CIZ
Europalaan 100
3526 KS Utrecht
Postbus 2222
3500 GE Utrecht

T 088 - 789 15 00
F 088 - 789 15 05
info.utrecht@ciz.nl
www.ciz.nl

ARCHITECTUUR INFORMATIEVOORZIENING
KADERS EN RICHTLIJNEN

centrum indicatiestelling zorg

Architectuur Informatievoorziening
Kaders en Richtlijnen

Documentbeheer

Titel	Architectuur Informatievoorziening Kaders en Richtlijnen
Versie	1.1
Datum	23-6-2016
Auteurs	Gert Jan Balster (CIO Office)
Status	Publicabel
Klassificatie	Intern
Versie info	Review en update door Moniek Jansen, Simeon Bas en Gert Jan Balster (CIO Office)

centrum indicatiestelling zorg

Architectuur Informatievoorziening Kaders en Richtlijnen

Inhoudsopgave

Architectuur Informatievoorziening
Kaders en Richtlijnen

1 Inleiding

1.1 Doel van dit document

Voor de inrichting van haar informatievoorziening hanteert het CIZ een werkwijze waarbij de planning en uitvoering van vernieuwingen plaatsvinden "met architectuur". Hierbij worden een aantal kaders en richtlijnen gehanteerd die moeten borgen dat de genoemde vernieuwingen passen binnen de algehele structuur en samenhang van de CIZ informatievoorziening en die bijdragen aan de ontwikkeling daarvan conform de CIZ informatiestrategie.

De betreffende *Architectuur Kaders en Richtlijnen* voor de CIZ informatievoorziening (IV) worden voor een belangrijk deel "extern" aangereikt vanuit de specifieke positie en taakstelling van het CIZ als publieke instantie met de rol van indicatiesteller in het kader van de Wet Langdurige Zorg. Het gaat dan om de toepasselijke wet- en regelgeving alsmede de verschillende normen, richtlijnen, afspraken en generieke voorzieningen binnen de (rijks)overheid en/of binnen de zorgsector. In aanvulling op deze externe kaders ontwikkelt het CIZ haar eigen, meer concrete en specifieke, kaders en richtlijnen.

De Architectuur Kaders en Richtlijnen voor de CIZ informatievoorziening kunnen worden gehanteerd bij het formuleren en beoordelen van wijzigings- en projectvoorstellen en van systeemontwerpen op impact, risico, haalbaarheid en toekomstvastheid. Daarnaast vormen ze een belangrijk instrument bij de uitvoering van projecten. Voor elk project zou daarom een Project Start Architectuur moeten worden opgesteld. Hierin wordt bij aanvang van een project aangegeven in hoeverre wordt voldaan aan de Architectuur Kaders en Richtlijnen alsmede welke aanvullende project-specifieke ontwerpkeuzen worden gemaakt.

Dit document bevat een compleet overzicht van de Architectuur Kaders en Richtlijnen voor de informatievoorziening van het CIZ en is daarmee bedoeld als een praktische referentie voor de bovengenoemde doeleinden.

1.2 Indeling

In de hoofdstukken 2, 3 en 4 wordt eerst ingegaan op de "externe" kaders en richtlijnen. Hoofdstuk 2 beschrijft de toepasselijke wet- en regelgeving. Hoofdstuk 3 identificeert de referentiearchitecturen en standaarden die van toepassing zijn op de omgeving en taakstelling van het CIZ. Hoofdstuk 4 behandelt de generieke voorzieningen die vanuit de overheid of de zorgketen worden aangeboden voor het uitwisselen van digitale informatie.

De hoofdstukken 5, 6 en 7 beschrijven de "eigen" toegespitste kaders en richtlijnen van en voor het CIZ. Hoofdstuk 5 gaat in op de voor de informatievoorziening relevante algemene CIZ beleidskaders, zoals het informatiebeveiligingsbeleid. Hoofdstuk 6 benoemt de reeds beschikbare doelarchitecturen waarin de gewenste toekomstige inrichting van de CIZ informatievoorziening is vastgelegd. Hoofdstuk 8 gaat over de principes en richtlijnen die gelden voor het uitvoeren van wijzigingen (projecten) in de CIZ informatievoorziening.

In hoofdstuk 7 wordt tenslotte nader beschreven op welke wijze de architectuurkaders moeten worden gehanteerd bij het formuleren en beoordelen van wijzigings- en projectvoorstellen, projectplannen en systeemontwerpen.

2 Wet- en regelgeving

Het behoeft geen nadere toelichting dat het CIZ te allen tijde moet voldoen aan de eisen die voortvloeien uit de Nederlandse wet- en regelgeving. Voor de informatievoorziening zijn enerzijds de daarop betrekking hebbende bepalingen uit de verschillende wetten voor de zorgsector relevant. Anderzijds gaat het om de wetten en de overheidsnormen op het gebied van persoonsgegevens en informatiebeveiliging.

2.1 Wetgeving zorgsector

2.1.1 Wet langdurige zorg (Wlz)

De kerntaak van het CIZ is het beoordelen of burgers recht hebben op zorg via de Wet langdurige zorg (Wlz). De Wlz vormt daarom het primaire wettelijke kader voor het CIZ. Voor de informatievoorziening zijn met name de informatiebepalingen uit de Wlz van belang (Wlz – Hoofdstuk 9). Deze gaan enerzijds over de verwerking van gegevens, waaronder bijzondere persoonsgegevens (Wlz – Artikel 9.1.1-9.1.7) en anderzijds over beleidsinformatie (Wlz – Artikel 9.2.1). De genoemde bepalingen zijn opgenomen in bijlage 1.

Referenties:

- *http://wetten.overheid.nl/BWBR0035917/2016-01-01*

2.1.2 Besluit Uitvoering Kinderbijslag (BUK) en Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Bopz)

Naast de taakstelling op grond van de Wlz geeft het CIZ advies aan de Sociale Verzekeringsbank omtrent de gezondheidssituatie van kinderen in het kader van het Besluit Uitvoering Kinderbijslag (BUK). Het CIZ toetst verder nog of cliënten opgenomen mogen worden in een besloten instelling, op basis van de Wet Bijzondere Opnemingen in Psychiatrische Ziekenhuizen (Bopz). De Bopz wordt op termijn vervangen door de Wet Zorg en Dwang en de Wet verplichte GGZ.

De betreffende wetten bevatten verder geen bepalingen die specifiek van toepassing zijn op de informatievoorziening.

Referenties:

- *http://wetten.overheid.nl/BWBR0035261/2016-01-01http://wetten.overheid.nl/BWBR0005700/2016-01-01*

2.1.3 Wet Maatschappelijke Ondersteuning (Wmo)

De Wet Maatschappelijke Ondersteuning (Wmo) regelt de gemeentelijke ondersteuning op het gebied van zelfredzaamheid, participatie, beschermd wonen en opvang. Op basis van deze wet geeft het CIZ aan gemeenten door of cliënten wel of niet de beschikking hebben over een Wlz-besluit in de vorm van een verblijfsindicatie.

Referenties:

- *http://wetten.overheid.nl/BWBR0035362/2016-06-14*

2.1.4 Wet gebruik Burgerservicenummers in de zorg (Wbsn-z)

De Wet gebruik Burgerservicenummer in de zorg (vaak afgekort tot Wbsn-z) vormt een uitbreiding op de Wet algemene bepalingen Burgerservicenummer (Wabb) en regelt het gebruik van het Burgerservicenummer (BSN) in de medische zorg. De wet stelt onder meer als eis dat een zorgaanbie-

der bij het verstrekken van persoonsgegevens met betrekking tot de verlening van, indicatiestelling voor, of verzekering van zorg aan een zorgaanbieder, een indicatieorgaan of een zorgverzekeraar steeds het Burgerservicenummer van de cliënt vermeldt (Wbsn-z – Artikel 9).

Referenties:

- *http://wetten.overheid.nl/BWBR0023864/2016-01-01*

2.2 Privacy en informatiebeveiliging

2.2.1 Wet bescherming persoonsgegevens

Het CIZ werkt als onderdeel van de zorgketen met medische en dus zeer gevoelige gegevens van burgers. De bescherming van de privacy van de betrokkenen is daarom van het grootste belang en moet dan ook voldoen aan de wet- en regelgeving die hiervoor is vastgesteld.

De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens. De Wbp regelt ook de taken en bevoegdheden van het College Bescherming Persoonsgegevens (CBP) als toezichthouder op deze en aanverwante wet- en regelgeving. De belangrijkste bepalingen uit de Wbp kunnen als volgt worden samengevat:

- Persoonsgegevens mogen alleen conform de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.
- Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en gebruikt.
- De personen waarvan de gegevens worden verwerkt moeten ten minste op de hoogte zijn van de identiteit van de organisatie die hun gegevens verwerkt en van het doel van de betreffende gegevensverwerking.
- De gegevensverwerking moet op een adequate manier worden beveiligd. Voor bijzondere gegevens, zoals ras, gezondheid en geloofsovertuiging gelden extra strenge regels.
- De voor de gegevensverzameling en bewerking verantwoordelijke instantie is verplicht er voor te zorgen dat een eventueel door hem ingeschakelde gegevensbewerker zich aan de bepalingen houdt en dient dit vast te leggen in een overeenkomst (de "bewerkersovereenkomst").
- Met ingang van 1 januari 2016 is een wijziging op de Wbp van kracht die onder meer voorziet in een meldingsplicht voor de instantie die verantwoordelijk is voor de gegevensverwerking wanneer sprake is van een (aanzienlijke kans op een) datalek met ernstige nadelige gevolgen voor de personen wiens gegevens het betreft. De meldingsplicht geldt zowel aan deze personen als aan de Autoriteit Persoonsgegevens.

Referenties:

- *http://wetten.overheid.nl/BWBR0011468/2016-01-01*
- *http://wetten.overheid.nl/BWBR0036695/geldigheidsdatum_18-11-2015*

2.2.2 Normenkaders overheid voor informatiebeveiliging

Vanuit de overheid worden verschillende normenkaders aangereikt voor het beveiligen van informatie en informatiesystemen. Deze normenkaders kunnen bindend of richtinggevend zijn. De voor het CIZ toepasselijke normenkaders worden hieronder kort besproken.

Het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) is een oorspronkelijk in 1995 van kracht geworden en in 2007 vernieuwd besluit dat algemene eisen stelt aan de beveiliging van de informatievoorziening en de informatiesystemen binnen de rijksoverheid, ongeacht de toegepaste technologie en het karakter van de informatie. Het gaat daarbij met name om het identificeren en toekennen van de verantwoordelijkheden in de organisatie. In het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) uit 2013 worden aanvullende maatregelen gespecificeerd voor de behandeling van vertrouwelijke informatie bij de rijksdienst en wordt hier ook een rubricering voor gedefinieerd.

Waar het VIR en het VIR-BI de algemene eisen beschrijven waaraan de beveiliging van de informatiesystemen moet voldoen, wordt in de Baseline Informatiebeveiliging Rijksdienst (BIR) een gemeenschappelijk normenkader aangereikt voor de maatregelen die moeten worden genomen om aan de beveiligingseisen te voldoen. De BIR richt zich daarbij specifiek op de eisen die gelden ten aanzien van informatie op het vertrouwelijkheidsniveau "Departementaal Vertrouwelijk" uit de VIR-BI en privacygevoelige informatie in risicoklasse 2, zoals gedefinieerd door de Registratiekamer (voorloper van de Autoriteit Persoonsgegevens). Tot deze laatstgenoemde risicoklasse behoren persoonsgegevens m.b.t. godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens.

De BIR bestaat uit een Technisch Normen Kader (BIR-TNK) en een Operationele Handreiking (BIR-OH). De BIR-TNK is gebaseerd op de internationale standaarden voor informatiebeveiliging NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 en geeft daarop een aantal nadere in- en aanvullingen voor de rijksoverheid. De BIR-TNK is bindend volgens het Comply-or-Explain principe. De BIR-OH bevat implementatierichtlijnen op basis van best practices waarmee invulling kan worden gegeven aan de TNK, maar deze zijn niet bindend.

2.2.3 Overige normen voor informatiebeveiliging

Zoals vermeld, is de BIR gebaseerd op de internationale standaarden NEN-ISO/IEC 27001 en 27002. Deze standaarden zijn (evenals de BIR zelf) ook opgenomen op de door het Forum Standaardisatie beheerde lijst van informatienormen waaraan overheidsinstellingen moeten voldoen op basis van het Comply-or-Explain beginsel.

NEN 7510 is een door het Nederlands Normalisatie-Instituut ontwikkelde en beheerde norm voor informatiebeveiliging in de zorg. De norm is van toepassing op alle organisaties werkzaam in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces. De norm geeft aan wat een organisatie moet doen om informatie te beveiligen, maar bevat geen expliciete aanwijzingen voor specifieke technische maatregelen. De norm kan worden gehanteerd in verschillende bij de zorg betrokken organisaties, zoals individuele zorgverleners, zorginstellingen, netwerkorganisaties, verzekeraars, certificerende organisaties en de Inspectie voor de Gezondheidszorg. Er zijn nog 2 aanvullende normen op NEN 7510: "NEN 7512 Informatiebeveiliging in de zorg – Vertrouwensbasis voor gegevensuitwisseling" en "NEN 7513 Medische Informatica – Logging – Vastleggen van acties op elektronische patiëntendossiers". Er is nog geen wettelijke verplichting of overheidsrichtlijn om aan NEN 7510 te voldoen, maar het is de verwachting dat dit voor zorginstellingen in de toekomst wel het geval zal worden. Wel hanteren de Inspectie voor de Gezondheidszorg en het ministerie van Volksgezondheid, Welzijn en Sport (WVS) al de NEN 7510 (en de afgeleide normen) bij het toetsen van zorginstellingen. Voor het CIZ is het daarom aan te bevelen om aan te sluiten bij deze norm waar deze relevant is voor de processen en systemen.

