

Specificatie van diensten en functies binnen het LSP



NICTIZ

Nationaal ICT Instituut in de Zorg

Status : concept
Versie : [1.2]

Ref : [aanbesteding LSP]
Datum : [19 maart 2005]

Postbus 262, 2260 AG Leidschendam
Overgoo 11, 2266 JZ Leidschendam
telefoon: (070) 317 34 50
e-mail: info@NICTIZ.nl / www.NICTIZ.nl

Versiebeheer:

versie:	datum:	korte omschrijving aanpassing:	Ref.:	status:
1.0	29 oktober 2004	Eerste versie ter ondersteuning CIBG	CIBG	Definitief
1.1	1 november 2004	Ter toetsing op verzoek van min. VWS door DCE Consultants	CIBG	Definitief
1.2	14 maart 2005	Ter toetsing in een consultatieronde voorafgaand aan Europese aanbesteding LSP	LSP	concept
2.0	gepland april 2005	Verwerking consultatieronde		

Referenties:

versie:	datum:	auteur	titel:
4.0	15 oktober 2004	NICTIZ	Architectuurontwerp basisinfrastructuur in de zorg
2.1	17 november 2004	NICTIZ	Specificatie van de basisinfrastructuur in de zorg
2.0	1 maart 2004	NICTIZ	Implementatiehandleiding HL7v3 infrastructurale domeinen
2.2	10 september 2004	NICTIZ	Implementatiehandleiding HL7v3 Zorg Informatie Makelaar
1.4	26 januari 2005	NICTIZ	Implementatiehandleiding HL7v3 waarneming huisartsen
2.2	30 juli 2005	NICTIZ	Implementatiehandleiding HL7v3 medicatieberichten
Ballot 7	mei 2004	NICTIZ	HL7 versie 3
1.0	10 december 2004	DCE Consultants	Audit AORTA architectuur en specificaties basisinfrastructuur gezondheidszorg
IRM ZO 05.013	3 maart 2005	KPMG	Onderzoek AORTA-specificaties

Inhoudsopgave:

1	Inleiding	5
1.1	Achtergrondinformatie	5
1.2	Doel van dit document	6
1.3	Doelgroep van dit document	6
1.4	Documentstructuur en relaties met andere documenten	6
1.5	Status van dit document	8
1.6	Uitgangspunten	8
1.7	Groeimodel: toekomstige diensten en openstaande punten	9
2	Het Landelijk Schakelpunt in vogelvlucht	11
2.1	Introductie en omgeving van het LSP	11
2.2	Omschrijving van diensten en functies op hoofdlijnen	12
3	Diensten van het Landelijk Schakelpunt	18
3.1	Algemeen	18
3.2	Diensten geleverd door het LSP	18
3.2.1	Informatie- en routeringsdiensten	18
3.2.2	Dienstverlening aan ZSP's	20
3.2.3	Dienstverlening aan Registerhouders	21
3.2.4	Beheerdiensten	21
3.2.4.1	<u>Toegangbeheer</u>	21
3.2.4.2	<u>Systeembeheer</u>	21
3.2.4.3	<u>Applicatiebeheer</u>	22
3.2.4.4	<u>Beheer IP-nummerplan</u>	23
3.2.4.5	<u>Beheer domeinnamen</u>	24
3.2.4.6	<u>Beheer van OID's</u>	24
3.2.4.7	<u>Productie en inspectie van een Audit Trail log bestand</u>	24
3.2.5	Ondersteuning van ZSP's d.m.v. een helpdesk	25
3.2.6	Opleveren managementinformatie	26
3.2.7	Acceptatietestdiensten	26
4	Functies van de Zorg Informatie Makelaar	28
4.1	Definitie van ZIM	28
4.2	Informatie & routeringsfuncties	29
4.3	Autorisatiebeheer	34
4.4	Toegangslogbeheer	37
4.5	Klantenondersteuning	39
4.6	Systeembeheer	40
4.7	Test-beheer	47
4.8	Applicatiebeheer	49
4.9	Aansturing en verantwoording	50
4.10	Connectiviteit	52
4.11	Beveiliging	54
4.12	Beschikbaarheid	55

4.13	Responstijden	56
4.14	Capaciteit.....	57
4.15	Schaalbaarheid	58
4.16	Betrouwbaarheid	58
4.17	Systeembeheer	59

5	Fasering van de te leveren diensten en functies	60
5.1	Inleiding	60
5.2	Ontwikkelfase.....	60
5.3	Integratietest met zorginformatiesystemen in het veld	60
5.4	Acceptatietest & Operationele fase	61
6	Bijlagen	63
6.1	Normatieve referenties	63
6.2	Afkortingen:.....	64

1 Inleiding

1.1 Achtergrondinformatie

Het Nationaal ICT Instituut in de Zorg (NICTIZ) richt zich op de totstandkoming van een betere informatievoorziening rondom en voor de patiënt/cliënt met behulp van ICT, met als doel een hogere doelmatigheid en kwaliteit in de zorg. In de dagelijkse praktijk in de zorg, blijkt er veel behoefte aan patiëntgegevens die niet binnen de eigen organisatie voorhanden zijn maar bij andere zorginstellingen aanwezig zijn. NICTIZ werkt met en voor betrokken partijen aan de ontwikkeling van een landelijke ICT-infrastructuur in de zorg (AORTA). De realisatie van een landelijk elektronisch medicatiedossier, een landelijk elektronisch waarneemdossier voor huisartsen en het 100% elektronisch declareren in 2006 zijn speerpunttoepassingen op weg naar een volledig Landelijk Elektronisch Patiënten Dossier (LEPD). Deze toepassingen maken gebruik van AORTA.

In 2002 is gestart met de opzet van het AORTA-1 programma waarin de architectuur en de wijze waarop een landelijke infrastructuur tot stand zou kunnen komen, is aangegeven. NICTIZ is in 2003 een regionaal versnellingsprogramma gestart, bestaande uit 5 regio's met als doel om met de bestaande standaarden ervaring op te doen met de technische mogelijkheden en de organisatorische consequenties rondom het elektronisch medicatiedossier. Hierbij is in 2004 vastgesteld, dat met bestaande standaarden onvoldoende perspectief geboden kan worden om te komen tot een landelijk medicatiedossier.

Inmiddels is door de minister van VWS besloten tot de ontwikkeling van een Landelijke Schakelpunt. Het Landelijk Schakelpunt is een belangrijk onderdeel van de basisinfrastructuur in de zorg en maakt het mogelijk, dat gestandaardiseerde berichten veilig en efficiënt uitgewisseld worden tussen alle zorgpartijen. Er is gekozen voor een integrale benadering die bestaat uit het centraal ontwikkelen en exploiteren van een Landelijk Schakelpunt (LSP) en het decentraal aanpassen en aansluiten van bestaande zorginformatiesystemen op de landelijke basisinfrastructuur.

Het LSP dient tijdens een eerste exploitatietermijn de drie voornoemde landelijke speerpunttoepassingen te faciliteren, het e-medicatiedossier, het e-waarneemdossier huisartsen en e-declareren.

De onderliggende architectuur voorziet bovendien in toekomstige, additionele toepassingen die gezamenlijk uiteindelijk moeten evolueren naar een landelijk dekkend elektronisch patiëntendossier (LEPD).

De totale AORTA-documentatie van de basisinfrastructuur in de zorg, waaronder de specificaties van het LSP, vormt de basis voor het LEPD inclusief de eerste speerpunttoepassingen.

1.2 Doel van dit document

Het Landelijk Schakelpunt (LSP) vervult een cruciale rol in de aanstaande nationale koppeling van alle zorginformatiesystemen.

Dit document en onderliggende documenten vormen de specificatie van diensten en functies ten behoeve van de realisatie van het Landelijk Schakelpunt. Dit document bevat de specificaties van een tweetal hoofdonderdelen: een aan te bieden centraal informatiesysteem (de Zorg Informatie Makelaar c.q. de ZIM) en de te ontwikkelen en te leveren diensten in een operationele situatie. Met het LSP wordt de organisatie bedoeld die diensten levert aan het zorgveld en daarbij onder andere gebruik maakt van de technische ICT-infrastructuur van de ZIM.

Kandidaat-aanbieders dienen primair dit document te beschouwen als bron van eisen en wensen. Bijbehorende onderliggende documenten worden benoemd in paragraaf 1.4.

Diensten en functies zijn hier beschreven als eisen aan het LSP. Door de dynamiek in de toepassingen is gekozen voor een groeimodel waarbij dit document met de bijbehorende documenten worden aangepast en aangevuld tijdens bouw en exploitatie van het LSP.

1.3 Doelgroep van dit document

Dit document is bedoeld voor partijen die zich in de consultatieronde willen informeren over de bouw van de Zorg Informatie Makelaar (ZIM) en de inrichting en het beheer van het LSP.

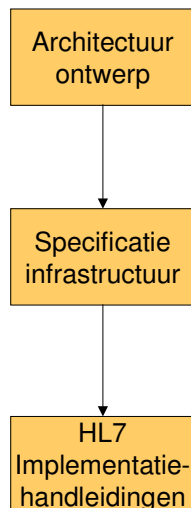
1.4 Documentstructuur en relaties met andere documenten

Dit document bevat zes hoofdstukken. Dit eerste hoofdstuk – de inleiding – gaat niet alleen in op het doel en de structuur van dit document, maar beschrijft ook de uitgangspunten en de context. Daarna volgt een beknopte introductie van het LSP en de ZIM.

Het derde hoofdstuk bevat de specificatie van de te leveren diensten door het LSP voor een eerste exploitatietermijn. Het vierde hoofdstuk bevat een beschrijving van de functies van de ZIM.

Het vijfde hoofdstuk beschrijft de fasering en het zesde hoofdstuk bevat tot slot de bijlagen.

De onderstaande figuur toont de relatie van de aan dit document onderliggende documenten, waarbij de pijlen wijzen naar het afgeleide document.



De onderliggende documenten van dit document 'Specificatie van diensten en functies binnen het LSP' zijn:

- Architectuurontwerp basisinfrastructuur in de zorg v4.0;
- Specificatie van de basisinfrastructuur in de zorg v2.1;
- Implementatiehandleiding HL7v3 infrastructurele domeinen, versie 2.0;
- Implementatiehandleiding HL7v3 Zorg Informatie Makelaar, versie 2.2;
- Implementatiehandleiding HL7v3 medicatieberichten, versie 2.2;
- Implementatiehandleiding HL7v3 waarneming huisartsen, versie 1.4

De eerste twee zijn de meest recente versies van reeds eerder verschenen basisdocumenten. Deze twee documenten zijn ontwikkeld vanaf 2002 met inbreng van drie vooraanstaande adviesbureaus en zijn in de tussenliggende periode reeds afgestemd met diverse partijen in het veld. Hieronder bevinden zich 18 ICT-leveranciers in de zorg, het Nederlands Normalisatie-instituut (NEN), vertegenwoordigers in de academische wereld en ICT-leveranciers in de Zorg. Uzorg heeft een belangrijk deel van deze specificaties gebruikt in een operationele verwijzingsindex die ca. 1.000.000 patiënten bevat.

In opdracht van het ministerie van VWS is een onafhankelijke audit uitgevoerd op deze documenten om een oordeel te kunnen vormen met betrekking tot het concept, de toekomstvastheid, verkrijgbaarheid van draagvlak en geschiktheid voor aanbiederselectie.

Een tweede onafhankelijke audit is in opdracht van NICTIZ uitgevoerd om deze documentatie te toetsen op volledigheid en toepasbaarheid in de praktijk. De rapporten van beide audits zijn beschikbaar op de NICTIZ-website www.nictiz.nl.

De vier implementatiehandleidingen vormen een nadere specificatie van de inhoud van de berichten die de ZIM dient te kunnen verwerken. Ten bate van een tweetal demonstraties zijn medicatieberichten en berichten voor de waarneming van huisartsen inmiddels door verschillende softwareleveranciers geïmplementeerd. Zie hiervoor o.a. het document "Technische evaluatie HL7v3-XML communicatie" (te downloaden via www.nictiz.nl). Verder worden onderdelen van deze documenten nog nader gespecificeerd.

1.5 Status van dit document

De huidige status van dit document is: concept per 19 maart 2005.
Een volgende versie is gepland in april na verwerking van de terugkoppeling uit de consultatieronde.

1.6 Uitgangspunten

De architectuur van de basisinfrastructuur kan diverse vormen van opslag van patiëntgegevens en overige data ondersteunen. Primair is gekozen voor opslag bij de bron. Alternatieven worden gevormd door het ASP-model (Application Service Provider) en de CDR (Clinical Data Repository).

Voor de bouw van de ZIM en het inrichten en beheer van het LSP gelden de algemene eisen van goed vakmanschap.

Van de opdrachtnemer wordt verwacht dat deze, waar noodzakelijk, in goede samenwerking met betrokken partijen contacten onderhoudt. Dit geldt voor zowel de periode tijdens de ontwikkeling van de ZIM als tijdens de exploitatie van het LSP.

De Nederlandse wetgeving beschermt de privacy van de patiënt. Alle informatie dient te allen tijde met de grootst mogelijke vertrouwelijkheid te worden behandeld. Dit geldt voor zowel de informatie binnen het LSP als de decentrale informatie die conform de architectuur van de basisinfrastructuur bij de bron wordt onderhouden. Richtlijnen hiervoor zijn o.a. vastgelegd in de normen ISO IEC 17799 en NEN 7510.

Algemeen wordt aangenomen dat het HL7v3 Reference Information Model en de definitie van de HL7v3 data types wereldwijd de basis zullen gaan vormen voor communicatie tussen zorgtoepassingen. HL7v3 is toekomstvast en wordt actief ingezet voor alle nieuwe standaardisatietrajecten. Zo zijn en worden communicatie-

standaarden voor huisartsen, perinatologie, jeugd gezondheidszorg, CVA-ketenzorg en DBC-registratie uitgewerkt op basis van HL7v3.

De standaard is gebaseerd op XML¹. De HL7v3-methodiek is modulair van opzet en maakt gebruik van een set van uniforme basisbegrippen: zorgaanbieder, patiënt, verrichting, etc. Dit staat voor consistentie in de communicatie. HL7v3 staat ook voor flexibiliteit.

Bijzonder aan dit document is dat, behalve de vereiste diensten van het LSP (output based), ook de vereiste functies van de ZIM worden gespecificeerd. In principe, zou men kunnen denken, hoeft de opdrachtnemer niet te worden voorgeschreven met welke systemen het LSP de vereiste diensten gaat leveren. De opdrachtgever zal de opdrachtnemer uiteindelijk afrekenen op de omvang en de kwaliteit van de diensten geleverd door het LSP, waarbij de opdrachtnemer de vrijheid kan worden geboden dat met zelf gekozen middelen klaar te spelen. De reden dat de functies van het te gebruiken systeem, de ZIM, toch worden voorgeschreven, is tweeledig:

- Enerzijds meent de opdrachtgever dat het niet mogelijk is de vereiste diensten te leveren zonder de beschreven functies van de ZIM;
- Anderzijds wenst de opdrachtgever aan het einde van de contractuele exploitatietermijn de optie te hebben om de apparatuur en programmatuur van de ZIM over te nemen van de opdrachtnemer.

De aan te sluiten systemen en netwerken op de centrale infrastructuur vallen buiten het bestek van deze aanbesteding.

