel uit van de documentatieset van de AORTA-basisinfrastructuur. Het kan samen gelezen worden met de kwalificatiedocumenten voor een ZSP. Het [Kwalificatiecriteria ZSP] beschrijft de betekenis van en processen rond kwalificatie van ZSP's. Dat beschrijft hoe de eisen uit dit document in dat kwalificatieproces gehanteerd worden.

## 2 Uitgangspunten

### 2.1 Normatieve referenties

De onderstaande documenten zijn beschouwd als leidend voor dit document:

| Identificatie                                   | Titel   | Bron   | Versie<br>Datum          |
|---|---|--------|--------------------------|
| <a href="#">[Documentatieoverzicht]</a>         | Documentatieoverzicht AORTA-basisinfrastructuur | Nictiz | 6.0.1.0<br>16 april 2009 |
| <a href="#">[Verklarende woordenlijst]</a>      | Verklarende woordenlijst AORTA                  | Nictiz | 6.0.1.0<br>16 april 2009 |
| <a href="#">[Architectuurvisie]</a>             | Architectuurvisie AORTA                         | Nictiz | 6.0.1.0<br>16 april 2009 |
| <a href="#">[Bedrijfsarchitectuur]</a>          | Bedrijfsarchitectuur AORTA                      | Nictiz | 6.0.1.0<br>16 april 2009 |
| <a href="#">[Informatiesysteemarchitectuur]</a> | Informatiesysteemarchitectuur AORTA             | Nictiz | 6.0.1.0<br>16 april 2009 |
| <a href="#">[Technische architectuur]</a>       | Technische architectuur AORTA                   | Nictiz | 6.0.1.0<br>16 april 2009 |

### 2.2 Informatieve referenties

Naast de bovengenoemde normatieve referenties, wordt aan de onderstaande overige documenten gerefereerd:

| Identificatie                                 | Titel                                   | Bron   | Versie<br>Datum          |
|---|---|--------|--------------------------|
| <a href="#">[Kwalificatiecriteria ZSP]</a> ** | Kwalificatiecriteria voor een ZSP (ZSP) | Nictiz | 6.0.1.0<br>16 april 2009 |

\*\* *Dit document wordt niet gepubliceerd*

## 2.3 Afkortingen en begrippen

Voor algemene begrippen en afkortingen wordt verwezen naar de AORTA-architectuurdocumentatie waaronder begrepen de [Verklarende woordenlijst]. Begrippen en afkortingen die in dit document een specifieke betekenis hebben zijn de volgende.

| Definities    |  |
|---------------|--|
| Term          | Definitie  |
| Datatransport | Het transport van IP-pakketten over een netwerk.   |
| Delay         | De totale vertraging die het datatransport ondergaat tussen twee eindpunten.   |
| Edge device   | Apparatuur die geplaatst is op de koppelvlakken van 2 dienstverleners. Apparatuur dient als entry-point van de dienstverlener.   |
| GBZ-domein    | Het domein van de zorgaanbieder, vanaf de LAN zijde van de edge device van het GBZ.  |
| Storing       | Een onbedoelde verstoring van de datacommunicatie waarbij de delay tussen de edge router van de LSP en de edge device van het GBZ de maximaal toegestane delay overschrijdt, buiten het tijdslot van gepland onderhoud.  |
| ZSP-domein    | Het domein waarbinnen de ZSP verantwoordelijkheid draagt voor het datatransport vanaf de LAN zijde van de edge router ter plaatse van het LSP tot en met de LAN zijde van de edge device op de klantlocatie (GBZ locatie) (dus inclusief de beide edge devices). |

Overal in dit document waar de voornaamwoorden "hij", "hem" of "zijn" staan, wordt "hij of zij" resp. "hem of haar" resp. "zijn of haar" bedoeld.

### 3 Overzicht van een ZSP

Dit hoofdstuk geeft een beeldende beschrijving van wat een ZSP zou kunnen zijn en is niet normatief. Dit is nodig omdat de eisen/wensen in de navolgende hoofdstukken, die wel normatief zijn, zoveel mogelijk SMART zijn geformuleerd en dus geen ruimte voor een beeldende beschrijving of een suggestief voorbeeld laten.

#### 3.1 Wat is een ZSP?

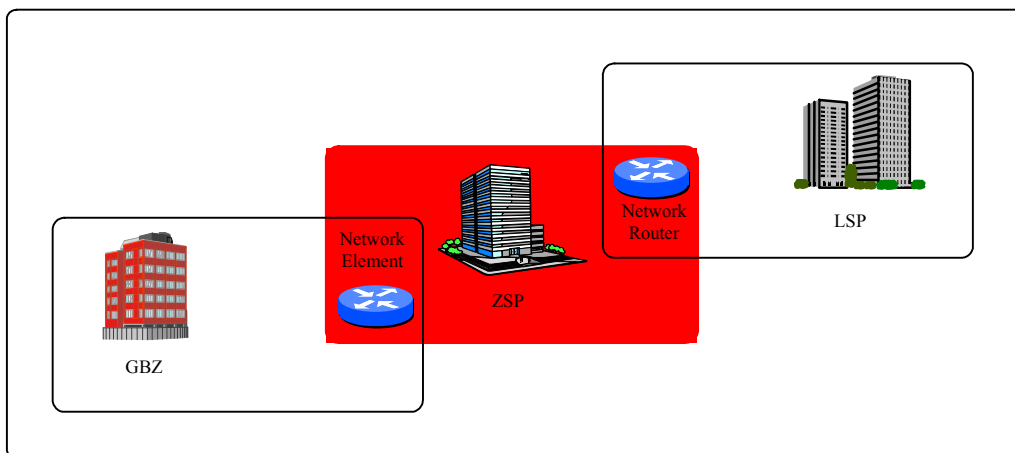
Een ZSP wordt gedefinieerd als de rechtspersoon die aan de zorgaanbieder diensten levert. De ZSP verbindt door een datacommunicatienetwerk (DCN) het GBZ met het LSP.

Een DCN wordt gedefinieerd als:

- een netwerk van datacommunicatieverbindingen,
- inclusief de daarvoor benodigde voorzieningen op de locatie van aangesloten partijen,
- dat door één datacommunicatiedienstverlener wordt beheerd en geëxploiteerd,
- ten behoeve van zorgaanbieders die hun GBZ willen aansluiten op het LSP.

De primaire dienstverlening van een ZSP betreft dus het bieden van een verbinding ten behoeve van datacommunicatie tussen GBZ en LSP en tussen GBZ'en onderling. Daarnaast zal een ZSP zijn netwerk moeten beheren en aanvullende diensten moeten leveren. Een ZSP levert zowel diensten aan GBZ'en als aan het LSP.

Onderstaande figuur geeft een schematische weergave van het domein van een ZSP in relatie tot GBZ en LSP.



**Figuur 1: Schematische weergave domeinen GBZ, ZSP en LSP**

#### Diensten aan GBZ'en

Diensten die een ZSP levert aan GBZ'en omvatten ten minste:

- een servicedesk ten behoeve van:
  - melden van verstoringen
  - melden van gepland onderhoud
  - voeren van overleg ten behoeve van instandhouding van de dienstverlening

- rapporteren over de geleverde prestatie
- het oplossen van al dan niet gemelde storingen
- preventief, correctief en adaptief onderhoud
- het beheer van de aansluiting van een GBZ op het LSP

Een ZSP kan vanuit zijn onderneming aanvullende diensten aanbieden aan een GBZ of de zorgaanbieder. Aan dergelijke diensten zijn in dit document geen eisen gesteld. Dergelijke diensten kunnen bijvoorbeeld zijn:

- diensten m.b.t het openbare internet
- combinatie met overige vormen van telecommunicatie
- ondersteuning bij de integratie met bestaande datacommunicatie-infrastructuur

Een ZSP mag, zolang de eisen uit de AORTA-documentatie niet in het gedrang komen:

- andere systemen dan die van GBZ en LSP op het DCN aansluiten
- koppelingen verzorgen tussen de aangesloten systemen en het openbare internet;
- een koppeling verzorgen met het DCN van andere ZSP

### **Diensten aan het LSP**

Diensten die een ZSP levert aan het LSP omvatten ten minste:

- een servicedesk ten behoeve van:
  - het melden van verstoringen
  - het melden van gepland onderhoud
  - het voeren van overleg ten behoeve van de instandhouding van de dienstverlening
  - het rapporteren over de geleverde prestatie
- het oplossen van al dan niet gemelde storingen
- het beheer van de aansluiting van het GBZ op het LSP

### **Aard en omvang van een ZSP**

ZSP's kunnen in aard en omvang verschillen.

Qua aard kan een ZSP bijvoorbeeld omvatten:

- een point-to-point verbinding tussen een ziekenhuisinformatiesysteem en het LSP op basis van DSL technologie via vaste dedicated redundante telecommunicatielijnen;
- een verzameling netwerkverbindingen tussen afzonderlijke HIS'en van een verzameling huisartsen enerzijds en het LSP anderzijds op basis van ADSL;
- een point-to-point verbinding tussen de locatie van een ASP en het LSP.

Qua omvang kan een DCN en/of een ZSP bijvoorbeeld omvatten:

- de datacommunicatie tussen het HIS van een landelijke verspreide groep huisartsen met de ZIM van het LSP;
- de datacommunicatie ten behoeve van de GBZ van één ziekenhuisinstelling met de ZIM van het LSP;
- de datacommunicatie ten behoeve van een verzameling GBZ'en die door één ASP wordt ondersteund en het LSP.

