

Programma van Eisen CI

Parelsnoer PvE CI



PARELSNOER INITIATIEF

Versie: 1.1
Status: definitief
Datum: 19 september 2008

Inhoud

1	Inleiding	3
1.1	Positionering van dit programma van eisen	3
1.2	Uitgangspunten.....	4
1.3	Leeswijzer	4
1.4	Gerelateerde documenten	4
1.5	Versiehistorie.....	5
2	Context.....	6
2.1	Parelsnoer	6
2.2	Project Parelsnoer Centrale Infrastructuur	6
2.3	Keuzes in de opzet van de centrale voorzieningen	7
2.3.1	Bundelen en Centrale opslag.....	7
2.3.2	Privacy en beveiliging	8
2.3.3	Parelsnoer Informatiemodel.....	8
2.4	Globale werking van de centrale voorzieningen	9
2.4.1	Informeren	9
2.4.2	Bundelen.....	10
2.4.3	Uitleveren	10
3	Dienstverlening en processen	11
3.1	Dienstverlening	11
3.2	Beheertaken CI.....	11
3.2.1	Beheer en onderhoud van de CI infrastructuur	11
3.2.2	Beheer en onderhoud van de Parelsnoer CI architectuur, ontwerp en standaarden.....	11
3.2.3	Rapportage.....	12
3.3	Beveiliging	12
3.3.1	Privacy en vertrouwelijkheid	12
3.3.2	Logging.....	12
3.3.3	PKI.....	13
3.3.4	Gescheiden systemen	13
4	Informatie en functionaliteit	14
4.1	Functionaliteit	14
4.2	Gegevensmodel	14
4.3	Koppelvlakken	15
4.4	Webrichtlijnen.....	15
5	Techniek	16
5.1	Netwerkverbinding	16
5.2	Tweezijdige SSL.....	16
5.3	Koppelvlak datasets.....	16
5.4	Koppelvlak beeldmateriaal.....	16
5.5	Eisen aan beveiliging certificaten.....	16

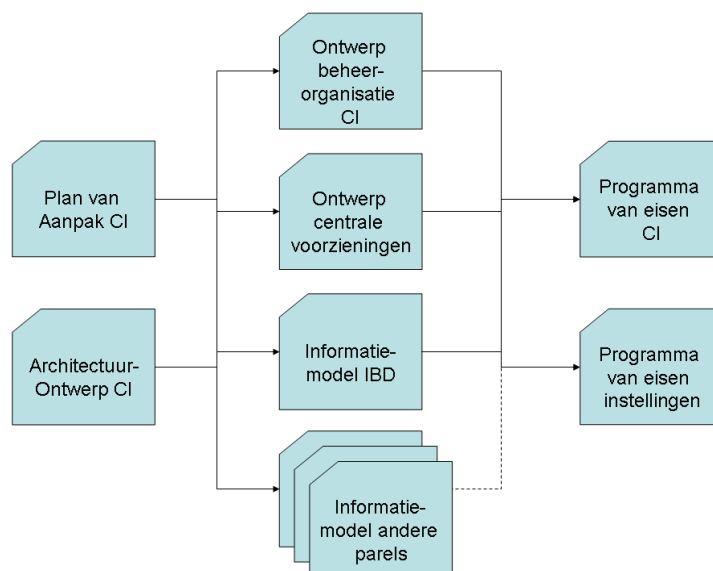
1 Inleiding

Het project Parelsnoer beoogt¹ binnen de academische centra een infrastructuur te realiseren voor het verzamelen van klinische data, beeldmateriaal en opzetten van biobanken op interuniversitair niveau. Voor de realisatie van de benodigde centrale voorzieningen is niet alleen een ontwerp van de techniek en de beheerorganisatie benodigd, ook de verwachtingen aan een instelling moeten expliciet gemaakt worden. Het voorliggende document betreft het programma van eisen voor instellingen binnen Parelsnoer.

In dit document wordt de term instelling gebruikt voor de aangesloten academische centra en niet UMC. Er is voor deze generieke term gekozen omdat op termijn ook externe partijen (niet UMC) aangesloten kunnen.

1.1 Positionering van dit programma van eisen

Dit programma van eisen is een van de documenten die binnen het Parelsnoer Centrale Infrastructuur project is opgesteld. Onderstaande figuur geeft een overzicht van alle ontwerpdocumenten binnen het project:



In de figuur is de volgorde van de documenten aangegeven. Dit wordt nader toegelicht in het Plan van Aanpak CI.

De volgende documenten zijn opgenomen in bovenstaande figuur:

- *Architectuurontwerp CI*
Dit architectuurontwerp bevat alle kaders en principes die gehanteerd worden bij de totstandkoming van de centrale infrastructuur. Het architectuurontwerp is uitgangspunt bij het opstellen van het ontwerp.
- *Plan van aanpak CI*
Dit document beschrijft de aanpak voor de realisatie van de centrale infrastructuur. Het plan beschrijft een incrementele aanpak voor de realisatie van de centrale infrastructuur. Dit ontwerp dient ook gezien te worden als het ontwerp voor de eerste increment. Voor de komende incrementen kan dit plan worden bijgewerkt.