Aan te sluiten Zorg Service Providers (ZSP's) en Goed Beheerde Zorgsystemen (GBZ'en) zullen in de uiteindelijke operationele situatie slechts aangesloten kunnen worden na certificering. Bepaling van de certificeringeisen voor ZSP's en GBZ'en wordt parallel uitgevoerd. GBZ'en kunnen slecht via ZSP's worden aangesloten.

Tijdens de ontwikkeling van het LSP en de exploitatieperiode wordt uitgegaan van een groeimodel. Hier wordt in de laatste paragraaf van dit hoofdstuk dieper op ingegaan.

1.7 Groeimodel: toekomstige diensten en openstaande punten

Het LSP zal in de toekomst een groei doormaken in zowel het palet aan diensten en functies als de schaal van het gebruik ervan. Daarbij dient de capaciteit van de ICT-infrastructuur gelijke tred te houden.

¹ Tijdens het congres MIC 2003 hebben 9 leveranciers in een demonstratieopstelling aangetoond dat de standaard implementeerbaar is. Daarnaast is er in een interne studie een performanceanalyse uitgewerkt die de bruikbaarheid onderschrijft.

Tijdens de contractuele exploitatietermijn kan de opdrachtgever besluiten de aard, omvang en kwaliteit van de diensten van het LSP uit te breiden. Toekomstige diensten die nu al worden voorzien:

- Adresboek voor zorgaanbieders;
- Autorisatieprofiel: door burgers instelbaar;
- Koppeling met overige landelijke registers;
- Koppeling met aanpalende architecturen in de zorg zoals (in willekeurige volgorde) de Jeugd Gezondheidszorg (JGZ), perinatologie, CVA-ketenzorg, verslavingszorg en traumaregistratie;
- Toegang voor de patiënt tot zijn eigen gegevens.

Voor deze toekomstige diensten moeten de overeenkomstige functies van de ZIM wel worden gespecificeerd en gebouwd, opdat de diensten snel kunnen worden ingeschakeld, wanneer de opdrachtnemer daarom vraagt. Deze eisen zijn gemerkt met "(toekomst)". Tijdens deze groeiperiode zullen de bijbehorende specificaties gaande weg worden ontwikkeld.

Op het moment van schrijven van dit document vinden nog ontwikkelingen plaats hetgeen leidt tot de, tot nu toe, volgende openstaande punten:

- in plaats van het eerder voorgenomen Zorg Informatie Nummer (ZIN) heeft het ministerie van VWS besloten het Burger Service Nummer te gebruiken als landelijk uniek patiëntnummer. Daarvoor is een wetsvoorstel in de maak, en is het project voor de ontwikkeling van het ZIN-register omgebogen in een project voor de ontwikkeling van een Sectorale Berichten Voorziening voor de Zorg (SBV-Z). De Europese aanbesteding voor de bouw van de SBV-Z is inmiddels in gang gezet. De geplande oplevering is begin 2006. De beschikbaarheid zal mede afhankelijk zijn van de ontwikkeling van een Overkoepelende Berichten Voorziening (OBV) door het ministerie van BZK.
- M.b.t. een tweetal discussiepunten zal nog, voorafgaand aan de Europese aanbesteding, definitieve besluitvorming en vastlegging plaatsvinden:
 - Gegevensuitwisseling tussen zorgaanbieders vindt plaats m.b.v. een aanduiding van het gevraagde type gegevens. De verzameling gegevenssoorten wordt nog vastgesteld.
 - Betrouwbaar transport van HL7v3-berichten.
- De rol van onafhankelijke toezichthouder van het LSP dient nog nader te worden ingevuld en van een juridisch kader te worden voorzien.
- De plaats van de autorisatiemanager dient nog te worden bepaald.
- Taken en verantwoordelijkheden met betrekking tot het certificeren van ZSP's en GBZ'en dienen nog definitief te worden belegd.
- Beschikbaarheid en toepasbaarheid van DigID en/of e-NIK in relatie tot toekomstige openstelling van toegang voor de patiënt zelf van delen van het eigen dossier, dient nog te worden bepaald.

2 Het Landelijk Schakelpunt in vogelvlucht

2.1 Introductie en omgeving van het LSP

Veilige communicatie en toegang tot gegevens

Het Landelijk Schakelpunt draagt er zorg voor dat zorginformatie alleen ter inzage beschikbaar is voor geautoriseerde zorgaanbieders. Dit gebeurt met behulp van de Unieke Zorgaanbieder Identificatie pas (UZI-pas), ook wel elektronisch paspoort voor de zorg genoemd. Zorgaanbieders worden na identificatie met deze UZI-pas door het Landelijk Schakelpunt geauthenticeerd; dat wil zeggen dat er wordt vastgesteld of de zorgverlener ook daadwerkelijk is wie hij/zij zegt dat hij/zij is en of de pas nog geldig is. Dit vindt plaats met behulp van het UZI-register dat onder toezicht staat van het agentschap Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport.

Historie van opvragen- en inzage in gegevens (logging)

Wie heeft wanneer welke type gegevens opgevraagd en ingezien? Om op deze vraag een antwoord te kunnen geven, worden de aanvragen van de aangesloten zorgaanbieders vastgelegd in logbestanden. De patiëntgegevens zelf komen overigens niet voor in deze logbestanden. Er komt een onafhankelijke partij die toezicht gaat houden op het aanvragen en inzien van gegevens. Deze partij zal controleren of de aanvragen en inzagen rechtmatig zijn.

Verkeersregelaar

Een belangrijke taak van het Landelijk Schakelpunt is die van verkeersregelaar voor berichten (de vragen naar zorginhoudelijk informatie en antwoorden) die over het netwerk gaan van aangesloten zorginformatiesystemen. Het Landelijk Schakelpunt is continu, via de centrale verwijsindex op de hoogte welke patiëntgegevens in welke zorginformatiesystemen zijn opgeslagen. Er worden dus geen medische gegevens opgeslagen bij het Landelijk Schakelpunt: deze gegevens blijven bij de zorginformatiesystemen van de aangesloten zorgaanbieders.

Identificatie van patiënten

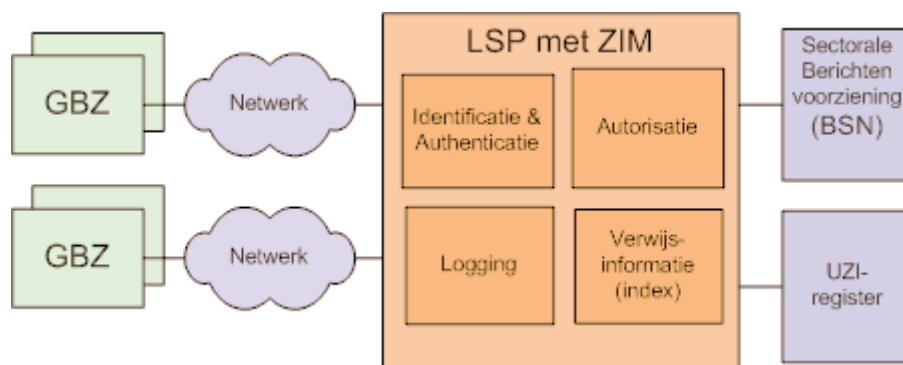
Het Landelijk Schakelpunt gebruikt het meegezonden Burger Service Nummer (BSN) van de patiënt om over de juiste patiënt de gegevens te verstrekken. Het BSN is qua nummer gelijk aan het huidige Sofi-nummer en wordt via het informatiesysteem van de Sectorale Berichten Voorziening in de Zorg (SBV-Z) beschikbaar gemaakt voor zorgaanbieders. De overheid is verantwoordelijk voor de uitgifte van het nummer en het inrichten van de berichtenvoorziening.

Helpdesk

Zorginformatiesystemen zullen via gecertificeerde commerciële dienstenaanbieders, de zogenoemde 'Zorg Service Providers', worden aangesloten op het Landelijk Schakelpunt. Deze Zorg Service Providers hebben een helpdesk voor de zorginstellingen met een Goed Beheerd Zorgsysteem. Het Landelijk Schakelpunt richt een helpdesk in voor dienstverlening aan de Zorg Service Providers. Deze helpdesk zal gedurende de exploitatieperiode aanvankelijk tijdens kantooruren bereikbaar zijn en na twee jaar 24 uur per dag en 7 dagen per week.

Autorisatie van gegevens

Het Landelijk Schakelpunt toetst of de patiënt vooraf bezwaar heeft gemaakt tegen gegevensuitwisseling tussen zorgaanbieders. Deze bezwaren worden vastgelegd in een autorisatieprofiel per patiënt. Aanvankelijk heeft een patiënt de keuze om wel of niet mee te doen, later zal differentiatie mogelijk zijn. Een patiënt kan dan aangeven welke zorgaanbieders wel en welke geen toestemming hebben om gegevens in te zien c.q. welk type gegevens wel of niet mogen worden uitgewisseld. Onderdelen hiervan worden nog nader uitgewerkt.

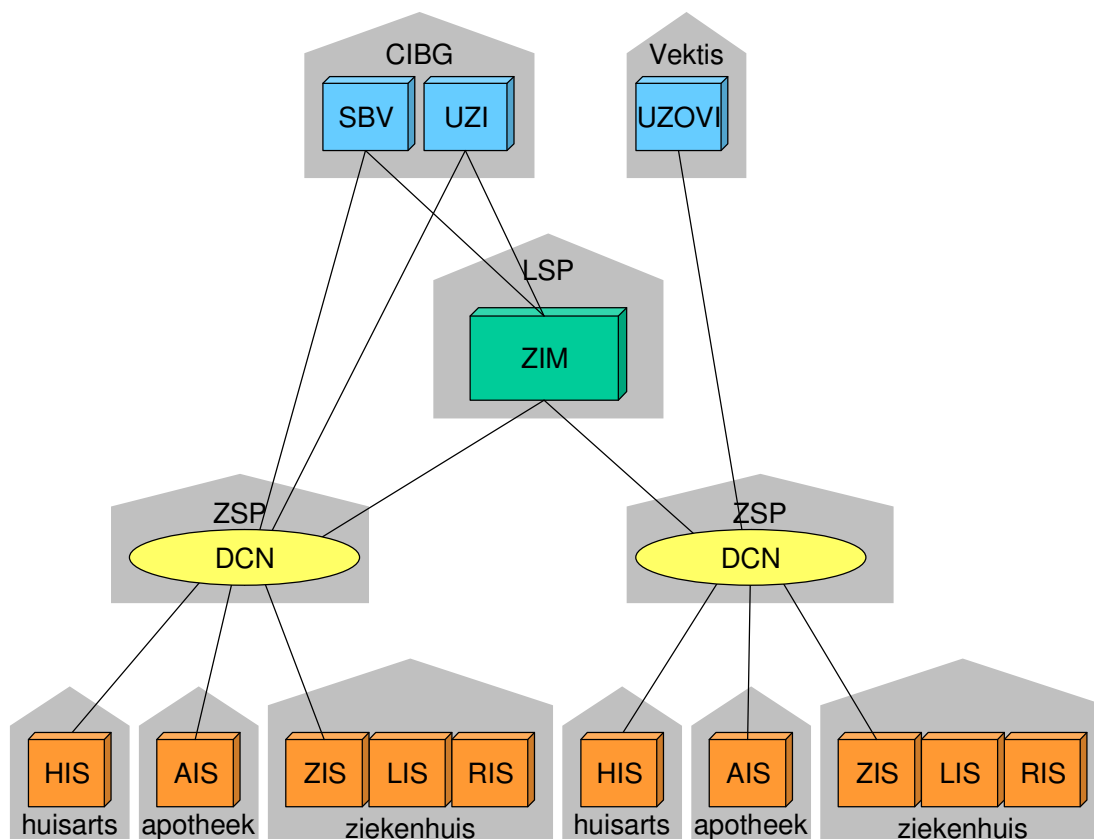


Voorzieningen van het Landelijk Schakelpunt voor de aangesloten Goed Beheerde Zorgsystemen

2.2 Omschrijving van diensten en functies op hoofdlijnen

Er wordt een LSP voorzien als organisatie die zich richt op de ondersteuning van de zorgsector door middel van een landelijke voorziening voor de uitwisseling van zorginformatie. Er wordt daarbij gebruik gemaakt van de technische infrastructuur genaamd de Zorg Informatie Makelaar (ZIM).

Het LSP zal met behulp van de ZIM allerlei informatie- en routeringsdiensten aanbieden aan zorgaanbieders via Zorg Service Providers (ZSP's). Daartoe zal het LSP identificatie- en authenticatiediensten moeten afnemen van het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), Zorgverzekeraars Nederland (ZN) en andere partijen. Zie onderstaande figuur.



Bovenstaande figuur toont een algemene schets van de samenhang en informatiestromen. Voor de gebruikte afkortingen zie paragraaf 6.2. Nadere uitleg volgt in hoofdstuk 3.

De ZSP's, als intermediair voor aangesloten zorginstellingen, kunnen de informatie- en routeringsdiensten verrijken met aanvullende informatie-, applicatie- en netwerkdiensten en deze aanbieden aan zorgaanbieders. Daartoe kan een ZSP telecommunicatie-, informatie- en applicatiediensten afnemen van telecombedrijven en andere dienstverleners. De rol van de ZSP is belangrijk vanuit de gedachte dat een LSP als landelijk centrale organisatie niet in staat zal zijn alle zorgaanbieders in Nederland individueel te benaderen en te ondersteunen. Op hun beurt zijn ZSP's verantwoordelijk voor het verschaffen van performancegegevens aan het LSP t.b.v. de end-to-end performancerapportage door het LSP. Deze eis aan de ZSP's zal mede worden opgenomen in de certificeringcriteria voor ZSP's. Non-conformiteit aan de certificeringcriteria dient te leiden tot blokkering van toegang tot het LSP.

Vertegenwoordigers van het LSP en ZSP's zullen verplicht worden periodiek overleg te voeren op het niveau van operationeel beheer.