Referenties:

- *http://wetten.overheid.nl/BWBR0022141/geldigheidsdatum_18-11-2015*
- *http://wetten.overheid.nl/BWBR0033507/geldigheidsdatum_18-11-2015*
- *"Baseline Informatiebeveiliging Rijksdienst – Tactisch Normenkader (TNK)", versie 1.0 Definitief, 1 december 2012*

- *"Baseline Informatiebeveiliging Rijksdienst – Operationele Handreiking", versie 1.0, 30 oktober 2013*
- *"NEN 7510:2011 (nl) Medische Informatica – Informatiebeveiliging in de Zorg"*

3 Referentiearchitecturen en standaarden

Het CIZ maakt deel uit van de rijksoverheid c.q. de rijksdienst en tevens van de zorgketen, waarbinnen publieke en private partijen samenwerken om de uitvoering van de zorg conform de daarvoor geldende wetgeving uit te voeren. Het aansluiten bij gemeenschappelijke standaarden en voorzieningen binnen de overheid en de zorgketen vormt dan ook een van de doelstellingen van de IV-strategie van het CIZ. Dit betekent dat het CIZ zich ook conformeert aan de referentiearchitecturen en de daaraan gerelateerde technische standaarden die voor deze sectoren beschikbaar zijn.

3.1 Referentiearchitecturen

3.1.1 Nederlandse Overheid Referentie Architectuur (NORA)

De Nederlandse Overheid Referentie Architectuur (NORA) bevat kaders en afspraken voor het inrichten van de informatiehuishouding van de Nederlandse overheid. NORA omvat principes, standaarden, bouwstenen en een begrippenkader. Centraal staan de zgn. basisprincipes die de kwaliteitseisen beschrijven aan de overheidsdienstverlening vanuit het perspectief van afnemers (de samenleving, burgers en bedrijven):

BP01: Een proactieve overheid
Afnemers krijgen de dienstverlening waar ze behoefte aan hebben.

BP02: Eenvoudig te vinden overheidsdienstverlening
Afnemers kunnen de dienst eenvoudig vinden.

BP03: Eenvoudig toegankelijke overheidsdienstverlening
Afnemers hebben eenvoudig toegang tot de dienst.

BP04: Uniforme overheidsdienstverlening
Afnemers ervaren uniformiteit in de dienstverlening door gebruik van standaardoplossingen.

BP05: Gebundelde overheidsdienstverlening
Afnemers krijgen gerelateerde diensten gebundeld aangeboden.

BP06: Een transparante overheid
Afnemers hebben inzage in voor hen relevante informatie.

BP07: Een overheid die alleen noodzakelijke vragen stelt
Afnemers worden niet geconfronteerd met overbodige vragen.

BP08: Een overheid die vertrouwelijkheid van informatie garandeert
Afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt.

BP09: Een betrouwbare overheid
Afnemers kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt.

BP10: Een overheid die ontvankelijk is voor feedback
Afnemers kunnen input leveren voor de dienstverlening.

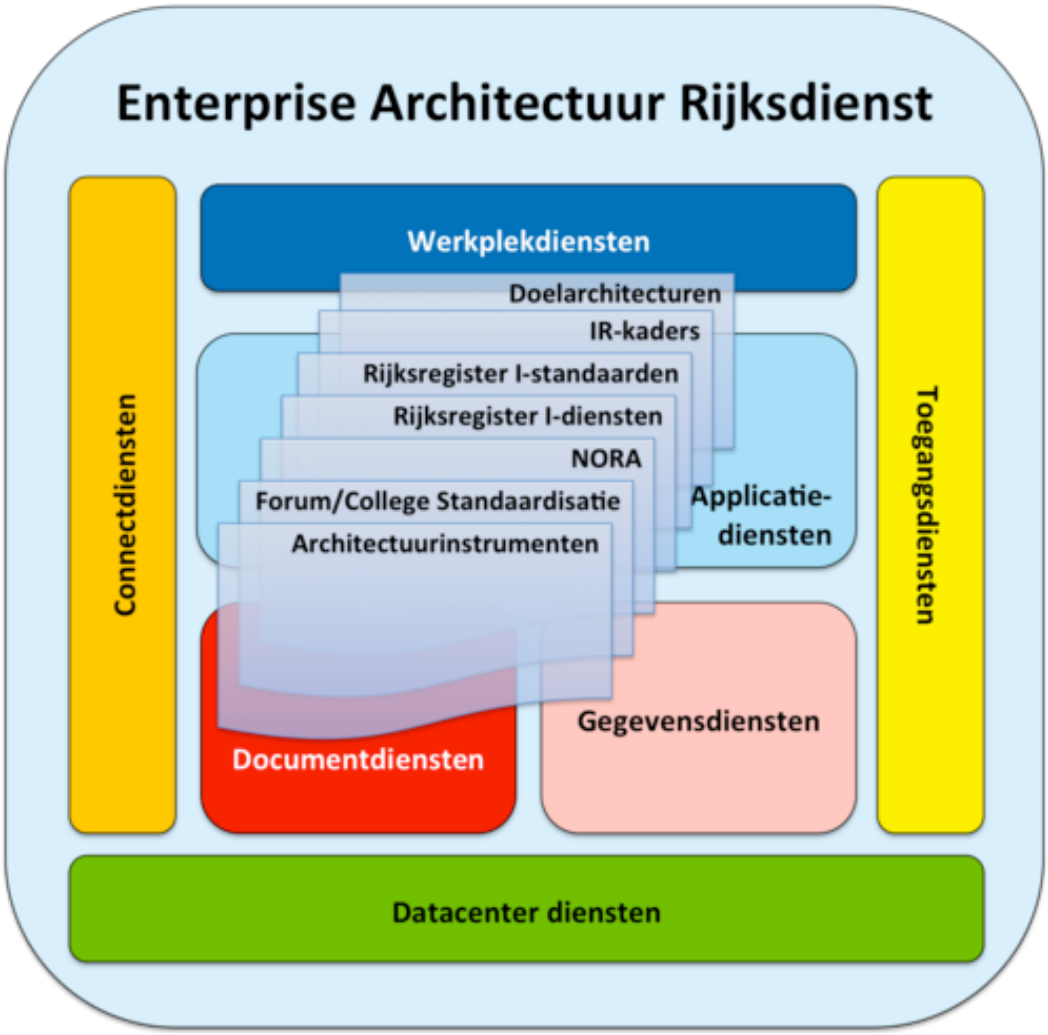
Referenties:

- *http://noraonline.nl*

3.1.2 Enterprise Architectuur Rijksdienst

De Enterprise Architectuur Rijksdienst (EAR) is de opvolger van de Model Architectuur Rijksdienst (MARIJ) en biedt een samenhangende beschrijving van de organisatie en de inrichting van de informatiediensten en voorzieningen van de rijksdienst, met als belangrijkste doel het verbeteren van

de samenwerking tussen de delen van de rijksdienst. EAR richt zich daarom enerzijds op de interoperabiliteit van de dienstverlening. Hiertoe worden de beginselen uit NORA nader gespecificeerd en gedetailleerd. Anderzijds richt EAR zich op een uniforme beschrijving van de inrichting van organisatie en informatievoorziening.



De EAR is gebaseerd op een indeling in domeinen. Door architectuur te ontwikkelen vanuit logische domeinen wordt EAR verdeeld in behapbare compartimenten. De rijksdienst als geheel is ook te beschouwen als een afgebakend gebied en dus een domein met subdomeinen. De EAR zelf is dus de overkoepelende domeinarchitectuur.

EAR maakt onderscheid tussen bedrijfsprocesdomeinen en informatiseringdomeinen. Binnen een informatiseringdomein worden vervolgens zeven deelgebieden onderscheiden, zoals verbeeld in bovenstaande figuur:

- Applicatiediensten
- Documentdiensten
- Gegevensdiensten
- Toegangsdiensten

- Werkplekdiensten
- Connectdiensten
- Datacenterdiensten

Enkele van deze domeinen bevatten inmiddels een doelarchitectuur of documenten die informatie bevatten die deels ook in doelarchitecturen is terug te vinden.

Het informatiseringdomein Werkplekdiensten richt zich op het leveren van betrouwbare en veilige diensten die bij het gebruik van de werkplek horen. Om samenwerken, gastgebruik en mobiliteit mogelijk te maken geldt: "Altijd, Overal, Ieder apparaat". In de "Functionele Doelarchitectuur Werkomgeving Rijksdienst (DWR)" wordt dit nader vertaald naar een functioneel beeld. Met betrekking tot "Ieder apparaat" wordt gestreefd naar ontkoppeling van functionaliteit en apparaat (in de functionele doelarchitectuur DWR wordt dat ook wel "zero footprint" werkplekken genoemd).

Daarnaast is het streven dat de medewerker van de rijksdienst zijn eigen "winkelmandje" met apparaten kan samenstellen. Dat mandje kan bestaan uit apparaten die beschikbaar worden gesteld (en beheerd) door de rijksdienst (Kies je eigen spullen) en door apparaten die de medewerker privé meeneemt (Breng je eigen spullen mee).

De ambities rondom Tijds-, Plaats- en Apparaatsonafhankelijk Werken (TPAW) zijn als onderdeel van de "I-strategie" en de "Hervormingsagenda" verder uitgewerkt in het "Streefbeeld TPAW 2015". Hierin wordt ook verwezen naar een groot aantal daaraan gerelateerde beleidsstukken, zoals de "Handreiking Tijd-, Plaats- en Apparaatonafhankelijk Werken".

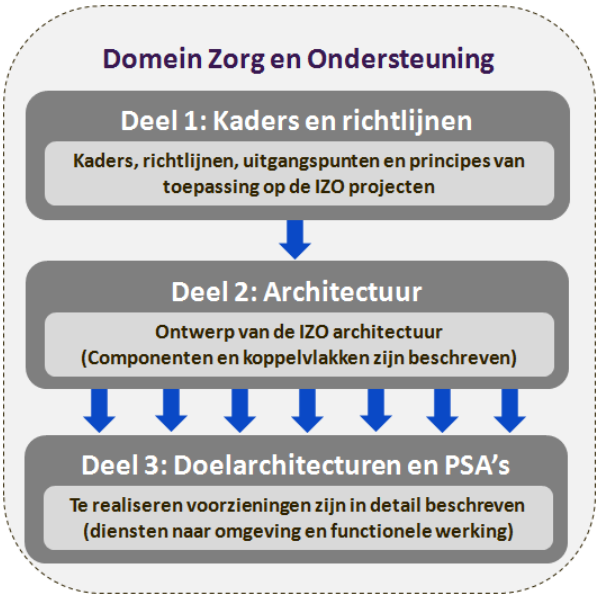
Referenties:

- *http://earonline.nl*
- *Functionele doelarchitectuur Digitale Werkomgeving Rijksdienst, versie 1.0, 12 december 2012.*
- *Streefbeeld TPAW 2015*
- *Handreiking Tijd-, Plaats- en Apparaatonafhankelijk Werken, Versie 2016, november 2015.*

3.1.3 Architectuur Informatievoorziening Zorg en Ondersteuning (IZO)

Door het Ministerie van VWS is het Platform Informatievoorziening Zorg en Ondersteuning (Platform IZO) ingesteld waarin ketenpartijen in de (langdurige) zorg gezamenlijk nieuwe initiatieven kunnen ontwikkelen en kunnen afstemmen op het gebied van de informatievoorziening. Dit moet bijdragen aan de versterking van de samenwerking en de synergie en aan een betere dienstverlening. Met ingang van 2016 is de organisatie van het platform en het beheer van de documentatie en informatie ondergebracht bij het Zorginstituut Nederland, waar ook al de verantwoordelijkheid ligt voor het beheer van de informatiestandaarden in de zorgsector (iStandaarden, zie ook par. 3.1.3). De communicatie verloopt via de website www.istandaarden.nl .

Het Platform IZO acteert vanuit een gedeeld toekomstbeeld dat ook als uitgangspunt is gehanteerd bij het ontwikkelen van de zgn. IZO-architectuur door een door het Platform IZO ingestelde architectuur-board. De IZO-architectuur richt zich primair op de technische interoperabiliteit van de diverse partijen in de keten. De IZO-architectuur omvat meerdere documenten waarin architectuurkaders en doelarchitecturen voor de gehele langdurige zorgketen, alsmede voor de specifieke domeinen daarbinnen worden beschreven.



Referentie: http://istandaarden.nl/architectuur .