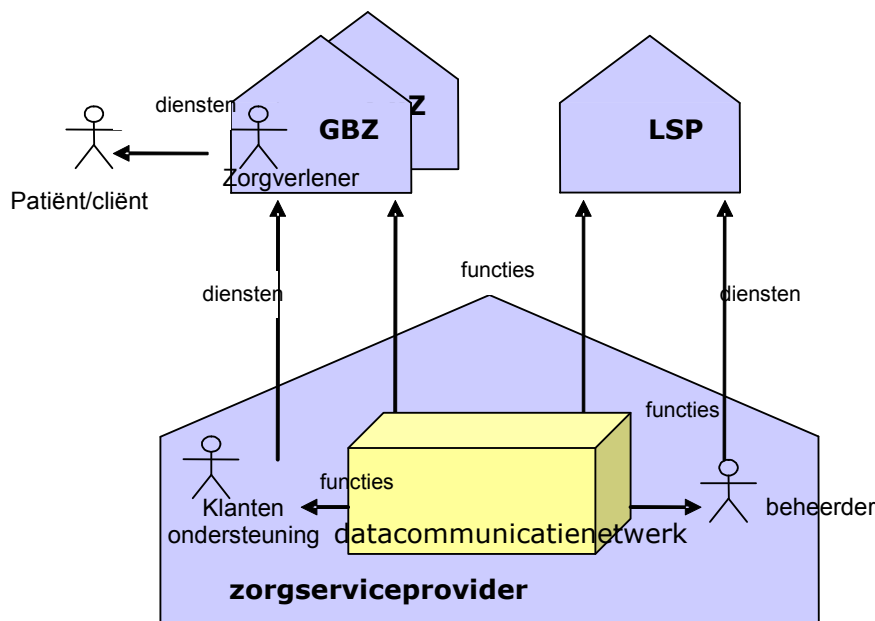
De bovenstaande voorbeelden zijn niet normatief. Er is pas sprake van een ZSP indien de datacommunicatiedienstverlener en diens netwerk voldoen aan de eisen zoals gespecificeerd in het Programma van Eisen voor een zorgserviceprovider.

## 3.2 Categorieën van eisen aan een ZSP

De eisen/wensen die worden gesteld aan een ZSP vallen uiteen in de volgende categorieën:

- *Functionaliteit-eisen/wensen aan de functie die (het DCN van) een ZSP vervult.* Het gaat hier om de *functies* die een ZSP realiseert onder een dienstverleningsovereenkomst met een GBZ. Deze eisen worden toegelicht in hoofdstuk 4.
- *Implementatie-eisen* waaraan een ZSP moet voldoen. Het gaat hier om eisen aan *de kwaliteit van en de wijze waarop een ZSP functies realiseert*. Het betreft hier onder meer eisen aan toe te passen technische middelen en voorschriften. Deze eisen worden toegelicht in hoofdstuk 5.
- *Exploitatie-eisen* waaraan een ZSP moet voldoen. Het gaat hier onder meer om de organisatorische inrichting van het gebruik en het beheer van de functies die een ZSP aan een GBZ beschikbaar stelt en de diensten die een ZSP dient te leveren. Het betreft hier bijvoorbeeld gebruiks- en beheer*procedures* die een ZSP in staat stellen diensten te leveren aan de buitenwereld, zijnde GBZ en LSP. Deze eisen worden toegelicht in hoofdstuk 6.

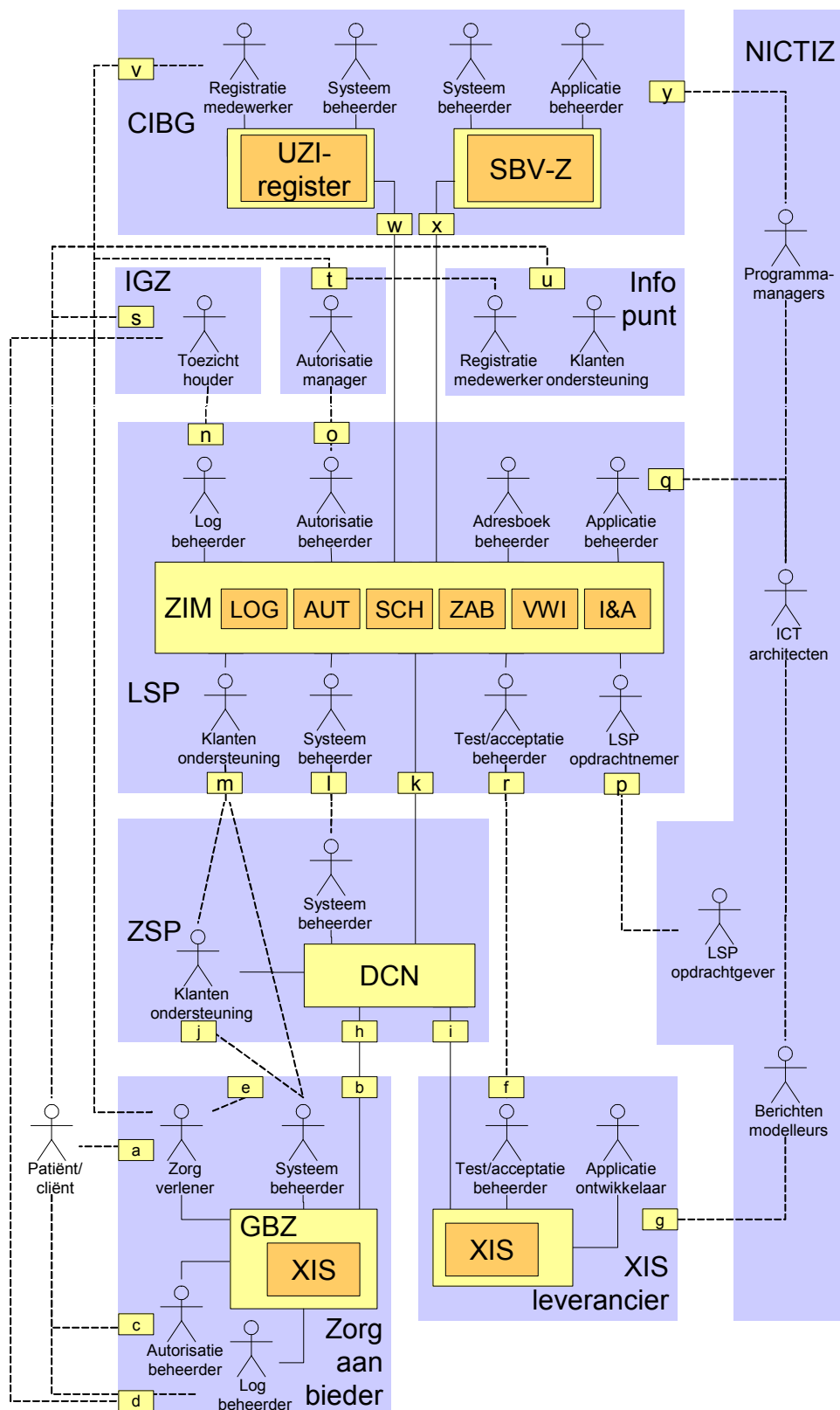
De onderstaande figuur toont hoe diensten en functies samenhangen binnen een ZSP:



**Figuur 2: Samenhang van diensten en functies binnen een ZSP**

### **3.3 Omgeving van een ZSP**

De onderstaande figuur toont hoe de diverse diensten en functies van een ZSP samenhangen met zijn omgeving.



**Figuur 3: Samenhang van diensten en functies tussen ZSP en omgeving**



De zorgaanbieder levert de volgende diensten:

- (a) de zorgverlener levert zorgdiensten aan de patiënt/cliënt en legt patiëntgegevens vast in zijn XIS en wisselt ze uit met andere zorgaanbieders via de ZIM.
- (b) de zorgverlener stelt met zijn XIS patiëntgegevens beschikbaar voor opvraag door andere zorgaanbieders via de ZIM.
- (c) de lokale autorisatiebeheerder biedt de patiënt/cliënt eventueel de mogelijkheid om een intern autorisatieprofiel in te stellen.
- (d) de lokale logbeheerder biedt de patiënt/cliënt en de toezichthouder eventueel de mogelijkheid om de interne en lokale toegangslag te raadplegen.
- (e) de systeembeheerder treedt op als eerste aanspreekpunt voor de gebruikers binnen de zorgaanbieder en meldt (niet afgebeeld) incidenten zonodig aan het LSP, de ZSP en/of de XIS-leverancier. Omgekeerd beantwoordt de systeembeheerder eventuele vragen en verzoeken van het LSP en de ZSP.

De XIS-leverancier van de zorgaanbieder levert de volgende diensten:

- (f) de XIS-test/acceptatie-beheerder test zijn XIS tegen de test-ZIM.
- (g) de XIS-applicatieontwikkelaar implementeert op verzoek van de LSP-opdrachtgever nieuwe functies en (versies van) gestandaardiseerde berichtformaten.

De ZSP van de zorgaanbieder levert de volgende diensten:

- (h) het DCN verbindt de XIS met de operationele ZIM.
- (i) het DCN verbindt de te testen XIS met de test-ZIM.
- (j) De ZSP-klantenondersteuning kan vragen en verzoeken van zorgaanbieders afhandelen.

Het LSP levert de volgende diensten:

- (k) het LSP levert verwijs-, routing, en zorgaanbieder/zorgverlener-selectiediensten aan de aangesloten XIS'en van zorgaanbieders.
- (l) de LSP-systeembeheerder regelt op verzoek van de ZSP-systeembeheerder de koppeling van XIS'en aan de ZIM via zijn DCN.
- (m) de LSP-klantenondersteuning handelt de vragen en verzoeken van zorgaanbieders en ZSP's af.
- (n) de LSP-logbeheerder doorzoekt op verzoek van de toezichthouder de toegangslag, al dan niet ten behoeve van een patiënt/cliënt. De adresboekbeheerder geeft op verzoek van de toezichthouder inzage in (wijzigingen van) postbusadressen van zorginformatiediensten.

- (o) de LSP-autorisatiebeheerder werkt op verzoek van de autorisatiemanager het landelijke autorisatieprotocol en de autorisatieprofielen van patiënten bij.
- (p) de LSP-opdrachtnemer rapporteert aan de LSP-opdrachtgever, over de diensten geleverd door het LSP en maakt afspraken met de LSP-opdrachtnemer over de eventuele uitbreiding danwel de bijstelling van de diensten.
- (q) de LSP-applicatiebeheerder implementeert op verzoek van de LSP-opdrachtgever nieuwe functies en (versies van) gestandaardiseerde berichtformaten.
- (r) de LSP-test/acceptatie-beheerder geeft XIS-leveranciers de mogelijkheid om hun XIS te testen op het voldoen aan de eisen voor een GBZ.