¹ Uit "Werkplan Parelsnoer"

- *Ontwerp Centrale Voorzieningen*
Dit is het ontwerp van de centrale infrastructuur. Het document vormt samen met het programma van eisen CI de basis voor de realisatie van de CI. Dit document in combinatie met het programma van eisen Instellingen vormt, aangevuld met eigen ontwerpdocumentatie, de basis voor de aansluiting van de instellingen op de CI.
- *Ontwerp Beheerorganisatie CI*
De CI betreft naast techniek ook een beheerorganisatie voor het uitvoeren van het beheer en het leveren van diensten aan onderzoekers. Deze organisatie is in dit document beschreven.
- *Parelsnoer InformatieModel (PIM)*
De PIM is een gegevensontwerp voor het vastleggen en uitwisselen van gegevens over Parels. De PIM is de basis voor de inrichting van de database van de centrale infrastructuur. Tevens is de PIM de afspraak volgens welke alle instellingen gegevens gaan uitwisselen met de centrale infrastructuur. Gestart wordt met IBD en daarop zullen snel de andere parels ook volgen.
- *Programma van eisen CI*
Het programma van eisen CI, het voorliggende document, vormt de basis van de realisatie van de centrale infrastructuur. Het bevat de functionele eisen (die uitvoerig beschreven zijn in het Ontwerp CI) en de niet-functionele eisen (eisen zoals schaalbaarheid, performance, beheerbaarheid, etc.)
- *Programma van eisen Instellingen*
Het programma van eisen Instellingen is de basis voor de aansluiting van een Instelling op de CI. Het bevat alle functionele en niet-functionele eisen die gesteld worden aan de Instellingen om te kunnen aansluiten op de CI.

1.2 Uitgangspunten

- In het architectuurontwerp worden uitgangspunten beschreven voor zowel 2008/2009 als mede voor daarna (geannoteerd met toekomst). Dit ontwerp gaat alleen uit van de uitgangspunten voor 2008/2009.
- De definitie van de PIM is zodanig dat de dataset (met uitzondering van het BSN) voldoende anoniem is. Hierdoor kan worden volstaan met alleen het vervangen van het BSN door een gepseudonimiseerd BSN.

1.3 Leeswijzer

Bij het lezen van dit programma van eisen wordt er vanuit gegaan dat de lezer bekend is met het architectuurontwerp en met het ontwerp van de CI.

In hoofdstuk 2 wordt eerst de context van Parelsnoer en de globale werking beschreven. Daarna worden de eisen aan instellingen beschreven vanuit vier verschillende perspectieven: procesmatig (hoofdstuk 3), functioneel/informatie (hoofdstuk 4), techniek (hoofdstuk 5).

1.4 Gerelateerde documenten

- Gerard van der Hoorn, Reinier Balt, Parelsnoer Centrale Infrastructuur: Projectplan 2007-2010. Versie 0.10. Amsterdam: Parelsnoer Initiative, 3 december 2007.
- Reinier Balt, Frans van den Dool, Architectuur Centrale Infrastructuur: Parelsnoer, Versie 1.1. Amsterdam: Parelsnoer Initiative, 30 november 2007.
- Reinier Balt, Joost Schalken, Eelco den Heijer, Ontwerp Centrale Voorzieningen Parelsnoer, versie 0.4. Amsterdam: Parelsnoer Initiative, 20 december 2007.

- Reinier Balt, Joost Schalken, Eelco den Heijer, Programma Van Eisen Instelling: Parelsnoer PvE Centrale Infrastructuur. Versie 0.0. Amsterdam: Parelsnoer Initiative, Q1 2008 (PM).
- Reinier Balt, Joost Schalken, Eelco den Heijer, Ontwerp Beheerorganisatie Centrale Voorzieningen, versie 0.0. Amsterdam: Parelsnoer Initiative, Q1 2008 (PM).
- Miranda de Gouw en Sandra Sliepenbeek, Parelsnoer Informatie Model (PIM). Versie 0.0. Amsterdam: Parelsnoer Initiative, Q1 2008 (PM).
- Eric Velleman, Stephen Hay, en Raph de Rooij, Normative document Web Guidelines for Quality Mark drempelvrij.nl - Success criteria for the Web Guidelines, including W3C's Web Content Accessibility Guidelines version 1.0, priority 1 & 2. Utrecht, drempelvrij.nl, juli 2007.
- Website voor overheid webrichtlijnen: <http://www.webrichtlijnen.nl/>

1.5 Versiehistorie

Datum	Versie / Status	Opmerkingen
5 februari 2008	0.1	Initiële concept versie
10 maart 2008	0.9	Commentaar team verwerkt
4 april 2008	1.0	Finaliseren
19 sep	1.1	Omzetten huisstijl; geen inhoudelijke wijzigingen

2 Context

2.1 Parelsnoer

In het huidige medisch wetenschappelijke onderzoek speelt de relatie tussen fundamentele kenmerken (genen) en processen in het lichaam (eiwitten, metaboliëten), én het klinisch beloop een belangrijke rol. In Nederland is, na de integratie van de academische ziekenhuizen en de medische faculteiten tot UMC's, het translationele onderzoek, dat kliniek en laboratorium koppelt, enorm tot bloei gekomen. Kennis over het ontstaan en het variabele beloop van ziekten is in toenemende mate gebaseerd op patiëntcohorten waarvan zowel de klinische data (inclusief digitaal beeldmateriaal) als analyses op lichaamsmateriaal aanwezig zijn. Daarnaast worden behandelingsopties sterk bepaald door waarnemingen in goed gedocumenteerde patiëntengroepen.