3.2 Technische standaarden

Een standaard is een document waarin de specificaties of criteria voor een product, dienst of methode zijn vastgelegd. De overheid hecht veel waarde aan het gebruik van standaarden, omdat daarmee de samenwerking en gegevensuitwisseling tussen organisaties wordt vereenvoudigd en bevorderd. De overheid stimuleert daarom het gebruik van z.g. open standaarden, die vrijelijk kunnen worden gebruikt. Binnen de overheid worden daarom open standaarden geselecteerd en ook ontwikkeld ten behoeve van de informatie-uitwisseling tussen overheidsorganisaties onderling en met burgers en bedrijven. Hieronder wordt ingegaan op de voor het CIZ meest relevante technische standaarden, die vanuit de overheid worden voorgeschreven of aanbevolen.

3.2.1 Overheids-brede en rijks-brede open standaarden

Het Forum Standaardisatie beheert een lijst met open standaarden voor informatie-uitwisseling en verwerking die van toepassing zijn op alle overheidsinstanties. Deze standaarden zijn bindend op basis van het Comply-or-Explain principe. De I-standaardisatie Commissie Rijksdienst vult deze lijst nog verder aan met standaarden die specifiek gelden binnen de rijksdienst. De volledige lijst van overheids-brede en rijksdienst-specifieke standaarden is opgenomen in bijlage 2.

Voor het CIZ interessante standaarden uit deze lijst zijn onder meer:

- BIR 2012
  Betreft de BIR-TNK, zoals beschreven in par. 2.2.2.
- Digikoppeling standaard
  Digikoppeling versie 2.0 (versie 3.0 is in ontwikkeling) bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties.
- StUF
  Standaard uitwisselingsformaat (StUF) is een universele berichtenstandaard voor het elektronisch uitwisselen van gegevens tussen applicaties. Het domein van de StUF-taal omvat

informatieketens tussen overheidsorganisaties (basisregistraties en landelijke voorzieningen) en gemeente-brede informatieketens en -functionaliteiten. StUF is beschreven in XML en gebaseerd op geaccepteerde internetstandaarden.

Referenties:

- *http://www.earonline.nl/index.php/Totaal_overzicht_Standaarden_Rijksdienst*

3.2.2 Informatiestandaarden Zorg en Ondersteuning ("iStandaarden")

Het Zorginstituut Nederland beheert drie standaarden die bedoeld zijn voor elektronische berichtenuitwisselingen binnen de zorg en ondersteuning in het kader van de Wlz, de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet (Jw). Deze "iStandaarden" zijn respectievelijk iWlz, iWmo en iJw.

Voor het CIZ is iWlz uiteraard het meest relevant. De iWlz legt een z.g. BEP-model vast voor de Wlz-keten. BEP staat voor Bedrijfsregels, EI-standaarden en Processen, die in samenhang worden beschreven. Op basis van het BEP-model wordt vastgelegd welke informatie moet worden uitgewisseld tussen de ketenpartijen en vervolgens welke berichtenformaten daarvoor moeten worden gehanteerd. Voor de uitwisselingen met het CIZ zijn de volgende berichtenformaten gedefinieerd in de meest actuele versie van iWlz, versie 1.1:

Bericht	Titel	Richting	Beschrijving
IO31	Indicatiebesluit	CIZ naar zorgkantoor	Bericht met informatie over de geïndiceerde Wlz-zorg.
IO32	Retourinformatie Indicatiebesluit	Zorgkantoor naar CIZ	Bericht voor retourinformatie over het indicatiebesluit.
IO35	Aanvraag Indicatiebesluit	Zorgaanbieder naar CIZ	Bericht met gegevens t.b.v. het aanvragen van een indicatiebesluit.
IO36	Retourinformatie Aanvraag Indicatiebesluit	CIZ naar zorgaanbieder	Bericht voor retourinformatie over een aanvraag indicatiebesluit.

Het CIZ maakt reeds gebruik van de IO31/IO32 formaten. De IO35/IO36 formaten zijn momenteel niet in gebruik bij het CIZ, mogelijk komen deze te vervallen in toekomstige versies van de iWlz.

Referenties:

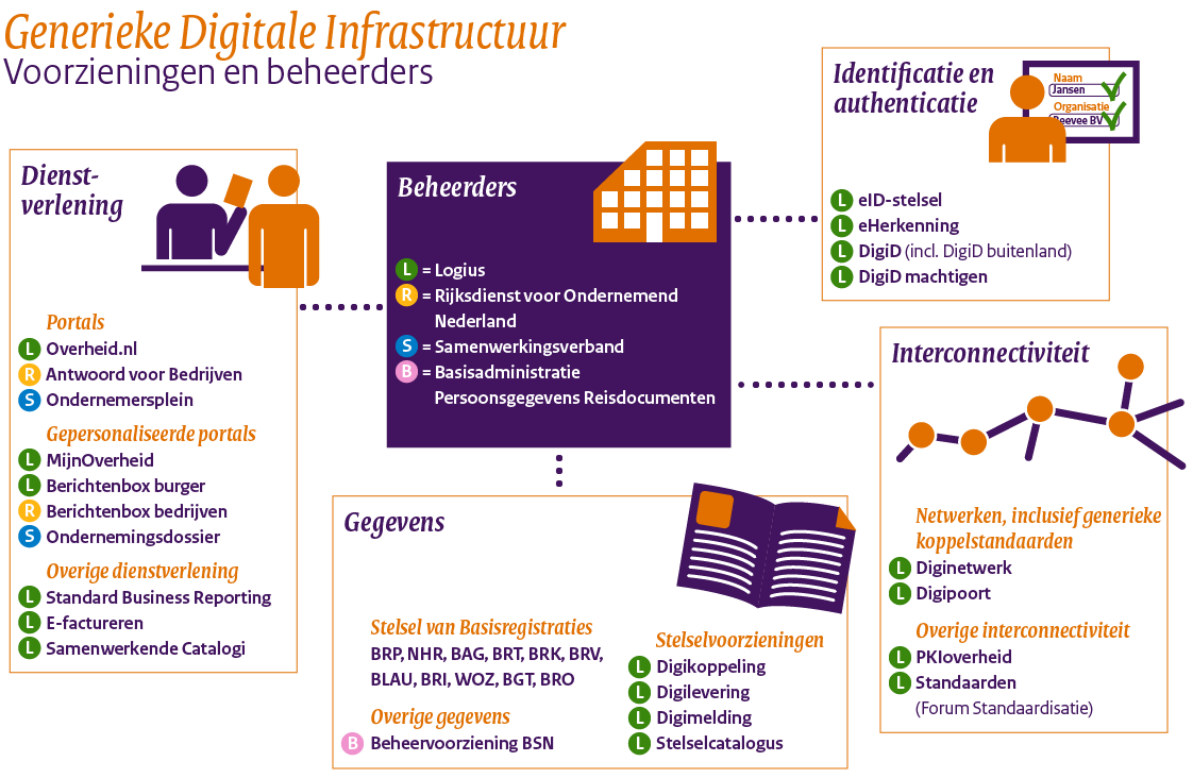
- *http://www.istandaarden.nl*

4 Generieke voorzieningen

Eén van de doelstellingen uit de IV-strategie van het CIZ is het zoveel mogelijk gebruik gaan maken van generieke diensten en "best practices" binnen de overheid en binnen de zorgketen. Naarmate vanuit de overheid en/of de samenwerkende partijen in de zorgketen gedeelde ICT diensten en oplossingen beschikbaar komen worden deze, indien relevant en gewenst door het CIZ, zo snel mogelijk opgenomen inde IV-dienstenportfolio van het CIZ. Hiermee wordt niet alleen geprofiteerd van meer schaalgrootte, maar wordt tevens gegarandeerd dat kan worden voldaan aan de verschillende vanuit de overheid en de zorgketen gestelde standaarden, kwaliteitseisen en integratiekoppelvlakken.

4.1 Generieke Digitale Infrastructuur

Verschillende overheidslagen, publieke organisaties en private partijen maken gebruik van de generieke digitale infrastructuur (GDI) van de Nederlandse overheid. De GDI bestaat uit standaarden, producten en diensten, die digitale informatie-uitwisselingen binnen en met de overheid mogelijk maken. Door het brede karakter valt de GDI niet onder de verantwoordelijkheid van één specifieke organisatie, sector of domein. De aansturing en coördinatie van de ontwikkeling van de GDI vallen onder de verantwoordelijkheid van de Digicommissaris.



De huidige GDI voorzieningen vallen binnen één van de volgende 4 categorieën:

- Identificatie en authenticatie
- Dienstverlening
- Gegevens

- Interconnectiviteit (& Veiligheid)

De specifieke voorzieningen binnen deze categorieën worden aangegeven in de bovenstaande figuur. Voor het CIZ zijn met name de volgende voorzieningen het noemen waard:

- Idensys (voorheen eID stelsel)
  Idensys (voorheen eID stelsel) omvat de standaarden en diensten voor een veilige toegang tot online dienstverlening, voor zowel burgers, consumenten als bedrijven. De huidige voorzieningen bestaan uit DigiD voor burgers en het stelsel eHerkenning voor bedrijven en organisaties.
- Diginetwerk
  Diginetwerk is een besloten en daardoor veilig(er) netwerk voor uitwisseling van gegevens tussen overheidsorganisaties. Het bestaat uit meerdere door verschillende partijen beheerde onderling gekoppelde besloten netwerken ("koppelnetwerken"), die voldoen aan de Diginetwerk standaarden en afspraken.
- Digipoort
  Digipoort is een "centrale" voor de uitwisseling van berichten tussen overheidsorganisaties enerzijds en bedrijven (private partijen) anderzijds. Zoals ook aangegeven in de IZO-architectuur (zie par. 3.1.3), wordt deze rol binnen de zorgketen echter ingevuld door Stichting RINIS (zie par. 4.2).
- PKIoverheid
  Uitgifte en het beheer van digitale PKI certificaten van de overheid voor het beveiligen van informatie-uitwisselingen en e-mail met encryptie en digitale handtekeningen.
- Standaarden (Forum Standaardisatie)
  Zie par. 3.2.1.
- Digikoppeling
  Zie par. 3.2.1.
- Digilevering
  Via Digilevering worden gegevens uit basisregistraties aangeleverd via een gebeurtenisbericht, bijvoorbeeld een verhuizing van een bedrijf of het overlijden van een persoon. Via Digimelding kunnen (vermoedelijk) onjuiste gegevens in een basisregistratie worden teruggemeld aan de beheerder er van.
- BRP
  De Basisregistratie Personen (BRP) maakt deel uit van het Stelsel van Basisregistraties (in totaal 12). Het bestaat uit een samenvoeging van de Gemeentelijke Basisadministratie Personen (GBA) en het Register Niet Ingezetenen (RNI). De BRP is nog in ontwikkeling. De eerste gebruikers (koplopers) moeten in 2018 worden aangesloten, daarna (2019-2020) volgen de overige partijen. Het CIZ gaat er daarom vanuit in die periode over te stappen van het gebruik van het GBA naar de BRP.
- MijnOverheid
  MijnOverheid is het internet webportaal waar burgers toegang hebben tot post via de dienst Berichtenbox, en tot hun Persoonlijke Gegevens en Lopende Zaken bij diverse overheidsdiensten, zoals het CIZ, de Belastingdienst, het Kadaster, RDW en SVB.

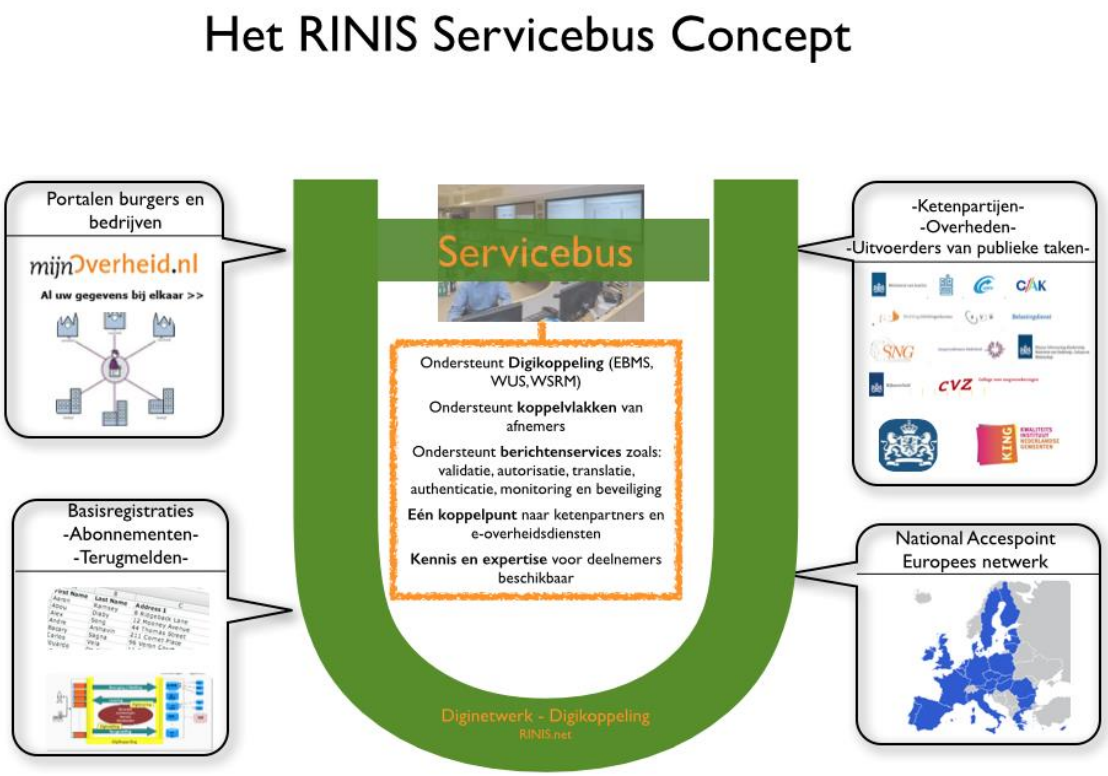
Het is de bedoeling om het gebruik van de GDI verplichtend te maken voor bestuursorganen. Hiervoor is de Wet Generieke Digitale Infrastructuur (WGDI) in voorbereiding. Deze zal als zogenoemde aanbouwwet in stappen worden ingevoerd en uitgebouwd. In de eerste tranche zullen de bestaande voorzieningen van de GDI worden geregeld, zoals MijnOverheid en DigiD.

