



Programma van Eisen voor de pseudonimisering van kwaliteitsregistraties door zorgaanbieders

**Voor een kwalitatief hoogwaardige standaardmethode van pseudonimiseren
en koppelen van (bijzondere) persoonsgegevens binnen de gezondheidszorg
in Nederland**

Inhoud

1	Introductie	4
1.1	Leeswijzer	4
2	Achtergrond toepassing, definitie en methode pseudonimisering.....	6
2.1	Achtergrond toepassing pseudonimisering	6
2.2	Wat wordt bedoeld met pseudonimisering?	6
2.3	Toelichting op de methode voor pseudonimisering	7
3	Opzet pseudonimisering en ICT-infrastructuur	9
3.1	Opzet van de openbare pseudonimiseringsdienst.....	9
3.1.1	<i>Pseudonimisering</i>	10
3.1.2	<i>Herleidbaarheid</i>	12
3.1.3	<i>Koppelbaarheid</i>	12
3.1.4	<i>Domeinconversie (her-pseudonimisering)</i>	13
3.1.5	<i>Sleutelconversie</i>	13
3.1.6	<i>Routeoverzicht</i>	14
3.2	ICT-infrastructuur rond de pseudonimiseringsdienst	14
3.2.1	<i>Webservice</i>	15
3.2.2	<i>Lokale service</i>	16
4	Interactie met de pseudonimiseringsdienst	19
4.1	Pseudonimisering via lokale service.....	19
4.1.1	<i>Bewerking in de aanleversoftware</i>	19
4.1.2	<i>(Cryptografische) bewerking in de centrale verwerking module</i>	22
4.1.3	<i>(Cryptografische) bewerking in afhaalsoftware</i>	23
4.1.4	<i>Gebruik van Hardware Security Modules in de centrale verwerkingsmodule</i>	24
4.2	Pseudonimisering via een API	25
4.2.1	<i>Gegevens leveren</i>	25
4.2.2	<i>Samenwerken</i>	26
4.2.3	<i>Beschikbaar stellen API functies</i>	26
4.2.4	<i>Identificatie en autorisatie</i>	26
4.2.5	<i>Pseudoniemen</i>	27
4.2.6	<i>Basis aanroep API</i>	28
4.2.7	<i>Decryptie aanroep API</i>	30
5	Bestandsformaten en inputvalidatie	30
5.1	Bestandsformaten	30

5.2	Omgang met en rapportage over fouten in aangeleverde bestanden	31
6	Gevraagde pseudonimisering dienstverlening	32
6.1	Kernfunctionaliteit van de pseudonimiseringsdienst.....	32
6.2	Conformiteit met de Algemene Verordening Gegevensbescherming	35
6.3	Beheer van de pseudonimiseringsdienst	36
6.4	Informatiebeveiliging van de pseudonimiseringsdienst	37
6.5	Dagelijkse ondersteuning van de pseudonimiseringsdienst	40
6.6	Incident management rond de pseudonimiseringsdienst	41
6.7	Rapportage over de pseudonimiseringsdienst.....	42
6.8	Request(s) for change	43
	Bijlage A: Referenties	44
	Bijlage B: Begrippenlijst.....	45
	Bijlage C: Richtlijnen rond pseudonimisering.....	47
	Bijlage D: specificatie van de VWS-pseudonimiseringsmethode.....	49
	Bijlage E: CSV dictionaire.....	50
	Bijlage F: XML-aanlevering	53
	Bijlage G: HL7-FHIR-aanlevering.....	56

1 Introductie

Dit document is primair bedoeld voor zorgaanbieders die op basis van dit Programma van Eisen een pseudonimiseringsdienst kunnen (laten) inrichten.

Na ingang van de gewijzigde Wkkgz zijn Zorgaanbieders verplicht data aan te leveren aan een in het register van Zorginstituut Nederland opgenomen kwaliteitsregistratie. Daarbij moeten zij voldoen aan (alle) eisen zoals gesteld in de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Deze wet vereist de toepassing van pseudonimisering als maatregel om de verwerkte persoonsgegevens passend te beschermen voor verzending vanuit de zorgaanbieder. Om te borgen dat de pseudonimisatie-oplossing van de zorgaanbieder voldoet aan de eisen zoals gesteld in de wet- en regelgeving en deze van hoogwaardige kwaliteit is, is een programma van eisen uitgewerkt. Ook beschrijft dit document waar het Programma van Eisen op voortborduurde en hoe dit aansluit bij pseudonimisatie voor andere doeleinden in de zorg.

Bij pseudonimisering worden direct identificerende persoonsgegevens in gegevensleveringen afkomstig van een organisatie (aanbieder) als input genomen voor het maken van één of meerdere pseudoniemen. Aanbieders die de te pseudonimiseren data aanleveren zijn in de context van kwaliteitsregistraties hoofdzakelijk zorgaanbieders. De belangrijkste afnemers in deze context zijn de registratiehouders. Dataverwerkers kunnen zowel namens aanbieders als afnemers werkzaamheden verrichten in de rol van verwerker.

Dit document beschrijft de technische eisen van de uit te voeren pseudonimisatie en de organisatorische eisen aan leveranciers van pseudonimiseringsdiensten. Zorgaanbieders kunnen op basis van dit Programma van Eisen pseudonimiseringsdienstverlening inkopen. Deze wordt doorgaans uitgevoerd door een externe dienstverlener in de rol van Trusted Third Party (TTP). Deze partij wordt in dit document 'Opdrachtnemer' genoemd.

De in dit document beschreven eisen voor de pseudonimiseringsdienst zijn gericht op de volgende partijen:

1. Zorgaanbieders, die verplicht zijn gegevens aan te leveren aan kwaliteitsregistraties.
2. Kwaliteitsregistraties, verwerkingsverantwoordelijke van de aangeleverde data volgens de definitie van de Wkkgz.
3. Dataverwerkers, die in opdracht van kwaliteitsregistraties of zorgaanbieders taken uitvoeren als verwerker van de data voor kwaliteitsdoeleinden.

1.1 Leeswijzer

Dit document is als volgt ingedeeld:

- Sectie 2 bevat achtergrondinformatie over de toepassing van pseudonimisering en gaat in op de definitie en methode.
- Sectie 3 beschrijft de pseudonimiseringsopzet en ICT-infrastructuur op hoofdlijnen.
- Sectie 4 beschrijft de interactie met de pseudonimiseringsdienst en bewerkingen binnen de pseudonimiseringsdienst; daarbij wordt gerefereerd naar cryptografische bewerkingen die in Bijlage D worden gespecificeerd.

- Sectie 5 beschrijft de input- en output-bestandsformaten die moeten worden ondersteund binnen de pseudonimiseringsdienst.
- Sectie 6 bevat de eisen die worden gesteld aan de pseudonimiseringsdienstverlening. Daarbij wordt voor specificaties en onderbouwing gerefereerd naar de overige secties uit dit document.

Dit document bevat de volgende bijlagen:

- Bijlage A bevat de referenties die in dit Programma van Eisen als acroniem tussen vierkante haken ([]) zijn opgenomen. Voorbeelden: [AES], [CSV] etc.
- Bijlage B: Begrippenlijst bevat een lijst met in dit document gebruikte begrippen.
- Bijlage C: Richtlijnen rond pseudonimisering bevat de vijf richtlijnen rond pseudonimisering van de Autoriteit Persoonsgegevens (destijds nog het College Bescherming Persoonsgegevens) uit 2007 waarmee conformiteit wordt geëist vanuit dit Programma van Eisen.
- Bijlage D: specificatie van de VWS-pseudonimiseringsmethode bevat de specificatie van de (openbare) cryptografische pseudonimiseringsmethode die binnen de pseudonimiseringsdienst dient te worden toegepast.
- Bijlage E: CSV dictionaire beschrijft een algemene CSV dictionaire ten behoeve van de pseudonimisering.
- Bijlage F: XML-aanlevering beschrijft de aanlevering van XML-bestanden.
- Bijlage G: HL7-FHIR-aanlevering beschrijft de HL7-FHIR XML Schema Definition (XSD) die voor aanleveringen wordt gehanteerd.

2 Achtergrond toepassing, definitie en methode pseudonimisering

2.1 Achtergrond toepassing pseudonimisering

Het toepassen van pseudonimisering is een onderdeel van de beveiliging van de verwerking van persoonsgegevens, helpt om de (informatie)beveiligingsrisico's voor de betrokkenen te verminderen en ondersteunt verwerkingsverantwoordelijken en dataverwerkers bij het nakomen van hun verplichtingen inzake gegevensbescherming.

De pseudonimisering dient te voldoen aan de norm NEN7524:2019 Medische informatica - Pseudonimisatiedienstverlening en de richtlijnen opgesteld door de Autoriteit Persoonsgegevens in 2007 (zie Bijlage C: Richtlijnen rond pseudonimisering). Vanuit dit programma van eisen wordt conformiteit met deze richtlijnen als beveiligingseis gesteld.