Het project Parelsnoer beoogt binnen de academische centra een infrastructuur te realiseren voor het verzamelen van klinische data, beeldmateriaal en opzetten van biobanken op interuniversitair niveau. Het Parelsnoer project richt zich in eerste instantie op het faciliteren van combinaties van bijzondere biobanken en patiëntcohorten voor acht ziektebeelden. Om de expertise van de UMC's ten volle te benutten zal de opzet van de infrastructuur en het onderzoek zich richten op topreferente en aan het UMC gelieerde patiëntenpopulaties.

De ziektebeelden ('parels') waarvoor in dit project een data- en biobank zal worden gerealiseerd zijn:

- neurodegeneratieve ziekten
- leukemie
- reumatoïde artritis
- erfelijke darmkanker
- diabetes mellitus
- nierfalen
- cerebro vasculair accident (CVA)
- inflammatoire darmziekten (IBD).

De wetenschappelijke gegevens die worden gecreëerd met behulp van bovengenoemde infrastructuur zullen leiden tot een betere gezondheid van patiënten met genoemde ziektebeelden, en mogelijk op termijn versterking van de economische positie van de farmaceutische industrie in Nederland. De gecreëerde infrastructuur plaatst Nederland op dit gebied tevens in een Europese koppositie.

2.2 Project Parelsnoer Centrale Infrastructuur

Voor het bereiken van de doelstellingen van Parelsnoer is het bundelen van de onderzoeksgegevens van de deelnemende instellingen nodig. Om dit mogelijk te maken is een centrale infrastructuur voorzien die het mogelijk maakt om de verschillende onderzoeksgegevens te bundelen en beschikbaar te stellen aan geautoriseerde onderzoekers. Voor de realisatie van deze centrale infrastructuur is het (deel)project Centrale Infrastructuur gedefinieerd. Dit project heeft als doelstelling:

- Een centrale voorziening in te richten waar onderzoekers terecht kunnen met
 - een geautoriseerd verzoek voor een verzameling met klinische gegevens en/of beeldmateriaal ten behoeve van onderzoek naar bepaalde ziektebeelden. Op basis van dit geautoriseerde verzoek wordt de verzameling samengesteld en aangeleverd aan de onderzoeker
 - een geautoriseerd verzoek voor biomateriaal dat is opgeslagen in de aangesloten instellingen. Op basis van dit geautoriseerde verzoek wordt

het biomateriaal opgehaald en afgeleverd bij de onderzoeker. De informatiestroom voor dit proces is onderdeel van dit project. Het fysieke transport van het biomateriaal niet.

Ten behoeve van deze verzoeken wordt een catalogus beschikbaar gesteld waarmee een onderzoeker kan bepalen welke onderzoeksgegevens w.o. beeldmateriaal en biomateriaal beschikbaar is

- Een infrastructuur te realiseren die het mogelijk maakt om de bronnen met klinische onderzoeksgegevens van de verschillende UMC's voor ziektebeelden te ontsluiten ten behoeve van andere onderzoekers
- Een referentiemodel te introduceren voor de structuur van de onderzoeksgegevens die over de infrastructuur worden uitgewisseld. Dit referentiemodel is een integraal informatie model over de ziektebeelden heen en biedt een model voor een specifiek ziektebeeld.

De CI zal niet alleen een technisch platform zijn. Rondom de CI wordt een beheerorganisatie ingericht. Deze organisatie heeft tot doel om onderzoekers te voorzien van onderzoeksgegevens en biomateriaal, het beheren van de technische infrastructuur, het bewaken van de gegevensaanlevering en het beheer van de architectuur en standaarden. In 2008 wordt een eerste invulling gegeven aan deze organisatie. Deze wordt daarna in 2009 verder doorontwikkeld.

In de aanpak van de realisatie van de centrale infrastructuur wordt een incrementele aanpak gehanteerd. De doelstelling is om in 2008 met minimaal een eerste Parel² productieel te zijn. Omdat nog vele onduidelijkheden bestaan binnen Parelnoer wordt gestart met een basisplatform voor uitwisseling van onderzoeksgegevens. Dit platform kan vervolgens incrementeel doorontwikkeld worden, mede op basis van gedane ervaringen en voortschrijdende inzichten.

2.3 Keuzes in de opzet van de centrale voorzieningen

Het architectuurontwerp van de centrale voorzieningen schetst de uitgangspunten en principes waaraan deze voorzieningen moeten voldoen. Hierin zijn keuzes gemaakt over

- De wijze van bundelen van onderzoeksgegevens van de instellingen
- Het waarborgen van de privacy van de patiënt en het beveiligingen van patiëntgegevens.
- Het standaardiseren van de vastlegging van de onderzoeksgegevens in de centrale infrastructuur in de vorm van een Parelnoer Informatiemodel (PIM)

Hieronder worden deze onderdelen nader beschreven.