De IGZ levert de volgende diensten:

- (s) de toezichthouder controleert de rechtmatigheid van landelijke toegang tot patiëntgegevens door zorgaanbieders, dit zowel op eigen initiatief als op verzoek van patiënten/cliënten.

Een nader aan te wijzen partij levert de volgende diensten:

- (t) de autorisatiemanager zorgt namens beroepsverenigingen van zorgverleners en namens patiënten/cliënten voor de juiste instellingen van het landelijke autorisatieprotocol respectievelijk de autorisatieprofielen.

Het Informatiepunt BSN in de zorg en landelijk EPD levert de volgende diensten:

- (u) medewerkers handelen vragen en verzoeken af en zorgen ervoor dat ingediende bezwaren van patiënten/cliënten via de autorisatiemanager worden vastgelegd in de autorisatieprofielen.

Het CIBG levert de volgende diensten:

- (v) het UZI-register geeft na zorgvuldige registratie aan zorgaanbieders en zorgverleners UZI-passen en UZI-servercertificaten uit.
- (w) het UZI-register publiceert certificaten van uitgegeven UZI-passen en lijsten van ingetrokken UZI-certificaten, onder meer ten behoeve van het LSP.
- (x) de SBV-Z levert aan het LSP een berichtendienst voor het opvragen danwel het verifiëren van het BSN van een patiënt/cliënt.
- (y) de applicatieontwikkelaar implementeert op verzoek van de LSP-opdrachtgever nieuwe functies en (versies van) gestandaardiseerde berichtformaten.

De menssymbolen in de figuur vertegenwoordigen de aanspreekpunten voor de verschillende diensten. Hiermee wordt geenszins bedoeld voor te schrijven op welke manier de getoonde partijen hun interne organisatie moeten inrichten.

### 3.4 Grenzen van een ZSP

Zoals Figuur 3 toont is een ZSP meer dan het DCN: het omvat alle aspecten van implementatie van netwerkvoorzieningen (ten behoeve van AORTA) bij de zorgaanbieder en bij het LSP, ondersteuning van de zorgaanbieder, samenwerking met LSP-systeembeheer en exploitatie door de datacommunicatie leverancier.

Ook de XIS-leverancier blijft een belangrijke rol spelen, bijvoorbeeld:

- Bij de ontwikkeling van een XIS zal een XIS-leverancier zich moeten conformeren aan GBZ-eisen en kan de XIS-leverancier een XIS-typekwalificatie voor zijn XIS verwerven. Voor het uitvoeren van de tests die hiervoor nodig zijn, kan de XIS-leverancier een ZSP inschakelen om een verbinding met de test-ZIM op het LSP te realiseren.
- Bij het beheer van een XIS kan de zorgaanbieder diverse taken (hosting, technisch beheer, applicatiebeheer) uitbesteden aan een XIS-leverancier. In geval van ASP zullen meerdere zorgaanbieders dat gezamenlijk doen bij één XIS-leverancier. In voorkomende gevallen kan de ASP namens de zorgaanbieder contact onderhouden met de ZSP ten behoeve van de klantondersteuning en het systeembeheer van de GBZ. In al deze gevallen blijft de zorgaanbieder verantwoordelijk.

Een zorgaanbieder kan meerdere ZSP's inschakelen voor één GBZ. Een zorgaanbieder met een ICT-afdeling kan deels ook zijn eigen ZSP zijn. Al deze nuances zijn weggelaten in Figuur 3.

De exacte grens tussen ZSP en GBZ kan verschillen per situatie, maar meestal loopt die door de netwerkaansluiting(en) van de aangesloten systemen die onderling patiëntgegevens uitwisselen conform AORTA. De zorgaanbieder en netwerkdienstverlener moeten die grens bepalen, zodat bij kwalificatie van beide duidelijk is aan welke eisen moet worden voldaan.

In de loop van de tijd kan een ZSP wijzigen. Zo kan bijvoorbeeld een ZSP beginnen met de aansluiting van de HIS van een beperkt aantal huisartsen en het aantal, soort en verdeling van XIS en GBZ laten groeien. In voorkomende gevallen kunnen ZSP's met elkaar fuseren en/of hun dienstverlening aan GBZ beëindigen of uitbreiden.

De grenzen van een ZSP worden in principe gevormd door één of meer netwerkaansluitingen waar de fysieke netwerkinfrastructuur van een GBZ (of diens ASP) is verbonden met de fysieke netwerkinfrastructuur van een ZSP. In de meeste gevallen zal een deel van de fysieke netwerkinfrastructuur van een ZSP (moeten) worden opgesteld in ruimten van een GBZ.

Een bijzonder geval is het ASP-model, waarbij deelnemende zorgaanbieders voor hun GBZ'en en de aansluiting daarvan op het LSP gebruik maken van gemeenschappelijke voorzieningen. Dat is toegestaan, maar de eisen die AORTA stelt ten aanzien van ZSP's en GBZ'en moeten wel gewaarborgd blijven. In het bijzonder geldt hier dat er een logische scheiding moet blijven tussen de zorgaanbieders c.q. hun (virtuele) systemen, zodat patiëntgegevens niet uitgewisseld worden op een wijze die in strijd is met wat AORTA beoogt.

### 3.5 ZSP-kwalificatie

Om te mogen aansluiten op het LSP dient een GBZ onder meer gebruik te maken van een gekwalificeerde ZSP. Het aansluiten van een zorgaanbieder op het LSP via een ZSP geschiedt op twee niveaus, zie ook [Technische architectuur]:

- op *netwerkniveau* wordt een GBZ als geheel gekoppeld aan het LSP via een ZSP,
- op *applicatieniveau* wordt iedere XIS-applicatie binnen dat GBZ afzonderlijk aangesloten via dezelfde ZSP.

Maar het is ook toegestaan om een GBZ, indien opgebouwd uit meerdere GBZ-delen (GBZ-id's), ieder deel met een eigen IP-adres afzonderlijk, via een ZSP, te koppelen met het LSP.

Daarvoor gelden de volgende voorwaarden:

- Er moet worden voldaan aan de *functionaliteits*-eisen die zijn toegelicht in hoofdstuk 4. Deze eisen dienen deels vooraf te worden getest door aansluiting op de testomgeving van het LSP.
- Er moet worden voldaan aan de *implementatie*-eisen en de *organisatie*-eisen die zijn toegelicht in de hoofdstukken 5 resp. 6. Deze eisen kunnen slechts beperkt vooraf worden getoetst. In sommige gevallen zal in de praktijk moeten blijken en worden getoetst of aan de eisen wordt voldaan.

Een ZSP-kwalificatie is een keurmerk dat op één tijdstip wordt verkregen en waarvan periodiek wordt gecontroleerd dat aan de gestelde eisen nog steeds is voldaan. In het [Kwalificatiecriteria ZSP] is gedefinieerd hoe het kwalificatieproces uitgevoerd wordt en wat de reikwijdte van een kwalificatie is, waarbij verwezen wordt naar van toepassing zijnde overeenkomsten.

### 3.6 Aansluitvoorwaarden versus gebruikerswensen

De ZSP-eisen zijn onder te verdelen in:

- *Aansluitvoorwaarden*, dit zijn de minimale eisen die door het GBZ worden gesteld aan een ZSP alvorens het DCN kan worden aangesloten op de GBZ. Alle eisen in hoofdstuk 4 zonder nadere aanduiding van dit document zijn aansluitvoorwaarden. Sommige eisen in hoofdstuk 5 en 6 van dit document zijn eveneens aansluitvoorwaarden.
- *Gebruikerswensen*, aanvullende eisen die door een zorgaanbieder kunnen worden gesteld aan een ZSP omdat de daardoor te realiseren mogelijkheden van de ZSP van nut zijn voor diens GBZ('en). Die eisen hebben het predikaat {wens}.

De wijze van toetsen van aansluitvoorwaarden en gebruikerswensen is opgenomen in [Kwalificatiecriteria ZSP].

### **3.7 Specificatie van eisen en wensen**

In dit document worden normatieve eisen en wensen toegelicht. Daarbij wordt de volgende conventie gehanteerd:

Eisen en wensen in dit document worden uniek geïdentificeerd door een kenmerk van de vorm AORTA·BI·ZSP·TT·CCC99:

- AORTA·BI staat voor de basisinfrastructuur in de zorg;
- ZSP staat voor het programma van eisen voor een ZSP;
- TT staat voor de typering van de eis (FE, IE of EE);
- CCC staat voor de categorie waarbinnen de eis of wens valt;
- e staat voor de aanduiding dat het een eis/wens betreft (in plaats van een ontwerpbeslissing of gebruiksscenario);
- 99 is het volgnummer van de eis.

Met behulp van deze identificatie kan binnen en buiten AORTA eenduidig aan specifieke eisen gerefereerd worden.

## 4 Functionaliteits-eisen

Dit hoofdstuk licht de *functionaliteits-eisen* toe waaraan een ZSP of diens DCN moet voldoen om te kunnen worden aangesloten op LSP en GBZ'en. Het gaat hier vooral om *functies* die een DCN moet kunnen uitvoeren.

### 4.1 Inleiding

Een DCN binnen een ZSP moet de volgende functies kunnen uitvoeren, ongeacht of de gebruikers die daadwerkelijk benutten:

- Datacommunicatiefuncties in opdracht van de XIS van een GBZ,
- Datacommunicatiefuncties in opdracht van het ZIM van het LSP

De datacommunicatiefuncties omvatten:

- (a) Het bieden van netwerktransport van data van GBZ naar de ZIM van het LSP en vice versa
- (b) Domain Name Systeem functies

In dit hoofdstuk zijn eisen die voortvloeien uit bijvoorbeeld de WGBO en de NEN 7510 nadrukkelijk niet opgenomen als aansluitvoorwaarde, omdat die eisen generiek van toepassing zijn op alle datacommunicatienetwerken in de zorgsector.

### 4.2 Datacommunicatiefuncties

#### 4.2.1 Connectiviteitsfuncties (CON)

Een DCN dient te voldoen aan de volgende connectiviteitseisen:

**CON · 01** Het DCN dient alle berichtuitwisseling tussen de ZIM/LSP en de GBZ'en, zoals gespecificeerd in de [Technische architectuur] mogelijk te maken.