2.2 Wat wordt bedoeld met pseudonimisering?

Wanneer over pseudonimisering wordt gesproken in dit document, dan wordt dit gezien vanuit de context uit Bijlage 0. Bij *pseudonimisering* worden direct identificerende persoonsgegevens in gegevensleveringen afkomstig van een organisatie (aanbieder) vervangen door daarop gebaseerde pseudoniemen en daarna gewist. Het eindresultaat wordt vervolgens verstrekt aan een andere organisatie (afnemer, de registratiehouder). Bij de pseudonimisering vinden bepaalde cryptografische operaties met behulp van cryptografische sleutels plaats. De wijze waarop de cryptografische operaties worden toegepast, wordt de *pseudonimiseringsmethode* genoemd. Alleen als dezelfde methode én dezelfde sleutels worden gebruikt, worden direct identificerende persoonsgegevens in dezelfde pseudoniemen omgezet.

De pseudonimiseringsmethode en sleutels voorkomen dat het mogelijk is om uit het pseudoniem de direct identificerende persoonsgegevens te achterhalen waarop het pseudoniem gebaseerd is. Pseudonimisering vindt bijvoorbeeld plaats op de combinatie naam, geboortedatum, geslacht en voorletter in een bestand, waarna deze gegevens worden vervangen door het pseudoniem. Ook kan pseudonimisering plaatsvinden op de postcode en het huisnummer, waarna alles wordt gewist op de vier cijfers van de postcode na. In de context waarin dit document is opgesteld, zijn de gegenereerde pseudoniemen specifiek voor de afnemer (in dit geval de registratiehouder). Dit betekent dat het pseudoniem gebaseerd op één of meerdere kenmerken van dezelfde persoon bij elke afnemer anders is.

Pseudonimisering als zodanig volstaat niet om de herleidbaarheid binnen een dataset weg te nemen. Hiervoor zijn aanvullende maatregelen nodig om in samenhang met de pseudonimisering een passend beschermingsniveau te bieden tegen ongeoorloofde toegang, verrijking en verstrekking van de gegevens. Deze maatregelen worden in samenhang beschreven in de data privacy impact assessment (DPIA, ook wel gegevensbeschermingseffectbeoordeling) die voor iedere gegevensverzameling waarbinnen persoonsgegevens worden verwerkt dient te worden uitgevoerd.

Binnen de context van pseudonimisering is ook *her-pseudonimisering* op een veilige wijze mogelijk. Dit maakt hergebruik van data, met een wettelijke grondslag, mogelijk alsmede zorgt dit ervoor dat als registraties op termijn samengevoegd moeten worden dat dit technisch mogelijk is op een veilige wijze. Bij her-pseudonimisering wordt een reeds gepseudonimiseerd bestand voor afnemer A omgezet naar een gepseudonimiseerd bestand voor afnemer B. Als een bestand met persoonsgegevens eerst wordt gepseudonimiseerd voor afnemer A en dan wordt her-gepseudonimiseerd voor afnemer B, dan levert dat hetzelfde resultaat op als bestand rechtstreeks was gepseudonimiseerd voor afnemer B. Binnen deze context is het bestand gecontinueerd beveiligd aangaande (eventueel) herleidbare gegevens, die middels pseudonisatie beveiligd zijn. De pseudoniemen die bij afnemer A in het bestand zitten zijn anders dan de pseudoniemen die bij afnemer B in het bestand zitten. Een bijzondere vorm van *her-pseudonimisering* is *sleutelconversie*. Hierbij vallen de aanbieder en afnemer samen en worden de pseudoniemen van de aanbieder omgezet naar nieuwe sleutels zodat ook nieuwe pseudoniemen ontstaan. Her-pseudonimisering wordt ook wel *domeinconversie* genoemd. Ook hierin is voorzien in het Programma van Eisen.

2.3 Toelichting op de methode voor pseudonimisering

Dit Programma van Eisen borduurt voort op de eisen die door de overheid zijn gehanteerd bij het aanbesteden van de pseudonimisering voor andere doeleinden in de zorg waarbij data gepseudonimiseerd worden voor aanlevering, zoals het Diagnose Behandel Combinatie-Informatiesysteem (DIS) en risicoverevening. Zo zorgt het programma van eisen ervoor dat het al geschikt is en blijft voor landelijke informatiesystemen in de zorg en is het Programma van Eisen al zoveel mogelijk bekend bij de zorgaanbieders die ermee te maken krijgen.

Ook borduurt dit Programma van Eisen voort op de openbare methodebeschrijving van pseudonisatie die in 2014 in opdracht van VWS ontwikkeld is (zie Bijlage D). Deze methode is bruikbaar voor dienstverleners die optreden als een TTP voor het verlenen van pseudonimiseringsdiensten en die aantoonbaar willen voldoen aan de NEN 7524-eisen. Met behulp van deze openbare VWS-methode kunnen verschillende leveranciers middels één standaard werken, waarmee onder andere de eis van koppelbaarheid over zorglocaties heen op een veilig wijze ondersteund kan worden. Deze methode is gespecificeerd in Bijlage D.

Voor de grootschalige toepassing van benodigde pseudonimisering aangaande de data-aanleveringen van kwaliteitsregistraties is uit analyse gebleken dat op dit moment de doorontwikkelde openbare methode voor pseudonimisering het beste als standaardmethode kan gelden. Dit heeft als hoofdredenen dat dit een methode betreft die bij (bijna) alle zorgaanbieders al bekend is en gebruikt wordt voor andere data-aanleveringen met een verplicht karakter, deze methode schaalbaar is en deze methode implementeerbaar en praktisch werkbaar is binnen een relatief kort tijdsbestek.

Ten behoeve van het verwerken van persoonlijke gezondheidsdata voor secundair gebruik in het algemeen en kwaliteitsregistraties in het bijzonder is de openbare methodebeschrijving (zoals hierboven beschreven) in opdracht van de Data-governancecommissie (DGC) aangevuld met aanvullende wettelijke en functionele eisen (zie Bijlage C). Omdat de VWS-methode nog niet voorziet in omkeerbare pseudonimisering, die voor de vereisten van de Wkkgz in relatie tot kwaliteitsregistraties benodigd is, is deze modaliteit aanvullend beschreven in dit document.

Tevens is gecontroleerd of de eisen nog voldoen voor de huidige stand van zaken in technologie en of de dienst aansluit op of aan kan sluiten bij bestaande verwerkingen die bijvoorbeeld in het kader van beleid en onderzoek gedaan worden. Door het voortborduren op toepassingen waarvoor pseudonimisatie al gebruikt wordt en de controle of het programma van eisen ook bruikbaar is voor andere doeleinden in de zorg zou het voor zorgaanbieders mogelijk moeten zijn om één pseudonimisatieservice aan te kunnen schaffen voor de verschillende doeleinden, wat de administratieve lasten ten goede moet komen. Dit is echter geen vereiste, er kunnen verschillende pseudonimisatiediensten voor verschillende doeleinden aangeschaft en gebruikt worden door zorgaanbieders. Ook centrale inkoop is een optie om de uniformiteit te bevorderen en de belasting voor de afzonderlijke zorgaanbieders te zoveel mogelijk te beperken.

Ook is gekeken hoe naast de borging van de kwaliteit en veiligheid de beschreven methode zo goed als mogelijk aansluit op de landelijke en Europese ontwikkelingen. Met het oog op deze ontwikkelingen is een webservice gebaseerde aanleverwijze waarbij volgens HL7 FHIR gestructureerde data beschreven in dit Programma van Eisen. Daarmee is een toekomstbestendige decentrale aanlevering mogelijk die aansluit op de gespecificeerde openbare methode. De specificaties voor een (decentrale), batchgewijze aanleverservice staan beschreven in sectie 4.2.1. Deze is met name bedoeld voor organisaties die nog niet klaar zijn voor aanlevering via de webservice.

3 Opzet pseudonimisering en ICT-infrastructuur

3.1 Opzet van de openbare pseudonimiseringsdienst

De pseudonimiseringsdienst die in de eisen in sectie 6 gespecificeerd wordt en toegelicht is in sectie 2, kan worden toegepast voor grootschalige verwerkingen met persoonlijke gezondheidsinformatie afkomstig uit de registratie in de zorg en welzijnssector.