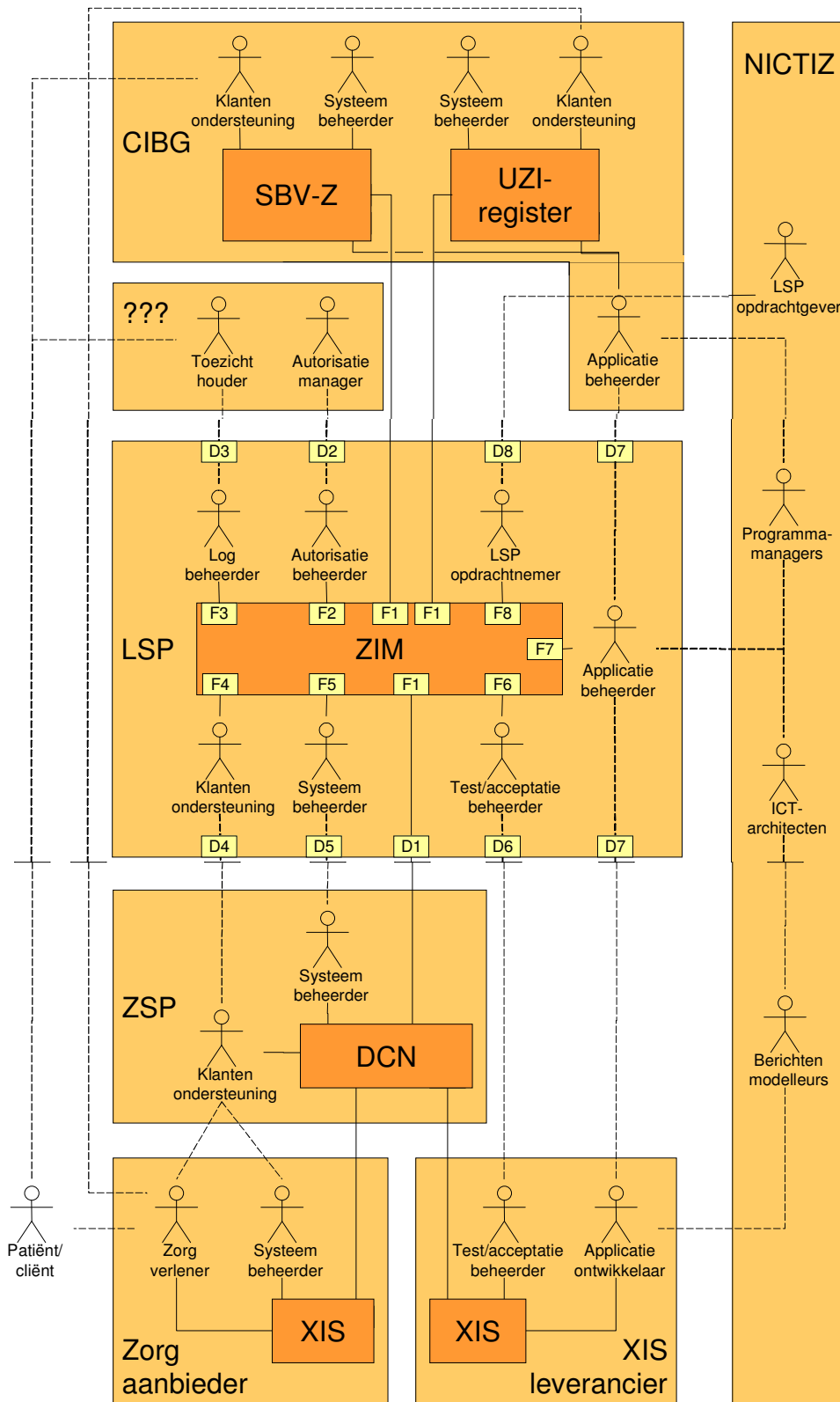
Toezicht op het LSP tijdens exploitatie zal worden uitgeoefend door een onafhankelijke partij.

De volgende figuur geeft een beeld van de samenhang tussen de diensten van het LSP en de bijbehorende functies van de ZIM.

De binnenste, donker ingekleurde, kaders vertegenwoordigen de gebruikte ICT-systemen. De lichter ingekleurde kaders vertegenwoordigen benoemde organisaties, bevolkt door personen/functionarissen. Stippellijnen geven informatiestromen aan tussen personen en ononderbroken lijnen duiden op informatiestromen met en tussen ICT-systemen.

Na de figuur volgt een uitwijding van LSP-diensten en ZIM-functies.

De onderstaande figuur toont de relaties tussen de LSP-diensten en de ZIM-functies:



Toelichting bij coderingen in voorgaande figuur voor diensten (Dn) en functies (Fn):

D1 – het LSP levert via ZSP's informatie- en routeringsdiensten aan zorgaanbieders opdat zij patiëntgegevens kunnen uitwisselen met andere zorgaanbieders. De ZIM biedt de benodigde functionaliteit F1 om berichten tussen de SBV-Z, het UZI-register en alle aangesloten GBZ'en via Datacommunicatie Netwerken (DCN'en) te routeren.

D2 – de autorisatiebeheerder van het LSP werkt op verzoek van de autorisatiemanager het autorisatieprotocol van zorgaanbieders en de autorisatieprofielen van burgers bij. De ZIM biedt de autorisatiebeheerder de benodigde functionaliteit F2 om de bijbehorende tabellen te beheren.

D3 – de logbeheerder van het LSP ontsluit voor de toezichthouder de toegangslag, ter controle van de rechtmatigheid of zorgaanbieders bepaalde patiëntgegevens hebben ingezien. De ZIM biedt de logbeheerder de benodigde functionaliteit F3 om deze toegangslag te inspecteren.

D4 – de klantenondersteuning van het LSP fungeert als helpdesk voor ZSP's. De klantenondersteuning van de ZSP's vormt de helpdesk voor zorgaanbieders. De ZIM biedt de klantenondersteuning functionaliteit F4 om de werking van een XIS van een zorgaanbieder, zijn ZSP en van de ZIM te controleren.

D5 – de systeembeheerder van het LSP is verantwoordelijk voor de goede werking van de ZIM en configureert op verzoek van de systeembeheerders van de ZSP's de koppelingen met DCN'en en XIS'en (met de status van GBZ). De ZIM biedt de systeembeheerder de benodigde functionaliteit F5 om de ZIM en de koppelingen met DCN'en en GBZ'en te bewaken, te besturen en te configureren.

D6 – de test/acceptatie-beheerder van het LSP geeft XIS-leveranciers de mogelijkheid om hun XIS te testen op het voldoen aan de eisen die aan een GBZ worden gesteld en hun XIS te demonstreren aan zorgaanbieders. De ZIM biedt de test/acceptatie-beheerder functionaliteit F6 om de werking van een XIS in combinatie met de ZIM te testen en accepteert nieuwe ZSP's en daarop aangesloten nieuwe GBZ'en.

D7 – de applicatiebeheerder van het LSP zorgt voor het verder ontwikkelen van de functionaliteit van de ZIM. Dit is nodig opdat bestaande functies kunnen worden verbeterd en nieuwe berichten kunnen worden uitgewisseld, zoals ontwikkeld door NICTIZ, de applicatieontwikkelaars van de XIS-leveranciers en de berichtenmodelleurs van NICTIZ. De ZIM biedt de applicatiebeheerder functionaliteit F7 om verschillende versies van applicaties en berichten te ondersteunen.

D8 – de LSP-opdrachtnemer rapporteert geregeld aan de LSP-opdrachtgever van NICTIZ, over aard, omvang en kwaliteit van de diensten geleverd door het LSP. De ZIM biedt de test/acceptatie-beheerder functionaliteit F8 om rapportages te maken. De LSP-opdrachtgever maakt verder afspraken met de LSP-opdrachtnemer over de eventuele uitbreiding of bijstelling van de diensten.

Als voorbeeld wordt hierna een karakteristieke gebruikersvraag gevolgd door de figuur op de vorige bladzijde:

Een huisarts, de zorgaanbieder die gebruik maakt van een XIS (nl. een HIS met GBZ-status) wil medicatie voorschrijven aan een van haar patiënten. Vooraf wil zij inzicht hebben in de medicatiehistorie van de patiënt. Zij raadpleegt haar eigen XIS en een bericht gaat uit naar het DCN van haar ZSP. Het DCN geeft het bericht ongewijzigd door aan de ZIM van het LSP. De ZIM moet nu op zoek gaan naar alle medicatieverstrekkers van deze patiënt.

Bij binnenkomst van het bericht wordt gecontroleerd of deze huisarts gerechtigd is de informatie op te vragen. Zo ja, dan wordt binnen de verwijsindex van de ZIM zelf nagegaan bij welke aangesloten XIS'en medicatie-informatie van deze bepaalde patiënt is te vinden. Daarna worden deze XIS'en (Apotheken en/of ziekenhuizen) uitgevraagd m.b.t. medicatiegegevens. De antwoorden worden door de ZIM verzameld en aan HIS van de vragende huisarts doorgestuurd. De huisarts heeft nu het medicatieoverzicht van haar patiënt en schrijft op basis van deze informatie een nieuw recept uit.

Als eerste dient de ZIM operationeel te zijn in elementaire vorm voor de referentieomgeving. De definitieve invulling zal gestalte krijgen nadat de basisfuncties stabiel blijken te zijn tijdens welke periode het LSP volledig operationeel dient te zijn.

3 Diensten van het Landelijk Schakelpunt

3.1 Algemeen

Ten behoeve van de uitwisseling van informatie in de zorgsector wordt een LSP voorzien voor het leveren van een aantal centrale diensten om de informatie-uitwisseling tussen zorgpartijen te ondersteunen. Het LSP zal informatie- en routeringsdiensten alleen aanbieden via ZSP's (Zorg Service Providers). Het LSP zal identificatiediensten afnemen van het CIBG, Vektis en eventueel andere partijen.

In dit hoofdstuk worden de diensten beschreven die door het LSP geleverd moeten gaan worden.

3.2 Diensten geleverd door het LSP

3.2.1 Informatie- en routeringsdiensten

De primaire taak van het LSP is het leveren van informatie- en routeringsdiensten op vastgestelde dienstenniveaus. Aangezien deze diensten direct worden geleverd door de te ontwikkelen ZIM vindt gedetailleerde specificatie van deze diensten plaats in paragraaf 4.2. Op hoofdlijnen gaat het om de volgende diensten:

1. Het op aanvraag leveren van een overzicht van de beschikbare medicatie-informatie voor zorgaanbieders en/of waarneeminformatie voor de huisarts op basis van de beschikbare gegevens in het LSP;
2. Het geheel of gedeeltelijk opleveren van de beschikbare medicatie-informatie en/of waarneeminformatie voor huisartsen uit de aangesloten systemen;
3. Het routeren van berichten tussen applicaties van zorgpartijen;
4. Het leveren van informatie over zorgaanbieders als intermediair voor bevraging van het UZI-register;
5. Het leveren van het BSN als intermediair voor bevraging van de SBV-Z.
6. Het routeren van IP-verkeer tussen Zorg Service Providers (ZSP's);

In een latere fase zullen de diensten van het LSP worden uitgebreid, zodat o.a. de volgende diensten ondersteund kunnen gaan worden; de functionaliteit van het LSP zal hierop moeten zijn voorbereid:

1. Het op aanvraag leveren van diverse overzichten van de beschikbare informatie over een patiënt op basis van de beschikbare gegevens in het LSP
2. Het op aanvraag geheel of gedeeltelijk opleveren van alle beschikbare informatie over een patiënt uit de aangesloten systemen;
3. Het aan de patiënt toegang verlenen tot de logging informatie die op deze patiënt betrekking heeft;

4. Het aan de patiënt bieden van de mogelijkheid om zijn eigen autorisatieprofiel in te stellen;
5. Het leveren van informatie over zorgaanbieders als intermediair voor bevraging van het UZI-register;

Om deze diensten te kunnen leveren dient te worden voorzien in de inrichting en het beheer van de centrale faciliteiten (ZIM) en de verbindingen met de buitenwereld, het bewaken van het berichtenverkeer en het ingrijpen bij dreigende of optredende storingen.

Met betrekking tot de inrichting en operationeel beheer van het LSP gelden de volgende **eisen**:

1. Voor het inrichten van het LSP gelden de algemene eisen van goed vakmanschap. Daarbij wordt verondersteld dat in ieder geval gebruik wordt gemaakt van bestaande normen zoals de Code voor Informatiebeveiliging (ISO IEC 17799) en de Norm NEN 7510 Informatiebeveiliging in de Zorg (IBIZ), met bijbehorende implementatierichtlijnen.
2. Er moet op een door de opdrachtgever nader te bepalen tijdstip een uitwijkvoorziening worden gerealiseerd op een geografisch duidelijk gescheiden locatie. De inrichting hiervan dient met zo min mogelijk consequenties voor zorgpartijen en ZSP's te worden gerealiseerd.
3. De LSP-beheerder dient aantoonbaar voldoende maatregelen te hebben genomen om de aangesloten GBZ'en en ZSP's te vrijwaren van spam, virussen en andere bedreigingen voor de informatievoorziening.
4. De ZIM wordt door de leverancier geïnstalleerd zowel in een test-/acceptatieomgeving als een operationele omgeving. Beide omgevingen worden door een systeembeheerder beheerd. Daarnaast dient er als equivalent van de operationele omgeving een uitwijkomgeving te bestaan.
5. T.a.v. het opslagmechanisme van gegevens gelden de volgende deeleisen
 - a. het opslagmechanisme dient voldoende stabiel te zijn; gegevensbeschadiging door fouten in de opslagsoftware moet praktisch uitgesloten zijn.
 - b. de gegevens in de ZIM dienen dagelijks veilig gesteld te kunnen worden op een separaat back-up medium.
 - c. opslag van het back-up medium vindt op een andere locatie plaats.
6. De dienstverlening moet in principe 24 uur per dag gedurende 7 dagen per week beschikbaar zijn.
7. Alle interacties die via het LSP worden gerealiseerd moeten worden gelogd (zie voor de eisen paragraaf 4.4). Deze informatie moet toegankelijk zijn voor een bevoegde instantie. Op basis van deze logging kan een controle plaatsvinden of toegang tot het medicatiedossier rechtmatig is geweest, bijvoorbeeld door toetsing aan andere bestanden zoals declaratie-informatie.

8. De leverancier richt ten behoeve van het beheer een adequate beheeromgeving in, waar de juiste werking van het gehele LSP kan worden gecontroleerd.
9. Het personeel dat beheerhandelingen moet uitvoeren moet gescreend zijn. Er moeten procedures worden afgesproken om ervoor zorg te dragen dat LSP-personeel alleen patiëntinformatie kan opvragen, dan wel inzien, wanneer dit echt noodzakelijk is. Indien mogelijk en zinvol dient hierbij het principe van taakscheiding te worden gehanteerd.
10. Voor ingrijpende beheerhandelingen, zoals bijvoorbeeld het blokkeren van GBZ'en of aanpassing van het autorisatieprotocol, dienen procedures te worden afgesproken met voldoende controlemechanismen om te voorkomen dat fouten en/of vergissingen in deze beheerhandelingen tot onbedoelde problemen zullen leiden.

3.2.2 Dienstverlening aan ZSP's

Door het LSP worden ook interconnectiediensten geleverd aan gecertificeerde Zorg Service providers (ZSP's). De eisen en certificeringsprocedure voor ZSP's worden in overleg met het veld nog nader vastgesteld.

Aan de dienstverlening aan ZSP's worden de volgende **eisen** gesteld:

1. Het LSP geeft de IP-adresreeksen uit voor het subnet van de desbetreffende ZSP. De ZSP zorgt voor een eventuele vertaling van adressen die intern in het ZSP-netwerk worden gebruikt naar deze IP-adressen.
2. Met ZSP's moeten afspraken worden gemaakt over op te stellen SLA's en de procedures bij dreigende of optredende storingen.
3. Voor het leveren van diensten voor de aansluiting van nieuwe ZSP's op de ZIM en het eventueel distribueren van (nieuwe versies van) de daarvoor benodigde voorzieningen (koppelmodules/aansluitkit) moeten service levels worden afgesproken in termen van:
 - werktijden en andere toegangsvoorwaarden,
 - installatiewerkzaamheden en zelfwerkzaamheid van de klant,
 - wacht-, reactie- en doorlooptijden,
 - etc.
4. De LSP-provider dient ZSP's in staat te stellen hun apparatuur te plaatsen in ruimtes vlakbij de ZIM (co-hosting).
5. Er dient een procedure (script) te worden opgesteld voor de aansluiting en acceptatie van een GBZ.
6. De LSP-provider dient een courante lijst van gecertificeerde ZSP's te onderhouden t.b.v. de opdrachtgever en andere betrokkenen.