Referenties:

- *https://www.digicommissaris.nl/over*

4.2 RINIS

Het Routerings Instituut (Inter)Nationale InformatieStromen (RINIS) is een Stichting die aan deelnemende organisaties uit de publieke sector diensten levert om onderling en met derden op een beveiligde en efficiënte manier digitale informatie uit te wisselen. RINIS fungeert daarmee als knooppunt voor systeem-naar-systeem berichtenverkeer in het publieke domein.



De deelnemende organisaties in RINIS zijn onder meer het CIZ, de Belastingdienst, CAK, SVB, Zorginstituut Nederland, Ministerie van BZK/Logius en Stichting Inlichtingenbureau Nederlandse Gemeenten.

RINIS heeft een technische infrastructuur ingericht op basis van een servicebus concept en routeert hiermee niet alleen berichtenstromen tussen de verschillende deelnemende ketenpartijen, maar biedt ook ontsluiting naar voorzieningen als MijnOverheid en Digilevering alsmede uitwisselingen met internationale en private domeinen. Onderdeel van de RINIS dienstverlening is het toegangsnetwerk, dat een van de koppelnetwerken is van het Diginetwerk (zie par. 4.1).

In de IZO-architectuur (par. 3.1.3) is RINIS opgenomen als koppelpunt tussen de publieke partijen binnen de zorgketen enerzijds en de private partijen anderzijds.

RINIS is geen onderdeel van de GDI en zal dus ook niet wettelijk verplicht worden in het kader van de WGDI. Wel is het een breed initiatief van partijen uit de publieke sector dat als zodanig past binnen de strategie van het CIZ om aan te sluiten bij dergelijke samenwerkingsverbanden.

Het CIZ is nu via RINIS aangesloten op de voorziening Lopende Zaken van MijnOverheid en is voornemens om ook aansluiting op de Berichtenbox van MijnOverheid te zoeken, middels RINIS. Mede aan de hand van de ervaringen die opgedaan worden met de koppeling naar MijnOverheid, zal daarna worden bepaald of de RINIS koppeling zal worden benut voor andere digitale berichten-uitwisselingen met ketenpartners.

Referenties:

- *http://www.rinis.nl*

5 CIZ beleidskaders

Vanuit de algemene doelstellingen en governance van het CIZ zijn met betrekking tot de inrichting van de informatievoorziening een aantal strategische en beleidsmatige uitgangspunten, doelstellingen en richtlijnen geformuleerd, die daarmee ook kaderstellend zijn voor IV projecten en wijzigingen.

5.1 IV strategie en informatieplan CIZ

In het kader van overgang van de primaire taakstelling van de AWBZ naar de Wlz is bij het CIZ in 2014 een grondige reorganisatie in gang gezet, waarbij de organisatie, processen, systemen en bemensing worden aangepast op de gewijzigde aard en omvang van het werk. Daarbij heeft het CIZ haar missie, visie en doelstellingen voor de komende jaren opnieuw geformuleerd. Als uitvloeisel daarvan is ook de besturing en de organisatie van de informatievoorziening (IV) opnieuw vormgegeven en zijn de belangrijkste strategische uitgangspunten en doelstellingen op IV gebied vastgesteld. Deze zijn nog niet uitgewerkt in een apart strategisch IV plan, maar een goede samenvatting van de strategische IV doelstellingen van het CIZ kan bijvoorbeeld worden gevonden in het document "Future State Architectuur Informatievoorziening". De IV strategie wordt ook beknopt beschreven in het informatieplan (I-plan) voor het CIZ. In het I-plan wordt verder aangegeven welke aanpassingen en vernieuwingen in de komende jaren in de informatievoorziening nodig zijn, vanuit de specifieke plannen, wensen en behoeften vanuit de verschillende organisatieonderdelen en –processen.

Referenties:

- *Hoofdstuk 3 uit "Future State Architectuur Informatievoorziening", CIZ, versie 1.3, 24-12-2015*
- *"I-plan CIZ 2015-2018"*

5.2 Informatiebeveiligingsbeleid CIZ

In 2013 is het informatiebeveiligingsbeleid van het CIZ beschreven en vastgesteld. Dit is nog steeds het actuele en daarmee vigerende beleid. Het beleid legt met name de organisatie van de informatiebeveiliging en de in te richten processen vast, en refereert voor wat betreft de in te richten maatregelen en voorziening aan de normenkaders BIR en ISO 27001/2. Het beleid voorziet een nadere uitwerking van deze normen voor het CIZ. Een initiële invulling daarvan is vastgelegd in een van de aanbestedingsdocumenten voor de aanbesteding van de IT dienstverlening in 2016.

Referenties:

- *"Informatiebeveiligingsbeleid", CIZ, versie 2.0, 10/7/2013*
- *"Informatiebeveiligingsbeleid en eisen CIZ ICT diensten, Europese aanbesteding 2016", CIZ, versie 1.2, 19/1/2016.*

5.3 Archiefbeleid CIZ

Het CIZ heeft in 2014 een archiefbeleid geformuleerd en vastgesteld, waarmee betrouwbaarheid, volledigheid en duurzame toegankelijkheid, en correcte vernietiging of overdracht van de documentaire informatie van het CIZ geborgd wordt. Het beleid houdt rekening met de verschillende wettelijke kaders, met name de Archiefwet, en is van toepassing op alle fysieke en digitale documenten en bijbehorende data die de medewerkers ontvangen en creëren voor de uitvoering van de bedrijfsprocessen van het CIZ. Het archiefbeleid beslaat de volgende facetten:

- Inrichting van het informatiebeheer, waar onder meer de taken en verantwoordelijkheden van iedere medewerker in relatie tot informatiebeheer, en de applicaties waar men informatie mag opslaan, zijn beschreven;
- Inrichten van (project)dossiers, dat vastlegt hoe een (project)dossier moet worden ingericht;
- Creëren, opslaan en beheren van informatie, waarin is beschreven hoe men nieuwe documenten – waaronder e-mails- maakt, opslaat en beheert;
- Beveiligen van informatie, waar de afspraken zijn vastgelegd met betrekking tot de interne en externe beveiliging (afscherming) van informatie, en het gebruik van niet door het CIZ verstrekte apparaten;
- Afsluiten en vernietigen van (project)dossiers, waar de afspraken zijn vermeld voor het afsluiten van ieder dossier, en het bepalen van de periode dat het daarna nog van belang is om te bewaren.

In aanvulling op het Archiefbeleid is een "Handleiding archivering" opgesteld, waarin voor de gehele CIZ organisatie wordt beschreven hoe medewerkers (digitale) documenten moeten bewaren, archiveren en vernietigen.

Referenties:

- *Archiefbeleid Centrum Indicatiestelling Zorg (CIZ), versie 1.0, 17 maart 2014*
- *Handleiding archivering, CIZ, versie 2.0, 1-1-2015*

6 IV doelarchitecturen en roadmaps

Doelarchitecturen en roadmaps voor de informatievoorziening vormen belangrijke stuurinstrumenten. Doelarchitecturen leggen vast hoe de toekomstige informatievoorziening van het CIZ er uit moet zien in termen van de informatiediensten en –functies waarmee de bedrijfsprocessen en de medewerkers optimaal kunnen worden ondersteund. Roadmaps geven aansluitend daarop een stappenplan om van de huidige naar de gewenste informatievoorziening te bewegen. Aan de hand van doelarchitecturen en de bijbehorende roadmaps kunnen dus gericht projecten worden geïdentificeerd en uitgevoerd, die hieraan invulling te geven. Anderzijds kunnen (voorgestelde) projecten en grote wijzigingen worden getoetst op de mate waarin ze bijdragen aan het realiseren van de doelarchitecturen en roadmaps.

In 2015 is begonnen met het opstellen van doelarchitecturen en roadmaps. Een algemene roadmap met een overzicht van de lopende en geplande projecten is inmiddels beschikbaar en wordt regulier bijgehouden.

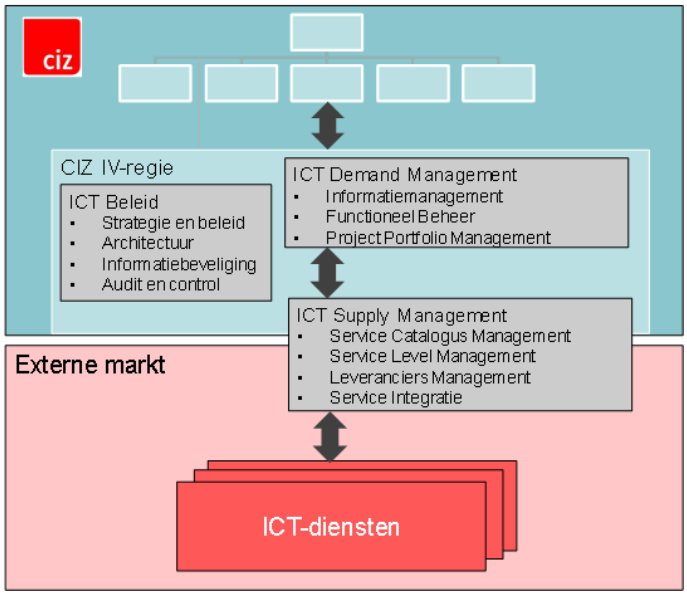
Referentie: "Roadmap – Projecten Portfolio CIZ 2016"

6.1 Future State Architectuur Informatievoorziening

Het CIZ architectuurdocument "Future State Architectuur Informatievoorziening (FSA)" beschrijft de gewenste inrichting van de informatievoorziening van het CIZ in de komende 5 jaar. Het betreft enerzijds de identificatie van de verschillende functionaliteiten en daaraan gerelateerde prestatie-eisen die vanuit de informatievoorziening moeten worden geleverd om de organisatiedoelstellingen en -processen optimaal te kunnen ondersteunen. Anderzijds gaat het om het aanreiken van een aantal samenhangende richtlijnen en keuzen ten aanzien van de wijze waarop de betreffende functionaliteiten moeten worden ingevuld in de vorm van meer specifieke ICT-diensten. De actuele versie van de FSA dateert uit 2016.

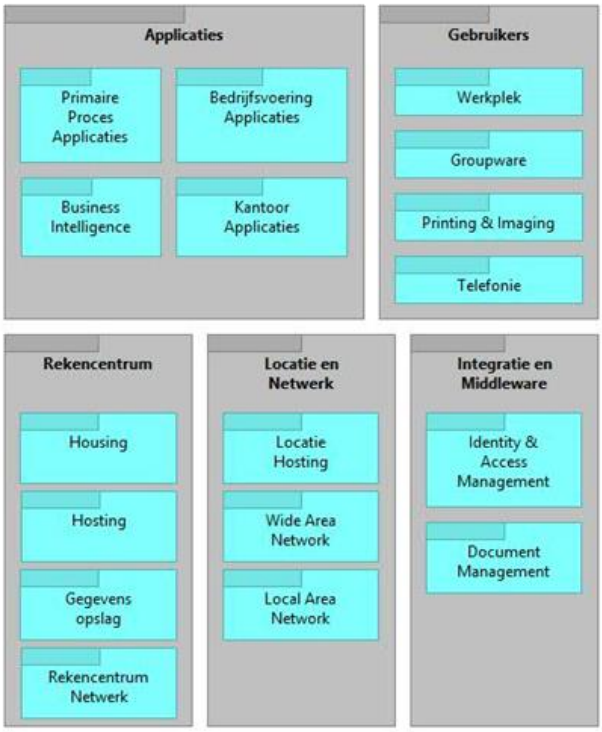
De FSA gaat uit van het volgens de IV strategie nagestreefde besturingsmodel (zie onderstaande figuur), waarbij de informatievoorziening voor het CIZ wordt ingericht in de vorm van IV diensten, die worden afgenomen van (zo weinig mogelijk) externe leveranciers. Het richt daarvoor een regiefuncties in die zich toelegt op de vertaling van bedrijfsdoelen en -eisen naar de specificatie van een daarop aansluitend dienstenportfolio en de realisatie daarvan door de inkoop van op elkaar afgestemde diensten (passend binnen de Architectuur Kaders en Richtlijnen).