De pseudonimiseringsdienst onderscheid *aanbieders* van gegevens en *afnemers* van gegevens. De pseudonimiseringsdienst treedt daarbij op als een te vertrouwen derde partij oftewel TTP namens een opdrachtgever. De opdrachtgever kan zowel een aanbieder als een afnemer van gepseudonimiseerde gegevens zijn. In de praktijk komt contractering vanuit één of meerdere afnemers het meest voor. Op deze wijze kan worden gegarandeerd dat gegevens afkomstig van verschillende aanbieders met hetzelfde sleutel materiaal worden gepseudonimiseerd. Daarmee worden pseudoniemen bruikbaar om personen te volgen in de tijd en over verschillende aanbieders heen. Het vertrouwen in de TTP is gebaseerd op aantoonbare conformiteit met technische en organisatorische eisen met betrekking tot de wijze waarop de pseudonimisering wordt uitgevoerd. De primaire taak van de TTP is adequaat sleutelbeheer. Een *aanbieder* biedt de dienst gegevens aan voor *pseudonimisering* die vervolgens door de dienst worden omgezet naar één of meerdere pseudoniemen. De input kan zowel een bestand zijn als een andere datastructuur. Het outputbestand bevat altijd gepseudonimiseerde persoonsgegevens. Dat wil zeggen dat de direct identificerende gegevens (zoals naam, geboortedatum, geslacht en voorletter) zijn vervangen door een *pseudoniem*. Dit proces wordt een *pseudonimisering (operatie)* genoemd van het persoonsgegeven. Een pseudoniem kent daarbij een type corresponderende met het soort direct identificerende gegevens (bijvoorbeeld naam, geboortedatum, geslacht en voorletter) waarop het gebaseerd is en een *pseudoniemdomein*. Met een pseudoniemdomein kan worden gezorgd dat pseudoniemen van hetzelfde type en dezelfde persoon toch niet koppelbaar zijn. Praktisch gesproken correspondeert een pseudoniemdomein met een cryptografische sleutel waarmee de direct identificerende gegevens omgezet zijn naar een pseudoniem: verschillende sleutels geven verschillende domeinen. Concreet betekent dit dat voor een persoon met identificerend kenmerk A het pseudoniem A^{ABC} wordt aangemaakt voor domein ABC (met afnemer ABC) en dat voor dezelfde persoon voor kenmerk A pseudoniem A^{XYZ} wordt aangemaakt voor domein XYZ (met afnemer XYZ). Dezelfde persoon krijgt dus verschillende pseudoniemen op basis van hetzelfde kenmerk.

Aanbieders zijn in de context van Kwaliteitsregistraties hoofdzakelijk zorgaanbieders. De belangrijkste afnemers zijn de registratiehouders. Dataverwerkers kunnen zowel namens aanbieders als afnemers werkzaamheden verrichten in de rol van verwerker. Een *afnemer* is de natuurlijke persoon of organisatie die de output na pseudonimisering ontvangt. In deze context is dat in principe de registratiehouder of diens verwerker. Echter kan een *afnemer* ook *aanbieder* van gegevens zijn, en dus ook de zorgaanbieder betreffen. Veelal zal een afnemer maar één pseudoniemdomein gebruiken. Maar indien bijvoorbeeld meerdere kwaliteitsregistraties binnen één organisatie worden uitgevoerd kunnen voor elke registratie de gepseudonimiseerde gegevens in verschillende pseudoniemdomeinen worden ondergebracht.

Zowel de input voor als de output na pseudonimisering zijn gedetailleerd gespecificeerd in dit document. De specificaties vormen het uitgangspunt voor de door de pseudonimiseringsdienst uit te voeren bewerkingen.

3.1.1 Pseudonimisering

De kernactiviteit van de dienst is het pseudonimiseren van gegevens. Deze kernactiviteit kan ten behoeve van verschillende toepassingen worden uitgevoerd:

1. Het aanmaken van een pseudoniem op basis van persoonsgegevens. Pseudoniemen kunnen:
 - a. Tijdelijk of definitief zijn;
 - b. Omkeerbaar of onomkeerbaar zijn;
 De varianten worden in volgende sub-secties toegelicht.
2. Het vertalen van een pseudoniem van het ene domein naar een ander domein. Dit noemen we *her-pseudonimisering* of *domeinconversie*. Dit proces is met name aan de orde bij koppelingen tussen registraties in het kader van onderzoek.
3. Het omkeren van een pseudoniem. Dit kan alleen voor omkeerbare pseudoniemen. Omkering betekent dat de onderliggende identiteit middels ontsleuteling door de dienstverlener wordt onthuld.

De volgende typen pseudoniemen op basis van (combinaties van) direct identificerende gegevens dienen ondersteund te worden.¹

#	Variabelen die onderdeel uitmaken van het pseudoniem	Toelichting
1	Postcode, huisnummer, huisnummertoevoeging	<i>PHH</i> - Adresgegevens bestaande uit Postcode woonadres, Huisnummer woonadres en Huisnummertoevoeging woonadres.
2	Naam, geboortedatum, geslacht, voorletters	<i>NGGV</i> - Naamgegevens, bestaande uit de achternaam, voorletters, geslacht en geboortedatum.
3	Naam, geboortedatum, geslacht	<i>NGG</i> - Zie 2, Minder onderscheidend vermogen dan 2, maar wel een hogere koppelkans. Kan in combinatie met andere pseudoniemen gebruikt worden om te bepalen of met voldoende waarschijnlijkheid sprake is van overlap.
4	Lokaal patiëntnummer	<i>MRN</i> – <i>Lokaal uniek (bron)gegeven</i> . Geschikt voor zowel onomkeerbare als omkeerbare pseudonimisering. In het bijzonder geschikt voor omkeerbaar pseudonimiseren met het oog op communicatie tussen kwaliteitsregistratie en zorgaanbieder in het kader van follow-up en datakwaliteit.
5	BSN ²	<i>B</i> - Burger Service Nummer (BSN)

¹ Gebaseerd op de lijst in de handreiking Pseudonimisering voor gegevensaanlevering aan Kwaliteitsregistraties van het Shared Service Center Data Governance (SSC DG).

² Technisch verwerkbaar, maar op dit moment niet toegestaan voor Kwaliteitsregistraties

		Voor secundair gebruik is het niet toegestaan om het BSN te verwerken. In het obstakel verwijdertraject ³ is dit verbod als weg te nemen obstakel onderzocht. De overheid bereidt naar aanleiding van de uitkomsten aanpassing in wetgeving voor. Deze uitwerking zal naar verwachting ten minste nog 2 jaar vergen. De service dient voorbereid te zijn op het (in de toekomst) kunnen pseudonimiseren van het BSN.
6	BSN, geboortedatum ⁴	<i>BG</i> - Burger Service Nummer (BSN), een getal bestaande uit negen cijfers inclusief een controlegetal in combinatie met geboortedatum. In het obstakel verwijdertraject ⁵ is het verbod op het verwerken van het BSN als weg te nemen obstakel onderzocht. De overheid bereidt naar aanleiding van de uitkomsten aanpassing in wetgeving voor. Deze uitwerking zal naar verwachting ten minste nog 2 jaar vergen. De service dient voorbereid te zijn op het (in de toekomst) kunnen pseudonimiseren van het BSN.
7	Postcode, geboortedatum, geslacht	<i>PGG</i> - bestaand uit postcode (4 cijfers en 2 letters), geboortedatum en geslacht
8	Postcode (4), geboortedatum, geslacht	<i>P4GG</i> - bestand uit de 4-cijferige postcode, geboortedatum en geslacht.
9	Geboortedatum, geslacht	<i>GG</i> - Geboortedatum en geslacht.

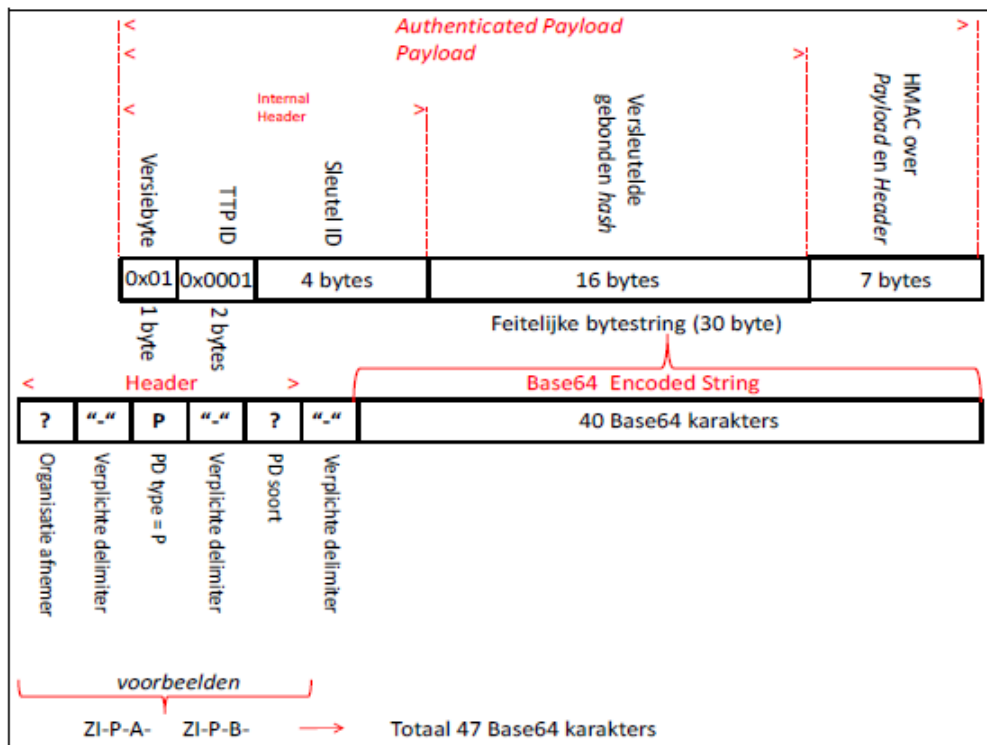
Tabel 1 Ondersteunde pseudoniemen

Een pseudoniem bevat naast een cryptogram (sleutel) ook gegevens over de afnemer en over het soort pseudoniem dat het betreft (metagegevens in een label). Daarnaast zal een pseudoniem ook enige technische gegevens bevatten zoals een versienummer en een referentie naar de gebruikte sleutels. Dit kan zoals in onderstaande figuur in schema worden weergegeven. Zie voor de toelichting bijlage D en [NEN].