3.2.3 Dienstverlening aan Registerhouders

1. Het LSP sluit aan op de SBV-Z, het UZI-register en in een later stadium het UZOVI-register.
2. Met de Registerhouders moeten afspraken worden gemaakt over op te stellen SLA's en de procedures bij dreigende of optredende storingen. Hierbij moeten afspraken worden gemaakt over:
 - a. werktijden en andere toegangsvoorwaarden,
 - b. installatiewerkzaamheden,
 - c. wacht-, reactie- en doorlooptijden,
 - d. etc.

3.2.4 Beheerdiensten

3.2.4.1 Toegangbeheer

Met betrekking tot toegangbeheer tot het LSP gelden de volgende **eisen**:

1. Het LSP dient te beschikken over een procedure voor authenticatie van de zorgpartijen. Een zorgpartij authenticereert zich bij het opzetten van een sessie met het LSP door middel van een persoonlijk UZI- certificaat. In een latere fase moet het ook mogelijk zijn UZOVI-certificaten te gaan gebruiken.
2. Het verstrekken van informatie aan zorgpartijen is gereguleerd door autorisatietabelregels en vindt plaats na een geslaagde authenticatie-procedure. Het technisch beheer van de tabelregels voor het autorisatieprotocol en autorisatieprofiel is belegd bij het LSP. Wijziging van de tabelregels voor het autorisatieprotocol dient binnen 3 werkdagen na opdrachtverlening door de opdrachtgever te zijn gerealiseerd. De procedure voor wijziging van de tabelregels voor het autorisatieprofiel is nog niet vastgesteld.
3. Een GBZ (via een ZSP) en een ZSP mogen alleen worden aangesloten indien wordt voldaan aan de certificeringseisen. De eisen en certificeringsprocedure worden op dit moment opgesteld. Het moet mogelijk zijn een GBZ om administratieve redenen af te sluiten zodat geen verkeer meer mogelijk is naar en van dat GBZ. Dit kan pas na aanwijzing door de opdrachtgever. Ook een GBZ dat niet (meer) aan de eisen voldoet moeten kunnen worden geblokkeerd (blacklist/whitelist). Dit kan bijvoorbeeld gedaan worden indien uit het systeembeheer blijkt dat in een bepaalde periode een maximum aantal gegenereerde fouten is opgetreden.

3.2.4.2 Systeembeheer

Het LSP dient te beschikken over faciliteiten om adequaat systeembeheer uit te kunnen voeren. Met betrekking tot het systeembeheer van het LSP gelden de volgende **eisen**:

1. GBZ'en die een nader te bepalen foutgedrag vertonen dienen te kunnen worden geïdentificeerd. Van deze GBZ'en moet het gedrag gemonitord kunnen worden. Indien uit de monitoring blijkt dat het GBZ niet naar behoren functioneert, dient correctieve actie te worden uitgevoerd. In eerste instantie betekent dit in contact treden met de GBZ-beheerder of zijn ZSP. In een latere fase kan ook blokkering van het GBZ worden overwogen.
2. Het moet mogelijk zijn om berichten naar GBZ'en tegen te houden en te bewaren indien een GBZ of diens verbinding met de ZIM uitvalt of indien een GBZ wegens administratieve of andere redenen wordt geblokkeerd. Na herstel van de connectiviteit met het GBZ dienen de berichten alsnog te worden verstuurd.
3. Er moeten back-upprocedures en recovery-procedures aanwezig zijn. De recovery-procedure dient 1 maal per jaar te worden getest. De resultaten hiervan dienen 5 jaar te worden bewaard.
4. Ten behoeve van het opstellen van rapportages en aanpassingen van de dimensionering van het systeem dienen de volgende karakteristieken van de communicatie te kunnen worden gemonitord:
 - het aantal actieve zorgpartijen;
 - het aantal sessies en het aantal berichten per sessie per zorgpartij;
 - het gedrag van het systeem, zodat analyses op verkeerskarakteristieken (zoals het voorkomen van bijvoorbeeld piekperioden) kunnen worden uitgevoerd;
 - de performance van het systeem.

3.2.4.3 Applicatiebeheer

Met betrekking tot onderhoud van de applicatiesoftware in het LSP gelden de volgende **eisen**:

1. Het LSP dient op een eenvoudige manier te kunnen migreren naar eventuele nieuwe versies van de standaard programmatuur².
2. Het is een optie voor de leverancier om de maatwerkprogrammatuur³ onderdeel te maken van de standaardprogrammatuur. Het maatwerk dient dan wel samen met de standaardprogrammatuur onderhouden en beheerd te worden. Wordt geen gebruik gemaakt van deze optie dan krijgt de opdrachtgever de beschikking over de maatwerkprogrammatuur met het recht deze voor eigen gebruik te wijzigen.
- 3. Eigendom infrastructuur:**

² Onder "standaard programmatuur" wordt die software verstaan die zonder verdere aanpassing kan worden toegepast voor een bepaald doel (ook wel aangeduid met COTS- of Commercially Off The Shelf Software)

³ Onder maatwerkprogrammatuur wordt die software verstaan die specifiek wordt ontwikkeld voor een bepaalde toepassing bij een klant; dit kunnen ook klantspecifieke aanpassingen van standaard programmatuur zijn.

- a. Bij overdragen eigenaarschap van de aangeschafte ontwikkelde apparatuur en/of programmatuur naar de opdrachtgever: de opdrachtgever dient zijn rechten met betrekking tot het eigendom van de ontwikkelde apparatuur en/of programmatuur over te kunnen dragen naar een andere partij. Hieraan zijn – indien gebruiksomstandigheden niet wijzigen - geen aanvullende kosten verbonden.
 - b. Bij doorberekenen van licentiekosten aan de opdrachtgever voor het gebruik van de aangeschafte ontwikkelde apparatuur en/of programmatuur: de opdrachtgever dient zijn rechten met betrekking tot het beheer en gebruik van de ontwikkelde apparatuur en programmatuur– zowel standaard als maatwerk - over te kunnen dragen naar een andere partij. Hieraan zijn – indien gebruiksomstandigheden niet wijzigen - geen aanvullende licentiekosten verbonden.
4. De opdrachtgever moet de mogelijkheid hebben het contract tussentijds te beëindigen indien de dienstverlening niet voldoet aan de in het SLA gestelde eisen. Indien nog geen eigendomsoverdracht heeft plaatsgevonden van de ontwikkelde apparatuur en programmatuur dient de ontwikkelde apparatuur en programmatuur tegen een door een onafhankelijk partij vastgestelde kostprijs te kunnen overnemen.
 5. Op het LSP dient correctief onderhoud plaats te vinden. Dit betreft in eerste instantie het oplossen van productie gerelateerde problemen. Het onderhoud betreft alleen updates waar gebruikers van de standaardprogrammatuur-componenten ook recht op hebben en correctief onderhoud van het maatwerk deel. Dit type onderhoud betreft geen platform-migraties en ook geen functionele wijzigingen.
 6. Ten behoeve van het release management zal een overlegstructuur worden ingericht waarbij opdrachtgever, LSP en vertegenwoordigers van de decentrale omgeving betrokken zijn. De opdrachtgever bepaalt het moment van overgang naar nieuwe releases.
 7. Functioneel onderhoud: de aanbieder dient aan te geven hoe nieuwe wensen van de opdrachtgever t.a.v. de functionaliteit kunnen worden gehonoreerd en hoe de verrekening van de kosten plaatsvindt.
 8. Voor handmatige acties op het LSP (raadplegen, muteren etc.) dient een aparte autorisatie opgezet te worden. Dit geldt voor alle applicatiebeheer-functies.

3.2.4.4 Beheer IP-nummerplan

De LSP-beheerder dient ervoor zorg te dragen dat er bij koppeling met andere VPN's geen dubbele adressen ontstaan die alleen door complexe vertalingen kunnen worden opgelost. ZSP's kunnen daarbij gebruik maken van publieke IP-adressen of van IP-reeksen uit een door het LSP beheerd privaat nummerplan. In

het laatste geval zullen ZSP's in overleg met de LSP-beheerders moeten komen tot een unieke adrestoekenning binnen deze private adresruimte.

Dit leidt tot de volgende **eisen**:

1. Er dient een overkoepelend IP-nummerplan voor het zorgdomein te worden opgesteld.
2. Aan ZSP's die daarom verzoeken dienen IP-adresreeksen binnen dit plan te worden uitgegeven. Dit geldt ook voor ZSP's die nog niet direct willen koppelen aan de ZIM, maar daar later wellicht wel gebruik van willen maken.

3.2.4.5 Beheer domeinnamen

Bij koppeling van VPN's en het realiseren van een overkoepelend DNS dient ook een unieke naamgeving te worden gerealiseerd.

Dit leidt tot de volgende **eisen**:

1. De LSP-beheerder zorgt voor de registratie van een eigen domeinnaam voor het totale zorgnetwerk bij de registrerende instantie (SIDN);
2. De uitgifte van namen binnen dit domein vindt door de LSP-beheerder plaats;
3. Het LSP beheert ook een DNS voor het zorgdomein.

3.2.4.6 Beheer van OID's

HL7 Versie 3 gebruikt unieke Object Identifiers (OID's) om wereldwijd unieke identificatie te realiseren. OID's worden toegekend door een Registration Authority. Een van de beheertaken van het LSP is het optreden als Registration Authority voor de uitgifte van OID's voor het Nederlandse zorgveld.

Dit leidt tot de volgende **eisen**:

1. Registratie als RA bij een organisatie die de formele RA-status heeft.
2. Uitgifte van OID's die voldoen aan de eisen gesteld in ISO/IEC 8824 "OSI Specification of Abstract Syntax Notation One (ASN.1)". Deze standaard specificeert o.a. de structuur en de notatie van OID's.
3. Registratie en publicatie van uitgegeven OID's conform ISO/IEC 9834 "Procedures for the operation of OSI Registration Authorities".

3.2.4.7 Productie en inspectie van een Audit Trail log bestand

Eisen:

1. Ten behoeve van de controle op juiste werking en volgen van de juiste procedures moeten alle beheerhandelingen worden vastgelegd in een audit trail logbestand.

2. De desbetreffende gegevens dienen door de opdrachtgever te kunnen worden gecontroleerd.

3.2.5 Ondersteuning van ZSP's d.m.v. een helpdesk

Het vanuit een helpdesk ondersteunen van ZSP's, zorgaanbieders en patiënten bij eventuele vragen, verzoeken, storingen, etc. Hiervoor moeten service levels worden afgesproken in termen van:

1. kanalen (Internet, telefoon, etc.) waarlangs de klantendienst bereikbaar is,
2. openingstijden van elk van de kanalen,
3. wacht-, reactie- en doorlooptijden,
4. etc.

De belangrijkste diensten zijn:

1. beantwoorden van vragen van ZSP's;
2. afhandelen van verzoeken van ZSP's tot registratie en acceptatie voor aansluiting, blokkering etc. van ZSP en/of GBZ;
3. registratie van gemelde storingen en ondersteunen bij storingsopheffing door ZSP's.

De geformuleerde **eisen** zijn:

1. De helpdesk is in ieder geval telefonisch en per e-mail bereikbaar;
2. Gedurende de eerste twee jaar is de help desk geopend op werkdagen van 9-17u. Daarna zal worden overgegaan op 7 x 24 uur dienstverlening.
3. Aangezien het hier alleen gaat om contacten met ZSP's is de verwachting dat in ieder geval een continu-bezetting gedurende de openstellingstijd van de helpdesk moet worden gerealiseerd. De aanbiedende partij dient voor het vaststellen van de bezetting uit te gaan van een ontwikkelingsmodel voor wat betreft het aantal aan te sluiten ZSP's.
4. Voor de telefonische helpdesk: alle binnenkomende gesprekken worden (door Helpdesk personeel) beantwoord binnen 20 seconden na binnenkomst.
5. Alle e-mail-berichten worden tijdens openingstijden van de help desk binnen 1 uur na ontvangst beantwoord.
6. Registratie van gebruikers en/of uitgifte van OID's, IP-nummers of domeinnamen dient binnen 1 uur na ontvangst te zijn afgehandeld.
7. Gemelde problemen bij storingen dienen binnen 8 werkuren na de eerste melding te zijn afgehandeld.
8. Ten behoeve van de dienstverlening dient een maandelijks managementoverzicht te worden opgesteld, dat in ieder geval bevat:
 - Het aantal en type binnenkomende gesprekken en e-mails;
 - Het aantal beantwoorde gesprekken en e-mails en de gerealiseerde responsetijden en afhandelingstijden.

3.2.6 Opleveren managementinformatie

Met betrekking tot managementinformatie uit het LSP gelden de volgende **eisen**:

1. Het LSP dient rapportages op te leveren waarin de kwaliteit van de zorginfrastructuur wordt aangegeven in termen van beschikbaarheid, throughput en responsetijden.
2. Het LSP dient te beschikken over algemene onderzoeksmogelijkheden middels een standaard rapportagehulpmiddel. Dat betreft rapportages zowel over gegevens in de verwijsindex als gegevens uit gestelde vragen aan het LSP en door het LSP gegeven antwoorden. Met het rapportagehulpmiddel moet het bijvoorbeeld mogelijk zijn eenvoudig rapportages samen te stellen over het aantal foutberichten aan zorgpartijen.
3. Het moet mogelijk zijn om met standaard hulpmiddelen voor selectie en rapportage, alle in het LSP opgenomen gegevens toegankelijk en beschikbaar te maken.
4. Standaardrapportages die in ieder geval worden voorzien, zijn:
 - Vanuit het LSP dient informatie over het aantal gestelde vragen en gegeven antwoorden per soort samengesteld te kunnen worden.
 - Vanuit het LSP dient informatie over het aantal verzonden en ontvangen berichten per soort bericht en per zorgaanbieder samengesteld te kunnen worden. Dit om het in gebreke blijven van leveringen door GBZ'en te kunnen ontdekken.
5. Het LSP beschikt over een functie om inconsistenties in de gegevens van de ZIM en/of aangesloten GBZ'en te rapporteren.

3.2.7 Acceptatietestdiensten

Met betrekking tot test- en demonstratiefaciliteiten in het LSP gelden de volgende **eisen**:

1. Er zijn afzonderlijke omgevingen voor exploitatie en voor (acceptatie)testen. De testomgeving is bedoeld als (acceptatie)testomgeving voor opdrachtgever en voor ZSP's en zorgpartijen.
2. Het LSP dient te zorgen voor een adequate ondersteuning van ZSP's bij het testen van de interconnectiediensten en het testen van de implementatie en configuratie van de gebruikte hard- en software van zorgpartijen.
3. Een leverancier van een zorginformatiesysteem moet in de test-/acceptatieomgeving kunnen aantonen over een correcte implementatie en configuratie van de gebruikte hard- en software te beschikken. Mede op basis hiervan kan certificatie van dit systeem plaatsvinden. Dat wil zeggen dat, met dit afnemerssysteem een correcte verbinding naar het LSP kan opzetten en correct met het LSP kan communiceren (zoekvragen stellen, antwoorden ontvangen). Dit betreft zowel het opzetten van een beveiligde (SSL) verbinding, het inloggen op basis van de afnemernaam, het uitvoeren van bevestigingen en het verwerken van de response van het LSP. Voor deze testsessies moet een vaste set van zoekvragen worden gevolgd, waarbij

voor elke vraag vooraf de response door het LSP is vastgesteld. Elke vraag- en antwoordcyclus verloopt voor deze schouwing en toetsing identiek aan het gebruik van het LSP in de exploitatiesituatie. De response door het LSP is geautomatiseerd, op basis van een testset met LSP-gegevens, die door de opdrachtgever zal worden samengesteld.