2.3.1 Bundelen en Centrale opslag

In het architectuurontwerp is gekozen voor een centrale opslag van een recente kopie van de onderzoeksgegevens van de instellingen. Het beheer van de onderzoeksgegevens blijft hierbij bij de instellingen.

Regelmatig zullen instellingen onderzoeksgegevens (klinische gegevens, gegevens over bio- en beeldmateriaal) elektronisch aanleveren bij de CI. Dit gebeurt per Parel. De CI zal per Parel de aangeleverde gegevens bundelen en centraal vastleggen. Uitgaande van acht Parels en acht UMC's, zal de CI 64 aanleveringen ontvangen en bundelen.

² Er is gekozen om te starten met Inflammatoire darmziekten (Inflammatory Bowel Disease, IBD)

Informatie over de parels als mede statistische kentallen over de beschikbare gegevens per parel zullen in een catalogus gepubliceerd worden voor (externe) onderzoekers.

Een (externe) onderzoeker die beschikking wil krijgen over delen van deze gebundelde gegevens zal hiervoor een verzoek indienen bij een Parelsnoer Commissie. Als deze toestemming verleent, zal het verzoek door de CI worden uitgevoerd op de centraal vastgelegde gebundelde klinische gegevens. Het resultaat hiervan wordt aan de onderzoeker beschikbaar gesteld (gebruiksrecht). Een instelling zal dus ontlast worden van de afhandeling van verzoeken om klinische gegevens.

2.3.2 Privacy en beveiliging

Aangezien het medische gegevens betreft van patiënten, dient zorgvuldig met de onderzoeksgegevens om te worden gegaan. In de architectuur is gekozen voor beveiliging op meerdere lagen.

In de eerste plaats worden alle onderzoeksgegevens gepseudonimiseerd. Dat wil zeggen dat de gegevens in een dataset die afgegeven is aan een externe onderzoeker niet herleidbaar is naar een specifieke patiënt. De pseudonimisatie wordt uitgevoerd door de instellingen voordat gegevens worden aangeleverd. De CI weet daardoor ook niet wie de patiënt is waarvan de gegevens in de centrale database zijn vastgelegd.

Er is gekozen voor pseudonimisatie zodat in uitzonderlijke gevallen, volgens een strikte procedure een patiënt wel achterhaald kan worden. Dit kan alleen met medewerking van de aanleverende instelling, omdat alleen daar de informatie bekend is om te de-pseudonimiseren.

Verder is gekozen voor beveiligde communicatie volgens PKI standaarden (tweezijdige SSL op basis van servercertificaten) tussen de instellingen en de CI voor de aanlevering van gegevens.

Ten slotte is voorzien in het verwijderen van gegevens in lijn met de eisen die in de WBP³ worden gesteld. Het verwijderen vindt plaats bij de bron, dus bij de instellingen. Zij verwijderen de gegevens uit hun systemen. Bij de volgende aanlevering worden eerst alle oude gegevens uit de CI verwijderd en daarna worden de nieuw aangeleverde gegevens (waarin de te verwijderen patiëntgegevens niet meer voorkomen) in de centrale database geplaatst.

2.3.3 Parelsnoer Informatiemodel

Een belangrijke keuze in het architectuurontwerp is het Parelsnoer Informatiemodel (PIM). Dit is het informatiemodel waarin alle Parels zijn gemodelleerd. Binnen Parelsnoer wordt daarmee met één model gewerkt waarin eenduidig is gedefinieerd hoe onderzoeksgegevens binnen een Parel worden vastgelegd.

De instellingen leveren hun onderzoeksgegevens bij de CI aan in een bestand. Het bestandsformaat voldoet aan deze PIM. Dit wil niet zeggen dat alle systemen van een instelling aangepast moeten worden om te werken volgens de PIM, maar een instelling moet wel haar onderzoeksgegevens kunnen aanleveren conform de PIM. Een instelling kan daarbij bijvoorbeeld kiezen om eerst haar bestaande gegevens te converteren naar het PIM.

Bij het ontwerpen van de Parels wordt het datamodel (syntax en semantiek) gedefinieerd voor de klinische gegevens, de gegevens over beschikbaar biomateriaal en de gegevens over beschikbaar beeldmateriaal. Verder wordt bij een Parel gekeken naar de