³ https://www.health-ri.nl/sites/healthri/files/2023-03/Obstakel%20Verwijder%20Traject_Plannen%20van%20aanpak.pdf

⁴ Technisch verwerkbaar, maar op dit moment niet toegestaan voor kwaliteitsregistraties

⁵ https://www.health-ri.nl/sites/healthri/files/2023-03/Obstakel%20Verwijder%20Traject_Plannen%20van%20aanpak.pdf



Een pseudoniem dat volgens deze structuur is opgebouwd kan er in de praktijk als volgt uitzien: KRXX-P-C-A/PjAAAAAdSFz/jJscXx8KV08fvn367doiBkf/jlVw==

3.1.2 Herleidbaarheid

Binnen de specificaties van de input wordt onderscheid gemaakt tussen direct identificerende gegevens en zorgdata (ook wel payload data genoemd). Zoals de naam aangeeft maken direct identificerende gegevens directe identificatie van de betrokkene mogelijk. De indirecte herleidbaarheid van de overige gegevens wordt op basis van een door de registratiehouder uitgevoerde gegevensbeschermingseffectbeoordeling (ook wel data privacy impact assessment of DPIA genoemd) zo veel mogelijk beperkt. Daarmee kan de output na pseudonimisering voor verschillende domeinen een verschillende mate van herleidbaarheid kennen.

Het is daarom van belang om per verwerking gegevensspecificaties op te stellen waarin nauwkeurig aangegeven wordt óf en waar zich een direct identificerend gegeven in de set bevindt. Het is de taak van de Opdrachtnemer (TTP) om die dan te vervangen door een pseudoniem. Hier zullen we later in meer detail op terugkomen.

3.1.3 Koppelbaarheid

De kwaliteit van koppelingen op basis van pseudoniemen is afhankelijk van de uniciteit van de onderliggende persoonsgegevens. In Nederland is het Burgerservicenummer (BSN) het meest unieke persoonsgegeven. Op het verwerken van het BSN berust echter een verbod, met uitzondering voor bij wet genoemde toepassingen. Veel verwerkingen op het gebied van secundair gebruik van zorgdata vallen niet onder de wettelijke uitzonderingen. Daardoor moet gebruik gemaakt worden van andere identificerende gegevens (zie tabel 1). De koppeling is daarmee een waarschijnlijkheidskoppeling

(probabilistische koppeling) waarbij de koppelkans afhankelijk is van de uniciteit van de beschikbare identificerende gegevens.

3.1.4 *Domeinconversie (her-pseudonimisering)*

Pseudoniemen zijn afnemer specifiek, wat wil zeggen dat afnemer A zijn pseudoniemen cryptografisch niet kan relateren aan die van een andere afnemer (B). De basis hiervoor is dat de Opdrachtnemer voor elke afnemer eigen pseudonimiserings sleutels beheert. De Opdrachtnemer kan deze relatie wel leggen met behulp van deze pseudonimiserings sleutels. En dat is precies wat er gebeurt als een aanbieder A gepseudonimiseerde gegevens aanbiedt voor een afnemer B: de Opdrachtnemer converteert de pseudoniemen van partij A naar die van partij B. Het proces om een pseudoniem om te zetten naar een ander domein wordt een *domeinconversie* genoemd.

Binnen de pseudonimiseringsdienst wordt gesproken van *routes*: pseudonimisering routes waar de input bestanden persoonsgegevens zijn en conversie routes als de input bestanden gepseudonimiseerde bestanden zijn. Een route bestaat uit drie parameters:

1. een specifieke afnemer (en impliciet de cryptografische pseudonimisering sleutels),
2. een detailbeschrijving van de inputbestanden die worden verwacht,
3. een detailbeschrijving van de outputbestanden die worden gevormd.

Elke route heeft voor elk pseudoniemtype en afnemer unieke cryptografische sleutels. Binnen de cryptografische pseudonimisering methode zoals gespecificeerd in Bijlage D (VWS-methode) zijn dit per pseudoniem type twee sleutels, een van type AES en een van type HMAC. Ook binnen de pseudonimisering methode van de huidige Opdrachtnemer heeft elk route en pseudoniem type zijn eigen sleutel materiaal.

3.1.5 *Sleutelconversie*

Een bijzondere vorm van *her-pseudonimisering* is een *sleutelconversie*. Hierbij vallen de aanbieder en afnemer samen en worden de pseudoniemen van de aanbieder omgezet naar nieuwe sleutels zodat ook nieuwe pseudoniemen ontstaan. Directe redenen voor het uitvoeren van een sleutelconversie kunnen onder meer zijn dat de gebruikte pseudonimiserings sleutels zijn gecompromitteerd of dat gepseudonimiseerde bestanden en de bronbestanden waarop ze zijn gebaseerd, gecompromitteerd zijn. Bij een gecompromitteerd bestand kan het gaan om een geconstateerde kwetsbaarheid in het gebruikte cryptografische algoritme. Dan moet er overgestapt kunnen worden naar een algoritme dat op dat moment als veilig wordt beschouwd. Een gecompromitteerd bestand kan ook gaan om bestand waarbij tijdens de verwerking een fout opgetreden is waardoor in de output zowel het pseudoniem als de onderliggende input zou kunnen worden doorgegeven. Voor de veiligheid dient een bestand ook in dat geval omgezet te worden qua gebruikt cryptografisch algoritme. Een fout tijdens de verwerking kan komen door een fout in de software of een fout in de aangeboden input.

Een sleutelconversie kan ook worden uitgevoerd als extra beveiligingsmaatregel. Ook de verandering van Hardware Security Module (HSM) leverancier, kan een reden zijn om een sleutelconversie uit te voeren. Dit speelt met name als de HSM's niet toelaten dat de AES sleutels verplaatsbaar zijn van de HSM van de ene leverancier naar de HSM van de andere. Sleutelconversie betreft technische en organisatorische redenen voor het wisselen van de sleutels.

3.1.6 Routeoverzicht

Vanuit functionaliteit en *governance* is het voor de Opdrachtgever (zorgaanbieder) essentieel dat een geconsolideerd overzicht bestaat van alle pseudonimiseringsroutes die de pseudonimiseringsdienst ondersteunt vanuit de overeenkomst. Daartoe ontwikkelt en beheert de Opdrachtnemer voor de Opdrachtgever een routeoverzicht zoals in onderstaande Tabel 2 is aangegeven.

Zoals illustratief aangegeven, beschrijft de tabel voor elke route:

- de aanbieders van de inputinformatie,
- de inputspecificaties (of verwijzing hiernaar); dit omvat ook of de input zelf gepseudonimiseerd is,
- de (pseudonimisering) bewerkingen die plaats vinden op de input (of verwijzing hiernaar),
- de outputspecificaties (of verwijzing hiernaar),
- de afnemers van de outputinformatie,
- de partij onder wiens (AVG) verantwoordelijkheid de gegevensverwerking plaatsvindt.

Het doel van het routeoverzicht is dat de Opdrachtgever een compleet, gedetailleerd overzicht heeft van alle pseudonimiseringsroutes die door de pseudonimiseringsdienst worden beheerd of zijn beheerd. Het routeoverzicht moet zodanig gedetailleerd zijn dat deze de Opdrachtgever in staat stelt de pseudonimiseringsdienst bij een andere leverancier onder te brengen.

Korte naam	Aanbieder(s)	Input Specificaties	Bewerking Specificaties	Output Specificaties	Afnehmer	Verantwoordelijkheid
Ladis	GGZ instellingen	Vergelijk Bijlage I	Vergelijk Bijlage I	Vergelijk Bijlage I	Stichting IVZ	VWS
LBZ	Ziekenhuizen...	Stichting DHD	NFU/NVZ

Tabel 2: Routeoverzicht

3.2 ICT-infrastructuur rond de pseudonimiseringsdienst

De pseudonimiseringsdienst kan in twee manieren worden aangeroepen. Via een:

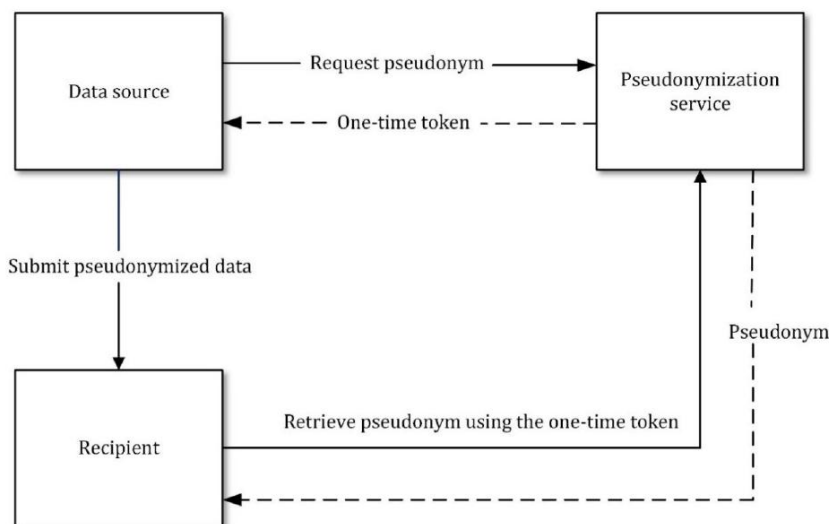
1. Webservice voor het aanvragen van of decrypteren van pseudoniemen.
2. Lokale service voor het aanleveren of afhalen van te pseudonimiseren én overige gegevens via de pseudonimiseringsdienst.