Referentie: "Future State Architectuur Informatievoorziening", CIZ, versie 1.41, 18-1-2016



De FSA beschrijft vervolgens op hoofdlijnen het gewenste toekomstige portfolio van IV diensten, onderverdeeld in de volgende categorieën (zie ook de figuur hieronder):

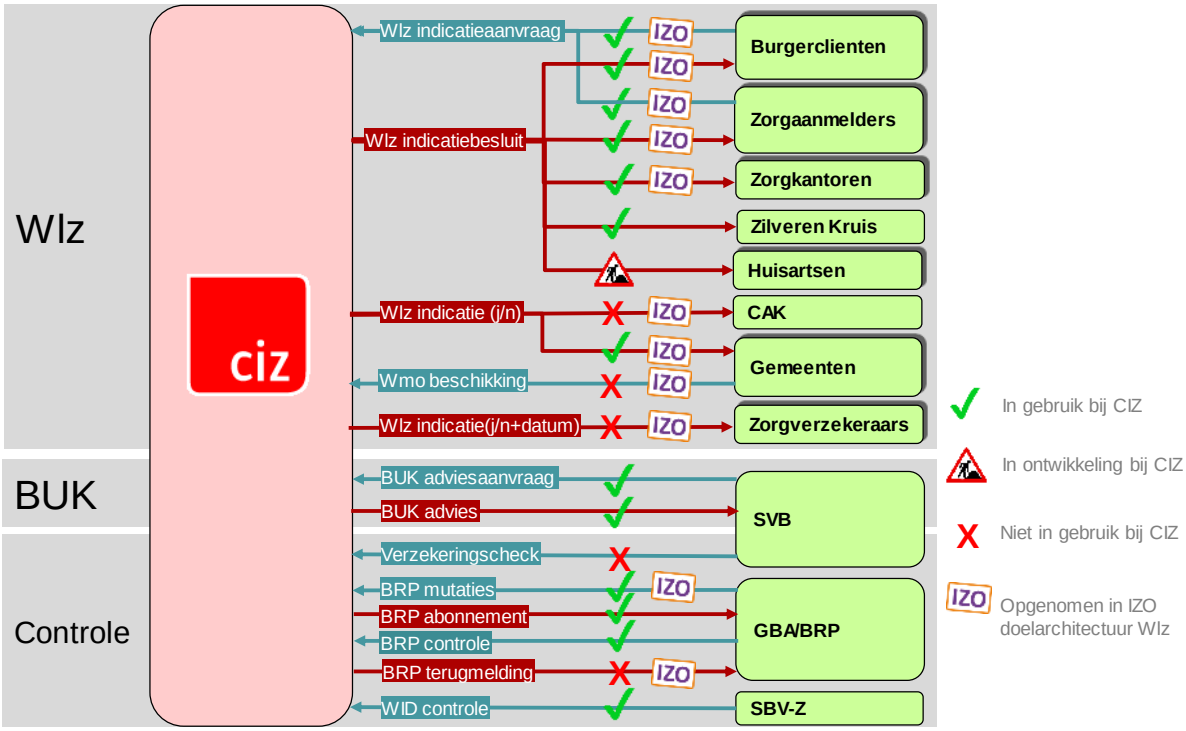
- Applicaties
- Gebruikers
- Rekencentrum
- Locatie en Netwerk
- Integratie en Middleware.



Referentie: "Future State Architectuur Informatievoorziening", CIZ, versie 1.41, 18-1-2016

6.2 Domeinarchitecturen

In toevoeging op en uitgaande van de "Future State Architectuur Informatievoorziening", die betrekking heeft op de integrale informatievoorziening en de daarvoor benodigde informatiesystemen, zullen domeinarchitecturen worden ontwikkeld, die op specifieke deelgebieden een nadere invulling geven aan de toekomstige gewenste situatie in termen van functionaliteiten en inrichting. Uitgewerkte en vastgestelde domeinarchitecturen zijn nog niet opgeleverd. Een eerste concept versie van een domeinarchitectuur met betrekking tot de "Informatieuitwisseling in de zorgketen" is wel beschikbaar. Hierin worden toekomstscenario's geschetst voor de technische inrichting van de verschillende gegevensuitwisselingen tussen het CIZ en de ketenpartners. Hieruit is ter illustratie de onderstaande figuur afkomstig met een overzicht van de uitwisselingen die volgende IZO architectuur zouden moeten worden ingericht alsmede de uitwisselingen die in 2016 daadwerkelijk operationeel zijn bij het CIZ.



Referenties:

- *"Informatieuitwisselingen binnen de zorgketen – Inventarisatie domeinarchitectuur", CIZ, versie 5.0*

6.3 Roadmaps

De (algemene) IV roadmap specificeert op hoofdlijnen welke wijzigingen in de IV systemen moeten worden gerealiseerd om de in de Future State Architectuur beschreven gewenste hoedanigheid van de informatievoorziening te realiseren en geeft aan waar deze in de tijd moeten worden gepositioneerd. In toevoeging daarop kunnen voor de verschillende domeinarchitecturen meer specifieke roadmaps worden ontwikkeld. Deze specifieke IV roadmaps moeten nog worden opgesteld.

7 CIZ architectuurprincipes

Architectuurprincipes zijn richtlijnen ten aanzien van het inrichten en onderhouden van de informatievoorziening en de informatiesystemen van het CIZ. Vanuit de verschillende externe referentiearchitecturen, zoals NORA, worden al een groot aantal architectuurprincipes aangereikt (zie ook par. 3.1.1). In toevoeging daarop hanteert het CIZ een aantal eigen architectuurprincipes die specifiek zijn voor de omstandigheden en behoeften van het CIZ. Hierbij kan onderscheid worden gemaakt tussen enerzijds basisprincipes (of algemene principes), die generiek van toepassing zijn op de integrale informatievoorziening, en anderzijds domeinprincipes (of afgeleide principes), die geldig zijn voor specifieke onderdelen (domeinen) daarbinnen.

7.1 Basisprincipes

In 2013 zijn door het Raad van Bestuur van het CIZ een aantal basis architectuurprincipes vastgesteld die bedoeld zijn als generieke afspraken voor alle ICT projecten en oplossingen binnen het CIZ. Het betreft de volgende uitspraken:

[CIZ-BP01] Het CIZ kiest voor Werken met Architectuur.

[CIZ-BP02] Het principe Comply-or-Explain is onverkort op alle wijzigingen van toepassing.

[CIZ-BP03] Het CIZ volgt Europese en Nederlandse standaards op het gebied van architectuur.

[CIZ-BP04] De inrichting van processen en systemen voldoet aan relevante Europese en Nederlandse wet- en regelgeving.

[CIZ-BP05] De inrichting van processen en systemen binnen het CIZ houdt rekening met de flexibiliteit en wendbaarheid die de strategie van het CIZ, alsmede de buitenwereld van het CIZ vraagt.

[CIZ-BP06] De inrichting van processen en systemen binnen het CIZ houdt er rekening mee dat wij een maatschappelijke functie hebben die wordt uitgevoerd met gemeenschapsgeld.

[CIZ-BP07] (Re-)Use before Buy before Build.

[CIZ-BP08] Het CIZ streeft naar vermindering van de complexiteit van de processen en ICT omgeving, met behoud van betrouwbaarheid, integriteit en vertrouwelijkheid.

[CIZ-BP09] Generieke diensten/systemen, die gebruikt kunnen worden voor de gehele organisatie, hebben de voorkeur boven specifieke oplossingen voor slechts een deel van de organisatie.

Deze principes worden nader toegelicht en uitgewerkt in het hieronder gerefereerde document.

Deze principes zijn dermate universeel en principieel dat ze nog steeds kunnen worden gehanteerd als vigerend voor het CIZ. Wel is het gewenst de algemene principes daar waar nodig te actualiseren en aan te vullenen/of specifieker te maken. Hiervoor dient een nieuwe versie van het document met architectuurprincipes voor het CIZ te worden opgesteld. Totdat dit beschikbaar en geaccordeerd is, blijven de huidige principes uit 2013 dus van kracht.

Referenties:

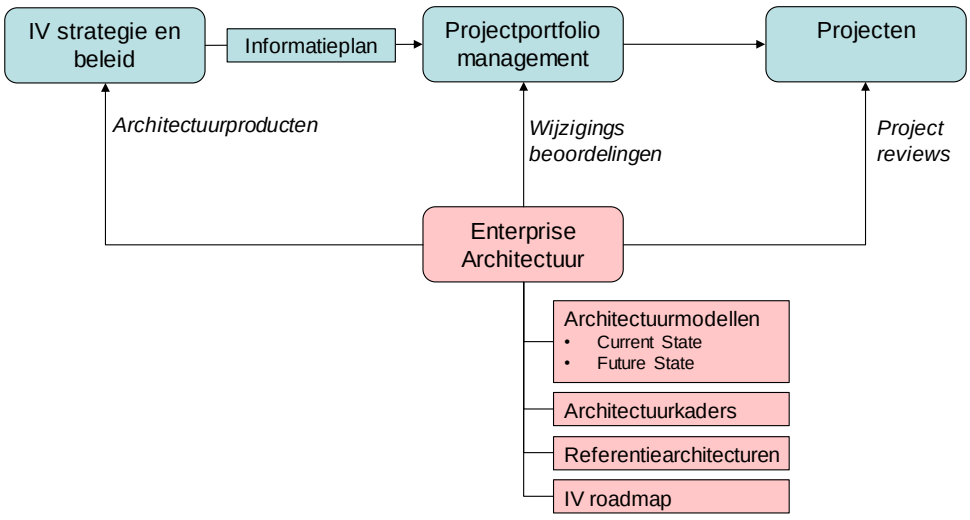
- *CIZ Enterprise Architectuur – Principes, versie 0.61, 14-06-2013*

7.2 Domein principes

Naast de hierboven besproken algemene principes of basisprincipes, die breed van toepassing zijn op de informatievoorziening en de informatiesystemen van het CIZ, kunnen binnen de afzonderlijke informatiedomeinen meer specifieke en/of afgeleide principes worden geformuleerd en vastgesteld. Dit is tot op heden nog niet gebeurd, maar het is de intentie om hiervoor een eerste baseline set te formuleren, dit op te nemen in het nieuwe document met architectuurprincipes en vervolgens op regelmatige basis te actualiseren.

8 Toepassing van de Architectuur Kaders en Richtlijnen

In hoofdstuk 1 is al aangegeven dat de Architectuurkaders en Richtlijnen vooral zijn bedoeld als instrument bij het formuleren en beoordelen van projectvoorstellen, wijzigingsvoorstellen en systeemontwerpen op het gebied van de informatievoorziening.



8.1 Project portfoliomanagement en change management

Binnen het CIZ is het bedrijfsbrede project portfoliomanagement belegd bij de afdeling A&A. Voor het selecteren en prioriteren van projecten is geen aparte change advisory board (meer) aanwezig, dit wordt gedaan binnen de reguliere management overleg- en besluitvormingsstructuren. Voor wat betreft projectvoorstellen op IV gebied of met IV component een beroep gedaan op de CIO Office om een impactscan uit te voeren. Als onderdeel van deze impactscan zou ook een toetsing plaats moeten vinden op conformiteit met de CIZ Architectuur Kaders en Richtlijnen. Ook bij het beoordelen van niet-standaard wijzigingen in de informatiesystemen of de IV-diensten zou moeten worden gecontroleerd of de betreffende wijzigingen passen binnen de Architectuur Kaders en Richtlijnen.

8.2 Projectuitvoering

De IV projecten of projecten met een IV component, die binnen het CIZ projectenprogramma of –portfolio worden uitgevoerd, moeten rekening houden met de Architectuur Kaders en Richtlijnen om te borgen dat ze zoveel mogelijk bijdragen aan de strategische IV-doelstellingen en te voorkomen dat er onnodige problemen ontstaan op het gebied van integratie, beheerbaarheid, kosten en dergelijke.

8.2.1 Project Start Architecturen

Om een goede projectplanning en -beoordeling mogelijk te maken dient aan het begin van elk IV project een z.g. Project Start Architectuur (PSA) te worden opgesteld, waarin wordt aangegeven welke ontwerpkeuzen zijn gemaakt of nog moeten worden gemaakt, in hoeverre deze voldoen aan de architectuurkaders (inclusief CIZ informatiebeveiligingsnormen). Ook wanneer de voor het betreffende project benodigde kaders nog niet beschikbaar zijn, moet dit in de PSA worden aangegeven. Aan de hand van de PSA kan de conformiteit met de Architectuur Kaders en Richtlijnen worden beoordeeld, en in het geval van afwijkingen kan daarover een advies worden uitgebracht aan de CIO. Vervolgens kunnen ook de binnen het project op te leveren specifieke systeemontwerpen worden beoordeeld op conformiteit met de Architectuur Kaders en Richtlijnen en de PSA.