**Doel:** Dit is nodig om zorgprocessen door landelijk uitwisseling van patiëntgegevens optimaal te kunnen ondersteunen.

**Gevolg:** Dit betekent voor een zorgaanbieder, zijn ICT-leveranciers en/of zijn ZSP dat zij mogelijk stappen zullen moeten zetten om huidige datacommunicatienetwerken en huidige dienstverlening zo aan te passen dat die voldoen aan de eisen die in het programma van eisen zijn gesteld.

**CON · 02** Het DCN dient ieder aangesloten GBZ toegang te bieden tot respectievelijk:

- de operationele ZIM,
- de test-ZIM,

**Doel:** Deze eis is nodig opdat GBZ'en soepel kunnen overschakelen van de ene ZIM naar de andere ZIM.

**Gevolg:** Dit betekent voor een ZSP dat zij de IP-koppelingen van zijn aangesloten GBZ'en met de verschillende ZIM-instanties moet hebben voorbereid, zodanig dat het overschakelen naar een andere ZIM transparant is. Zie voor een toelichting op deze eis ook de [Technische architectuur] §6.1.

**CON · 03** Het DCN dient een willekeurige GBZ te kunnen aansluiten, waarbij:

- een vast IP-adres wordt uitgegeven, afkomstig uit een IP-adresblok toegekend aan het DCN door het LSP,
- de ZSP zorgt voor een eventuele vertaling van adressen die intern in het ZSP-netwerk worden gebruikt naar IP-adressen die het LSP uitgeeft voor het subnet van de betreffende ZSP,
- Intern door de ZSP gebruikte adressering mag niet conflicteren met het landelijke LSP nummerplan.
- Uitgegeven IP-adressen in het blok van de ZSP worden door de (kandidaat-)ZSP bewaakt.

**Doel:** Deze eis is nodig opdat een GBZ uniek voor datacommunicatie kan worden geadresseerd, het kan hier gaan om een GBZ deel (met eigen GBZ-id) dat specifiek enkele XIS applicaties ontsluit. Een zorgaanbieder kan meerdere GBZ-delen hebben, deze kunnen als één GBZ worden beschouwd. De communicatie vindt plaats tussen gekende partijen, terwijl de ZSP zijn datacommunicatienetwerken met voldoende flexibiliteit kan inrichten.

**Gevolg:** Dit betekent voor een ZSP dat zij zorg moet besteden aan het ontwerp en de instandhouding van het datacommunicatienetwerk en van de administratieve organisatie. De technieken, processen en procedures van uitgifte en registratie van IP-adressen dient gestructureerd en beschreven te zijn. Daarnaast kan, doordat, omwille van de beveiliging, een IP-adres voor langere tijd aan een GBZ(-deel) is gekoppeld, geen gebruik gemaakt worden van de dynamische uitgifte protocollen van een IP-adres (zoals DHCP). Statische uitgifte via DHCP is wel toegestaan.

**CON · 04** {Wens} Het DCN dient IP-verkeer met een DCN van een andere ZSP (onafhankelijk van het LSP) mogelijk te maken.

**Doel:** Verwacht wordt dat in de toekomst voor bepaalde zorgtoepassingen, onder bepaalde voorwaarden (bijvoorbeeld ten aanzien van de beveiliging) directe datacommunicatie (op enig moment zonder tussenkomst van het LSP) tussen GBZ'en en hun ZPS's nodig is. Een voorbeeld hiervan zou het uitwisselen van omvangrijke visuele medische informatie (zoals röntgenbeelden) kunnen zijn.

**Gevolg:** Dit betekent voor een ZSP dat hun datacommunicatievoorzieningen en organisatie in voldoende mate op de toekomst voorbereid dienen te zijn.

**CON · 05** Het koppelvlak tussen de ZSP en het LSP moet voldoen aan de volgende specificaties:

- a. Gebaseerd op UTP;
- b. Snelheid:10/100/1000 Mb/s;
- c. Snelheden en duplex-mode worden fixed ingesteld.
- d. De koppeling vindt plaats op basis van laag 3 (IP-routering en geen laag 2-koppelingen vanwege complexiteit en stabiliteit).
- e. <Vervallen door wijziging #1824>.

- f. ZSP maakt gebruik van redundante koppelingen op de LSP entry points. Echter vanuit het LSP is de routing gebaseerd zijn op het IP-next-hop adres, waarbij het de verantwoordelijkheid is van de ZSP om te bepalen op welke locatie/systeem dit IP-adres actief is (bijvoorbeeld door middel van handmatig /VRRP /HSRP /GLBP, etc.).

**Doel:** Doel van deze eis is om voor het koppelvlak tussen ZIM en DCN te streven naar een zodanige standaardisatie dat een uniforme en stabiele implementatie van de ZIM mogelijk is die voor ieder DCN op gelijke wijze in stand kan worden gehouden en beheerd.

**Gevolg:** Het gevolg van deze eis voor een ZSP is dat in voorkomende gevallen zijn huidige datacommunicatievoorzieningen hiervoor dienen te worden aangepast.

**CON · 06** De ZSP dient als domeinscheiding en ten behoeve van monitoring functionaliteit, op de GBZ locatie een door de ZSP te beheren netwerkcomponent (laag 2 of 3) te plaatsen.

**Doel:** Doel van deze eis is om het domein van de ZSP te scheiden van het domein van de GBZ. Zodoende vormen gebeurtenissen in het netwerk van de ZSP in mindere mate een operationeel risico voor het netwerk van de GBZ en andersom. Daarnaast kan ter plekke van de scheidingvlak het netwerkverkeer bewaakt worden.

**Gevolg:** Het gevolg van deze eis voor een ZSP is dat deze installatie-, beheer- en onderhoudswerkzaamheden ter plaatse van een GBZ dient te verrichten. Een GBZ dient hiervoor ruimte en een aansluiting op het elektriciteitsnetwerk ter beschikking te stellen en de ZSP-medewerker toegang te verlenen tot de voorziening.

**CON · 07** De ZSP mag voor het verkeer tussen GBZ'en en het LSP geen DCN toepassen waarin onderdelen zijn opgenomen die gebaseerd zijn op het openbare internet.

**Doel:** Doel van deze eis is om ervoor te zorgen dat voor alle datacommunicatievoorzieningen aansprakelijkheden en afspraken bekend zijn bij ZSP, GBZ en LSP. Daarnaast acht Nictiz het (deel-)voorwaarde voor een voldoende mate van bescherming tegen bedreigingen van de integriteit, vertrouwelijkheid en authenticiteit van de gegevensuitwisseling tussen GBZ'en het LSP.

**Gevolg:** Het gevolg van deze eis voor een ZSP is dat zij voor het verkeer tussen GBZ'en en het LSP besloten netwerkvoorzieningen toepast die ofwel in eigen beheer ontwikkelt zijn danwel van een telecom carrier afgenomen worden. Deze eis is niet bedoeld om uit te sluiten dat een ZSP aan een GBZ de dienst levert van een aansluiting op het openbare internet (voor andere doeleinden). Zie ook overige beveiligingseisen.

**CON · 08** Het DCN moet ieder aangesloten GBZ toegang bieden tot het UZI-register via de routeerfunctie van het LSP.

**Doel:** Doel van deze eis is om ervoor te zorgen dat GBZ'en gegevens kunnen uitwisselen met de Certificate Authority van de certificaten die door het UZI-register zijn uitgegeven en (de enigen zijn die in dit kader) door de GBZ'en worden toegepast.

Gevolg: Het gevolg van deze eis voor een ZSP is onder meer dat zij hiervoor een DNS registratie dient te voeren en dat netwerkelementen het desbetreffende verkeer dienen toe te laten. Dus firewalls mogen dit niet tegenhouden.

**CON · 09** Het DCN moet een aangesloten GBZ via de routeerfunctie van het LSP toegang kunnen bieden tot de CA van het servercertificaat van de ZIM en alle CA's in diens vertrouwensketen voor LDAP en OCSP

Doel: Doel van deze eis is om ervoor te zorgen dat GBZ'en gegevens kunnen uitwisselen met de Certificate Authorities

Gevolg: Het gevolg van deze eis voor een ZSP is onder meer dat zij hiervoor een DNS registratie dient te voeren en dat netwerkelementen het desbetreffende verkeer dienen toe te laten. Dus firewalls mogen dit niet tegenhouden.

**CON · 10** De ZSP moet de voor het LSP aangewezen IP-reeks routeren naar het 'LSP entry point'.

Doel: Doel van deze eis is om alle verkeer naar het LSP bij het LSP af te leveren.

Gevolg: De ZSP moet het IP-adres handmatig dan wel via een routeringsprotocol dusdanig configureren dat deze op de next-hop IP-adres in het LSP wordt afgeleverd.

**CON · 11** Het gebruiken van NAT (Network Address Translation) mag geen negatieve invloed hebben op de communicatie tussen systemen en/of systemen onderling.

Doel: Gebruik van NAT moet transparant zijn en geen verstoringen veroorzaken.

Gevolg: Gevolg van deze eis is dat de ZSP moet nagaan of het gebruik van NAT invloed heeft op de gebruikte communicatie tussen systemen.

## 4.2.2 Domain Name System functies (DNS)

Een ZSP dient als volgt DNS-diensten te bieden:

**DNS · 01** Aansluiting op het LSP - De ZSP registreert in de DNS:

- alle host- en domeinnamen van alle op de ZSP aangesloten GBZ'en;
- de forwarding naar de DNS van het LSP voor alle zones waarvoor de ZSP niet authoritative is;

Doel: Doel van deze eis is om ervoor te zorgen dat aangesloten GBZ'en het huidige IP-adres kunnen bepalen van een bestemming die een GBZ enkel bij naam kent. In voorkomende gevallen dient deze voorziening er tevens toe om de naam van een afzender van het berichtenverkeer te achterhalen. Deze eis dient er tevens toe om de ZSP de mogelijkheid te geven om enigszins flexibel om te gaan met de toekenning van IP-nummers aan GBZ'en.

Gevolg: Het gevolg van deze eis voor een ZSP is dat zij technische en organisatorische voorzieningen dient te treffen voor de ontwikkeling en instandhouding van deze functionaliteit.