³ Wet Bescherming Persoonsgegevens

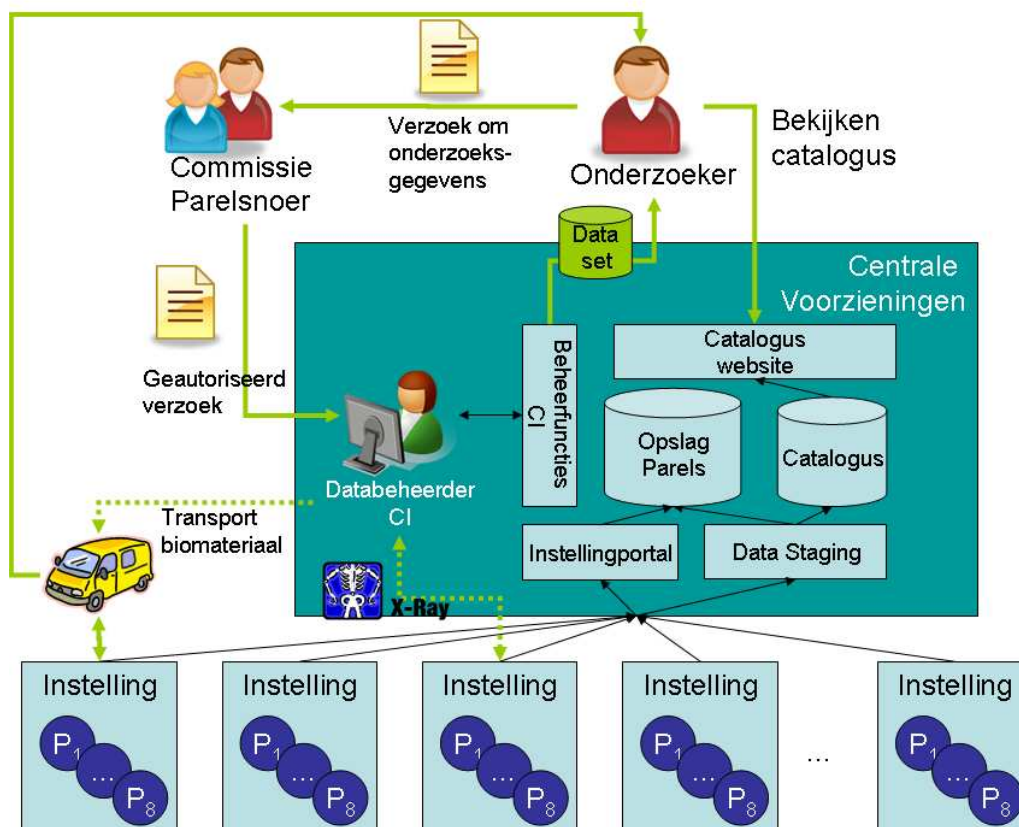
kwaliteitsnormen van de vastlegging van de onderzoeksgegevens. De invoering daarvan valt buiten de scope van de CI. De CI gaat er vanuit dat alleen gecontroleerd moet worden of de aanlevering conform het PIM is en zal geen andere kwaliteitscontroles uitvoeren.

2.4 Globale werking van de centrale voorzieningen

De centrale voorzieningen hebben de volgende functionele hoofddoelen:

- Het informeren van onderzoekers en geïnteresseerden via een catalogus
- Het bundelen van onderzoeksgegevens van de aangesloten instellingen
- Het uitleveren van gegevensverzamelingen op basis van een geautoriseerd verzoek van een onderzoeker.

De hierboven beschreven functionele werking van de centrale voorzieningen zijn in de figuur hieronder weergegeven. Midden-boven staat de onderzoeker die de catalogus kan bekijken en een verzoek bij de commissie kan indienen. Na autorisatie komt dit verzoek bij de databeheerder van CI die dit verzoek zal afhandelen. Het resultaat wordt vervolgens bij de onderzoeker afgeleverd.



De hoofdfuncties van de CI wordt in de komende paragrafen nader toegelicht.

2.4.1 Informeren

De CI zal de catalogus als website beschikbaar stellen. De catalogus is een publiek toegankelijke website op Internet. Het doel is om geïnteresseerden en onderzoekers te informeren over Parelsnoer, de Parels en over de beschikbare gegevens. De website toont alleen totalen en metagegevens, maar niet de gegevens zelf.

2.4.2 Bundelen

Voor het aanleveren van onderzoeksgegevens is het doel dat instellingen op regelmatige basis een volledige verzameling onderzoeksgegevens aanleveren bij de CI. Elke instelling levert één gegevensverzameling aan per parel. De gegevensverzameling is gestandaardiseerd volgens het Parelsnoer Informatiemodel (PIM).

Stel dat acht instellingen voor alle acht parels gegevensverzamelingen aanleveren, dan krijgt de CI $8 \times 8 = 64$ gegevensverzamelingen aangeleverd. De CI zorgt voor bundeling van de gegevensverzamelingen in de centrale database.

Een instelling kan zelf bepalen uit welk systeem of systemen de gegevens geëxporteerd worden naar een bestand en met welk systeem of systemen de upload van het bestand wordt uitgevoerd.

2.4.3 Uitleveren

Een onderzoeker die beschikking wil hebben over gegevens van Parelsnoer, zal zijn verzoek moeten indienen bij een wetenschappelijke Parelsnoer commissie. De commissie beslist over het wel of niet beschikbaar stellen van onderzoeksgegevens van Parelsnoer.

Om het verzoek te kunnen opstellen is informatie over de beschikbare onderzoeksgegevens beschikbaar in een catalogus. Met behulp van deze catalogus moet een onderzoeker in staat zijn om een verzoek te kunnen indienen bij de commissie.

Als de CI vanuit de commissie een geautoriseerd verzoek heeft ontvangen, zal de databasebeheerder deze vertalen naar een zoekopdracht op de centrale database. De resulterende gegevens wordt omgezet naar een exportbestand. Dit bestand wordt beschikbaar gesteld aan een onderzoeker.