8.3 Bindendheid van Architectuur Kaders en Richtlijnen

8.3.1 Comply-or-Explain

De Architectuur Kaders en Richtlijnen voor de informatievoorziening van het CIZ vormen uiteraard geen doel op zichzelf, maar zijn een hulpmiddel dat er mede voor moet zorgen dat de keuzebepaling en besluitvorming over aanpassingen en vernieuwingen in de informatiehuishouding optimaal aansluiten bij de organisatiebehoeften en doelstellingen van het CIZ. De Architectuur Kaders en Richtlijnen zijn afgeleid uit strategische doelstellingen van het CIZ, dus met het oog op de gehele organisatie en de langere termijn. Het kan echter voorkomen dat het nodig is om van de Architectuur Kaders en Richtlijnen af te wijken, om aan urgente behoeften en eisen op de kortere termijn te kunnen voldoen. Dat is niet erg, zolang dit maar een bewuste keuze is waarbij alle consequenties (dus ook die voor de langere termijn) worden meegewogen en financieel en planmatig rekening wordt gehouden met het op termijn uitfaseren dan wel naar de gewenste inrichting migreren van de gekozen oplossing

Het CIZ hanteert dus het principe van "Comply-or-Explain" (ook wel: "pas toe-of-leg uit") voor de in dit document opgenomen Architectuur Kaders en Richtlijnen. Dit houdt in dat indien niet wordt voldaan aan de kaders en richtlijnen, een additionele motivatie wordt opgesteld die onderbouwt waarom bewust wordt afgeweken van de kaders en richtlijnen. De betreffende afwijking moet vervolgens worden geaccordeerd door de verantwoordelijke manager. Voor grotere wijzigingen zal dit in het algemeen de CIO zijn.

8.3.2 Verplicht

Om voor de hand liggende redenen geldt het Comply-or-Explain principe niet voor de Architectuur Kaders en Richtlijnen die direct voortkomen uit wettelijke verplichtingen. Deze zijn te allen tijde verplicht. Hetzelfde geldt voor beleidskaders op het gebied van de informatiebeveiliging, die door de directie van het CIZ als verplicht zijn vastgesteld. Dit betekent dat de volgende in dit document beschreven Architectuur Kaders en Richtlijnen bindend zijn:

- Alle wettelijke kaders, zoals beschreven in paragrafen 2.1 en 2.2.1.
- CIZ basisprincipe [CIZ-BP04] (De inrichting van processen en systemen voldoet aan relevante Europese en Nederlandse wet- en regelgeving.)
- Conformiteit met de BIR (zie paragraaf 2.2.2).

Bijlage 1. Informatiebepalingen uit de Wlz

§ 1. Verwerking van gegevens, waaronder bijzondere persoonsgegevens

Artikel 9.1.1

1. De artikelen 4 en 6 tot en met 9 van de Wet gebruik burgerservicenummer in de zorg zijn, voor de uitvoering van deze wet, van overeenkomstige toepassing op de Wlz-uitvoerder.

2. De Wlz-uitvoerder stelt de identiteit en het burgerservicenummer van de verzekerde vast:
a. wanneer de persoon zich ter inschrijving bij de Wlz-uitvoerder meldt;
b. voor zover dat redelijkerwijs nodig is ter uitvoering van artikel 12 van de Wet algemene bepalingen burgerservicenummer.

3. Bij gegevensuitwisseling tussen de Wlz-uitvoerders en de in de artikelen 9.1.2 tot en met 9.1.5 genoemde personen en instanties wordt voor zover die personen en instanties tot gebruik van dat nummer bevoegd zijn, het burgerservicenummer gebruikt.

4. Bij ministeriële regeling kan worden bepaald aan welke beveiligingseisen het gebruik van het burgerservicenummer door de Wlz-uitvoerder, alsmede de opname daarvan in zijn administratie, voldoet.

5. Bij algemene maatregel van bestuur kunnen vormen van zorg als bedoeld in artikel 3.1.1, alsmede categorieën van Wlz-uitvoerders en in de artikelen 9.1.2 tot en met 9.1.5 genoemde personen en instanties worden uitgezonderd van de toepassing van het bepaalde bij of krachtens eerste tot en met het derde lid.

6. Het CIZ stelt bij de aanvraag van een indicatiebesluit de identiteit van de verzekerde vast aan de hand van documenten als bedoeld in artikel 1 van de Wet op de identificatieplicht, die de verzekerde hem desgevraagd ter inzage geeft.

Artikel 9.1.2

1. Wlz-uitvoerders, zorgaanbieders, het CAK en het CIZ, verstrekken elkaar kosteloos de persoonsgegevens van de verzekerde, waaronder persoonsgegevens betreffende de gezondheid als bedoeld in de Wet bescherming persoonsgegevens, dan wel stellen elkaar deze gegevens voor dit doel voor inzage of het nemen van afschrift ter beschikking, voor zover die gegevens noodzakelijk zijn voor:
a. het nemen van indicatiebesluiten op grond van artikel 3.2.3, eerste lid, of artikel 3.2.4 en het onderzoek dat het CIZ daarvoor verricht,
b. het sluiten van schriftelijke overeenkomsten met zorgaanbieders, bedoeld in artikel 4.2.2,
c. de zorgplichten, bedoeld in artikel 4.2.1, eerste en tweede lid, waaronder mede begrepen het opmaken van wachtlijsten,
d. de beoordeling van de Wlz-uitvoerder of de zorg op verantwoorde wijze kan worden verleend zonder dat de verzekerde verblijft in een instelling of met een persoonsgebonden budget,
e. de zorglevering,
f. het in rekening brengen van tarieven voor de geleverde prestaties en het daartoe ontvangen en verrichten van de betalingen of vergoedingen aan zorgaanbieders van de geleverde prestaties, of de vergoeding van zorgkosten aan een verzekerde,
g. de vaststellingen de inning van eigen bijdragen door het CAK, bedoeld in artikel 3.2.5,

h. het namens een Wlz-uitvoerder of het Zorginstituut verrichten van betalingen door het CAK aan zorgaanbieders, bedoeld in artikel 6.1.2, onder c,
i. het verrichten van controle of fraudeonderzoek door de Wlz-uitvoerders,
j. het uitoefenen van het verhaalsrecht.

2. Voor zover de verzekerde daartoe uitdrukkelijk toestemming heeft verleend, verstrekken het CIZ en een zorgaanbieder elkaar kosteloos de persoonsgegevens van de verzekerde, waaronder persoonsgegevens betreffende de gezondheid als bedoeld in de Wet bescherming persoonsgegevens.

3. Indien een zorgaanbieder anders dan krachtens een door hem met de Wlz-uitvoerder gesloten overeenkomst aan een verzekerde zorg heeft verleend als bedoeld in deze wet, verstrekt hij de verzekerde kosteloos de persoonsgegevens, waaronder persoonsgegevens betreffende zijn gezondheid als bedoeld in de Wet bescherming persoonsgegevens, die voor zijn Wlz-uitvoerder noodzakelijk zijn voor de uitvoering van deze wet.

4. Personen werkzaam ten behoeve van een zorgaanbieder of het CIZ, verstrekken die zorgaanbieder of het CIZ de persoonsgegevens die zij nodig hebben om te kunnen voldoen aan hun verplichtingen, bedoeld in het eerste, tweede of derde lid.

5. Personen werkzaam bij een Wlz-uitvoerder, voor wie niet reeds uit hoofde van ambt of beroep een geheimhoudingplicht geldt, zijn verplicht tot geheimhouding van de gegevens als bedoeld in het eerste of derde lid, behoudens voor zover enig wettelijk voorschrift hen mededeling toestaat.

6. Voor het verrichten van de controle als bedoeld in het eerste lid, onder i, zijn in ieder geval noodzakelijk:
a. de beschrijving van de prestatie zoals die
    1 op grond van de Wet marktordening gezondheidszorg voor een zorgaanbieder is vastgesteld, of
    2 tussen de verzekerde en de zorgaanbieder is overeengekomen indien voor die zorgaanbieder niet een prestatiebeschrijving op grond van de Wet marktordening gezondheidszorg behoeft te worden vastgesteld, en
b. diagnose-informatie indien deze onderdeel uitmaakt van de beschrijving van de prestatie of andere informatie die tot een diagnose kan leiden.

7. Bij ministeriële regeling kan worden bepaald:
a. tot welke andere gegevens dan bedoeld in het zesde lid de verplichting, bedoeld in het eerste of derde lid, zich in ieder geval of mede uitstrekt, alsmede de aard en de omvang daarvan;
b. op welke wijze gegevens, bedoeld in het eerste, tweede of derde lid, worden verwerkt;
c. volgens welke technische standaarden gegevensverwerking plaatsvindt;
d. aan welke beveiligingseisen gegevensverwerking voldoet;
e. in welke gevallen gegevens, bedoeld in het eerste of derde lid, verder worden verwerkt met het oog op de uitvoering van deze wet, een zorgverzekering als bedoeld in de Zorgverzekeringswet of een aanvullende ziektekostenverzekering, voor zover deze gegevens niet worden gebruikt voor het beoordelen en accepteren van een aspirant-verzekerde voor een aanvullende verzekering en bovendien noodzakelijk zijn voor de in het eerste lid genoemde taken.

Artikel 9.1.3

1. Een Wlz-uitvoerder, het CAK, en het CIZ verstrekken op verzoek, binnen een bij dat verzoek genoemde termijn, uit de onder hun verantwoordelijkheid gevoerde administratie, kosteloos, de

gegevens, waaronder persoonsgegevens betreffende de gezondheid als bedoeld in de Wet bescherming persoonsgegevens, aan:

a. zorgverzekeraars en het Zorginstituut, voor zover die gegevens noodzakelijk zijn voor de onderlinge afstemming van op grond van de Zorgverzekeringswet verzekerde zorg en zorg die is verzekerd op grond van deze wet en het voorkomen van dubbele verstrekkingen;
b. het Zorginstituut, voor zover die gegevens noodzakelijk zijn voor de bevordering van de rechtmatige uitvoering, bedoeld in artikel 5.1.1;
c. de Sociale verzekeringsbank, voor zover die gegevens noodzakelijk voor de verzekerdenadministratie, bedoeld in artikel 35 van de Wet structuur uitvoeringsorganisatie werk en inkomen, of de betalingen ten laste van de persoonsgebonden budgetten en het daarmee verbonden budgetbeheer, bedoeld in artikel 3.3.3, zevende lid.

2. De in het eerste lid, onderdelen a tot en met c genoemde instanties, zijn, voor de in die onderdelen genoemde doelen, bevoegd uit eigen beweging en verplicht op verzoek, de gegevens, waaronder persoonsgegevens betreffende de gezondheid als bedoeld in de Wet bescherming persoonsgegevens, te verstrekken aan een Wlz-uitvoerder, het CAK, of het CIZ.

3. Voor zover de verzekerde daartoe uitdrukkelijk toestemming heeft verleend, verstrekken het college van burgemeester en wethouders en de Wlz-uitvoerder elkaar kosteloos de persoonsgegevens van de verzekerde, waaronder persoonsgegevens betreffende de gezondheid als bedoeld in de Wet bescherming persoonsgegevens, voor zover die gegevens noodzakelijk zijn voor de onderlinge afstemming van deze wet en de Wet maatschappelijke ondersteuning 2015 of Jeugdwet of voor het voorkomen van dubbele verstrekkingen.

4. De inspecteur of ontvanger is verplicht desgevraagd aan het CAK de gegevens omtrent het inkomen en vermogen van de verzekerde en diens echtgenoot te verstrekken, voor zover die noodzakelijk zijn voor de vaststelling van de bijdrage, bedoeld in artikel 3.2.5.

5. De in het eerste tot en met vierde lid bedoelde gegevens en inlichtingen worden op verzoek verstrekt in schriftelijke vorm of in een andere vorm die redelijkerwijs kan worden verlangd, binnen een termijn die schriftelijk wordt gesteld bij het in het eerste lid bedoelde verzoek.

6. Alle ambtenaren tot afgifte van uittreksels uit registers van burgerlijke stand bevoegd, zijn verplicht aan een in het tweede lid genoemde instantie de door deze gevraagde uittreksels uit de registers kosteloos toe te zenden.

7. Griffiers van colleges, geheel of ten dele met rechtspraak belast, verstrekken op verzoek, kosteloos, aan een Wlz-uitvoerder, aan het CIZ, aan het CAK, aan het Zorginstituut of aan de zorgautoriteit alle gegevens, inlichtingen en uittreksels uit of afschriften van uitspraken, registers en andere stukken, die noodzakelijk zijn voor de uitvoering van deze wet door de Wlz-uitvoerder of het desbetreffende college.

8. Bij ministeriële regeling kunnen nadere regels worden gesteld met betrekking tot het eerste tot en met zesde lid.

Artikel 9.1.4

1. De zorgautoriteit, onderscheidenlijk het Zorginstituut, kan na overleg met het Zorginstituut, onderscheidenlijk de zorgautoriteit, bij regeling bepalen welke gegevens en inlichtingen regelmatig door de Wlz-uitvoerders en het CAK moeten worden verstrekt.

2. De regels kunnen mede omvatten het tijdstip en de wijze waarop de gegevens en inlichtingen

moeten worden verstrekt, alsmede dat een accountant als bedoeld in artikel 393 van Boek 2 van het Burgerlijk Wetboek de juistheid van de verstrekte gegevens en inlichtingen bevestigt.

3. Bij ministeriële regeling kan worden bepaald welke statistische gegevens de Wlz-uitvoerders en het CAK verzamelen betreffende vormen van zorg.

4. Een Wlz-uitvoerder en het CAK verlenen op verzoek van het Zorginstituut dan wel van de zorgautoriteit aan door het desbetreffende college aangewezen personen inzage in alle bescheiden en andere gegevensdragers, stelt deze op verzoek ter beschikking voor het nemen van afschrift en verleent de ter zake verlangde medewerking, voor zover het desbetreffende college dit nodig acht voor de uitoefening van zijn taak.