Deze manieren houden enerzijds rekening met de bestaande en beproefde werkwijze voor pseudonimiseren en anderzijds de landelijke visie en ontwikkelingen op het gebied van infrastructuren voor secundair gebruik van zorgdata.

In beide gevallen worden de gegevens in gestructureerde vorm en conform de daartoe opgestelde specificaties aangeboden aan de service (de pseudonimiseringsdienst). De specificaties van de te pseudonimiseren gegevens worden opgesteld door de kwaliteitsregistratiehouder. De zorgaanbieder maakt vervolgens zelf een keuze qua modaliteit en wijze van interactie (zie sectie 5) die passend is voor de eigen organisatie. De verschillende manieren worden hieronder verder toegelicht.

3.2.1 Webservice

Bij deze wijze van het aanroepen van de pseudonimiseringdienst vraagt de aanbieder van gegevens via een beveiligde Webservice pseudoniemen aan bij de pseudonimisatieservice van Opdrachtnemer. Als resultaat ontvangt de aanbieder pseudoniemen die zijn versleuteld voor de afnemer.



Figuur 1 Webservice voor pseudonimisering

De aanbieder voegt de versleutelde pseudoniemen toe aan de aan de afnemer (bijvoorbeeld een kwaliteitsregistratie) te versturen gegevens. De afnemer kan vervolgens de versleutelde pseudoniemen omwisselen voor definitieve pseudoniemen bij de pseudonimisatieservice van de Opdrachtnemer via een vergelijkbare aanroep van de pseudonimisatieservice. De tussenstap met tijdelijke pseudoniemen is nodig omdat je niet wilt dat er een gedeeld identificerend gegeven aanwezig is bij zowel de aanbieder (zorgaanbieder) als de afnemer (registratiehouder).

Figuur 1. Is afkomstig uit de NEN 7524. De term one-time uit dit type transactie wordt afwijkend ingevuld. Tijdelijk is niet gelijk aan eenmalig. De geldigheid van een tijdelijk pseudoniem is instelbaar. Binnen de toegestane tijd kan een tijdelijk pseudoniem meermaals worden aangeboden. Daarbuiten volgt een foutmelding. Deze keuze biedt ruimte voor heraanlevering van het tijdelijke pseudoniem binnen het ingestelde tijdsvenster.

In opzet voor dit model wordt uitgegaan van op basis van zorginformatiebouwstenen (zib's) gestructureerde data die in HL7 FHIR formaat wordt aangeboden aan de pseudonimisatieservice van Opdrachtnemer. De pseudoniemen worden ontleend aan het 'nl core patient' profiel⁶. Deze werkwijze sluit aan bij de landelijke afspraken op het gebied van het uitwisselen van zorginformatie.

Kenmerken van deze aanleverwijze:

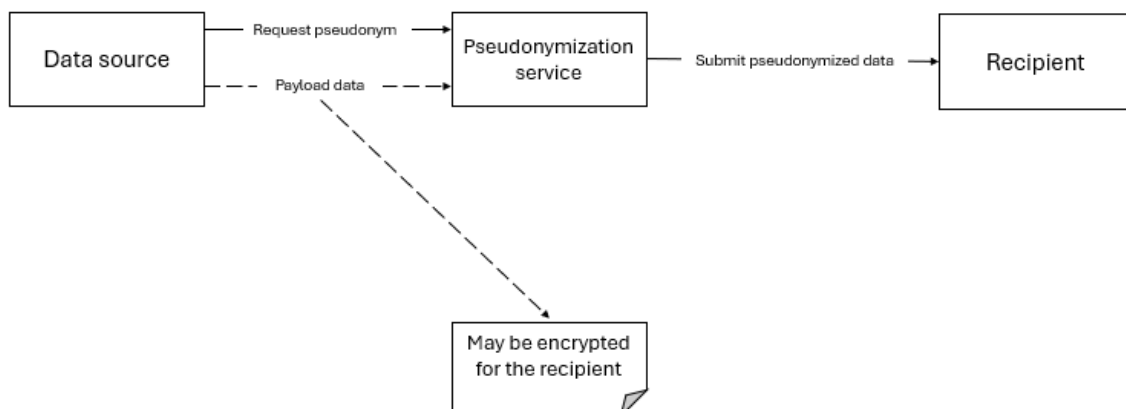
- De aanbieder stuurt (als bron) de te pseudonimiseren persoonsgegevens naar de pseudonimisatieservice (TTP);
- Daarbij maakt de aanbieder gebruik van een beveiligde internetverbinding (TLS);

⁶ <https://simplifier.net/nictiz-r4-zib2020/nlcorepatient>

- De pseudonimisatieservice (TTP) genereert de pseudoniemen en stuurt deze retour aan de aanbieder. De aanbieder beschikt daarmee over zogenaamde 'bronpseudoniemen'. De TTP blijft beheerder van de sleutels;
- De aanbieder levert deze bronpseudoniemen en de inhoudelijke gegevens via eigen kanalen aan (de dataverwerker van) de afnemer (de registratiehouder);
- De (dataverwerker van de) registratiehouder biedt middels een API-aanroep de pseudoniemen voor conversie aan bij de TTP. De TTP zet de bronpseudoniemen om naar koppelbare pseudoniemen. Koppelbare pseudoniemen zijn nodig voor koppeling van data betreffende één individu vanuit verschillende bronnen (verschillende zorgaanbieders, en/of verschillende type bronnen zoals een EPD of een landelijke registratie). Conversie slaat hier op omzetten van tijdelijk naar definitief. De eerder aangeboden tijdelijke pseudoniemen worden overschreven door de definitieve pseudoniemen. Definitieve pseudoniemen zijn uniek per registratiehouder maar kunnen wel gebruikt worden voor koppeling met andere registraties via een omzetting door de TTP waarbij de TTP pseudoniemen van hetzelfde type behorende bij de ene registratie kan vertalen naar pseudoniemen voor een andere registratie.
- De (dataverwerker van de) registratiehouder ontvangt de koppelpseudoniemen en gebruikt deze om de informatieproducten te maken;
- De bronpseudoniemen hebben - uit oogpunt van beveiliging - een beperkte houdbaarheid. Dat betekent dat de pseudoniemen na een instelbare periode niet meer te converteren en daarmee niet langer koppelbaar zijn. Het is dus van belang dat de pseudoniemen binnen de ingestelde periode na het aanmaken, worden geconverteerd naar lang te bewaren koppelpseudoniemen.

3.2.2 Lokale service

In dit model stelt de Opdrachtnemer een aanleverservice voor aanbieders en een afhaalservice voor afnemers beschikbaar. De Opdrachtnemer stelt hiervoor software beschikbaar, waarmee gegevens kunnen worden aangeleverd (aanbieders) of worden afgehaald (afnemers).

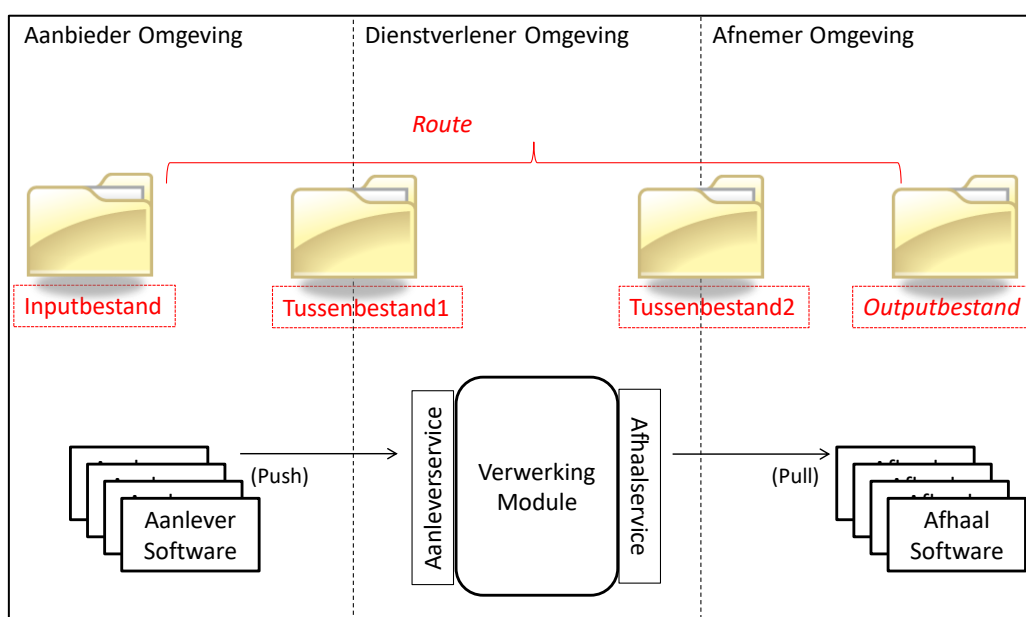


Figuur 2 Lokale service voor pseudonimisering

Aan de hand van het inputbestand bepaalt de aanleversoftware bij de aanbieder:

1. voor welke afnemer(s) het bestand bedoeld is,
2. hoe het bestand is opgebouwd, i.e., waar zich
 - eventuele identificerende gegevens (bijvoorbeeld Naam, Geboortedatum, Geslacht en Voorletter) of pseudoniemen bevinden, en
 - waar zich metadata bevinden.