Voor het beoordelen van deze testsessies moet de LSP-beheerder per sessie en per bevraging kunnen vaststellen welke gegevens met een vraagactie en welke gegevens met het bijbehorende antwoord zijn uitgewisseld. Deze verslaglegging of logging moet uit het LSP ook in een printbaar overzicht of bestand verstrekt kunnen worden.

4 Functies van de Zorg Informatie Makelaar

Dit hoofdstuk definieert de eisen die worden gesteld aan het te ontwikkelen systeem op basis waarvan het Landelijk Schakelpunt de vereiste diensten zal gaan leveren. Dit te ontwikkelen systeem wordt Zorg Informatie Makelaar (ZIM) genoemd.

Voor een compleet beeld van de samenhang tussen de functies van de ZIM en die van de aangesloten systemen (GBZ'en, DCN'en, SBV en UZI-register) wordt verwezen naar de "Specificatie van de Basisinfrastructuur in de Zorg", versie 2.1.

4.1 Definitie van ZIM

De ZIM wordt gedefinieerd als:

- de apparatuur en programmatuur die zelfstandig in staat is tot landelijke uitwisseling van patiëntgegevens en zorgaanbiedergegevens tussen GBZ'en, het UZI-register en de SBV-Z,
- inclusief alle aangesloten randapparatuur en hulpprogrammatuur, voor zover die onder beheer van het LSP of een door het LSP gedelegeerde beheerder staan,
- tot en met de toegang tot de DCN'en met alle aangesloten GBZ'en.
- dat tezamen fungeert als operationele-ZIM, dan wel als uitwijk-ZIM, dan wel als test-ZIM.

Opmerking: het vorige hoofdstuk eist dat er een aparte operationele omgeving, een aparte testomgeving en later ook een aparte uitwijkomgeving moet komen. De bovenstaande definitie is mede bedoeld om aan te geven dat iedere omgeving een ZIM moet hebben dat voldoet aan de eisen gespecificeerd in dit hoofdstuk.

4.2 Informatie & routeringsfuncties

In de volgende paragrafen wordt verwezen naar de functies (F1...F8) zoals deze zijn geïntroduceerd bij de laatste figuur met toelichting in paragraaf 2.2.

De ZIM dient te voorzien in de volgende functies (F1):

- (a) De ZIM dient HL7v3-berichten uit het domein *identificaties* te accepteren van een GBZ-gebruiker, deze door te sturen naar het relevante register en het antwoord van het register terug te sturen naar de GBZ-gebruiker, zoals aangegeven in de onderstaande tabel.
- (b) De ZIM dient HL7v3-berichten uit het domein *verwijsindex* te accepteren van een GBZ-gebruiker, en te beantwoorden, zoals aangegeven in de onderstaande tabel, waarbij:
 - a. een eerste aanmelding leidt tot een nieuwe verwijzing in de verwijsindex voor de vermelde patiënt, gegevenssoort en actualiteit,
 - b. een bijgewerkte aanmelding leidt tot een overschreven verwijzing in de verwijsindex voor de vermelde patiënt, gegevenssoort en actualiteit,
 - c. het opvragen van een overzicht leidt tot het opleveren van alle verwijzingen voor de vermelde patiënt, gegevenssoort en actualiteit, behalve die m.b.t. patiëntgegevens waarvoor de GBZ-gebruiker niet geautoriseerd is.
- (c) De ZIM dient HL7v3-opvraagberichten uit de overige domeinen te accepteren van een GBZ-gebruiker, deze door te sturen naar alle GBZ'en genoemd in de verwijsindex voor de vermelde patiënt, gegevenssoort en actualiteit, en de antwoorden van die GBZ'en terug te sturen naar de opvragende GBZ-gebruiker, zoals aangegeven in de onderstaande tabel, waarbij:
 - a. de ZIM de antwoorden moet doseren indien de opvragende GBZ-gebruiker dit had gevraagd,
 - b. de ZIM de antwoorden moet samenvoegen in een batch indien de opvragende GBZ-gebruiker dit had gevraagd,Mechanismen voor samenvoegen en doseren worden beschreven in bijlage C van de "Specificatie van de Basisinfrastructuur in de Zorg".
- (d) De ZIM dient HL7v3-verstuurberichten uit de overige domeinen te accepteren van een GBZ-gebruiker, door te sturen naar het in het bericht vermelde GBZ en een bevestiging terug te sturen naar de versturende GBZ-gebruiker, zoals aangegeven in de onderstaande tabel, waarbij:

- a. de ZIM het bericht onmiddellijk aflevert bij het bestemde GBZ en indien deze niet beschikbaar is meteen een foutmelding oplevert aan de versturende GBZ-gebruiker.
- (e) De ZIM dient elk van de HL7v3-berichten in de onderstaande tabel van een GBZ-gebruiker te beantwoorden met een MCCI_IN000002-bericht met foutmelding in de volgende gevallen:
- a. indien de GBZ-gebruiker zich niet geauthenticeerd heeft,
 - b. indien de GBZ-gebruiker niet geautoriseerd is,
 - c. indien de ZIM het type HL7v3-bericht niet ondersteunt,
 - d. indien de ZIM het type HL7v3-bericht niet verwacht,
 - e. indien de ZIM nog bezig is met het afhandelen van een transactie naar aanleiding van het vorige HL7v3-bericht,
 - f. indien de ZIM het HL7v3-bericht niet kan verwerken wegens capaciteitstekort,
 - g. indien het bestemde systeem de gevraagde gegevens niet beschikbaar heeft,
 - h. indien het bestemde systeem niet beschikbaar is,
 - i. indien het bestemde systeem niet bekend is,
 - j. indien het bestemde systeem niet binnen de time-out reageert,
 - k. indien het bestemde systeem het type HL7v3-bericht niet ondersteunt,

Zie verder de foutmeldingen in de "HL7v3 Implementatiegids Infrastructurele Domeinen".

- (f) De ZIM dient elk van de uitgewisselde HL7v3-berichten in de onderstaande tabel te loggen in de toegangslog.
- (g) De ZIM dient het overige IP-verkeer tussen verschillende DCN'en te routeren.
- (h) De ZIM dient een website te onderhouden dat zorgaanbieders, ZSP's, XIS-leveranciers en patiënten/cliënten wegwijs maakt in de diensten geleverd door het LSP.
- (i) (toekomst) De ZIM dient patiënten/cliënten via het web toegang te verlenen tot hun autorisatieprofiel en toegangslog, zoals beschreven in paragraaf 4.3 en paragraaf 4.4.

Merk op dat sommige HL7v3-berichten van een GBZ-gebruiker een retourbericht voor die GBZ-gebruiker oplevert en andere niet. Alle HL7v3-berichten kunnen echter een MCCI_IN000002-bericht met foutmelding opleveren.

De onderstaande tabel geeft een overzicht van:

- welke berichten de ZIM kan ontvangen van een GBZ-gebruiker,
- naar welke systemen de ZIM dit bericht eventueel moet doorsturen, en
- welke berichten de ZIM moet antwoorden aan de initiërende GBZ-gebruiker.

<i>Bericht te ontvangen van GBZ</i>	<i>HL7-code</i>	<i>Door te sturen naar</i>	<i>Bericht te antwoorden aan GBZ</i>	<i>HL7-code</i>	<i>Time-out</i>
<i>Domein Identificaties</i>					
OpvragenPatiëntIdentificatie met BSN	QUPA_IN 101101	SBV	opleverenPatiëntIdentificatie	QUPA_IN 101102	6 sec
opvragenPatiëntIdentificatie zonder BSN	QUPA_IN 101103	SBV	opleverenPatiëntIdentificatie	QUPA_IN 101104	6 sec
opvragenZorgaanbiederIdentificatie	PRPM_IN 406010	UZI-register	opleverenZorgaanbiederIdentificatie	PRPM_IN 406110	6 sec
<i>Domein Verwijsindex</i>					
AanmeldenGegevens (eerste aanmelding)	MFMT_IN 002101	Niet			
AanmeldenGegevens (bijgewerkte aanmelding)	MFMT_IN 002102	Niet			
afmeldenGegevens	MFMT_IN 002103	Niet			
opvragenOverzicht	QUMT_IN 020010	Niet	opleverenOverzicht	QUMT_IN 020020	
<i>Domein Medicatie</i>					
versturenMedicatievoorschrift	PORX_IN 932000NL	GBZ vermeld in bericht			6 sec
versturenMedicatieverstrekking	PORX_IN 924000NL	GBZ vermeld in bericht			6 sec
opvragenMedicatievoorschriften (eerste opvraag)	QURX_IN 990001NL	GBZ'en vermeld in VWI	opleverenMedicatievoorschriften	QURX_IN 990003NL	6 sec
opvragenMedicatievoorschriften (vervolg opvraag)	QUQI_IN 000003	GBZ'en vermeld in VWI	opleverenMedicatievoorschriften	QURX_IN 990003NL	6 sec

OpvragenMedicatieverstrekingen (eerste opvraag)	QURX_IN 990011NL	GBZ'en vermeld in VWI	opleverenMedicatieverstrekingen	QURX_IN 990013NL	6 sec
opvragenMedicatieverstrekingen (vervolg opvraag)	QUQI_IN 000003	GBZ'en vermeld in VWI	opleverenMedicatieverstrekingen	QURX_IN 990013NL	6 sec
<i>Domein Waarneming Huisartsen</i>					
opvragenProfessioneleSamenvatting	QUGP_IN 100001	GBZ'en vermeld in VWI	opleverenProfessioneleSamenvatting	QUGP_IN 100002	6 sec
versturenWaarneemRetourbericht	QUGP_IN 100003	GBZ vermeld in bericht			6 sec

De HL7-code is een verwijzing naar de HL7v3-standaard, die exact definieert hoe de berichten moeten worden geformatteerd, gevuld, verpakt en verzonden.

De time-out is het tijdinterval dat de ZIM na doorsturen van het ontvangen bericht moet wachten op antwoord, voordat een foutmelding wordt teruggegeven aan het GBZ. In geval van een opvraagbericht met meerdere antwoordberichten, gaat het om het eerste antwoordbericht.

De time-out is instelbaar door de systeembeheerder. De waarde van 6 seconde is voorlopig een uitgangspunt, waarvan in de praktijk moet blijken of deze bijgesteld moet worden voor een optimale uitwisseling van berichten.

4.3 Autorisatiebeheer

De ZIM dient te voorzien in de volgende functies (F2) ten behoeve van de autorisatiebeheerder voor de volgende taken:

- beheren algemeen autorisatieprotocol,
- beheren medisch autorisatieprotocol,
- beheren autorisatieprofielen.

(toekomst) en ten behoeve van de patiënt/cliënt voor het beheren van zijn eigen autorisatieprofiel.

Voor alle taken geldt:

- (a) De autorisatiebeheerder moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen tot de ZIM.
- (b) de autorisatiebeheerder moet het algemene en het medische autorisatieprotocol en de autorisatieprofielen kunnen raadplegen, waarbij hij kan kiezen voor:
 - de actuele situatie,
 - een historische situatie, door invoer van een datum in het verleden.
- (c) de ZIM moet bijhouden in de autorisatielog welke autorisatiebeheerder op welk tijdstip welke wijziging heeft doorgevoerd.
- (d) de autorisatiebeheerder moet logregels in de autorisatielog tot 10 jaar oud kunnen raadplegen, waarbij:
 - logregels jonger dan 3 maanden binnen 5 seconden na oproep verschijnen,
 - logregels ouder dan 3 maanden binnen 15 minuten na oproep verschijnen,
 - zekerheid bestaat dat eenmaal aan de autorisatielog toegevoegde logregels niet meer kunnen worden gewijzigd of verwijderd.

Voor de taak *beheren algemeen autorisatieprotocol* geldt:

- (e) de autorisatiebeheerder moet het algemene autorisatieprotocol kunnen aanpassen, door voor iedere combinatie van
 - opvragende zorgpartij
 - opleverende zorgpartij
 - de gegevensklassede bevoegdheid vast te leggen met:
 - de bevoegde transactie(s): aan/afmelden, opvragen, versturen

- autorisatieniveau
- vereiste vertrouwensniveau: laag, midden, hoog
- ingangsdatum van wijziging

Voor de taak *beheren medisch autorisatieprotocol* geldt:

- (f) de autorisatiebeheerder moet het medische autorisatieprotocol kunnen aanpassen, door voor iedere combinatie van
- de functie van de zorgaanbieder
 - de betrokkenheid van de zorgaanbieder: hoofdbehandelaar, waarnemer, medebehandelaar
 - de gegevenssoort
- de bevoegdheid vast te leggen met:
- de bevoegde transactie(s): aan/afmelden, opvragen, versturen
 - autorisatieniveau
 - vereist vertrouwensniveau: laag, midden, hoog
 - ingangsdatum van wijziging

Voor de taak *beheren autorisatieprofielen* geldt:

- (g) de autorisatiebeheerder moet voor een patiënt/cliënt kunnen wijzigen:
- het wel/niet akkoord gaan met elektronische uitwisseling van zijn patiëntgegevens door zorgaanbieders,
 - (toekomst) het wel/niet akkoord gaan met elektronisch inkijken in de toegangslog door hemzelf,
 - (toekomst) het wel/niet akkoord gaan met elektronisch inkijken van zijn autorisatieprofiel door hemzelf,
 - (toekomst) het wel/niet akkoord gaan met elektronisch wijzigen van zijn autorisatieprofiel door hemzelf.
- (h) de autorisatiebeheerder moet het autorisatieprofiel van een patiënt/cliënt kunnen aanpassen, door voor iedere combinatie van
- zorgpartij, eventueel uitgedrukt in functie of identiteit
 - de gegevensklasse
- de bevoegdheid tot toegang vastleggen met:
- altijd
 - alleen in noodsituatie
 - na expliciete toestemming
 - nooit
- (i) de autorisatiebeheerder moet een juridisch geldig bewijs vastleggen (op papier of elektronisch) van het feit dat de patiënt/cliënt de nieuwe instellingen heeft gezien en daarmee uitdrukkelijk akkoord gaat.

(j) (toekomst) de patiënt/cliënt moet zijn autorisatieprofiel kunnen aanpassen zoals vermeld onder (g) en (h).