Momenteel is weinig bekend over de wijze waarop een onderzoeker zijn vraag zal / kan stellen. Voor dit ontwerp wordt dan ook uitgegaan dat een menselijke functionaris de vraag van de onderzoeker moet vertalen naar een zoekopdracht op de database. Op basis van praktijkervaring kan bekeken worden of het aanleveren van de zoekvraag door een onderzoekers meer geautomatiseerd kan worden zodat de handmatige vertaling overbodig (of uitzonderlijk) wordt.

Als het verzoek biomateriaal betreft, zal de CI alle benodigde gegevens hiervoor beschikbaar stellen aan de functionaris die de logistiek van transport van het biomateriaal verzorgt. Deze zal het transport van het betreffende materiaal organiseren vanaf de instelling waar zich het materiaal bevindt tot de locatie van de aanvragende onderzoeker.

Als het verzoek beeldmateriaal betreft, zorgt de gegevensbeheerder van CI voor het opvragen van het beeldmateriaal bij de verschillende instellingen. Dit proces dient nog nader te worden vormgegeven.

3 Dienstverlening en processen

3.1 Dienstverlening

De CI realiseert een beheerorganisatie conform het ontwerp van de beheerorganisatie. Dit betekent dat de CI de volgende diensten zal bieden

- Diensten voor onderzoekers
 - Beschikbaar stellen van een dataset
 - Beschikbaar stellen van de catalogus
 - Beschikbaar stellen van biomateriaal
 - Beschikbaar stellen van beeldmateriaal
 - Afhandelen verzoeken de-pseudonimisatie
- Diensten voor instellingen
 - Testen met de CI
 - Aansluiten op de CI
 - Technische ondersteuning aansluiten en aanleveringen

De CI dient te voldoen aan de SLA-normen die voor deze diensten zijn opgenomen in het ontwerp van de beheerorganisatie.

3.2 Beheertaken CI

De beheerorganisatie van de CI heeft naast operationele beheerverantwoordelijkheid ook een verantwoordelijkheid voor het beheren van de architectuur, ontwerp/specificaties en de standaarden binnen Parelsnoer.

3.2.1 Beheer en onderhoud van de CI infrastructuur

De CI zal deze beheertaken uitvoeren op basis van de volgende standaarden voor beheer:

- Technisch beheer conform ITIL
- Applicatie beheer conform ASL
- Functioneel beheer conform BiSL

Dit is nader beschreven in het ontwerp en de beheerorganisatie CI.

Voor Parelsnoer zijn een aantal specifieke beheerprocessen gedefinieerd in het ontwerp van de CI :

- Bewaken van aanleveringen van datasets door instellingen.
- Bewaken van aanleveringen van digitaal beeldmateriaal.
- Bewaken van aanleveringen van biomateriaal.

3.2.2 Beheer en onderhoud van de Parelsnoer CI architectuur, ontwerp en standaarden

De CI is verantwoordelijk voor het beheren van de verschillende ontwerpdocumenten van de CI. Hierop vervult zij de volgende taken zoals beschreven in ontwerp van de beheerorganisatie CI:

- Onderhoud op de Architectuur CI
- Onderhoud op de ontwerpdocumentatie
 - Programma van eisen Instellingen
 - Programma van eisen CI
 - Ontwerp CI
 - Ontwerp beheerorganisatie CI

- Onderhoud Parelsnoer Informatiemodel
 - Datadictionary PIM
 - Onderhoud bestaande Parels
 - Toevoegen nieuwe Parels
 - Beheer Parelsnoer-eigen codetabellen

3.2.3 Rapportage

In haar beheertaak verzorgt de CI reguliere SLA-rapportage zoals beschreven in het ontwerp van de CI en het ontwerp van de beheerorganisatie. Het betreft rapportage over:

- De uitvoering van diensten, zoals beschreven onder rapportage bij elke dienstbeschrijving in het ontwerp van de beheerorganisatie:
 - Rapportages over het operationeel beheer. Dit is de SLA-rapportage
 - Rapportages over het applicatie beheer. Hieronder valt rapportages over de aanlevering door instellingen van datasets van de parels. Ook de kwaliteit van deze datasets wordt gerapporteerd.
 - Rapportages over het gebruik van de dienstverlening van de CI.

Naast bovengenoemde reguliere rapportages is het ook mogelijk dat de opdrachtgever verzoekt om ad-hoc rapportages:

- Inzicht verzoeken tot de-pseudonimisatie
- Inzicht verzoeken tot aansluiting
- Inzien log
- Inzien gearchiveerde verzoeken

3.3 Beveiliging

3.3.1 Privacy en vertrouwelijkheid

In het architectuur document wordt gesteld dat:

- Vertrouwelijkheid van de gegevens wordt gewaarborgd door toegangsbeveiliging in combinatie met transportbeveiliging (versleuteling) bij overdracht (Architectuurprincipe 28).
- Indien wordt gecommuniceerd met systemen dient de authenticiteit van deze systemen te worden vastgesteld (systeemauthenticatie) (Architectuurprincipe 29).

In de architectuur is het uitgangspunt opgenomen dat de door de UMC's opgeleverde gegevens niet direct herleidbaar tot personen. Alleen onder bepaalde, nog te definiëren strikte voorwaarden, is deze herleidbaarheid wel mogelijk (Architectuurprincipe 2).