- DNS · 02** De ZSP beheert een authoritative DNS-server voor diens domein, zodanig dat:
- de ZSP de primaire DNS-server beheert;
  - het ZSP of LSP de secundaire DNS-server beheert;
  - per forward DNS-zone wordt ook een reverse DNS-zone aangemaakt;
  - voor ieder (sub-) domein (zowel voor forward als reverse zones) de DNS-server van het LSP slave kan zijn.

**Doel:** Deze eis dient verschillende doelen. In de eerste plaats dient het de duidelijkheid en daarmee de beveiliging dat er run-time precies één autoriteit is die voor dat domein weet welk IP-nummer bij welke naam van een GBZ hoort. Daarnaast draagt het inrichten van primaire en secundaire DNS-servers bij aan de continuïteit van de gegevensuitwisseling tussen GBZ en LSP. Indien de DNS server van de ZSP niet beschikbaar (meer) is wordt de secundaire DNS server van het ZSP of LSP nog geacht beschikbaar te zijn voor bij deze ZSP aangesloten GBZ' en. Als derde zorgt deze eis voor enige mate van onafhankelijkheid van LSP en ZSP. Het beheer van netwerken kan daardoor meestal zelfstandig worden uitgevoerd. Dit verlaagt de beheerlast van het LSP, terwijl een willekeurige ZSP toch in zekere mate een eigen inrichting kan kiezen.

**Gevolg:** Het gevolg van deze eis voor een ZSP is dat zij technische en organisatorische voorzieningen dient te treffen voor de ontwikkeling en instandhouding van deze functionaliteit.

- DNS · 03** Indien een ZSP subdomeinnamen beschikbaar stelt aan een GBZ dan gelden voor deze subdomeinnamen de volgende eisen:
- per subdomeinnaam maximaal 15 tekens;
  - de namen dienen voor de gebruiker betekenis te hebben;
  - aantal niveaus in subdomeinen is maximaal 3.

**Doel:** Deze eis beoogt de namen die bij gegevensuitwisseling worden gebruikt te standaardiseren en daarmee de ontwikkeling en instandhouding van GBZ'en, ZSP's en het LSP te vereenvoudigen.

**Gevolg:** Het gevolg van deze eis voor een ZSP is dat zij een controle van de uit te geven namen dient uit te voeren en daarvoor technische en/of organisatorische voorzieningen zal ontwikkelen en in standhouden.

- DNS · 04** De ZSP dient op verzoek van het LSP de DNS-caches te verversen.

**Doel:** Doordat (wijzigingen van) DNS informatie op verschillende ogenblikken vanuit verschillende bronnen en domeinen ontstaat en naar verschillende ZSP's gedistribueerd wordt kan het in voorkomende situaties noodzakelijk zijn om deze onderling te synchroniseren en te effectueren. Het LSP neemt daarbij het initiatief en verzoekt een ZSP landelijk informatie over te nemen en te effectueren voor het domein van die ZSP.

**Gevolg:** Het gevolg van deze eis voor een ZSP is dat zij voorbereid en beschikbaar dient te zijn om enkele netwerkbeheerhandelingen uit te voeren. Beschikbaarheidseisen zijn beschreven in hoofdstuk 5.

**DNS · 05** De ZSP heeft de DNS caching op GBZ en ZSP geminimaliseerd middels TTL.

**Doel:** Doel van deze eis is dat DNS wijzigingen ten behoeve van loadbalancing en failover transparant door het netwerk worden verwerkt.

**Gevolg:** Gevolg van deze eis is dat responsetijden niet meer gegarandeerd kunnen worden omdat gegevens niet meer in DNS gecached worden.

**DNS · 06** De ZSP forward de zones in AORTA-ZORG.NL waarvoor zij niet 'authoritative' is default naar de DNS van het LSP.

**Doel:** Doel van deze eis is dat iedere beheerorganisatie slechts zijn deel van de DNS tree beheert waardoor wijzingen snel door het netwerk prolongeren.

**Gevolg:** De DNS van de ZSP wordt onderdeel van de DNS-tree waardoor er meer afhankelijkheden tussen DNS-systemen optreden.

## 5 Implementatie-eisen

### 5.1 Inleiding

Een DCN van een ZSP moet de volgende kwaliteiten kunnen leveren:

- Beveiliging,
- Beschikbaarheid,
- Responstijden.

Het gaat hier om eisen die niet alleen afhangen van het door een ZSP geleverde DCN maar die ook afhangen van:

- de hardwareplatformen waarop deze draaien,
- overige ICT-voorzieningen als routers, firewalls, etc.

In dit hoofdstuk zijn eisen die voortvloeien uit bijvoorbeeld de WGBO en de NEN 7510 nadrukkelijk niet toegelicht, omdat die eisen generiek van toepassing zijn op alle data-communicatienetwerken in de zorgsector.

### 5.2 Beveiliging (BVL)

Een DCN dient te voldoen aan de volgende beveiligingseisen:

**BVL 01** De ZSP heeft een informatiebeveiligingsbeleid opgesteld en geïmplementeerd. Hierbij wordt aandacht besteed aan o.a. voldoende beveiligingsniveau van alle netwerkkoppelingen naast die van de eigen beheersystemen, LSP, GBZ'en, de SBV-Z, het UZI-register en {toekomst} het UZOVI-register.

**Doel:** Het doel van deze eis is om voldoende bescherming te krijgen tegen en inzicht in de bedreigingen van de integriteit, vertrouwelijkheid en authenticiteit van de gegevensuitwisseling tussen GBZ en LSP vanwege de koppelingen die de ZSP met de omgeving heeft. Hiertoe beoogt het voldoende organisatorische waarborgen te realiseren zodat het doel en het belang van informatiebeveiliging voldoende in de ZSP-organisatie wordt verankerd. Het informatiebeveiligingsbeleid dient de intenties van de leiding van de organisatie rond informatiebeveiliging weer te geven en de beleidsmaatregelen, uitgangspunten en gedragsregels ten aanzien van de informatiebeveiliging, met daarbij aangegeven welke zaken voor de instelling van wezenlijk belang zijn. Tevens vormt het een communicatiemiddel naar ZSP-medewerkers, zodat deze zich aan de geldende voorschriften, gedragsregels en maatregelen kunnen houden.

**Gevolg:** Het gevolg van deze eis is dat de ZSP organisatorische en technische maatregelen dient te treffen om een voldoende beveiligingsniveau te kunnen bereiken en in stand houden. Naast het opstellen van het beleidsdocument is het tevens belangrijk om het beleid te implementeren, te toetsen en regelmatig bij te stellen op basis van incidenten en regelmatig risicoanalyses uit te voeren.

**BVL · 02** De ZSP heeft haar informatiebeveiliging organisatorisch geborgd in de organisatie.

**Doel:** Het doel van deze eis is om de informatiebeveiliging te waarborgen en in stand te houden.

**Gevolg:** Het gevolg van deze eis is dat de ZSP organisatorische taken, bevoegdheden en verantwoordelijkheden in het kader van informatiebeveiliging toekent aan (het bestuur van haar organisatie en) alle ZSP-medewerkers.

**BVL · 03** De ZSP heeft beveiligingseisen geformuleerd ten aanzien van haar personeel.

**Doel:** Het doel van deze eis is om een voldoende niveau van de informatiebeveiliging te waarborgen en in stand te houden. Omdat in voorkomende gevallen ZSP personeel tot op een persoon herleidbare gegevens onder ogen kunnen krijgen. Bijvoorbeeld bij de analyse van problemen in het netwerk of bij werkzaamheden bij de (potentiële) GBZ is een maatregel zoals een geheimhoudingsverklaring noodzakelijk. Daarnaast dienen werknemers die op een ernstige wijze zich niet houden aan de vastgestelde procedures volgens een bekend gemaakt disciplinair proces beoordeeld c.q. gestraft te worden. Bij de beëindiging van de relatie met een werknemer of een externe partij wordt nagegaan welke risico's bestaan en worden te nemen maatregelen bepaald.

**Gevolg:** Het gevolg van deze eis is dat de ZSP, als onderdeel van het arbeidscontract met zijn personeel in voorkomende gevallen geheimhoudingsverklaringen opneemt en laat tekenen. De geheimhouding heeft betrekking op tot op persoon/patiënt herleidbare informatie en medische informatie. De ZSP dient disciplinaire procedures bekend te maken en te hanteren. Bij beëindiging van de relatie dient de ZSP mogelijke risico's te inventariseren en te managen. De ZSP dient een procedure te volgen dat bij beëindiging van de relatie met de werknemer of externe partij leidt tot intrekken van diens toegangsrechten.

**BVL · 04** De netwerkaanbieder heeft beveiligingseisen geformuleerd ten aanzien van de fysieke beveiliging en beveiliging van de omgeving.

**Doel:** Het doel van deze eis is om een voldoende niveau van de informatiebeveiliging te waarborgen en in stand te houden. Deze eis heeft onder meer ten doel de mogelijkheid van non-beschikbaarheid van systemen en informatie te verkleinen door de kans op grootschalige calamiteiten te beperken.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische voorzieningen dient te treffen. Zo dient kritische of gevoelige apparatuur voor informatieverwerking (zoals ICT hardware en bekabeling) te zijn opgesteld in beveiligde ruimten, omgeven door een goed gedefinieerde beveiligingsgrens, met passende toegangsbelemmeringen en ingangscntroles inclusief fysieke beveiliging tegen ongeoorloofde toegang, het toebrengen van schade en andere niet toegestane inmenging. Tevens zijn er voorzieningen getroffen tegen schade door brand, wateroverlast, explosies, ordeverstoringen en andere door natuurlijke, of door mensen veroorzaakte calamiteiten. Ook dient er een functionerende noodstroomvoorziening ingericht te zijn zodat in het geval van stroomuitval de integriteit van data gewaarborgd is.

**BVL · 05** De ZSP dient het LSP en aangesloten GBZ'en te vrijwaren van spam, virussen en overige dreigingen van andere systemen die –via het openbare internet of anderszins– toegang hebben tot het DCN van de ZSP.