Zoals het eerste vereiste suggereert moet de aanleversoftware in staat zijn om meerdere afnemers aan te geven. Veelal zal er sprake zijn van slechts één afnemer maar in voorkomende gevallen kunnen dat er meer zijn.



Figuur 1:

Bestanden binnen de pseudonimiseringsdienst

De aanleversoftware bij de aanbieder voert vervolgens bewerkingen uit op het inputbestand waaronder een cryptografische ('eerste encryptie') zoals vereist vanuit de eisen in Bijlage C. Zie ook Sectie 6. Het resultaat hiervan levert een tussenbestand op dat door de aanleversoftware wordt gestuurd naar de aanleverservice. Voor latere referentie geven wij dit tussenbestand voortaan aan met *Tussenbestand1*. De aanleverservice plaatst *Tussenbestand1* in een wachtrij van de centrale verwerkingsmodule die actief is tussen de aanleverservice en de afhaalservice. Deze centrale verwerking module (die wij ook wel simpelweg verwerking module zullen noemen) is feitelijk de kern van de Opdrachtnemer. De aanleversoftware bij de aanbieder voert vervolgens enige bewerkingen uit op het inputbestand waaronder een cryptografische ('eerste encryptie') zoals vereist vanuit de eisen in Bijlage C.

De verwerkingsmodule pakt Tussenbestand1 op en voert hier bewerkingen op uit waaronder een cryptografische ('tweede encryptie') zoals vereist vanuit de eisen in Bijlage C. Zie Sectie 6 en Bijlage C. Het resultaat hiervan levert een tussenbestand op dat door de verwerkingsmodule wordt gestuurd naar de afhaalservice voor afnemers. Voor latere referentie geven wij dit tussenbestand voortaan aan met *Tussenbestand2*. De beoogde afnemer wordt genotificeerd dat het tussenbestand voor hem klaar staat en start de afhaalsoftware op.

De afhaalsoftware bij de afnemer legt contact met de afhaalservice en haalt Tussenbestand2 op en voert hier (cryptografische) bewerkingen op uit (zie Sectie 6). Het resultaat hiervan levert het finale outputbestand op.

Daarnaast wordt door de pseudonimiseringsdienst een logboek geactualiseerd en beschikbaar gesteld aan Opdrachtgevers. Het logboek bevat een chronologisch overzicht van alle transacties die in het kader van de dienst zijn uitgevoerd.

Samenvattend onderkent de pseudonimiseringsdienst aldus een Inputbestand, Tussenbestand1, Tussenbestand2 en het Outputbestand zoals aangegeven in Figuur 1. Daarbij staan de specificaties van het input- en het outputbestand vast binnen de pseudonimiseringsdienst. De specificaties van de beide tussenbestanden liggen niet gedetailleerd vast hoewel de pseudonimisering richtlijnen in Bijlage D hier wel impliciet eisen aan stellen. Hierop wordt verder ingegaan in Sectie 5.

Inputbestanden voor de aanleversoftware zijn zo georganiseerd dat de aanleversoftware op basis van metagegevens gegevens betreffende individuen kan onderscheiden en verwerken. Zie Bijlagen E en F voor een beschrijving van de bestandsformaten in meer detail. Tussen de aanleverservice en de afhaalservice is een verwerkingsmodule actief.

Een organisatie die alleen gegevens aanlevert (zoals een zorgaanbieder) heeft alleen aanleversoftware, een partij die alleen gegevens afneemt heeft alleen de afhaalsoftware. Er zijn ook scenario's denkbaar waarbij één organisatie zowel aanlevert als afhaalt (zoals bij domeinconversie). Voor dat doel krijgt een organisatie zowel aanlever- als afhaal software indien gebruik wordt gemaakt van de lokale aanleverservice.

4 Interactie met de pseudonimiseringsdienst

Te pseudonimiseren data dienen te worden opgenomen in een gespecificeerd inputbestand. Het inputbestand wordt geüpload naar de pseudonimiseringsdienst. Na interactie met de dienst volgt er een output bestand met pseudoniemen als resultaat. Het aanbieden van het input bestand kan via een lokale service (sectie 4.1) of via een webservice (sectie 4.2) plaatsvinden. De interactie via de lokale service en de webservice wordt hierna in detail beschreven.

4.1 Pseudonimisering via lokale service

De pseudonimiseringsdienst zet een gespecificeerd inputbestand aangeboden door een aanbieder om in een gespecificeerd outputbestand voor de afnemer. Deze omzetting gebeurt in drie stappen uitgevoerd door de aanleversoftware, de verwerking module en de afhaal software en levert twee tussenbestanden op zoals eerder aangegeven in sectie .

Alle bestanden binnen de pseudonimiseringsdienst zijn gebouwd uit *regels*, ook wel records genoemd. Een regel in het inputbestand bij de aanbieder wordt omgezet in een regel in het uiteindelijke outputbestand bij de afnemer. Deze opzet zet zich daarom voort bij alle bestanden: het resultaat van een bewerking op een regel in een inputbestand is een regel in een vervolg bestand.

Zoals eerder aangegeven zijn de tussenbestanden niet vast gespecificeerd binnen de pseudonimiseringsdienst zodat de Opdrachtnemer hier vrijheid heeft deze in te vullen. Dat betekent dat de Opdrachtnemer niet verplicht is om de tussenbestanden ook letterlijk regelgewijs te representeren. De Opdrachtnemer kan ook een andere representatie wijze toepassen. Deze representatie moet in opzet altijd weer te herleiden zijn tot een regelgewijze representatie omdat anders het outputbestand bij de afnemer niet kan worden gevormd volgens de specificaties. Ook de beschrijving in dit document is regelgewijs georiënteerd.

In de volgende drie secties zullen wij de regelwijze bewerkingen bespreken die de aanleversoftware, de verwerking module en de afhaal software uitvoeren.

4.1.1 *Bewerking in de aanleversoftware*

Het startpunt van de lokale pseudonimiseringsdienst is een gebruiker bij een aanbieder die de aanleversoftware opstart en deze een inputbestand aanbiedt. Het inputbestand kan direct identificerende persoonsgegevens bevatten zoals Naam, Geboortedatum, Geslacht en Voorletter of kan reeds gepseudonimiseerd zijn. In het eerste geval is sprake van pseudonimisering en in het tweede geval is sprake van her-pseudonimisering, ook wel domeinconversie genoemd.

De aanleversoftware is geconfigureerd voor de routebeschrijving en beschikt behalve over het webadres (Uniform Resource Locator) van de aanleverservice ook over een digitaal certificaat (X.509) van de Opdrachtnemer. De aanleversoftware is bedoeld voor aanlevering van bestanden voor een of meer afnemers en de software beschikt over de X.509 certificaten van deze afnemers. Met deze certificaten is de aanleversoftware in staat om informatie te versleutelen zodanig dat alleen de eigenaar van de private sleutel behorende bij het certificaat deze kan ontsleutelen.

De aanleversoftware ondersteunt ook sleutelconversie (zie Sectie 0) waarbij de aanbieder en afnemer dezelfde organisatie zijn.

Verder beschikt de aanleversoftware over een private signeer sleutel en (bijpassend) X.509 certificaat waarmee de zorgaanbieder het eindresultaat van zijn bewerking, i.e. Tussenbestand1, digitaal kan ondertekenen.

Het in bezit zijn van een X.509 certificaat betreft een technische eis. Functioneel gaat het er vervolgens om dat certificaten worden gebruikt om berichten te ondertekenen en te versleutelen. Het gaat er daarbij om dat je wilt weten van wie een bericht afkomstig is en dat een bericht alleen door een ontvanger die over de bijpassende sleutel beschikt kan worden ontsleuteld.

De authenticiteit van het getekende Tussenbestand1 kan aldus worden gerealiseerd door de digitale handtekening op het Tussenbestand1. We merken op dat de handtekening pas kan worden geverifieerd als het *gehele* bestand is overgestuurd naar de Opdrachtnemer.