4.4 Toegangslogbeheer

De ZIM dient te voorzien in de volgende functies (F3) ten behoeve van de logbeheerder en (toekomst) de patiënt/cliënt:

- (a) De logbeheerder moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen tot de ZIM.
- (b) De logbeheerder moet een lijst van logregels kunnen oproepen, die per logregel de volgende attributen kunnen tonen, voor zover relevant:
 - de identiteit van de patiënt/cliënt,
 - de functie, identiteit en betrokkenheid van de agerende zorgaanbieder,
 - de functie en identiteit van de eventueel reagerende zorgaanbieder(s)
 - de uitgevoerde transactie,
 - de gegevenssoort, dan wel het overzicht van gegevenssoorten,
 - het tijdstip van de transactie,
 - het toegepaste vertrouwensniveau,
 - een indicatie of een beroep is gedaan op een noodsituatie,
 - een indicatie van eventueel opgetreden foutsituaties.
- (c) De logbeheerder moet voor de lijst van logregels kunnen selecteren dat uitsluitend worden getoond:
 - logregels voor een bepaalde patiënt/cliënt,
 - logregels binnen een bepaald tijdvenster,
 - logregels van bepaalde transactiesoorten,
 - bepaalde attributen per logregel.
- (d) De logbeheerder moet:
 - kunnen bladeren door de lijst van logregels,
 - kunnen bepalen volgens welk attribuut de logregels in de lijst op volgorde worden gezet,
 - kunnen zoeken in de lijst naar logregels met een aangegeven waarde voor één of meer van de attributen,
 - een te bepalen deel van de lijst kunnen afdrukken,
 - een te bepalen deel van de lijst kunnen exporteren naar een intelligent analysegereedschap.
- (e) De logbeheerder moet logregels tot 10 jaar oud kunnen raadplegen, waarbij:

- logregels jonger dan 3 maanden binnen 5 seconden na oproep verschijnen,
 - logregels ouder dan 3 maanden binnen 15 minuten na oproep verschijnen,
 - zekerheid bestaat dat eenmaal aan de toegangslog toegevoegde logregels niet meer kunnen worden gewijzigd of verwijderd.
- (f) De logbeheerder moet de zekerheid hebben dat eenmaal aan de toegangslog toegevoegde logregels niet meer kunnen worden gewijzigd of verwijderd.
- (g) (toekomst) De patiënt/cliënt moet dezelfde functies krijgen als de logbeheerder, met dien verstande dat hij alleen logregels m.b.t. hemzelf kan inzien.

4.5 Klantenondersteuning

De ZIM dient te voorzien in de volgende functies (F4) ten behoeve van de ondersteuning van de ZSP's als klant:

- (a) De klantenondersteuning moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen tot de ZIM.
- (b) De klantenondersteuning moet een overzicht kunnen oproepen van alle variabelen voor iedere geconfigureerde ZIM, zoals nader gespecificeerd onder F5.
- (c) De klantenondersteuning moet een overzicht kunnen oproepen van alle variabelen voor ieder geconfigureerd DCN, zoals nader gespecificeerd onder F5.
- (d) De klantenondersteuning moet een overzicht kunnen oproepen van alle variabelen voor ieder geconfigureerd GBZ, zoals nader gespecificeerd onder F5.

Merk op dat de ZIM niet hoeft te voorzien in functies voor het vastleggen, bijhouden en volgen van hulpaanvragen. Hiervoor bestaan nl. goede COTS-oplossingen.

4.6 Systeembeheer

De ZIM dient te voorzien in de volgende functies (F5) ten behoeve van de systeembeheerder voor de volgende taken:

- beheren ZIM,
- beheren DCN-koppeling aan ZIM,
- beheren GBZ-koppeling aan ZIM,
- beheren alarmmeldingen.

Voor alle taken geldt:

- (a) De systeembeheerder moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen tot de ZIM.
- (b) Bij het oproepen van een overzicht van variabelen van beheerobjecten, moet de gebruiker kunnen kiezen uit:
 - *actuele* waarden: lopende gemiddelden/totalen over een instelbaar dynamisch tijdsinterval (bijv. seconde, minuut, uur).
 - *historische* waarden: gerealiseerde gemiddelden/totalen over een instelbaar historisch tijdsinterval (bijv. jaar, maand, week, dag).
- (c) Bij het oproepen van een overzicht van variabelen van beheerobjecten, moet de systeembeheerder kunnen kiezen uit:
 - *grafiek*: grafische presentatie van het verloop van de actuele of historische waarden van te kiezen variabelen over een instelbaar tijdsinterval.
 - *tabel*: tabellarische presentatie van het verloop van de historische waarden van te kiezen variabelen over een instelbaar tijdsinterval met instelbare tussenstappen (bijv. alle maandelijke waarden van een jaar).
 - *diagram*: presentatie van een statisch diagram (dat bijv. de aansluiting van een GBZ voorstelt) waarin de actuele waarden van te kiezen variabelen dynamisch worden gepresenteerd, in de kleur die overeenkomt met de eventuele alarmtoestand, zie use case 6.4.
 - *log*: chronologische lijst van gewijzigde variabelen, waarbij in geval van stuurparameters of configuratieparameters wordt vermeld welke systeembeheerder op welk tijdstip welke wijziging heeft doorgevoerd.

Voor de taak *beheren ZIM* geldt:

- (d) De systeembeheerder moet een overzicht kunnen oproepen van de volgende *variabelen* voor iedere geconfigureerde ZIM:

- beschikbaarheid van deze ZIM,
 - aantal GBZ'en dat is:
 - geconfigureerd voor aansluiting op de ZIM,
 - daadwerkelijk aangesloten op de ZIM,
 - aantal gebruikers dat:
 - nieuw heeft ingelogd,
 - vergeefs heeft geprobeerd in te loggen,
 - actief ingelogd is,
 - zojuist heeft uitgelogd,
 - gebruikte on-line opslagruimte door de:
 - berichtenwachtrij,
 - toegangslog,
 - autorisatielog,
 - systeemlog,
 - alarmlog.
 - tijdstip van de laatste volledige resp. incrementele backup,
 - alle stuurparameters en configuratieparameters voor deze ZIM,
- en de volgende variabelen voor iedere afzonderlijke schakelpunt binnen deze ZIM, plus de totalen/gemiddelden over alle schakelpunten van deze ZIM indien zinvol:
- beschikbaarheid van het schakelpunt,
 - per transactiesoort en per gegevenssoort:
 - aantal transacties per seconde,
 - aantal mislukte transacties, uitgesplitst naar foutsoort,
 - aantal transacties dat via een ander schakelpunt afgehandeld moest worden,
 - gemiddeld aantal uitgewisselde patiëntstukken per transactie,
 - gemiddeld aantal uitgewisselde bytes per transactie,
 - minimum, gemiddelde en maximum responstijd,
 - aantal applicaties dat:
 - geconfigureerd is voor aansluiting op het schakelpunt,
 - daadwerkelijk is aangesloten op het schakelpunt,
 - alle stuurparameters en configuratieparameters van dit schakelpunt.

(e) De systeembeheerder moet de volgende *stuurparameters* kunnen instellen voor iedere geconfigureerde ZIM:

- status van de koppeling van deze ZIM met andere ZIM's:
 - opengesteld,
 - geblokkeerd,
- modus van de ZIM:
 - operationeel,
 - test,
 - gereed,

- onderhoud,
 - beschikbare on-line opslagruimte voor de:
 - berichtenwachtrij,
 - toegangslog,
 - autorisatielog,
 - systeemlog,
 - alarmlog,
 - tijdsinterval tussen het laatste HL7v3-bericht en het moment waarop de ZIM de SSL-verbinding met het GBZ automatisch afbreekt,
 - tijdsinterval tussen het laatste HL7v3-bericht en het moment waarop de ZIM de SSL-verbinding met de GBZ-gebruiker automatisch afbreekt,
 - maximum aantal gelijktijdige SSL-verbindingen met een GBZ-gebruiker (gebruikerssessies) per GBZ,
- en de volgende stuurparameters kunnen instellen voor iedere afzonderlijk schakelpunt, dan wel voor alle schakelpunten tegelijk indien zinvol:
- beschikbaarheid van het schakelpunt,
 - per gegevenssoort:
 - maximum aantal patiëntstukken dat het schakelpunt per opvraag zal opleveren aan een opvragende applicatie,
 - maximum aantal patiëntstukken dat het schakelpunt per opvraag zal opvragen bij een achterliggende applicatie,
 - tijdsinterval na een aanmelding aan de verwijzindex, waarbinnen de applicatie nieuwe patiëntgegevens niet opnieuw hoeft aan te melden,
 - maximum tijdsinterval dat het schakelpunt wacht op een opleverende applicatie, voordat het schakelpunt een foutmelding teruggeeft aan de opvragende applicatie,
 - maximum tijdsinterval dat het schakelpunt wacht op een ontvangstbevestiging, voordat het schakelpunt een foutmelding teruggeeft aan de versturende applicatie.

(f) De systeembeheerder moet binnen iedere ZIM schakelpunten kunnen toevoegen en verwijderen, en voor de ZIM de volgende *configuratieparameters* kunnen instellen:

- URL,
- IP-adres,
- UZI-nummer van de systeemgebonden UZI-pas,
- E-mail-adres van de ZIM-beheerder,
- telefoonnummer van de ZIM-beheerder,

en voor ieder afzonderlijk schakelpunt:

- OID,
- naam van het schakelpunt zoals gebezigd door de beheerders,

- HL7v3 conformance claim,
 - gebruikte HL7v3-release.
- (g) De systeembeheerder moet voor iedere ZIM de volgende acties kunnen ondernemen op de verwijfsindex:
- verwijderen van alle verwijzingen naar een bepaalde applicatie van een bepaald GBZ,
 - synchroniseren met de verwijfsindices van de andere ZIM's,
 - kopiëren van de inhoud van de verwijfsindex van een andere ZIM.
- (h) De systeembeheerder moet voor iedere ZIM de volgende acties kunnen ondernemen op de logboeken:
- archiveren van de logboeken op een off-line opslagmedium,
 - terughalen van (een deel van) een logboek naar de on-line opslagruimte.
- (i) De systeembeheerder moet voor iedere ZIM de volgende acties kunnen ondernemen:
- maken van een volledige back-up,
 - maken van een incrementele back-up,
 - terughalen van een back-up.

Voor de taak *beheren DCN-koppeling aan ZIM* geldt:

- (j) De systeembeheerder moet een overzicht kunnen oproepen van de volgende *variabelen* voor ieder geconfigureerd DCN:
- netwerkbelasting van HL7v3-verkeer met de ZIM,
 - netwerkbelasting van overig IP-verkeer met ieder ander DCN.
- (k) De systeembeheerder moet de volgende *stuurparameters* kunnen instellen voor ieder geconfigureerd DCN:
- status van de koppeling van het DCN aan de ZIM:
 - opengesteld,
 - geblokkeerd,
 - maximum aantal aangesloten GBZ'en via dit DCN.
- (l) De systeembeheerder moet een DCN-koppeling kunnen toevoegen en verwijderen, en daarbij de volgende *configuratieparameters* kunnen instellen:
- IP-adresreeks voor het DCN,
 - naam van het DCN zoals bekend bij de ZSP en de zorginstellingen,
 - E-mail-adres van de DCN-beheerder,
 - telefoonnummer van de DCN-beheerder,

- DCN-kwalificatieniveau,
- datum eerste toelating,
- tekstuele toelichting,
- URL van de ZIM waarop dit DCN primair wordt aangesloten,
- URL van de alternatieve ZIM waarop dit DCN kan terugvallen.

Voor de taak *beheren GBZ-koppeling aan ZIM* geldt:

(m) De systeembeheerder moet een overzicht kunnen oproepen van de volgende *variabelen* voor ieder geconfigureerd GBZ:

- beschikbaarheid van het GBZ,
- alle stuurparameters en configuratieparameters voor dat GBZ,
- per gebruikerssessie:
 - UZI-nummer van de gebruiker,
 - vertrouwensniveau van de sessie,
 - tijdstip van inloggen,

en de volgende variabelen voor iedere afzonderlijke applicatie binnen dat GBZ, plus de totalen/gemiddelden over alle applicaties van dat GBZ indien zinvol:

- beschikbaarheid van de applicatie,
- per transactiesoort:
 - aantal transacties per seconde,
 - aantal mislukte transacties, uitgesplitst naar foutsoort,
 - aantal transacties dat via een ander schakelpunt afgehandeld moest worden,
 - minimum, gemiddelde en maximum responstijd bij actie,
 - minimum, gemiddelde en maximum responstijd bij reactie,
 - gemiddeld aantal uitgewisselde patiëntstukken per transactie,
 - gemiddeld aantal uitgewisselde bytes per transactie,
- alle stuurparameters en configuratieparameters voor die applicatie.

(n) De systeembeheerder moet de volgende *stuurparameters* kunnen instellen voor ieder geconfigureerd GBZ:

- status van de koppeling van het GBZ aan de ZIM:
 - opengesteld,
 - geblokkeerd,

en de volgende stuurparameters kunnen instellen voor iedere afzonderlijke applicatie, dan wel voor alle applicaties van dat GBZ tezamen indien zinvol:

- modus van de applicatie:
 - operationeel,
 - test,
 - gereed,
 - onderhoud.

(o) De systeembeheerder moet een GBZ-koppeling kunnen toevoegen en verwijderen, en daarbij de volgende *configuratieparameters* kunnen instellen:

- URL van het GBZ,
- IP-adres van het GBZ,
- naam van het GBZ zoals bekend bij de zorginstelling,
- nummer van de zorginstelling in het UZI-register,
- UZI-nummer van de systeemgebonden UZI-pas,
- E-mail adres van de GBZ-beheerder,
- telefoonnummer van de GBZ-beheerder,
- GBZ-kwalificatieniveau,
- datum eerste toelating,
- tekstuele toelichting,
- naam van het DCN waarop dit GBZ is aangesloten,

en binnen dat GBZ verscheidene applicaties kunnen toevoegen en verwijderen, en daarvoor de volgende configuratieparameters kunnen instellen:

- OID van de applicatie,
- naam van de applicatie zoals bekend bij de zorginstelling,
- HL7v3 conformance claim van de applicatie,
- gebruikte HL7v3-release.

(p) De systeembeheerder moet een tekstbericht kunnen sturen naar alle GBZ-gebruikers van:

- één bepaalde GBZ,
- alle GBZ'en aangesloten op een bepaalde DCN of ZIM,
- alle GBZ'en van alle ZIM's.

Voor de taak *beheren alarmmeldingen* geldt:

(q) De systeembeheerder moet voor iedere variabele van ieder type beheerobject één of meer alarmtoestanden kunnen definiëren met de volgende eigenschappen:

- de grenswaarde die bij onder- of overschrijding leidt tot een alarmtoestand,
- de alarmklasse waarin de variabele wordt gezet bij passeren van de grenswaarde,
- een tekstuele omschrijving van de alarmtoestand.