**Doel:** Het doel van deze eis is om een voldoende niveau van de informatiebeveiliging te waarborgen en in stand te houden. Zo dienen onderlinge bedreigingen vanuit ontwikkel-, toets-, opleidings- en productievoorzieningen door (onder)scheiding te worden verminderd. Ook kunnen denial-of-service bedreigingen hierdoor beter worden weerstaan. Tevens dient de ZSP de beschikbare capaciteit van het netwerk en de in redelijkheid te verwachten groei in benodigde capaciteit en belasting in een actief proces te bewaken ten einde te voorkomen dat de dienstverlening in de toekomst in gevaar komt.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Binnen de bedrijfskritische systemen (bijv. netwerk-beheersysteem) zijn maatregelen noodzakelijk, zoals virusscanners, inbraak detectie systemen, etc. Ook worden maatregelen getroffen om invoer in de beschermde omgeving van kwaadaardige programmatuur te voorkomen.

**BVL · 06** De ZSP heeft eisen opgesteld betreffende toegangsbeveiliging.

**Doel:** Het doel van deze eis is om een voldoende niveau van de informatiebeveiliging te waarborgen en in stand te houden. Hiertoe moet elke (geregistreerde) gebruiker van de informatiesystemen (en –diensten) uniek identificeerbaar en traceerbaar zijn.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Hiertoe behoren eisen aan de gebruikersregistratie ten behoeve van gebruikers die toegang moeten hebben tot informatiesystemen. Er moet een registratie zijn van gebruikers die toegangspersmissie hebben tot informatiesystemen (en –diensten). Het betreffen hier de informatiesystemen van de (kandidaat) ZSP, bijvoorbeeld het netwerk management systeem. Het betreft hier alleen de applicaties die worden gebruikt ten behoeve van de (potentiële) GBZ'en/LSP en dus niet de financiële administratie van de (kandidaat) ZSP, mail, etc. De ZSP zal procedures willen opstellen, die aantoonbaar worden nageleefd, voor het melden en afmelden van gebruikers. Omdat als gebruikers niet bekend zijn, het onmogelijk is ze toe te laten tot de informatie, te controleren en rechten in te trekken. Daarnaast zijn procedures noodzakelijk voor het toewijzen van unieke gebruikersidentificaties. Ook de toegang via koppelingen met andere computersystemen vindt pas plaats nadat de authenticiteit van deze systemen is vastgesteld. Toegang tot toepassingen, systemen en netwerkvoorzieningen is zodanig ingericht dat toegang slechts mogelijk is met geldige bevoegdheden. Hiervoor zal een ZSP een autorisatiematrix willen opstellen die beschrijft welke bevoegdheden iedere medewerkerrol (ook in noodsituaties) heeft en welke procedure wordt gevolgd om deze te wijzigen. Een ZSP zal een beleid met regels en rechten voor toegang voor elke gebruiker of groep van gebruikers willen opstellen. In beheersmaatregelen en procedures wordt dat beleid geconcretiseerd.

**BVL · 07** De ZSP heeft eisen opgesteld betreffende continuïteitsbeheer.

**Doel:** Het doel van deze eis is om de continuïteit van de dienstverlening door de ZSP in voldoende mate te waarborgen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP een proces van continuïteitsbeheer willen implementeren. Hierbij wordt geadresseerd:

- het vaststellen en verminderen van risico's;
- het beperken van de gevolgen van incidenten die schade toebrengen;
- het zo spoedig mogelijk hervatten van de connectiviteit;
- het opstellen en testen van een continuïteitsplan.

Ook zal een ZSP hiervoor bedrijfsplannen en werkinstructies opstellen om na onderbreking en storing van kritische bedrijfsprocessen de bedrijfsactiviteiten in stand te houden of tijdig te herstellen. Hiervoor dienen ook verantwoordelijken te worden aangesteld die de taak hebben de continuïteitsplannen te beproeven en te onderhouden.

**BVL · 08** De ZSP heeft eisen opgesteld betreffende beveiligingsincidenten.

**Doel:** Het doel van deze eis is om een voldoende niveau van de informatiebeveiliging te waarborgen en in stand te houden.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP een audit-log moeten bijhouden en archiveren waarin uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging in worden vastgelegd en zal de ZSP kunnen aangeven waarom juist die gebeurtenissen van belang zijn en geen andere. Daarnaast zal de ZSP in procedures willen beschrijven hoe om te gaan met incidenten en hoe het gebruik en misbruik van het systeem wordt gesignaleerd en geregistreerd. Het is van belang dat aan de indiener van incidentmeldingen ook de verwerking ervan wordt gerapporteerd opdat de indiener ziet wat het nuttig effect van zijn bijdrage aan informatiebeveiliging is geweest.

## 5.3 Beschikbaarheid (BSC)

Een DCN dient te voldoen aan de volgende beschikbaarheidseisen:

**BSC · 01** De ZSP is ingericht om 24 uur per dag, 7 dagen per week beschikbaar te zijn voor het afhandelen van berichten tussen het LSP en de GBZ'en en tussen GBZ'en onderling.

**Doel:** Het doel van deze eis is om een voldoende niveau van continuïteit van de dienstverlening van de ZSP te waarborgen en in stand te houden, opdat GBZ'en en LSP vrijwel altijd gegevens met elkaar kunnen uitwisselen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. In de bedrijfsvoering van een ZSP mogen niet bij voorbaat tijdperioden gepland worden waarin netwerkverkeer tussen GBZ'en en het LSP niet mogelijk is. De ZSP zal haar infrastructuur zo inrichten dat de faalkans en de hersteltijd van componenten in overeenstemming zijn met de gestelde eisen.

**BSC · 02** <Vervallen door wijziging #1585>

**BSC · 03** <Vervallen door wijziging #1585>

**BSC · 04** Storingen mogen naar hun omvangklasse (zie ORG·06) en hun hersteltijd niet vaker voorkomen dan zoals opgenomen in onderstaande tabel:

| Hersteltijd:   |   | Kleiner dan 15 minuten | Tussen 15 minuten en 12 uur | Tussen 12 uur en 4 dagen | Meer dan 4 dagen |
|----------------|---|------------------------|-----------------------------|--------------------------|------------------|
| Omvang-klasse: |   |                        |                             |                          |                  |
|                | 1 | 4 maal per jaar        | 2 maal per jaar             | 1 maal per jaar          | 0 maal per jaar  |
|                | 2 | 12 maal per jaar       | 4 maal per jaar             | 2 maal per jaar          | 0 maal per jaar  |
|                | 3 | 12 maal per jaar       | 12 maal per jaar            | 4 maal per jaar          | 0 maal per jaar  |

**Doel:** Het doel van deze eis is om een voldoende niveau van continuïteit van de dienstverlening van de ZSP te waarborgen en in stand te houden, opdat GBZ'en en LSP vrijwel altijd gegevens met elkaar kunnen uitwisselen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. De ZSP zal haar infrastructuur zo inrichten dat de faalkans en de hersteltijd van componenten in overeenstemming zijn met de gestelde eisen.

**BSC · 05** De ZSP dient te voorzien in zodanige back-upvoorzieningen dat (enkelvoudig) falen van componenten niet resulteert in de uitval van connectiviteit- en DNS-diensten van de ZSP aan het LSP.

**Doel:** Het doel van deze eis is om een voldoende niveau van continuïteit van de dienstverlening van de ZSP te waarborgen en in stand te houden, opdat GBZ'en en LSP vrijwel altijd gegevens met elkaar kunnen uitwisselen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. De ZSP zal haar infrastructuur zo inrichten dat (enkelvoudig) falen van componenten niet resulteert in uitval van de dienstverlening.

**BSC · 06** De ZSP dient aan de zorgaanbieder aan te kondigen: aanvang, voortgang en einde van gebeurtenissen waarbij de functies van ZSP of LSP voor een GBZ geheel of gedeeltelijk niet beschikbaar zijn.

**Doel:** Het doel van deze eis is om tijdig passende maatregelen door een GBZ te kunnen voorbereiden en te effectueren indien tijdelijk de diensten van ZSP of LSP niet beschikbaar zijn.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures ontwikkelen en in stand houden die voor aankondiging van gebeurtenissen worden gevolgd.

**BSC · 07** De ZSP dient onderhoud gepland te laten plaatsvinden in de periode tussen 03:00 en 07:00 uur. Indien gepland onderhoud een onderbreking is van de functies van het DCN dan dient dat te worden opgevat als een verstoring en gelden hiervoor de eisen BSC-01 en BSC-04.

**Doel:** Het doel van deze eis is om gepland onderhoud een zo min mogelijk verstrend effect te laten hebben.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP onderhoudsprocedures ontwikkelen en in stand houden die voor het uitvoeren van onderhoud worden gevolgd. Ook zal de ZSP in voorkomende gevallen bepaalde componenten redundant willen uitvoeren.

**BSC · 08** Wanneer het DCN na onderhoud of storing door diens beheerder weer beschikbaar wordt gemaakt, dient de DCN-beheerder dit te melden aan de beheerders van het LSP en de betrokken GBZ'en.

**Doel:** Het doel van deze eis is om tijdig maatregelen die door een GBZ ten behoeve van het ZSP onderhoud is genomen te niet te doen alsmede om de betrokken zorgverleners te kunnen informeren.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures ontwikkelen en in stand houden die voor aankondiging van gebeurtenissen met betrekking tot onderhoud worden gevolgd.

## 5.4 Responstijden (RSP)

Een DCN dient te voldoen aan de volgende eisen m.b.t. responstijden:

**RSP · 01** De *netwerkroundtrip delay* tussen een aangesloten GBZ en het LSP dient in 90% van de gevallen minder dan 200 ms te bedragen.

**Doel:** Het doel van deze eis is om aan zorgverleners een tijdige uitwisseling van gegevens te kunnen waarborgen. Hiertoe zijn beperkingen gesteld aan de tijd die berichten in het netwerk van de ZSP door mogen brengen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft.

**RSP · 02** <Vervallen door wijziging #1635>.

**RSP · 03** Prioritering van netwerkverkeer naar het LSP moet mogelijk zijn.

**Doel:** Het doel van deze eis is om er voor te zorgen dat verkeer naar het LSP niet negatief wordt beïnvloed door het overige verkeer.

**Gevolg:** Het gevolg van deze eis is dat de ZSP adequate technische en organisatorische maatregelen treft. Afstemming tussen ZSP GBZ en ZSP LSP is hiervoor noodzakelijk.