In het ontwerp voor de centrale infrastructuur is aangegeven dat voor de-pseudonimisatie de tussenkomst van het betrokken UMC vereist is.

Bovenstaande leidt er toe dat gangbare beveiligingsmaatregelen (up-to-date houden systeemsoftware, installatie van gangbare firewall en antivirus maatregelen, hardening van het systeem waarop de software draait) afdoende zijn om de systeemomgeving te beveiligen. Bijzondere maatregelen (zoals verzwaarde fysieke toegangsbeveiliging en biometrie) zijn gezien bovenstaand niet noodzakelijk, wel dient (middels systeemauthenticatie) voor te worden dat het systeem gefalsificeerde data ontvangt.

3.3.2 Logging

Alle beheerhandelingen worden vastgelegd. Dit betekent alle geautomatiseerde en ook alle niet-geautomatiseerde handelingen.

3.3.3 PKI

De CI zal in eerste instantie optreden als CA voor het uitreiken van servercertificaten aan instellingen. De CI dient hiervoor een procedure in te richten conform de aansluitprocessen die beschreven zijn in het ontwerp beheerorganisatie.

Verder dient de beheerorganisatie een procedure op te stellen voor het intrekken van certificaten en het beschikbaar stellen van de lijst met ingetrokken certificaten (CRL) op basis van de gebruikelijke PKI standaarden.

De beheerorganisatie zal het servercertificaat van de CI voldoende beveiligen. Dit betekent ten minste:

- de identiteit van de aanvrager van een certificaat wordt via meer dan één kanaal gecontroleerd voordat een certificaat wordt verleend.
- de autorisatie van de aanvrager om het certificaat aan te vragen wordt gecontroleerd. De vraag die beantwoord dient te worden is, of de aanvrager gerechtigd is om namens de instelling het certificaat aan te vragen.
- het Root certificaat van de Centrale Infrastructuur, dat wordt gebruikt om certificaten af te geven wordt alleen opgeslagen op een computer dan wel andersoortig opslagmiddel dat afdoende fysiek beschermd is en die geen vaste verbinding met het Internet heeft.

3.3.4 Gescheiden systemen

Omdat het catalogus systeem continue met het internet verbonden is, dient dit systeem niet op dezelfde server te staan als de server die gebruikt wordt om de klinische Parelsnoer gegevens te bewaren. Dit ter bescherming van de klinische gegevens.

De server die het catalogussysteem huisvest mag vanwege dezelfde regels geen bevoorrechte toegang hebben tot de server waarop de klinische Parelsnoer gegevens staan. De gegevens van de catalogus moeten daarom vanuit de server met de brongegevens naar de catalogus server gestuurd worden en niet andersom. Om dezelfde reden is het vereist om de netwerken te scheiden tussen een beheersnetwerk (voor verkeer tussen de gegevens server en de catalogus server) en een publiek netwerk (voor de catalogus netwerk).

4 Informatie en functionaliteit

4.1 Functionaliteit

De CI biedt de functionaliteit zoals beschreven in ontwerp CI. Dit betekent dat de CI de volgende scenario's realiseert:

Scenario's voor de aanleverende instelling

3.4.1	Reguliere aanlevering dataset
3.4.2	Incidentele aanlevering dataset
3.4.3	Bekijken status van aanleveringen
3.4.4	Bekijken logbestand
3.4.5	Verwijderen van patiëntgegevens
3.4.6	De-pseudonimisatie

Scenario's voor de (externe) onderzoeker

3.5.1	Bekijken informatie over Parelsnoer en de parels
3.5.2	Opvragen statistische kentallen van een Parel
3.5.3	Opvragen datadictionary van een Parel
3.5.4	Indienen verzoek voor een dataset
3.5.5	Indienen verzoek voor biomateriaal
3.5.6	Indienen verzoek voor beeldmateriaal
3.5.7	De-pseudonimisatie

Scenario's voor de gegevensbeheerder CI

3.6.1	Verwerken ontvangen datasets in de centrale database
3.6.2	Beschikbaarstellen dataset
3.6.3	Afhandelen verzoek biomateriaal
3.6.4	Afhandelen verzoek beeldmateriaal
3.6.5	Afhandelen verzoek tot de-pseudonimisatie
3.6.6	Inzien log
3.6.7	Bekijken gearchiveerde verzoeken

Scenario's voor de beheerder CI

3.7.1	Operationeel beheer CI
3.7.2	Bijwerken datadictionary
3.7.3	Inzien log CI
3.7.4	Gebruikersbeheer instellingportal
3.7.5	Aansluiten instelling
3.7.6	Afsluiten instelling
3.7.7	Management rapportages
3.7.8	Bewaking aanlevering

4.2 Gegevensmodel

De CI conformeert zich aan de PIM. Daarnaast zal de CI extra benodigde tabellen realiseren voor haar beheertaak, zoals beschreven in hoofdstuk 5 in het ontwerp CI.

4.3 Koppelvlakken

De CI heeft de volgende koppelvlakken zoals beschreven in het ontwerp CI.