(r) De systeembeheerder moet verscheidene alarmklassen kunnen definiëren met de volgende eigenschappen:

- in welke kleur de alarmtoestand moet worden getoond in de lijst van alarmregels en in een overzicht van variabelen,
 - of bij eerste optreden een visueel en/of auditief signaal moet worden gegeven.
- (s) De systeembeheerder moet een lijst van alarmregels kunnen oproepen, die per alarmregel de volgende attributen kan tonen:
- de OID van het object,
 - de grenswaarde die was onder- of overschreden,
 - de opgetreden alarmklasse,
 - het tijdstip van dit optreden,
 - een tekstuele omschrijving van de alarmtoestand,
 - een indicatie of de alarmmelding reeds is "erkend",
 - de afhandelingstatus van de alarmtoestand,
 - de identificatie van de systeembeheerder die de afhandelingstatus het laatst heeft gewijzigd,
 - een tekstuele toelichting van die systeembeheerder,
- waarbij de kleur van de alarmregel overeenkomt met de alarmklasse.
- (t) De systeembeheerder moet voor de lijst van alarmregels kunnen selecteren dat uitsluitend worden getoond:
- alarmregels van bepaalde typen object,
 - alarmregels opgetreden binnen een bepaald tijdvenster,
 - alarmregels van bepaalde alarmklassen,
 - alarmregels met bepaalde afhandelingstatus,
 - bepaalde attributen per alarmregel.
- (u) De systeembeheerder moet:
- kunnen bladeren door de lijst van alarmregels,
 - kunnen bepalen volgens welk attribuut de alarmregels in de lijst op volgorde worden gezet,
 - de afhandelingstatus van een alarmregel kunnen wijzigen in:
 - nieuw,
 - erkend,
 - afgehandeld,
 - een tekstuele toelichting kunnen toevoegen aan een alarmregel,
 - een te bepalen deel van de lijst kunnen afdrukken,
 - een te bepalen deel van de lijst kunnen exporteren naar een intelligent analysegereedschap.

4.7 Test-beheer

De ZIM dient te voorzien in de volgende functies (F6) ten behoeve van de test-beheerder voor de volgende taken:

- beheren test-ZIM,
- beheren DCN-koppeling aan test-ZIM,
- beheren GBZ-koppeling aan test-ZIM,
- beheren alarmmeldingen van test-ZIM.

Voor alle taken geldt:

- (a) De test-beheerder moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen tot de ZIM die door de systeembeheerder in de modus *test* is gezet.

Voor de taak *beheren test-ZIM* geldt:

- (b) De test-beheerder moet een overzicht kunnen oproepen van alle variabelen voor de ZIM, zoals nader gespecificeerd onder F5.

Voor de taak *beheren DCN-koppeling aan test-ZIM* geldt:

- (c) De test-beheerder moet een overzicht kunnen oproepen van alle variabelen voor ieder in de test-ZIM geconfigureerd DCN, zoals nader gespecificeerd onder F5.
- (d) De test-beheerder systeembeheerder moet alle *stuurparameters* kunnen instellen voor ieder in de test-ZIM geconfigureerd DCN, zoals nader gespecificeerd onder F5.
- (e) De test-beheerder moet een DCN-koppeling aan de test-ZIM kunnen toevoegen en verwijderen, en daarbij alle *configuratieparameters* kunnen instellen, zoals nader gespecificeerd onder F5.

Voor de taak *beheren GBZ-koppeling aan test-ZIM* geldt:

- (f) De test-beheerder moet een overzicht kunnen oproepen van alle variabelen voor ieder in de test-ZIM geconfigureerd GBZ, zoals nader gespecificeerd onder F5.
- (g) De test-beheerder moet alle *stuurparameters* kunnen instellen voor ieder in de test-ZIM geconfigureerd GBZ, zoals nader gespecificeerd onder F5.

- (h) De test-beheerder moet een GBZ-koppeling aan de test-ZIM kunnen toevoegen en verwijderen, en daarbij alle *configuratieparameters* kunnen instellen, zoals nader gespecificeerd onder F5.

Voor de taak *beheren alarmmeldingen van test-ZIM* geldt:

- (i) De test-beheerder moet alarmmeldingen van de test-ZIM kunnen beheren, zoals nader gespecificeerd onder F5.

Merk op dat de taken van de test-beheerder sterk overeenkomen met die van de systeembeheerder, doch worden beperkt tot de ZIM die door de systeembeheerder in de modus *test* is gezet.

4.8 Applicatiebeheer

De ZIM dient te voorzien in de volgende functies (F7) ten behoeve van de applicatiebeheerder:

- (a) De applicatiebeheerder moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen tot de ZIM die door de systeembeheerder in de modus *onderhoud* is gezet.
- (b) de applicatiebeheerder moet nieuwe soorten en versies van HL7v3-berichten kunnen implementeren in de ZIM.
- (c) de applicatiebeheerder moet nieuwe zorgaanbiederfuncties kunnen definiëren door het vastleggen van:
 - de naam van de functie
 - de OID van de functiezodanig dat deze door de andere LSP-beheerders kunnen worden gebruikt.
- (d) de applicatiebeheerder moet nieuwe gegevenssoorten kunnen definiëren door het vastleggen van:
 - de naam van de gegevenssoort
 - de OID van de gegevenssoortzodanig dat deze door de andere LSP-beheerders kunnen worden gebruikt.
- (e) de applicatiebeheerder moet nieuwe versies van softwarecomponenten kunnen plaatsen op een ZIM met de modus *onderhoud*.

4.9 Aansturing en verantwoording

De ZIM dient te voorzien in de volgende functies (F8) ten behoeve van de LSP-opdrachtnemer:

- rapporteren aan LSP-opdrachtgever,
- beheren LSP-medewerkers.

Voor alle taken geldt:

- (a) De LSP-opdrachtnemer moet zich kunnen identificeren en authenticeren en vervolgens toegang krijgen de ZIM.

Voor de taak *rapporteren aan LSP-opdrachtgever* geldt:

- (b) De LSP-opdrachtnemer moet een overzicht kunnen maken van alle variabelen voor iedere geconfigureerde ZIM, zoals nader gespecificeerd onder F5.
- (c) De LSP-opdrachtnemer moet een overzicht kunnen oproepen van alle variabelen voor ieder geconfigureerd DCN, zoals nader gespecificeerd onder F5.
- (d) De LSP-opdrachtnemer moet een overzicht kunnen oproepen van alle variabelen voor ieder geconfigureerd GBZ, zoals nader gespecificeerd onder F5.
- (e) Bij het oproepen van een overzicht van variabelen van beheerobjecten, moet de LSP-opdrachtnemer kunnen kiezen uit grafiek, tabel en log, zoals nader gespecificeerd onder F5.
- (f) Na het oproepen van een overzicht van variabelen van beheerobjecten, moet de LSP-opdrachtnemer kunnen kiezen voor:
- *export*: vastleggen van geselecteerde historische waarden in een exportbestand dat kan worden geladen in een intelligent analyse-gereedschap.
 - *rapportage*: vastleggen van het gepresenteerde in een rapport, dat kan worden opgeslagen, teruggehaald, gepresenteerd, afgedrukt en per E-mail verstuurd.

Voor de taak *beheren LSP-medewerkers* geldt:

(g) De LSP-opdrachtnemer moet LSP-medewerkers kunnen autoriseren voor één van de volgende beheerfuncties:

- autorisatiebeheerder,
- logbeheerder,
- klantenondersteuning,
- systeembeheerder,
- test-beheerder,
- applicatiebeheerder,
- LSP-opdrachtnemer.

(h) De LSP-opdrachtnemer moet voor iedere LSP-medewerker de omvang van de geleverde diensten kunnen bewaken:

- *autorisatiebeheerder*: aantal afgehandelde verzoeken van de autorisatiemanager,
- *logbeheerder*: aantal afgehandelde verzoeken van de toezichthouder,
- *klantenondersteuning*: aantal afgehandelde hulpvragen van de ZSP-klantenondersteuning,
- *systeembeheerder*: aantal afgehandelde alarmmeldingen en configuratieverzoeken van de ZSP-systeembeheerder,
- *test-beheerder*: aantal afgehandelde tests van zorgaanbieders en XIS-leveranciers,
- *applicatiebeheerder*: aantal nieuwe soorten en versies van HL7v3-berichten geïmplementeerd op verzoek van NICTIZ-programmanagers,
- *LSP-opdrachtnemer*: aantal opgeleverde rapportages.

Merk op dat de ZIM niet hoeft te voorzien in een intelligent analysegereedschap. Hiervoor bestaan nl. goede COTS-oplossingen.

4.10 Connectiviteit

De ZIM dient ten behoeve van F1 te voldoen aan de volgende connectiviteitseisen:

- (a) De ZIM dient te kunnen worden gekoppeld met GBZ'en via verscheidene DCN'en.
- (b) De ZIM dient te zijn gekoppeld met de SBV en het UZI-register via een directe verbinding.
- (c) De ZIM dient voor berichtuitwisseling met de GBZ'en de volgende protocolstack te ondersteunen:
 - HTTP
 - SSL v3.0 of TLS v1.0
 - TCP
 - IP
- (d) De ZIM dient voor het sturen van HL7v3-berichten naar een GBZ, een SSL/TLS-verbinding met dat GBZ'en te maken, waarbij:
 - tweezijdige authenticatie tussen het vertrouwensmiddel van de ZIM en dat van het GBZ (systeemgebonden UZI-pas) plaatsvindt,
 - de ZIM de SSL/TLS-verbinding afbreekt wanneer het door het systeembeheerder ingestelde tijdsinterval sinds het laatste HL7v3-bericht is verstreken, maar niet eerder dan dat een transactie is afgehandeld.
- (e) De ZIM dient voor het ontvangen van HL7v3-berichten van een GBZ-gebruiker, het GBZ in staat te stellen een SSL/TLS-verbinding met de ZIM te maken, waarbij:
 - tweezijdige authenticatie tussen het vertrouwensmiddel van de ZIM en dat van de GBZ-gebruiker (persoonsgebonden UZI-pas) plaatsvindt,
 - de ZIM de SSL/TLS-verbinding afbreekt wanneer het door het systeembeheerder ingestelde tijdsinterval sinds het laatste HL7v3-bericht is verstreken, maar niet eerder dan dat een gebruikerstransactie is afgehandeld,
 - het maximum aantal gelijktijdige gebruikerssessies per GBZ niet wordt overschreden.
- (f) (toekomst) De ZIM dient voor webtoegang door een Internetgebruiker, gangbare webbladeraars in staat te stellen een SSL/TLS-verbinding met de ZIM te maken, waarbij:

- eenzijdige authenticatie tussen het vertrouwensmiddel van de ZIM en dat van de internet-gebruiker (e-NIK) plaatsvindt,
- de ZIM de SSL/TLS-verbinding afbreekt wanneer het door het systeembeheerder ingestelde tijdsinterval sinds de laatste HTTP-interactie is verstreken,
- het maximum aantal gelijktijdige internetsessies niet wordt overschreden.

4.11 Beveiliging

De ZIM dient te voldoen aan de volgende beveiligingseisen:

- (a) De ZIM dient redelijkerwijs te worden beschermd tegen dreigingen van buiten (bijv. brand, stroomuitval, blikseminslag).
- (b) De ZIM dient te worden beschermd tegen fysieke indringers, door plaatsing in ruimten die alleen toegankelijk zijn voor medewerkers van het LSP die noodzakelijkerwijs fysieke toegang tot die onderdelen moeten hebben in het belang van goed functioneren.
- (c) De ZIM dient zoveel mogelijk te worden beschermd tegen elektronische indringers, door middel van *intrusion detection* en *intrusion prevention*.
- (d) De ZIM dient een systeemidentificatiemiddel te hebben dat op naam staat van de LSP-opdrachtgever en is gecertificeerd door een CA onder de root van de Staat der Nederlanden.
- (e) De ZIM dient zijn systeemidentificatiemiddel zodanig te beschermen dat deze niet kan worden gekopieerd, gewijzigd of verwijderd, zonder toestemming van de LSP-opdrachtgever.
- (f) De ZIM dient een SSL/TLS-verbinding met een GBZ of een GBZ-gebruiker te weigeren indien voor het vertrouwensmiddel (UZI-pas) van dat GBZ resp. de GBZ-gebruiker blijkt dat:
 - de geldigheidstermijn is verlopen of nog niet aangevangen,
 - het niet correct is ondertekend door de CA van het UZI-register,
 - het staat op de lijst van ingetrokken vertrouwensmiddellen (CRL) van het UZI-register.
- (g) De ZIM dient minimaal eens in de 4 uur een nieuwe lijst van ingetrokken vertrouwensmiddellen (CRL) op te halen van het UZI-register.
- (h) (toekomst) De ZIM dient een SSL/TLS-verbinding met een internet-gebruiker te weigeren indien voor het vertrouwensmiddel (e-NIK) van die gebruiker blijkt dat:
 - de geldigheidstermijn is verlopen of nog niet aan is gevangen,
 - het niet correct is ondertekend door de desbetreffende CA,
 - het staat op de lijst van ingetrokken vertrouwensmiddellen (CRL) van het e-NIK-register.

4.12 Beschikbaarheid

De ZIM dient te voldoen aan de volgende beschikbaarheidseisen, gemeten over een kalenderjaar:

- (a) De ZIM dient 24 uur per dag en 7 dagen per week beschikbaar te zijn voor het afhandelen van berichten vanuit alle aangesloten GBZ'en en bediening van de andere functies door de medewerkers van het LSP.
- (b) Kleine storingen in de ZIM mogen maximaal 12 keer per jaar voorkomen (MTBF) en dienen dan binnen 1 kwartier (MTTR) te zijn opgelost.
- (c) Grote storingen in de ZIM mogen maximaal 1 keer per jaar voorkomen (MTBF) en dienen dan binnen 24 uur (MTTR) te zijn hersteld, waarbij:
 - a. binnen 1 uur na optreden van de storing wordt overgeschakeld naar een andere ZIM;
 - b. binnen 1 kwartier na herstel van de storing wordt teruggestakeld.
- (d) Gepland onderhoud van de ZIM waarbij GBZ'en moeten overschakelen, mag maximaal 2 keer per jaar geschieden (MTBF) in het weekend en dient dan binnen 24 uur (MTTR) te zijn afgerond, waarbij:
 - a. de beheerders van de over te schakelen GBZ'en 2 weken van te voren moeten worden ingelicht,
 - b. de gebruikers van de over te schakelen GBZ'en 1 uur van te voren moeten worden ingelicht,
 - c. binnen 1 kwartier na aanvang van het onderhoud wordt overgeschakeld naar een andere ZIM;
 - d. binnen 1 kwartier na afronding van het onderhoud wordt teruggestakeld.
- (e) Storingen in de ZIM als gevolg van overmacht (bijv. overstroming, aardbeving, bomaanslag) dienen binnen redelijke termijn te worden hersteld, waarbij:
 - a. binnen 1 dag na optreden van de storing wordt overgeschakeld naar een uitwijk-ZIM;
 - b. binnen 1 dag na herstel van de storing wordt teruggestakeld.

4.13 Responstijden

De ZIM dient te voldoen aan de volgende eisen:

- (a) De ZIM dient de onderstaande responstijden te kunnen halen, waarbij:
- responstijden worden gemeten over een jaar,
 - een opvraagtransactie gedoseerd wordt tot deelopvragen met als antwoord een hoeveelheid patiëntgegevens dat redelijkerwijs op één scherm getoond kan worden,
 - de capaciteit van de ZIM is zoals beschreven in paragraaf 4.14.