## 6 Exploitatie-eisen

### 6.1 Organisatie (ORG)

Een ZSP dient te voldoen aan de volgende eisen t.a.v. zijn organisatie:

**ORG · 01** De ZSP dient een geldige inschrijving te hebben bij een Kamer van Koophandel.

Doel: Het doel van deze eis is om GBZ'en en het LSP de mogelijkheid te bieden om de ondernemingsgegevens van een ZSP te verifiëren.

Gevolg: Het gevolg van deze eis is dat de ZSP organisatorische maatregelen treft.

**ORG · 02** Indien een ZSP gebruik maakt van diensten van derden dan dient de ZSP op te treden als hoofdaannemer.

Doel: Het doel van deze eis is om voldoende waarborgen te krijgen met betrekking tot de aansprakelijkheid van de ZSP.

Gevolg: Het gevolg van deze eis is dat de ZSP adequate organisatorische maatregelen treft. Tevens hoeft een GBZ hierdoor geen anderen dan de ZSP aan te spreken op de diensten die de ZSP levert.

**ORG · 03** De ZSP dient, behoudens overmacht, deel te nemen aan de overlegsituaties die door het LSP worden georganiseerd.

Doel: Het doel van deze eis is om de verbetering en instandhouding van de diensten van de ZSP te bevorderen.

Gevolg: Het gevolg van deze eis is dat de ZSP personeel vrijmaakt om dergelijke overleggen voor te bereiden en bij te wonen.

**ORG · 04** {wens} De ZSP dient SLA's af te sluiten met de organisaties van de GBZ'en en met het LSP voor onderhoud en ondersteuning.

Doel: Het doel van deze eis is om een duidelijk en beschreven begrip te hebben over de door de ZSP aan het GBZ te leveren diensten en de voorwaarden waaronder zij worden geleverd.

Gevolg: Het gevolg van deze eis is dat de ZSP grondige organisatorische maatregelen treft. De ZSP zal hiervoor een service management en delivery proces willen inrichten.

**ORG · 05** De ZSP dient te beschikken over een goed bereikbare servicedesk ten behoeve van ondersteuning van de zorgaanbieders van de GBZ'en en het LSP. Deze servicedesk dient:

- op werkdagen tussen 08:00 en 17:00 uur bereikbaar te zijn;
- een inschatting te geven van de verwachte oplostermijn;
- regelmatig te rapporteren over de voortgang van de oplossing.

- voor het LSP buiten deze periode (tussen 08:00 en 17:00 uur op werkdagen) voor noodgevallen op een noodnummer bereikbaar te zijn;
- voor diens GBZ'en buiten de periode van 08.00-17.00 op werkdagen voor noodgevallen op een noodnummer bereikbaar te zijn;
- de servicedesk heeft een script om vragen via een vast protocol af te handelen.

Doel: Het doel van deze eis is om de dienstverlening van ZSP's aan GBZ'en en het LSP te waarborgen.

Gevolg: Het gevolg van deze eis is dat de ZSP grondige organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen de medewerkers van de servicedesk met service-, incident- of call-management instrumenten willen ondersteunen.

**ORG · 06** De ZSP dient voor het oplossen van problemen en correctief onderhoud een prioriteitsstelling te hanteren die gebaseerd is op de onderstaande classificering van aangemelde problemen:

- klasse 1: het DCN is (nagenoeg) onbeschikbaar. Hieronder valt de onbereikbaarheid van de ZIM;
- klasse 2: het DCN kan slechts voor een beperkte functionaliteit worden gebruikt
- klasse 3: het DCN vertoont hinderlijke tekortkomingen maar kan worden gebruikt

Doel: Het doel van deze eis is om te waarborgen dat het oplossen van problemen en het uitvoeren van onderhoud met correcte prioriteit ter hand kan worden genomen.

Gevolg: Het gevolg van deze eis is dat de ZSP grondige organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen de medewerkers van de servicedesk met service-, incident- of callmanagement instrumenten willen ondersteunen.

**ORG · 07** De ZSP vangt aan met het uitvoeren van correctief onderhoud per prioriteitgroep binnen de volgende termijnen:

- prioriteit 1: onmiddellijk
- prioriteit 2: binnen 4 uur gedurende de werkweek
- prioriteit 3: binnen 24 uur gedurende de werkweek

Doel: Het doel van deze eis is om te waarborgen dat het oplossen van problemen en het uitvoeren van onderhoud naar gelang hun prioriteit tijdig ter hand wordt genomen.

Gevolg: Het gevolg van deze eis is dat de ZSP grondige organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen de medewerkers van de servicedesk met een service-, incident- of callmanagement instrumenten willen ondersteunen.

## 6.2 Beheerfuncties (BEH)

Een DCN dient te voldoen aan de volgende eisen inzake beheer:

**BEH · 01** De beheerder van het DCN en diens vervangers dienen met telefoonnummers bekend te zijn bij de beheerder van het LSP, waarbij altijd (7x24 uur) ten minste één beheerder bereikbaar is en in staat is de nodige beheertaken uit te voeren.

**Doel:** Het doel van deze eis is om te waarborgen dat het ZSP altijd kan worden beheerd, opdat de gegevensuitwisseling tussen GBZ'en en LSP een optimale beschikbaarheid kent.

**Gevolg:** Het gevolg van deze eis is dat de ZSP organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen zijn beheermedewerkers van mobiele telecommunicatiemiddelen en middelen voor beheer op afstand willen voorzien.

**BEH · 02** De ZSP dient in staat te zijn op netwerkniveau te bepalen in welk domein een door een zorgaanbieder of het LSP aangemeld probleem zich bevindt.

**Doel:** Het doel van deze eis is om een voortvarende oplossing van een probleem te bevorderen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen een monitorinstrument willen inrichten waarmee een bij een probleem betrokken bericht kan worden gerelateerd aan het IP-adres van betrokken communicatiepartijen.

**BEH · 03** De ZSP dient op verzoek metingen te verrichten en te rapporteren aan het LSP over de geleverde en gebruikte bandbreedte per verbinding per GBZ binnen het netwerk. Bij voorkeur worden metingen proactief uitgevoerd en gelogd. Minimaal moet het mogelijk zijn 20 connecties tegelijk op verzoek te kunnen doormeten.

**Doel:** Het doel van deze eis is om capaciteit- en communicatieproblemen te voorkomen, te lokaliseren of op te lossen. Dat kunnen zowel problemen (blijken te) zijn waarvan de oorzaak gelegen is in het LSP, de GBZ'en of de (of enige andere) ZSP.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen adequate en bij voorkeur proactieve, monitorinstrumenten willen inrichten.

**BEH · 04** De ZSP dient maandelijks informatie aan het LSP te leveren over de frequentie en de tijdsduur dat netwerkverkeer tussen LSP en de GBZ'en niet mogelijk is geweest vanwege storingen in de ZSP.

**Doel:** Het uiteindelijke doel van deze eis is de optimale beschikbaarheid van GBZ'en. En in het kader daarvan het verkrijgen van inzicht in (mogelijkheden tot verbetering van) de prestatie van de ZSP (en diens netwerk). Een tweede doel betreft het toetsen van een GBZ aan de GBZ-eisen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische- en organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen adequate en bij voorkeur proactieve, monitorinstrumenten willen inrichten.

**BEH · 05** De ZSP dient achteraf per maand aan het LSP en de GBZ'en aan te kunnen geven wat de hersteltijden zijn geweest van alle storingen.

**Doel:** Het uiteindelijke doel van deze eis is de optimale beschikbaarheid van GBZ'en. En in het kader daarvan het verkrijgen van inzicht in (mogelijkheden van verbetering van) de prestaties van de ZSP (en diens netwerk).

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal een ZSP in voorkomende gevallen adequate en bij voorkeur proactieve, monitorinstrumenten willen inrichten.

**BEH · 06** De ZSP dient gepland onderhoud indien dat tot onderbreking van de functies van het DCN leidt minimaal 5 werkdagen van tevoren aan te kondigen aan de betrokken zorgaanbieders en het LSP.

**Doel:** Het doel van deze eis is om zonodig tijdig passende maatregelen door een GBZ te kunnen laten voorbereiden en te effectueren indien tijdelijk de diensten van ZSP niet beschikbaar zijn.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures ontwikkelen en in stand houden die voor aankondiging van onderhoudsgebeurtenissen worden gevolgd.

**BEH · 07** De ZSP dient het verhuizen van netwerkverbindingen van de GBZ tussen de ZSP's en de GBZ'en mogelijk te maken en dient de verhuizing binnen 3 weken te realiseren gerekend vanaf het moment dat de benodigde (telecommunicatie-) infrastructuur bij de nieuwe ZSP-dienstverlener aanwezig en bruikbaar is.

**Doel:** Het doel van deze eis is om vrije marktwerking te bevorderen door belemmeringen voor GBZ'en, om van ZSP te wisselen, te verminderen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures ontwikkelen en in stand houden die bij het verhuizen van netwerkverbindingen wordt gevolgd. Voor zover nodig zal de ZSP de huidige routing binnen haar netwerk voor de betreffende GBZ'en teniet doen.

**BEH · 08** De ZSP is verplicht de noodzakelijke medewerking te verlenen bij het overgaan van een GBZ van de ene ZSP naar een andere ZSP zodanig dat dit geen verlies van continuïteit tot gevolg heeft.

**Doel:** Het doel van deze eis is om vrije marktwerking te bevorderen door belemmeringen voor GBZ'en, om van ZSP te wisselen, te verminderen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures ontwikkelen en in stand houden die bij het verhuizen van netwerkverbindingen wordt gevolgd. Voor zover nodig zal de ZSP de huidige routing binnen haar netwerk voor de betreffende GBZ'en teniet doen.

## 6.3 Gebruikerondersteuning (GBO)

Een ZSP dient te voldoen aan de volgende eisen inzake gebruikerondersteuning:

**GBO · 01** De ZSP biedt gebruikersondersteuning aan en biedt een serviceniveau dat is afgestemd op de prioriteit (ernst) van het aangemelde probleem. Services die o.a. worden geboden zijn ondersteuning bij de aansluiting en opereren als vraagbaak m.b.t. de aansluiting en het bieden van hulp bij het gebruiken van de functies van de ZSP.