Omdat enkel een digitale handtekening voor authenticatie wordt gebruikt dient de Opdrachtnemer (TTP) aanvullende maatregelen te nemen om de volgende twee risico's te mitigeren:

1. het risico van Denial of Service (DOS) op de centrale verwerkingsmodule,
2. het risico van replay van aanleveringen.

Denial of Service is een aanval waarbij je de dienst zodanig overspoelt met vragen dat deze niet langer bereikbaar is. Replay van aanleveringen slaat op het herhalen van aanleveringen en daarmee kennis op te doen om de pseudonimisering te doorbreken. De aanbieder van de dienst moet maatregelen nemen om dit te voorkomen.

Beide risico's kunnen worden gemitigeerd met dubbelzijdige TLS maar er zijn ook andere mogelijkheden. Een Opdrachtnemer zou bijvoorbeeld de aanleveringen vanuit de aanbieders kunnen voorzien van een kort header bestand ("metafile") waarin een aantal karakteristieke elementen van de daadwerkelijke aanlevering zijn opgenomen, waaronder een unieke *identifiser* van de zending, een tijdstempel en een hash van de daadwerkelijke aanlevering. De metafile wordt dan getekend met het afnemer certificaat en als eerste opgestuurd naar de centrale verwerkingsmodule. Pas als de handtekening succesvol is geverifieerd en vastgesteld is dat er geen sprake is van een replay wordt de daadwerkelijke aanlevering geaccepteerd. Bij de vaststelling dat er geen sprake is van een replay wordt gebruik gemaakt van de unieke zender *identifiser*, het tijdstempel en de hash van de daadwerkelijke aanlevering.

Op basis van zijn configuratie en op basis van het inputbestand zelf, waaronder de bestandsnaam (zie Sectie 5.1), is de aanleversoftware in staat een specificatie van het inputbestand te bepalen.

Specifiek kan de aanleversoftware bepalen:

- voor welke afnemer het bestand bedoeld is,

Hoewel het technisch denkbaar is dat er zich binnen een bestand zowel identificerende gegevens als pseudoniemen bevinden, laten de huidige bestandspecificaties volgens dit programma van eisen dit niet toe. Zie Sectie 5.

De aanleversoftware opent het inputbestand en verwerkt deze regelgewijs. Het resultaat van de bewerking wordt opgeslagen in Tussenbestand1 dat regelgewijs wordt opgebouwd. Bewerkingen zijn afhankelijk van het record type. Behalve bewerkingen wordt ook input validatie uitgevoerd. Zie Secties 5 en 5.2. In onderstaande Tabel 3 staat beschreven welke bewerking wordt uitgevoerd door de aanleversoftware.

#	Type record en bewerking
0	<p>Bestandsnaam</p> <p>Er geldt een verplichte bestandsnaamconventie waarin zowel de domeinnaam als de ontvanger moet worden benoemd. Deze zijn van belang voor de correcte verwerking van het bestand.</p>
1	<p>Header (zie Sectie 1)</p> <p>Deze is verplicht aanwezig als eerste regel in het bestand en wordt ongewijzigd overgenomen in Tussenbestand1.</p> <p>Puntkomma (;) wordt als separator tussen de verschillende headers gebruikt. Het CSV-bestand dient rechthoekig van vorm te zijn en niet te rafelen.</p> <p>Eén of meerdere headers moeten verplicht voorkomen maar (andere) headers mogen leeg zijn. Er moeten voldoende cellen gevuld zijn voor het genereren van een (bepaald) pseudoniem, zie Bijlage E. De te volgen karakterset betreft UTF-8.UTF-8 (8-bit Unicode Transformation Format) is een manier om Unicode/ISO 10646-tekenen op te slaan als een stroom van bytes, een zogenaamde tekencodering.</p>
2	<p>Variabelen</p> <p>Er geldt een verplichte notatiewijze voor variabelen die input vormen voor pseudoniemen. Zo dient geboortedatum aan het format jjjmmdd te voldoen, zie Bijlage E.</p> <p>Voldoet een variabele niet aan het format dan kan het niet worden gebruikt als input voor een pseudoniem. Bij een onjuiste geboortedatum kunnen de pseudoniemen C, RGG, NGGV, GG, G, BG en NGG niet worden aangemaakt.</p>

Tabel 3: Bewerkingen door aanleversoftware

Tot slot maakt de aanleversoftware nogmaals gebruik van zijn private signeursleutel en X.509 certificaat en maakt een tweezijdig geauthentiseerde TLS verbinding met de aanleverservice. Zie [TLS]. Indien dit succesvol is, wordt het getekende Tussenbestand1 afgeleverd bij de aanleverservice. De aanleversoftware informeert de gebruiker over geconstateerde fouten in de vorm van een verwerkingsverslag (Zie Sectie 5.2) en of de aflevering is geslaagd. Als de aflevering niet is geslaagd maar de totstandkoming van het getekende Tussenbestand1 wel, dan biedt de aanleversoftware de gebruiker de mogelijkheid om het getekende Tussenbestand1 nogmaals aan te bieden zonder het gehele verwerking proces opnieuw te doorlopen. Als de aflevering wel is geslaagd dan wordt het getekende Tussenbestand1 binnen de afnemer installatie op definitieve wijze gewist bijvoorbeeld volgens [WIS]. [WIS] is een methode voor het wissen van data, zie de referentielijst is bijlage A.

Een geconsolideerde versie van het verwerkingsverslag wordt meegestuurd voor de afnemer en maakt deel uit van Tussenbestand 1. Het is versleuteld met de publieke sleutel van de afnemer. Zie Sectie 5.2.

4.1.2 (Cryptografische) bewerking in de centrale verwerking module

Het startpunt van de verwerking module is een binnengekomen bestand van het type Tussenbestand1 vanuit de aanleverservice. Het bestand wordt verwerkt door de verwerkingsmodule in lijn met Tabel 2. Specifiek kan de verwerking module bepalen voor welke afnemer het bestand bedoeld is.

De verwerkingsmodule beschikt over de X.509 certificaten van afnemers. Met dergelijke certificaten is de verwerkingsmodule in staat om informatie te versleutelen zodanig dat alleen de eigenaar van de private sleutel behorende bij het certificaat deze kan ontsleutelen. Een dergelijke versleuteling kan technisch op verschillende wijzen worden vormgegeven die we verder niet zullen specificeren.

Verder beschikt de verwerkingsmodule over een private signeer sleutel en bijpassend X.509 certificaat waarmee de verwerkingsmodule het eindresultaat van zijn bewerking, i.e. Tussenbestand1, digitaal kan ondertekenen.

De verwerkingsmodule start met het valideren van de digitale handtekening op het outputbestand. Indien deze validatie faalt, dan wordt dit geregistreerd en de verdere bewerking wordt afgebroken. Vervolgens treedt een exceptieproces door de beheerders van de dienst in werking. Dit proces voorziet in een analyse en het resultaat maakt deel uit van de maandelijkse rapportage (dit geeft informatie over het functioneren en de kwaliteit van de bestanden die aangedragen worden aan de verwerkingsmodule). Als deze validatie succesvol is dan voert de verwerkingsmodule regelgewijze bewerkingen uit resulterende in een nieuw outputbestand, Tussenbestand2. Vergelijk Figuur 1: Bestanden binnen de pseudonimiseringsdienst.

Net zoals de bewerkingen van de aanleversoftware zijn ook de bewerkingen van de verwerkingsmodule regelgewijs ingericht. In onderstaande Tabel 4 is per type regel in Tussenbestand1 aangegeven welke bewerking wordt uitgevoerd door de centrale module. De referenties in de eerste kolom verwijzen naar de eerste kolom in Tabel 3.

Zoals in onderstaande tabel is aangegeven dient de Opdrachtnemer de pseudonimiseringsmethode toe te passen zoals gespecificeerd in Bijlage D. Deze methode onderkent cryptografische sleutels van het type AES en van type HMAC. Daarbij is de Opdrachtnemer verplicht de cryptografische sleutels van het type AES te beheren in een zogenaamde Hardware Security Module (HSM).