Artikel 9.1.5

1. Het Zorginstituut en de zorgautoriteit verstrekken desgevraagd aan Onze Minister of aan het College sanering, genoemd in artikel 32 van de Wet toelating zorginstellingen, de voor de uitoefening van hun taak benodigde inlichtingen en gegevens.

2. Het Zorginstituut en de zorgautoriteit verlenen aan door Onze Minister of door het College sanering aangewezen personen toegang tot en inzage in zakelijke gegevens en bescheiden, voor zover dat voor de vervulling van hun taak redelijkerwijs nodig is.

Artikel 9.1.6

1. De in artikel 9.1.2, eerste lid, genoemde instanties maken voor de in dat artikel genoemde verstrekking of ontvangst van gegevens gebruik van elektronisch gegevensverkeer.

2. Bij ministeriële regeling, bedoeld in artikel 9.1.2, zevende lid, kan tevens worden bepaald:
a. dat bij het elektronisch gegevensverkeer gebruik wordt gemaakt van een elektronische infrastructuur;
b. op welke wijze de in artikel 9.1.2, eerste lid, genoemde instanties op die infrastructuur zijn aangesloten;
c. de wijze waarop het gebruik van de infrastructuur wordt georganiseerd en beheerd, waaronder begrepen de inrichting en instandhouding van een gemeenschappelijke database;
d. de financiering van het gebruik van de infrastructuur en de wijze waarop de kosten ervan worden verdeeld.

Artikel 9.1.7

1. Het is een ieder die uit hoofde van de toepassing van deze wet of van krachtens deze wet genomen besluiten enige taak vervult of heeft vervuld, verboden van vertrouwelijke gegevens of inlichtingen die ingevolge deze wet dan wel ingevolge titel 5.2 van de Algemene wet bestuursrecht zijn verstrekt of verkregen, verder of anders gebruik te maken of daaraan verder of anders bekendheid te geven dan voor de uitvoering van zijn taak of bij of krachtens deze wet wordt geëist.

2. In afwijking van het eerste lid kunnen de zorgautoriteit en het Zorginstituut met gebruikmaking van vertrouwelijke gegevens of inlichtingen verkregen bij de uitvoering van hun taken op grond van deze wet, mededelingen doen, indien deze niet kunnen worden herleid tot afzonderlijke personen of ondernemingen.
3. In afwijking van het eerste lid zijn de zorgautoriteit en het Zorginstituut, voor zover dat voor hun taakuitoefening noodzakelijk is, bevoegd aan elkaar en aan Onze Minister vertrouwelijk gegevens of inlichtingen omtrent afzonderlijke Wlz-uitvoerders te verschaffen.

4. Het eerste lid laat, ten aanzien van degene op wie dat lid van toepassing is, onverlet:
a. de toepasselijkheid van de bepalingen van het Wetboek van Strafvordering welke betrekking hebben op het als getuige of deskundige in strafzaken afleggen van een verklaring omtrent gegevens of inlichtingen verkregen bij de vervulling van de ingevolge deze wet opgedragen taak;
b. de toepasselijkheid van de bepalingen van het Wetboek van Burgerlijke Rechtsvordering en van artikel 66 van de Faillissementswet welke betrekking hebben op het als getuige of als partij in een comparitie van partijen dan wel als deskundige in burgerlijke zaken afleggen van een verklaring omtrent gegevens of inlichtingen verkregen bij de vervulling van zijn ingevolge deze wet opgedragen taak, voor zover het gaat om gegevens of inlichtingen omtrent een Wlz-uitvoerder die in staat van faillissement is verklaard of op grond van een rechterlijke uitspraak is ontbonden;
c. de bevoegdheden van de Algemene Rekenkamer ingevolge artikel 91 van de Comptabiliteitswet 2001.

5. Het vierde lid, onderdeel b, geldt niet voor gegevens of inlichtingen die betrekking hebben op Wlz-uitvoerders die betrokken zijn of zijn geweest bij een poging de desbetreffende Wlz-uitvoerder in staat te stellen zijn bedrijf voort te zetten.

§ 2. Beleidsinformatie

Artikel 9.2.1

1. Bij of krachtens algemene maatregel van bestuur kunnen in het belang van de zorgverlening, de bekostiging daarvan en de afstemming op andere wettelijke voorzieningen, regels worden gesteld over de kosteloze verstrekking van informatie van beleidsmatige en beheersmatige aard:
a. door zorgaanbieders aan Wlz-uitvoerders, de zorgautoriteit en Onze Minister,
b. door Wlz-uitvoerders aan de zorgautoriteit en Onze Minister.

2. De bij of krachtens algemene maatregel van bestuur te stellen regels als bedoeld in het eerste lid, hebben geen betrekking op persoonsgegevens als bedoeld in de Wet bescherming persoonsgegevens en worden niet gesteld dan nadat met door zorgaanbieders of de Wlz-uitvoerders voorgedragen koepelorganisaties, overleg is gevoerd over de inhoud van de in het eerste lid bedoelde gegevens en standaardisering van de wijze waarop de gegevens worden verstrekt.

3. Bij of krachtens algemene maatregel van bestuur kan worden bepaald dat het overleg, bedoeld in het tweede lid, ook plaatsvindt met andere organisaties en instanties dan genoemd in het tweede lid, en kan worden bepaald dat het eerste en tweede lid ook van toepassing is ten aanzien van die organisaties en instanties.

Bijlage 2. Overzicht standaarden Overheid en Rijksdienst

Aquo standaard	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* IDsW
Beschrijving:	De Aquo-standaard maakt het mogelijk om op een uniforme manier gegevens uit te wisselen tussen partijen die betrokken zijn bij het waterbeheer en draagt daarmee bij aan een kwaliteitsverbetering van het waterbeheer.			
ArchiMate	*Status:* Vastgesteld	*Werking:* Rijksbreed generiek	*I-domein:* I-domein totaal, Overig	*Beheer:* The Open Group
Beschrijving:	Archimate een open en onafhankelijke, in Nederland ontworpen, modelleertaal voor enterprise architectuur. ArchiMate biedt modellen voor de ondersteuning van enterprise architecten in het beschrijven, analyseren en visualiseren van de relaties tussen verschillende domeinen op een eenduidige manier. Door gebruik van deze standaard kunnen architecturen van verschillende organisaties makkelijker worden geïntegreerd en/of uitgewisseld en hergebruikt.			
BIR 2012	*Status:* Vastgesteld	*Werking:* Rijksbreed generiek	*I-domein:* I-domein totaal, Overig	*Beheer:* BZK/DGOBR
Beschrijving:	De nieuwe Baseline Informatiebeveiliging Rijksdienst – Tactisch Normenkader (TNK) biedt één normenkader voor de beveiliging van de informatiehuishouding van de Rijksdienst. Het bestaat uit een concrete set van maatregelen op organisatorisch en technisch vlak die er aan bijdragen dat bedrijfsprocessen ongestoorde doorgang vinden. Informatiebeveiliging is niet alleen zorgen voor de vertrouwelijkheid, ook de integriteit (is de informatie juist en niet, bijvoorbeeld, ongeautoriseerd veranderd?) en beschikbaarheid van informatie maakt hier onderdeel van uit. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen.			
BWB	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* Juriconnect
Beschrijving:	De standaard biedt een eenduidige manier van verwijzen naar (onderdelen van) wet- en regelgeving waarmee de interoperabiliteit van juridische documenten en systemen die veel verwijzingen kennen naar wet- en regelgeving wordt bevorderd.			
CMIS - Content Management Interoperability Services	*Status:* Vastgesteld	*Werking:*	*I-domein:* Connectdiensten	*Beheer:* OASIS
Beschrijving:	Content Management Interoperability Services (CMIS) is een open standaard die een scheiding mogelijk maakt tussen zogenaamde 'content repositories' en content applicaties. Hierdoor kunnen content (ongestructureerde data, zoals			

	documenten en e-mails) en bijbehorende metadata (beschrijvende data) gemakkelijker worden uitgewisseld.			
DKIM	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Toegangsdiensten, Applicatiediensten, Gegevensdiensten	*Beheer:* IETF
Beschrijving:	DomainKeys Identified Mail Signatures (DKIM) koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. Het stelt de ontvanger in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail. Daardoor kunnen spam- en phishing-mails beter worden gefilterd.			
DNSSEC	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Connectdiensten	*Beheer:* IETF
Beschrijving:	Domain Name System Security Extensions (DNSSEC) is een standaard gericht op voorkomen van DNS spoofing (domeinnaam frauduleus koppelen aan een ander IP-adres). Gebruikers kunnen door DNS spoofing worden geleid naar frauduleuze c.q. gevaarlijke websites.			
DigiKoppeling Standaard	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Connectdiensten, Overig	*Beheer:* Logius
Beschrijving:	DigiKoppeling versie 2.0 (voorheen OSB) bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties. Twee hoofdvormen van berichtenverkeer: 1. Bevragingen; een vraag waar direct een reactie op wordt verwacht. Hierbij is snelheid van afleveren belangrijk. Als een service niet beschikbaar is, dan hoeft de vraag niet opnieuw worden aangeboden. 2. Meldingen; men levert een bericht en pas (veel) later komt eventueel een reactie terug. In dat geval is snelheid van afleveren minder belangrijk. Als een partij even niet beschikbaar is om het bericht aan te nemen, dan is het juist wel gewenst dat het bericht nogmaals wordt aangeboden. Agenda Forum Standaardisatie Digikoppeling versie 3.0 is in ontwikkeling en staat op de agenda voor de PTLU-lijst.			
E-portfolio NL	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* NEN
Beschrijving:	NTA 2035 E-portfolio NL is een toepassingsprofiel voor studenten en werknemers bij Nederlandse organisaties, van de internationale IMS ePortfolio specificatie. Hiermee kunnen de competenties van een individu worden bijgehouden. Het voordeel van deze standaard is dat de student/lerende medewerker zijn profiel mee kan nemen naar verschillende organisaties.			
ECLI	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* Juriconnect

Beschrijving:	Met de ECLI standaard kunnen: 1) alle rechterlijke uitspraken in de Europese Unie (zowel van nationale als van Europese gerechten) worden voorzien van een gelijkaardige, unieke en persistente identifier. Deze identifier kan worden gebruikt voor identificatie en citatie van rechterlijke uitspraken en derhalve om deze te vinden in binnenlandse of, buitenlandse, Europese of internationale jurisprudentiedatabanken. 2) alle rechterlijke uitspraken worden voorzien van uniforme metadata, gebaseerd op de Dublin Core standaard. Het zoeken van uitspraken in allerlei databanken worden daardoor gefaciliteerd.			
EML NL	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten, Connectdiensten	*Beheer:* Kiesraad
Beschrijving:	Agenda Forum Standaardisatie De EML_NL standaard versie 1.0 definieert de gegevens en de uitwisseling van gegevens bij verkiezingen die vallen onder de Nederlandse Kieswet. Het gaat daarbij om de uitwisseling van kandidaatgegevens en uitslaggegevens.			
Geo standaarden	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* Geonovum
Beschrijving:	In Nederland (en ook daarbuiten) zijn veel organisaties betrokken bij het registreren en uitwisselen van informatie met een geografische component. Dat wil zeggen: informatie over objecten die gerelateerd zijn aan een locatie ten opzichte van het aardoppervlakte. Hierbinnen zijn verschillende domeinen te onderkennen, zoals kadastrale informatie en informatie over waterhuishouding. Om te waarborgen dat de geo-informatiehuishouding van deze domeinen goed op elkaar aansluit, en dat informatie tussen domeinen uitgewisseld kan worden, zijn afspraken nodig over de te gebruiken standaarden. De set Geo-standaarden voorziet hierin.			
IFC	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten, Connectdiensten	*Beheer:* buildingSMART
Beschrijving:	Industry Foudation Classes (IFC) is een standaard voor uitwisseling van 3D-bouwinformatiemodellen			
IPv4-IPv6	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Werkplekdiensten, Connectdiensten, Datacenterdiensten	*Beheer:* IETF
Beschrijving:	Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. De belangrijkste motivatie voor de ontwikkeling van IPv6 was het vergroten van de hoeveelheid beschikbare adressen ten opzichte van de tegenwoordig gangbare voorganger IPv4.			