**Doel:** Het doel van deze eis is om de acceptatie van landelijke informatie-uitwisseling van gegevens onder zorgverleners te bevorderen en het gebruik van de diensten van de ZSP te vergemakkelijken en verstoringen daarin te voorkomen en te verhelpen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures ontwikkelen en in stand houden die bij het ondersteunen van gebruikers worden gevolgd.

**GBO · 02** De ZSP dient problemen die door zorgaanbieders worden gemeld af te handelen en te beheren.

**Doel:** Het doel van deze eis is om de kwaliteit van de landelijke informatie-uitwisseling van gegevens onder zorgverleners te bevorderen, de diensten van de ZSP te verbeteren en verstoringen te signaleren, te voorkomen en te verhelpen.

**Gevolg:** Het gevolg van deze eis is dat de ZSP grondige technische en organisatorische maatregelen treft. Zo zal de ZSP procedures willen ontwikkelen en in stand houden die bij het afhandelen en beheren van meldingen worden gevolgd. In voorkomende gevallen zal een ZSP een incident-management instrument inzetten.

**GBO · 03** {Wens} De ZSP dient een servicedesk te hebben voor problemen die door zorgaanbieders worden gemeld over functionaliteit met betrekking op GBZ, ZSP en LSP systemen. Deze servicedesk dient open te staan voor alle klanten, ook die niet tot eigen 'afnemers' behoren.

**Doel:** Het doel van deze eis is om een servicedesk te bieden waarbij storingen en problemen kunnen worden gemeld en bewaakt.

**Gevolg:** Een ZSP zal, afhankelijk van de aard van het incident en de geleverde diensten aan de zorgaanbieder, namens de zorgaanbieder het contact voeren met het LSP.

## **7 Voorbeelden van een ZSP**

Dit hoofdstuk beschrijft informatief enkele voorbeelden van ZSP's.

### **7.1 Inleiding**

ZSP's kunnen verschillende gedaanten hebben, afhankelijk van de omvang van de aangesloten zorginstelling, maar ook afhankelijk van de technologie waarop de XIS, ASP en/of ZSP gebaseerd is en de dienstverlening die een ZSP biedt. Onderstaande voorbeelden geven hiervan een indruk, zijn niet normatief, vormen mogelijkwijs geen realistisch commercieel bedrijfsmodel en gelijkenis met een bestaande situatie berust op toeval.

### **7.2 Voorbeeld 1**

Dit voorbeeld betreft een ZSP die regionaal opereert. Het ZSP verbindt uitsluitend HIS'en met het LSP, door middel van een verzameling netwerklijnen die de ZSP afneemt van een of meer telecom-operators. De ZSP is hierbij hoofdaannemer in relatie tot de telecom-operators. De ZSP draagt zorg voor aanvraag en het toezicht op de installatie van een telecomverbinding bij de telecom-operator ten behoeve van de huisartsen. De telecom-operator draagt zorg voor de aanleg naar en installatie in het pand van de huisarts van een telecomverbinding. De ZSP verzorgt de installatie van de netwerkinfrastructuur (bijvoorbeeld een ADSL-modem) in het pand van de huisarts en de configuratie en het aansluiten van de verbinding met het LSP. De ZSP heeft mogelijkwijs een organisatorische relatie met een zorgkoepel en of een XIS-leverancier en verzorgt tegelijkertijd met de installatie bijvoorbeeld de uitrol van een upgrade van het betreffende HIS ten behoeve van de aansluiting op het LSP.

Ieder van deze huisartsen zal bij verstoring van bijvoorbeeld de communicatie met hun regionale apothekerinformatiesystemen een beroep doen op de servicedesk van de regionale ZSP. De ZSP verzorgt de eerstelijns servicedesk voor het aangesloten GBZ en voert de communicatie met beheerders van het LSP. Beheerders van het LSP voeren zonodig overleg met de servicedesks van andere zorginstellingen ten behoeve van het afhandelen van incidenten. De servicedesk is zodoende het enige aanspreekpunt voor de zorgaanbieder voor wat betreft de landelijke uitwisseling van informatie met overige zorginstellingen.

### **7.3 Voorbeeld 2**

Dit is een voorbeeld van een ZSP die lokaal opereert. Het ZSP verbindt heel verschillende XIS'en binnen verschillende panden van één grote zorgaanbieder zoals een ziekenhuis, die één GBZ vormen, met het landelijk schakelpunt door middel van een verzameling netwerklijnen die de ZSP huurt van een of meer telecom-operators. De ZSP is hierbij hoofdaannemer in relatie tot de telecom-operators. De ZSP is tevens mogelijkwijs interne netwerkleverancier en deel van de organisatie van de zorginstelling. De ZSP draagt, namens de zorgaanbieder, zorg voor aanvraag en het toezicht op de installatie van telecomverbindingen in de panden van de zorginstelling. De ZSP doet de installatie van de netwerkinfrastructuur in de panden van de zorginstelling en de configuratie en het aansluiten van de verbindingen tussen XIS'en en het LSP.

Een zorgverlener van de zorginstelling zal bij verstoring van de communicatie met willekeurig andere zorginformatiesystemen een beroep doen op een servicedesk. De GBZ verzorgt zelf de eerstelijns servicedesk voor de zorgverleners van de GBZ en voert de communicatie met de beheerders van de XIS'en die in het ziekenhuis in gebruik zijn en met het LSP. Beheerders van het LSP voeren zondig overleg met de servicedesks van andere zorginstellingen ten behoeve van het afhandelen van incidenten. De servicedesk is zodoende het enige aanspreekpunt voor de zorgaanbieder voor wat betreft de landelijke uitwisseling van informatie met overige zorginstellingen.

## **7.4 Voorbeeld 3**

Dit is een voorbeeld van een ZSP die landelijk opereert. Het ZSP verbindt landelijk verspreide GBZ'en met ieder geheel verschillende XIS'en. Het ZSP kan deel uitmaken van de organisatie van een grote telecom-operator die in hoofdaanneming netwerkdiensten inhuurt van een grote telecom-carrier. De zorgaanbieders dragen zorg voor de aanvraag en het toezicht op de installatie van telecomverbindingen en netwerkinfrastructuur in hun panden door de ZSP. De ZSP doet de installatie van de netwerkinfrastructuur in de panden van de zorginstellingen en de configuratie en het aansluiten van de verbinding tussen de XIS van de GBZ en het LSP.

Ieder van de zorgaanbieders zal bij verstoring van de communicatie met willekeurig andere zorginstellingen een beroep doen op de servicedesk. De ZSP verzorgt de eerstelijns servicedesk voor de aangesloten GBZ'en en voert de communicatie met beheerders van het LSP. Beheerders van het LSP voeren zondig overleg met de servicedesks van andere zorginstellingen ten behoeve van het afhandelen van incidenten. De servicedesk is zodoende het enige aanspreekpunt voor de aangesloten zorgaanbieders voor wat betreft de landelijke uitwisseling van informatie met overige zorginstellingen.

## **7.5 Voorbeeld 4**

Dit is een voorbeeld van een ZSP die landelijk opereert. De ZSP verbindt één ASP met het LSP, door middel van enkele netwerklijnen die de ZSP huurt van een of meer telecom-operators. De ASP verbindt de panden van een verzameling zorgaanbieders, die ieder verantwoordelijk zijn voor hun eigen GBZ, met een applicatieserver waarop een of meer XIS'en geïnstalleerd zijn. De ASP neemt een verzameling netwerkverbindingen af van een of meer telecom-operators. De ZSP is hierbij hoofdaannemer in relatie tot de telecom-operator ten aanzien van de netwerkverbindingen tussen de ASP installatie en het LSP. De ASP is hierbij wellicht hoofdaannemer in relatie tot de telecom-operators ten aanzien van de netwerkverbindingen tussen de ASP-installatie en de panden van de zorgaanbieders.

De ZSP draagt zorg voor aanvraag en het toezicht op de installatie van enkele telecomverbindingen bij de telecom-operator ten behoeve van de koppeling van de ASP en het LSP. De telecom-operator draagt voor deze verbindingen zorg voor de aanleg naar en installatie in het pand van de ASP. De ZSP verzorgt de installatie van de netwerkinfrastructuur in het pand van de ASP en de configuratie en het aansluiten van de verbinding met het LSP.

De ASP draagt zorg voor aanvraag en het toezicht op de installatie van een verzameling telecomverbindingen bij de telecom-operator ten behoeve van de koppeling van de ASP en de panden van de aangesloten zorgaanbieders. De telecom-operator draagt voor deze

verbindingen zorg voor de aanleg naar en installatie in het pand van de ASP. De ASP verzorgt de installatie van de netwerkinfrastructuur in het pand van de ASP en de configuratie en het aansluiten van ieder XIS.

Ieder van deze zorgaanbieders zal bij verstoring van de communicatie met willekeurig andere zorginstellingen een beroep doen op de servicedesk van de ASP. De ASP verzorgt de eerstelijns servicedesk en voert de communicatie met beheerders van het LSP. Beheerders van het LSP voeren zonodig overleg met de servicedesks van andere zorginstellingen ten behoeve van het afhandelen van incidenten. De ASP is het enige aanspreekpunt voor de zorgaanbieder. Het LSP is het enige aanspreekpunt voor de ASP.

## **7.6 Voorbeeld 5**

Dit is een voorbeeld waarbij meerdere ZSP's binnen één GBZ actief zijn. In een ziekenhuis met meerdere GBZ-applicaties van verschillende leveranciers, wil men deze applicaties ieder via een eigen IP-adres met het LSP koppelen. Er worden dus meerdere IP-adressen aan het GBZ uitgedeeld (een GBZ wordt opgedeeld met meerdere GBZ-id's). Nu wil het ziekenhuis ook dat een bepaalde applicatie via een ander ZSP contact maakt met het LSP. Hierdoor is het mogelijk dat meerdere ZSP's de koppeling verzorgen van één GBZ. Voorwaarde is wel dat de applicaties die via verschillende ZSP's aan het LSP gekoppeld zijn ook IP-adressen uitgedeeld krijgen uit de range IP-adressen die aan het gebruikte ZSP is toegewezen door het LSP.