<i>Transactiesoort</i>	<i>Gemiddelde responstijd</i>	<i>90% binnen responstijd</i>
<i>Domein Identificaties</i>		
opvragenPatiëntIdentificatie	2 sec	4 sec
opvragenZorgaanbiederIdentificatie	2 sec	4 sec
<i>Domein Verwijsindex</i>		
aanmeldenGegevens	1 sec	2 sec
afmeldenGegevens	1 sec	2 sec
opvragenOverzicht	1 sec	2 sec
<i>Domein Medicatie</i>		
versturenMedicatievoorschrift	1 sec	2 sec
versturenMedicatieverstrekking	1 sec	2 sec
opvragenMedicatievoorschriften	2 sec	4 sec
opvragenMedicatieverstrekingen	2 sec	4 sec
<i>Domein Waarneming Huisartsen</i>		
opvragenProfessioneleSamenvatting	2 sec	4 sec
versturenWaarneemRetourbericht	1 sec	2 sec

4.14 Capaciteit

De ZIM dient te voldoen aan de volgende capaciteitseisen:

(a) De ZIM dient bij aanvang van de exploitatietermijn het aantal berichten zoals vermeld in onderstaande tabel te kunnen verwerken, met daarbij:

- 7000 aangesloten GBZ'en;
- 10 aangesloten DCN'en;
- 1000 gelijktijdige gebruikerssessies;
- gemiddeld 5 kByte per uitgewisseld bericht.

<i>Transactiesoort</i>	<i>Aantal berichten te ontvangen van en te beantwoorden aan GBZ</i>	<i>Aantal berichten door te sturen naar en te ontvangen van ander GBZ of register</i>
<i>Domein Identificaties</i>		
opvragenPatiëntIdentificatie	6.400.000/jr	6.400.000/jr
opvragenZorgaanbiederIdentificatie	2.800.000/jr	2.800.000/jr
<i>Domein Verwijsindex</i>		
aanmeldenGegegevens	28.000.000/jr	0
afmeldenGegegevens	2.800.000/jr	0
opvragenOverzicht	800.000/jr	0
<i>Domein Medicatie</i>		
versturenMedicatievoorschrift	28.000.000/jr	28.000.000/jr
versturenMedicatieverstrekking	2.800.000/jr	2.800.000/jr
opvragenMedicatievoorschriften	2.800.000/jr	5.600.000/jr
opvragenMedicatieverstrekingen	28.000.000/jr	56.000.000/jr
<i>Domein Waarneming Huisartsen</i>		
opvragenProfessioneleSamenvatting	800.000/jr	800.000/jr
versturenWaarneemRetourbericht	800.000/jr	800.000/jr

De aantallen berichten in de tabel zijn gebaseerd op de onderstaande aannamen:

- 140.000.000 medicatievoorschriften per jaar, die leiden tot:
 - voor 10% tot opvragenPatiëntIdentificatie door de huisarts
 - voor 10% tot opvragenPatiëntIdentificatie door de apotheek
 - voor 10% tot opvragenZorgaanbiederIdentificatie door de huisarts
 - voor 100% tot versturenMedicatievoorschrift van huisarts aan apotheek
 - voor 10% tot aanmeldenGegegevens door de huisarts
 - voor 10% tot aanmeldenGegegevens door de apotheek
 - voor 10% tot versturenMedicatieverstrekking van apotheek aan huisarts

- voor 10% tot opvragen Medicatievoorschriften door huisarts of apotheek
- voor 50% tot opvragen Medicatieverstrekkingen door huisarts
- voor 50% tot opvragen Medicatieverstrekkingen door apotheek
- een opvraag leidt tot gem. 2 opleveringen door een verschillende bron
- 100.000.000 huisartscontacten per jaar, waarvan 5% interveniërende waarnemingen, die leiden tot:
 - voor 80% tot opvragen PatiëntIdentificatie door de waarnemer
 - voor 80% tot opvragen Overzicht door de waarnemer
 - voor 80% tot opvragen Professionele Samenvatting door de waarnemer
 - voor 80% tot versturen WaarneemRetourbericht door de waarnemer
- bij aanvang van de exploitatietermijn moet de ZIM in staat zijn tenminste 20% van de uiteindelijke berichtenstroom voor medicatie een waarneming huisartsen te verwerken.

4.15 Schaalbaarheid

De ZIM dient te voldoen aan de volgende schaalbaarheidseisen:

- (a) De ZIM dient zodanig ontworpen te worden dat er geen intrinsieke beperkingen zijn voor opschaling naar:
- 20.000 aangesloten GBZ'en
 - 50 aangesloten DCN'en
 - 10.000 gelijktijdige gebruikerssessies
 - 10 keer zoveel berichten als vermeld in de tabel van paragraaf 4.14 door uitbreiding van het aantal hardwarecomponenten.
- (b) het LSP dient binnen 2 maanden na geconstateerde overschrijding van de responstijden, de capaciteit van de ZIM te vergroten, zodanig dat de gemiddelde responstijden weer zijn zoals voor de overschrijding d.w.z. terug binnen de gestelde grenzen.

4.16 Betrouwbaarheid

De ZIM dient te voldoen aan de volgende betrouwbaarheidseisen:

- (a) Wanneer de ZIM uitvalt, nadat verstuurbedichten waren ontvangen van een GBZ en bevestigd aan het GBZ, maar voordat deze berichten waren

afgehandeld conform paragraaf 4.2, dient de ZIM deze berichten binnen 1 uur na volledig herstel van de ZIM, alsnog af te afhandelen.

- (b) Wanneer een GBZ of diens verbinding met de ZIM uitvalt, dient de ZIM alle verstuurbedichten voor dit GBZ te bewaren, en binnen 1 kwartier na herstel van het GBZ, alsnog toe te sturen, voorzover deze verstuurbedichten nog niet met een foutmelding waren teruggegeven aan de versturende GBZ-gebruiker.

4.17 Systeembeheer

De ZIM dient te voldoen aan de volgende eisen betreffende beheer:

- (a) Wanneer de ZIM door diens beheerder wordt INgeschakeld, en dus (weer) beschikbaar is, dient de ZIM dit te melden aan alle aangesloten GBZ'en.
- (b) Wanneer de ZIM door diens beheerder wordt UITgeschakeld, en dus niet langer beschikbaar is, dient de ZIM dit vooraf te melden aan alle aangesloten GBZ'en met een inschatting van de tijdsduur van onbeschikbaarheid.
- (c) De beheerder van de ZIM en diens vervangers dienen met telefoonnummers bekend te zijn bij de beheerders van alle GBZ'en, waarbij altijd tenminste één beheerder bereikbaar is en in staat is de nodige beheertaken uit te voeren.
- (d) De ZIM dient binnen een nader te specificeren aantal dagen na het beschikbaar komen van nieuwe patches voor het dichten van beveiligingslekken, deze patches te hebben geïnstalleerd.

5 Fasering van de te leveren diensten en functies

5.1 Inleiding

Binnen deze fasering wordt een groeimodel gehanteerd. De planning van de beoogde dienstverlening is ambitieus en is nog maar op een zeer beperkt aantal plaatsen in de wereld op een landelijke schaal operationeel. Dit betekent dat de aan te besteden dienst in nauwe samenwerking met de opdrachtgever in een aantal fasen zal moeten groeien naar operationele dienstverlening op landelijke schaal. Hierbij zullen tussentijds voldoende afstemmingsmomenten worden ingebouwd om, indien noodzakelijk, te komen tot bijstellingen of uitbreiding van de eisen of van de verdere invulling van de dienstverlening.

Na de ontwikkelfase van de technische infrastructuur (ZIM) en de bijbehorende organisatorische invulling (LSP) zal een integratietest met veldpartijen noodzakelijk zijn om de juiste werking van het LSP in samenhang met zijn omgeving aan te tonen. Dit betekent dat wordt aangetoond dat alle functies van het ontwikkelde systeem en de dienstverlening op beperkte schaal werken volgens de gedefinieerde eisen. Bovendien dient de samenwerking met andere dienstenleveranciers in de keten te zijn beproefd en de correcte werking daarvan te zijn aangetoond.

Aansluitend zal in een aantal veldtests worden beproefd of de dienstverlening ook in de praktijksituatie van de zorgaanbieder en overige zorgwerkers voldoet. Bovendien moet worden onderzocht in hoeverre de gekozen oplossingen voldoende flexibel en schaalbaar zijn om een sterke groei van het aantal aangesloten zorgsystemen te kunnen accommoderen.

Afgesloten zal worden met de acceptatie, direct gevolgd door de operationele fase. Tijdens de operationele fase zal bij een relatief klein gebruikersvolume in eerste instantie nog geen full-service dienstverlening worden geëist.

5.2 Ontwikkelfase

De leverancier zal op basis van het programma van eisen een ZIM en de processen van de LSP ontwikkelen en testen. Van de opdrachtnemer wordt verwacht dat hij zelf programma-, integratie- en systeemtesten van zijn eigen systeem uitvoert en daar een rapportage over verstrekt aan de opdrachtgever.

5.3 Integratietest met zorginformatiesystemen in het veld

In deze fase zullen de procedures voor aansluiting van zorgsystemen worden

beproefd. Voor deze procedure dient een script voor aansluiting in samenwerking met de leveranciers van de betrokken GBZ'en en de ZSP te worden ontwikkeld en vastgesteld. Dit script zal dan in de praktijk moeten worden beproefd.

Achtereenvolgens zullen in een beperkt aantal zorginstellingen/regio's veldtesten worden uitgevoerd om de operationele werking van het LSP te beproeven. Per regio wordt daartoe een aantal zorgsystemen aangesloten conform het opgestelde script. Het betreft hier een aantal, dat als bron voor medicatie-informatie dienen en een aantal huisarts- en ziekenhuissystemen die inzage in het medicatiedossier kunnen bieden en tevens kunnen worden gebruikt om het e-waarneemdossier voor huisartsen te implementeren.

Uitgangspunt is dat tijdens de veldtests verschillende GBZ-uitvoeringsvormen worden beproefd om te bepalen wat vanuit de praktijk het beste evolutiescenario is om te migreren van de huidige situatie naar de gewenste eindsituatie.

Voor elke proefregio zal de veldtest worden afgesloten met een uitgebreide evaluatie op de volgende punten:

- Script voor aansluiting GBZ
- Functies testen
- Technische en organisatorische aspecten
- Gebruikerstevredenheid
- Impact op zorgproces
- Schaalbaarheid van de oplossing

5.4 Acceptatietest & Operationele fase

Het LSP-ontwerp zal schaalbaar moeten zijn om de gedefinieerde diensten te leveren voor het beoogde aantal gebruikers en klanten op landelijke schaal. Dit wordt beproefd in de acceptatietestfase, middels een stresstest, maar zal ook in de praktijk worden getest aan de hand van de groei in het aantal aangesloten zorgsystemen en regionale zorgnetwerken.

Een uitgebreidere acceptatietest zal worden uitgevoerd door de ZIM te koppelen aan een beperkt aantal GBZ'en.

Daartoe zal met een aantal leveranciers van zorgsystemen afspraken worden gemaakt om hun systemen geschikt te maken voor de AORTA-basisinfrastructuur.

Met die systemen zullen de volgende testen worden uitgevoerd:

- Aansluiten GBZ en ZIM;
- Toetsen communicatie en foutcondities;
- Controleren of aanmelding bij en vulling van de verwijfsindex (VWI) goed verloopt;
- Toetsen of Queries goed worden beantwoord;

- Routing van de berichten stromen;
- Controleren of authenticatie van de zorgaanbieder goed verloopt;
- Testen of autorisatie correct werkt;

In een eind-tot-eind test bepalen of de gedefinieerde responsetijden worden gehaald.

Na een geslaagde systeemtest vindt samen met de opdrachtgever een acceptatietest plaats. Het testplan hiervoor zal gezamenlijk met de opdrachtgever worden opgesteld. Dit testplan omvat naast de bovenbeschreven technische en functionele testen ook een beproeving om te bepalen of de dienstverlening en organisatorische aspecten voldoen aan de gestelde eisen. Tenslotte wordt beproefd of wordt voldaan aan de eisen van schaalbaarheid door een aantal stresstesten uit te voeren. Na het geslaagd doorlopen van het testplan kan tot acceptatie van het systeem worden overgegaan.

Na geslaagde veldtests zullen steeds meer zorgaanbieders worden aangesloten en meer regio's gebruik gaan maken van de dienstverlening van het LSP. Het is de bedoeling dat de dienstverlening in 2006 zal toe groeien naar een potentiële dekking op landelijk niveau door alle regio's te laten aansluiten. Met het uitbreiden van het aantal zorgaanbieders dat gebruik kan gaan maken van de dienstverlening is waarschijnlijk een langere periode gemoeid.

6 Bijlagen

6.1 Normatieve referenties

De onderstaande documenten worden als leidend beschouwd voor deze specificatie:

[Masterplan] "Masterplan Nationaal ICT Instituut in de Zorg" april 2002, NICTIZ.

[Actieplan] "Actieplan 2003 en programma naar 2005", september 2002, NICTIZ.

[Architectuurontwerp] "Architectuurontwerp Basisinfrastructuur in de Zorg", versie 4.1, april 2004, NICTIZ.

[HL7 v3] "HL7 Version 3 Standard" © 2002 Health Level Seven ®, Inc. Deze standaard is belangrijk voor het voorliggende document. Echter, HL7 richt zich op de informatie-uitwisseling *tussen* systemen en doet geen uitspraken over informatieverwerking of -ordening *binnen* systemen.

[WBP] "Wet Bescherming Persoonsgegevens"

[WGBO] "Wet op de geneeskundige behandelingsovereenkomst"

De aanstaande wet op het ZIN/BSN

6.2 Afkortingen:

AIS	Apotheek Informatie systeem
BGP-4	Border Gateway Protocol version 4
BSN	Burger Service Nummer
CIBG	Centraal Informatiepunt Beroepen Gezondheidszorg
CVA	Cerebro Vasculair Accident
DBC	Diagnose Behandeling Combinaties
DCN	Data Communicatie Netwerk
DNS	Domain Name System
EPD	Elektronisch Patiënten Dossier
GBZ	Goed Beheerd Zorgsysteem
HIS	Huisarts Informatie Systeem
HL7v3	Health Level 7 versie 3
HTTP	HyperText Transport Protocol
IBIZ	InformatieBeveiliging In de Zorg
ICT	Informatie & Communicatie Technologie
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
LEPD	Landelijk Elektronisch Patiënten Dossier
LIS	Laboratorium Informatie Systeem
MIC	Medisch Informatica Congres
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NEN	Het Nederlands Normalisatie-instituut
NICTIZ	Nationaal ICT Instituut in de Zorg
OIZ	vereniging van Organisaties voor ICT in de Zorg
OSPF	Open Shortest Path First (=protocol)
OZIS	Open Zorg Informatie Systeem
PAB	Patiënten AdresBoek
RIM	Referentie Informatie Model
RIS	Radiologie Informatie Systeem
SBV-Z	Sectorale Berichten Voorziening in de Zorg
SIDN	Stichting Internet Domeinregistratie Nederland
SLA	Service Level Agreement
SSC	Shared Service Centre
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security (=protocol)
TTP	Trusted Third Party
UZI	Uniek Zorgverleners Identificatie
UZOVI	Unieke Identificatie voor de Zorgverzekeraars
VPN	Virtual Private Network
WBP	Wet Bescherming Persoonsgegevens
WGBO	Wet op de geneeskundige behandelingsovereenkomst
XML	Extensible Markup Language
ZAB	Zorgverleners AdresBoek
ZIM	Zorg Informatie Makelaar
ZIN	Zorg Identificatie Nummer
ZIS	Ziekenhuis Informatie Systeem
ZSP	Zorg Service Provider

Tenslotte: overal in dit document waar de voornaamwoorden "hij" of "zijn" staat, wordt "hij of zij" resp. "zijn of haar" bedoeld.