- Dataintake via FTP: dit koppelvlak wordt beschreven door de FTP standaard voor bestandsuitwisseling van de IETF en de PIM voor de bestandsstructuur.
- Dataintake via webservices: dit koppelvlak wordt beschreven door de SOAP standaard voor remote procedure calls van de W3C en de PIM voor de inhoud van de berichtstructuur.
- Catalogus via Internet: dit koppelvlak wordt beschreven door de HTTP/1.1 standaard voor webverkeer van de IETF/W3C en de (X)HTML standaard voor webpagina's van de W3C.
- Opgeleverde datasets: dit koppelvlak wordt beschreven door de PIM

4.4 Webrichtlijnen

De website met daarop algemene informatie over het Parelsnoer Initiatief en de catalog zal voldoen aan de gangbare eisen op het gebied van de toegankelijkheid van website door visueel gehandicapten.

De website voldoet aan de Webrichtlijnen van de overheid en het document van drempelvrij.nl. Dit houdt in dat zowel best-practices van de W3C op het gebied van content beheer als best-practices op het gebied van toegankelijkheid verplicht worden gesteld. In globale lijnen komt dit neer op:

- Gebruik alleen geldige HTML/XHTML pagina's die aan de definities voldoen.
- Gebruik alleen CSS voor layout van pagina's.
- Biedt altijd een gelijkwaardig alternatief aan indien JavaScripting gebruikt wordt.
- Gebruik HTML/XHTML elementen alleen waarvoor ze bedoelt zijn (dus geen tabellen voor lay-out van een pagina).
- Gebruik stabiele URL's,
- Toon de verschillen aan in websites met revisie markeringen.

Naast de webrichtlijnen, is het noodzakelijk dat website alleen gebruik maken van de voor Parelsnoer ontwikkelde huisstijl.

Documenten op de website worden of voor read-only gebruik aangeboden of tevens om bewerkt te worden. Documenten die niet bedoelt zijn om gewijzigd te worden, worden aangeleverd in PDF formaat. Documenten die wel bedoelt zijn om gewijzigd te worden, worden in Open Document Format (.odf) aangeleverd.

5 Techniek

5.1 Netwerkverbinding

De verbinding tussen een instelling en de CI verloopt over het publieke Internet. Deze verbinding wordt met SSL beveiligd.

5.2 Tweezijdige SSL

Voor de beveiligde verbinding is gekozen voor tweezijdige SSL. Hierbij wordt SSL 3.0 of TLS 1.0 toegepast. Zie ook 4.7 in het ontwerp CI. Hierbij dient zowel de CI als de instelling een certificaat te hebben. Een verbinding komt alleen tot stand als beide partijen elkaars certificaat accepteren. Deze acceptatie bestaat uit de volgende controles die beide partijen op het certificaat van de andere partij uitvoeren:

- het certificaat is onveranderd
- het certificaat is uitgegeven door een vertrouwde CA⁴ - in de beginfase is dit de Parelsnoer CI organisatie
- het certificaat is niet verlopen
- het certificaat is niet ingetrokken (staat niet op de lijst met ingetrokken certificaten: de Certificate Revocation List ofwel CRL⁵)

Dit zijn standaard controles binnen SSL en PKI en worden ondersteund door de gangbare SSL-software

Daarnaast zal de CI controleren of de instelling geautoriseerd is op basis van de identificatie van de instelling in het certificaat bij de verbinding wordt gebruikt. Een instelling dient hetzelfde te doen met de naam in het certificaat van de CI.

5.3 Koppelvlak datasets

Het ontvangen van een dataset wordt gefaciliteerd via zowel FTP als via SOAP/HTTP, zie ook 4.1.1 in het ontwerp CI. Beide protocollen worden gebruikt over een SSL-verbinding zoals beschreven in de vorige paragraaf.

Voor CI betekent dit dat zij een FTP-server moet gebruiken die in staat is om een tweezijdige SSL verbinding op te zetten.

Voor CI betekent dit dat zij gebruik moet maken van een HTTP-server die tweezijdige SSL ondersteunt. De meeste gangbare webbrowsers ondersteunen dit. Ook de standaard Java en .NET omgevingen bieden deze ondersteuning.

5.4 Koppelvlak beeldmateriaal

Op verzoek van de CI stelt een instelling beeldmateriaal beschikbaar. De precieze wijze waarop dit zal plaatsvinden zal nog nader worden bepaald.

5.5 Eisen aan beveiliging certificaten

De CI voorziet instellingen van een certificaat waarmee de instelling zich identificeert en authenticert voor het aanleveren van datasets (voor tweezijdige authenticatie). Een

⁴ CA staat voor certification authority. Dit is de dienstverlener die verantwoordelijk is voor de uitgifte van de certificaten

⁵ De CRL is een bestand dat gedownload kan worden bij de CA

instelling moet voorkomen dat deze (en dan met name de private key) door onbevoegden kan worden benaderd. Hiervoor kunnen reguliere beveiligingsmethoden worden toegepast (zie bijvoorbeeld de adviezen van NEN7510 voor informatiebeveiliging). De CI moet voorkomen dat het eigen certificaat (en dan met name de private key) en het Root certificaat (voor de verstrekking van certificaten aan instelling) door onbevoegden kan worden benaderd. Hiervoor kunnen reguliere beveiligingsmethoden worden toegepast (zie bijvoorbeeld de adviezen van NEN7510 voor informatiebeveiliging).