	Let op: Om interoperabiliteit maximaal te waarborgen heeft College Standaardisatie 'pas toe of leg uit' van toepassing verklaard op de combinatie van IPv4 en IPv6. Een organisatie moet dus beide versies vragen bij de aanschaf van een ICT-product/-dienst.			
JCDR	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* Juriconnect
Beschrijving:	De standaard biedt een eenduidige manier van verwijzen naar (onderdelen van) decentrale regelgeving waarmee de interoperabiliteit van juridische documenten en systemen die veel verwijzingen kennen naar decentrale regelgeving wordt bevorderd			
JPEG	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten	*Beheer:* ISO/IEC
Beschrijving:	JPEG is een formaat voor afbeeldingen dat gebruik maakt van niet-omkeerbare datacompressie (ofwel lossy compression)			
Metagegevens Rijk	*Status:* Vastgesteld	*Werking:* Rijksbreed generiek	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* Nationaal Archief
Beschrijving:	Het Toepassingsprofiel Metagegevens Rijksoverheid is een uitwerking van de ISO / NEN 23081 metadata standaard. Het toepassingsprofiel is de vertaling naar metadata voor de Rijksoverheid. Het beschrijft de rijksbrede afspraken over de wijze van vastleggen van metagegevens en de afspraken over metagegevens die minimaal vereist zijn. Metagegevens zorgen voor vindbaarheid, authenticiteit, betrouwbaarheid, zorgvuldigheid in de omgang (vertrouwelijkheid, openbaarheid), leesbaarheid en uitwisselbaarheid van gegevens. De afspraken dragen daarom onder andere bij aan: • adequate informatie-uitwisseling tussen overheden; • mogelijkheden tot tijd-, plaats-, en apparaat onafhankelijk werken; • adequate samenwerking en kennisdeling.			
NEN-ISO/IEC 27001	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* I-domein totaal, Overig	*Beheer:* NEN
Beschrijving:	ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden.			
NEN-ISO/IEC 27002	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* I-domein totaal, Overig	*Beheer:* NEN

Beschrijving:	ISO 27002 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.			
NILT	*Status:* Vastgesteld	*Werking:* Rijksbreed generiek	*I-domein:* Toegangsdiensten	*Beheer:* TBGI (Tactische Besturing Generieke ICT); Beheerorganisatie Rijkspas
Beschrijving:	Het Normenkader Infrastructuur Logische Toegang beschrijft de generieke infrastructuur en de verschillende toepassingen van de Rijkspas voor logische toegang tot systemen, netwerken en applicaties. Het normenkader betreft uitsluitend departementale logische toegang, en stelt geen eisen aan interdepartementale logische toegang.			
NL LOM	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* EduStandaard
Beschrijving:	In deze afspraak staat beschreven welke metadata toegekend moeten worden aan educatieve content om de vindbaarheid en vergelijkbaarheid te vergroten. Metadata beschrijven de kenmerken van leerobjecten. Deze afspraak is gemaakt voor de sectoren primair onderwijs, voortgezet onderwijs, middelbaar beroepsonderwijs en hoger onderwijs.			
NTA 9040	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* NEN
Beschrijving:	De Nederlandse Technische afspraak 9040 (NTA 9040) beschrijft afspraken over het koppelvlak waarover informatie wordt uitgewisseld binnen het ondernemingsdossier-concept. De standaard maakt het mogelijk meerdere aanbieders en branches in verschillend tempo en met eigen invulling een ondernemingsdossier te laten starten. De standaard bestaat uit vier NTA's. Hiervan zijn de drie die van toepassing zijn op de overheid aangemeld: NTA 9040-1: Regelhulp; NTA 9040-2: Aanvraag en rapportage; NTA 9040-3: Toezicht;			
OAI-PMH	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten, Connectdiensten	*Beheer:* Open Archives Initiative
Beschrijving:	OAI-PMH is een standaard voor harvesting van metadata uit repositories. Met metadata worden kenmerken van en extra opgeslagen informatie over een document of ander object bedoeld. Te denken valt aan auteursgegevens, titel, uitgever, taal, etc. Een repository is een bibliotheek met documenten/objecten (ook wel 'content' genoemd), bijvoorbeeld een (digitaal) archief. OAI-PMH maakt het mogelijk om deze metadata (dus niet de documenten/objecten			

	zelf) uit verschillende repositories te verzamelen. Vanuit een centraal systeem kan dan gezocht worden naar documenten/objecten in de verschillende aangesloten repositories.			
ODF	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Documentdiensten	*Beheer:* OASIS
Beschrijving:	ISO/IEC 26300:2006 definieert een XML-schema dat kan worden gebruikt door office-applicaties Het schema is geschikt voor officedocumenten, zoals tekstdocumenten, spreadsheets, grafieken en grafische documenten zoals tekeningen en presentaties, maar het is niet beperkt tot deze soort documenten.			
OWMS	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* ICTU / De werkmaatschappij BZK
Beschrijving:	Overheids Web Metadata Standaard (OWMS) is een semantische standaard voor metadata, de eigenschappen om informatieobjecten mee te beschrijven. Het voorschrijven van een semantische standaard voor metadata verhoogt de vindbaarheid en de samenhang van informatie die door overheidsorganisaties wordt aangeboden op internet.			
PDF/A-1	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Documentdiensten	*Beheer:* NEN
Beschrijving:	PDF/A-1. Documentbeheer - Elektronische bestandsformaat document voor langdurige bescherming - Gebruik van PDF 1.4 (PDF/A-1) Versie: NEN-ISO 19005-1:2005 en Dit deel van ISO 19005 specificeert hoe Portable Document Format (PDF) 1.4 voor lange termijn archivering van elektronische documenten dient te worden gebruikt. Het heeft betrekking op documenten die combinaties van data in de vorm van karakters, rasters en vectoren			
PDF/A-2	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Documentdiensten	*Beheer:* ISO
Beschrijving:	PDF/A-2 slaat de brug tussen PDF/A-1 en PDF 1.7 waarbij PDF/A-2 een betere geschiktheid heeft voor langdurig archiveren van documenten waar "elementen" inzitten die niet door PDF/A-1 worden ondersteund en waarbij PDF 1.7 kan worden gebruikt voor "elementen" die niet door PDF/A-2 ondersteund worden.			
PDFv1.7	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Documentdiensten	*Beheer:* ISO
Beschrijving:	PDF v1.7 specificeert een bestandsformaat voor het weergeven van elektronische documenten. Het uitgangspunt van de standaard is dat het gebruikers mogelijk wordt gemaakt documenten uit te wisselen en te bekijken, zowel onafhankelijk van de omgeving waarin ze zijn gecreëerd, alsook de omgeving waarin ze worden uitgeprint of bekeken. Elk PDF v1.7 document bevat een			

	complete beschrijving van een document, inclusief tekst, font objects (embedded of met typeface beschrijving), afbeeldingen, audio, video, en 2D/3D graphics.			
PNG	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Documentdiensten	*Beheer:* ISO/IEC
Beschrijving:	Portable Network Graphics (PNG) is een formaat voor rasterafbeeldingen (ofwel bitmaps) dat gebruik maakt van exact omkeerbare datacompressie (ofwel lossless compression).			
PRINCE II	*Status:* Vastgesteld	*Werking:* Rijksbreed generiek	*I-domein:* Overig	*Beheer:* Axelos
Beschrijving:	PRINCE2® (PRojects IN Controlled Environments) is een internationaal veel toegepaste, gestructureerde methode voor projectmanagement. De methode is gericht op het management, de besturing en de organisatie van een project. PRINCE2 is ontwikkeld en wordt onderhouden door de Britse semi-overheidsorganisatie the Cabinet Office.			
SAML	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Werkplekdiensten, Toegangsdiensten, Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* OASIS
Beschrijving:	Security Assertion Markup Language (SAML).De Security Assertion Markup Language (SAML), is een XML-gebaseerd raamwerk voor het communiceren van gebruikers authenticatie, rechten, en attribuut informatie. SAML biedt organisatie entiteiten de mogelijkheid om claims te maken over de identiteit, attributen en rechten van een subject (een entiteit welke vaak een menselijke gebruiker is) aan andere entiteiten zoals Internet applicaties of diensten.			
SEPA	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* European Payments Control
Beschrijving:	De SEPA-standaarden zijn bedoeld voor giraal betalingsverkeer in euro in Europa (incl.binnenlands betalingsverkeer).			
SETU	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten, Connectdiensten	*Beheer:* SETU
Beschrijving:	De SETU-standaard is de Nederlandse implementatie van de internationale HR-XML standaard en is ontwikkeld door de grote uitzendorganisaties. Door toepassing van de SETU standaard ontstaat uniformering van het elektronisch berichtenverkeer tussen aanbieders en afnemers (inleners) van tijdelijk personeel (flexibele arbeid). Dit leidt tot vereenvoudiging van het inhuurproces.			

SIKB0101	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* SIKB (Stichting Infrastructuur Kwaliteitsborging Bodembeheer)
Beschrijving:	Protocol voor digitale data-uitwisseling bodemgegevens, standaard voor uitwisselen kwaliteitsgegevens van de bodem, inclusief geografische en administratieve gegevens.			
STOSAG	*Status:* Vastgesteld	*Werking:* Overig	*I-domein:*	*Beheer:* STOSAG/NVRD
Beschrijving:	Container- en Pasmanagement voor Afval en Grondstoffen			
Sem. Mod. e-factureren	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* Logius
Beschrijving:	Het Semanitische factuurmodel is een standaard voor electronisch factureren. De standaard beschrijft welke gegevenselementen er in een elektronische factuur opgenomen dienen en kunnen worden, wat de samenhang is tussen deze elementen en wat de betekenis is van deze elementen. Daarnaast bevat de standaard mappings van de gegevenselementen naar SETU (staat op de 'pas toe of leg uit' –lijst) en de internationale UBL standaard. Dit zijn twee veelgebruikte standaarden voor elektronisch factureren. Dankzij de mappings kunnen gebruikers van deze standaarden op een eenvoudige uniforme wijze elektronisch naar de overheid factureren. Mappings naar andere standaarden zijn bovendien ook mogelijk. De opname van het semantische factuurmodel geeft duidelijkheid aan overheden en bedrijven (gebruikers en ICT-aanbieders) over de elementen die op facturen naar overheidsorganisaties gebruikt dienen te worden (specifiek voor de Nederlandse situatie).			
StUF	*Status:* Vastgesteld	*Werking:* Overig	*I-domein:*	*Beheer:* VNG/KING
Beschrijving:	Standaard uitwisselings formaat (StUF) is een universele berichtenstandaard voor het elektronisch uitwisselen van gegevens tussen applicaties. Het domein van de StUF-taal omvat informatieketens tussen overheidsorganisaties (basisregistraties en landelijke voorzieningen) en gemeentebrede informatieketens en -functionaliteit. StUF is beschreven in XML en gebaseerd op geaccepteerde internetstandaarden			
TLS	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Connectdiensten, Informatiebeveiliging	*Beheer:* Internet Engineering Task Force (IETF)
Beschrijving:	TLS is een protocol, dat tot doel heeft om beveiligde verbindingen op de transportlaag over het internet te verzorgen. De standaard wordt gebruikt bovenop standaard internet transport protocollen (TCP/IP) en biedt een beveiligde basis, waar applicatie protocollen als HTTP (webverkeer) of SMTP en			

	IMAP (mailuitwisseling) op hun beurt weer op kunnen bouwen en gebruik van kunnen maken.			
TOGAF	*Status:* Vastgesteld	*Werking:* Rijksbreed generiek	*I-domein:* I-domein totaal, Overig	*Beheer:* The Open Group
Beschrijving:	The Open Group Architecture Framework TOGAF is een methode voor het ontwikkelen en beheren van de enterprise-architectuur. TOGAF is een open standaard. TOGAF bevat een verzameling aan technieken en best-practices. Centraal in de methode staat de Architecture Development Method (ADM). Deze beschrijft de verschillende fasen van ontwikkeling en beheer van de enterprise-architectuur			
VISI	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten, Connectdiensten	*Beheer:* CROW
Beschrijving:	VISI is een door de Nederlandse bouwsector geaccepteerd afsprakenstelsel voor de digitale uitwisseling van formele communicatie.			
WDO Datamodel	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* Wereld Douane Organisatie en binnen Nederland het Nationaal Plaform Data-Model (NPDM)
Beschrijving:	Het WDO Datamodel is bedoeld om gegevensaanlevering van het bedrijfsleven naar de overheid op het gebied van grensoverschrijdend personen- en goederenverkeer meer te simplificeren en te harmoniseren. Het WDO Datamodel bevat zogenaamde 'informatiepakketten' voor gegevensuitwisseling. Een informatiepakket beschrijft de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties (Message Implementation Guidelines). Informatiepakketten kunnen aan elkaar gerelateerd worden, waardoor samenhang ontstaat. Het WDO Datamodel integreert op deze manier de semantiek voor verschillende toepassingsdomeinen. Hierbij gaat het niet alleen om de Douane, maar ook om tal van andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer (Voedsel en Waren Autoriteit, Havenautoriteiten etc.).			
Webrichtlijnen	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Documentdiensten, Gegevensdiensten	*Beheer:* Logius
Beschrijving:	De Webrichtlijnen bevatten richtlijnen en principes voor het toegankelijk maken van webcontent die onder uiteenlopende situaties te gebruiken moet zijn, uitwisselbaar en duurzaam is. Het volgen van deze richtlijnen en principes maakt content optimaal bruikbaar en toegankelijk voor mensen en systemen, waaronder gebruikers van uiteenlopende webapparaten, besturingssystemen			

	en hulptechnologieën. De Webrichtlijnen versie 2 biedt een technologieonafhankelijke standaard die toepassing van verschillende technologieën toestaat en die is voorbereid op toekomstige technologieën.			
XBRL Dimensions	*Status:* Vastgesteld	*Werking:* Overheidsbreed	*I-domein:* Applicatiediensten, Gegevensdiensten	*Beheer:* XBRL International
Beschrijving:	Organisaties wisselen bedrijfsinformatie uit op de meest uiteenlopende manieren (op papier of elektronisch, als Word-document, als Pdf, als spreadsheet, etc.). XBRL, eXtensible Business Reporting Language, is een internationale open standaard om deze gegevens op eenvoudige wijze te verzamelen, elektronisch uit te wisselen, te analyseren en zonodig nader te bewerken.			