#	Type regel en bewerking
0	<i>CSV-header (zie Bijlage E)</i> Deze is verplicht aanwezig in CSV bestanden als eerste regel
A.1	<i>Versleuteld geschoond datarecord en voorlopige pseudoniem(en)</i> <ul style="list-style-type: none"> ○ het versleutelde, geschoonde datarecord wordt letterlijk opgenomen als onderdeel van de beoogde outputregel in Tussenbestand2; ○ de versleutelde voorlopige pseudoniemen worden ontsleuteld met behulp van de private Opdrachtnemer sleutel; ○ de voorlopige pseudoniemen worden omgezet naar het pseudoniem in het domein van de beoogde afnemer. Dit is de 'tweede encryptie' impliciet aangegeven in de richtlijnen in Bijlage 0. Vergelijk ook Bijlage D waarin de specificatie is opgenomen die de Opdrachtnemer dient toe te passen;

	<ul style="list-style-type: none"> o de gegenereerde pseudoniemen worden versleuteld met de publieke sleutel van de beoogde afnemer en vervolgens opgenomen als onderdeel van de beoogde outputregel in Tussenbestand2; o de bewerking van de regel wordt afgesloten met het wegschrijven van de outputregel in Tussenbestand2. <p><i>De output regel bestaat aldus uit versleutelde versies van het geschoonde datarecord en een of meer pseudoniemen. Deze onderdelen zijn onderscheidbaar gecodeerd in de outputregel voor de afhaal software.</i></p>
B.2	<p><i>Versleuteld geschoond datarecord en eerder gegenereerde pseudoniemen</i></p> <ul style="list-style-type: none"> o het versleutelde, geschoond wordt letterlijk opgenomen als onderdeel van de beoogde outputregel in Tussenbestand2; o de versleutelde pseudoniemen worden ontsleuteld met behulp van de private Opdrachtnemer sleutel; o de pseudoniemen worden geconverteerd naar het pseudoniem in het domein van de beoogde afnemer. Dit is een variant op de 'tweede encryptie' impliciet aangegeven in de richtlijnen in Bijlage C. Vergelijk ook Bijlage D waarin de specificatie is opgenomen die de Opdrachtnemer dient toe te passen; o de gegenereerde pseudoniemen worden versleuteld met de publieke sleutel van de beoogde afnemer en vervolgens opgenomen als onderdeel van de beoogde outputregel in Tussenbestand2; o de bewerking van de regel wordt afgesloten met het wegschrijven van de outputregel in Tussenbestand2. <p><i>De output regel bestaat aldus uit versleutelde versies van het geschoonde datarecord en een of meer pseudoniemen. Deze onderdelen zijn onderscheidbaar gecodeerd in de outputregel voor de afhaal software.</i></p>

Tabel 4: Bewerkingen door verwerkingsmodule

Nadat alle records zijn verwerkt, wordt de ordening informatie van de regels gebaseerd op de oorspronkelijke records verwijderd. Dit gebeurt om te zorgen dat informatie over een eventuele ordening aangebracht door de aanbieder in de input niet beschikbaar komt bij de afnemer.

De wijze waarop de ordening informatie wordt verwijderd, zullen wij niet nader specificeren. Een eenvoudige manier om dit te realiseren is om alle records te ordenen, bijvoorbeeld lexicografisch. De verwijdering van de ordening mag ook plaatsvinden in de aanlever software.

Vervolgens wordt het opgebouwde Tussenbestand2 digitaal ondertekend door de verwerkingsmodule middels de aanwezige private signeer sleutel, waarbij de digitale handtekening wordt toegevoegd aan het bestand. Tot slot maakt de verwerkingsmodule het Tussenbestand2 beschikbaar vanuit de afhaalservice voor de beoogde afnemer en wordt deze genotificeerd over de beschikbaarheid.

4.1.3 (Cryptografische) bewerking in afhaalsoftware

Het startpunt is dat een afnemer wordt genotificeerd dat een bestand van type Tussenbestand2 beschikbaar is. De afnemer start daartoe de afhaal software op. Deze software is geconfigureerd voor de afnemer en beschikt over het webadres (Uniform Resource Locator) van de afhaalservice en over een X.509 certificaat van de Opdrachtnemer dan wel over een *root* certificaat om door de afhaalservice verstrekte X.509 certificaten op echtheid te valideren.

De afhaal software bouwt (verplicht) een TLS verbinding met de aanlevering service. Zie [TLS]. Indien dit succesvol is dan verkrijgt de afhaal software het beschikbare bestand van type Tussenbestand2.

De afhaal software start met het valideren van de digitale handtekening op het outputbestand. Indien deze validatie faalt, dan wordt dit geregistreerd en de verdere bewerking afgebroken. De afnemer zal dan contact moeten opnemen met de beheerders van de dienst. Als deze validatie succesvol is dan voert de verwerkingsmodule regelgewijze bewerkingen uit resulterende in het finale outputbestand.

Net zoals de bewerkingen van de aanleversoftware en van de verwerkingsmodule zijn ook de bewerkingen van de afhaal software regelgewijs ingericht. In onderstaande Tabel 5 is per type regel in Tussenbestand2 aangegeven welke bewerking wordt uitgevoerd door de afhaal software. Deze referenties in de eerste kolom verwijzen naar de eerste kolommen in Tabel 3 en Tabel 4.

#	Type regel en bewerking
0	<i>CSV-header (zie Sectie 4.1 en Bijlage E)</i> De eerste regel van ieder bestand bevat kolom labels (headers), beginnend met de kolom met daarin de pseudoniemen.
A.1	<i>Versleuteld geschoond datarecord en pseudoniemen</i> <ul style="list-style-type: none"> ○ met behulp van de private sleutel van de afnemer worden het geschoonde datarecord en de pseudoniemen ontsleuteld; ○ de bewerking van de regel wordt afgesloten met het wegschrijven van de outputregel in het finale outputbestand, conform de berichtspecificaties. Zie Sectie 5.1. <p><i>De output regel bestaat aldus uit het geschoonde datarecord en een of meer pseudoniemen.</i></p>

Tabel 5: Bewerkingen door de afhaal software

Nadat alle records zijn verwerkt meldt de afhaal software aan de afnemer dat het finale outputbestand beschikbaar is.

De afnemer krijgt ook beschikking over het geconsolideerde verwerkingsverslag. Zie Sectie 5.2.

4.1.4 Gebruik van Hardware Security Modules in de centrale verwerkingsmodule

De Opdrachtnemer dient de pseudonimisering methode toe te passen zoals gespecificeerd in Bijlage D. Deze methode onderkent cryptografische sleutels van het type AES en van type HMAC.

De AES en HMAC sleutels zijn eigendom van de Opdrachtgever. Na afronding van de overeenkomst moet de Opdrachtnemer alle gebruikte sleutels ter beschikking stellen aan de Opdrachtgever en/of aan een nieuwe pseudonimisering dienstverlener en eventuele kopieën wissen.

De Opdrachtnemer is verplicht de cryptografische sleutels van het type AES te beheren in een zogenaamde Hardware Security Module (HSM). In een HSM kunnen cryptografische sleutels beschermd worden gegenereerd, gebruikt en opgeslagen.

De AES sleutels mogen alleen als back-up exporteerbaar zijn uit de HSM onder de volgende drie condities:

1. in aanwezigheid van het management van de Opdrachtnemer en van Opdrachtgever, hetgeen technisch dient te worden afgedwongen,
2. in versleutelde vorm van hetzelfde cryptografische beveiligingsniveau als dat van de sleutel zelf
3. import van de AES sleutels mag alleen in een andere HSM plaatsvinden onder dezelfde beveiligingscondities en dit mag alleen kunnen in aanwezigheid van het management van de Opdrachtnemer en van Opdrachtgever; dit dient technisch te worden afgedwongen.

De HMAC sleutels mogen ook in de HSM worden verwerkt maar dat is niet verplicht. Deze HMAC sleutels mogen ook in een softwarematige keystore in de Centrale Verwerkingsmodule worden beheerd mits dit voldoende veilig gebeurt, i.e. in lijn met de opgelegde beveiligingsnormen. De HMAC sleutels moeten echter exporteerbaar zijn in plain text vanuit de omgeving van de Opdrachtnemer zodat deze kunnen worden overgedragen aan een nieuwe pseudonimisering dienstverlener.

Noot

Omdat binnen de pseudonimiseringsdienst hele grote aantallen pseudoniemen moeten worden geproduceerd, is het van belang dat de HSM een hoge *throughput* kan leveren. De vereiste pseudonimisering methode (Bijlage D) ondersteunt dit doordat deze gebruik maakt van de eenvoudigste 'mode of operation' van AES versleuteling namelijk AES-ECB. De pseudoniem input is 16 bytes die middels de AES sleutel wordt omgezet in versleutelde output van wederom 16 bytes. Deze versleutelde output wordt vervolgens voorzien van metadata en voorzien van een HMAC waarde. In een recht-toe-rechtaan implementatie zou men de pseudoniemen sequentieel vormen waarbij elke pseudoniem vorming een eigen HSM aanroep krijgt. Door de tijd die het kost om de HSM aan te roepen en het antwoord te krijgen, zal een dergelijke implementatie slechts een lage *throughput* leveren. Door echter pseudoniem input te bundelen en in 1 keer aan te bieden aan de HSM (in AES-ECB mode) verkrijgt men met de gebundelde output. Na ontbundeling daarvan (op delen in blokken van 16 bytes) verkrijgt men hetzelfde resultaat als bij de sequentiële aanroep. Bij de gebundelde opzet wordt op HSM roundtrip tijd bespaard en kan wel een hoge *throughput* bereikt worden. Dit effect wordt nog verstrekt door de HMAC waarde in de Centrale Verwerkingsmodule te berekenen in plaats van in de HSM. Indien op deze wijze bijvoorbeeld 5.000 pseudoniemen gebundeld worden verwerkt kan zo voldoende hoge *throughput* bereikt worden.

4.2 Pseudonimisering via een API

In deze sectie wordt interactie via de webservice API beschreven voor zowel aanbieders als afnemers van te pseudonimiseren gegevens.

4.2.1 Gegevens leveren

Voor de pseudonimisatie biedt Opdrachtnemer een API die geschikt is voor gebruik door zowel de aanbieder als de afnemer. De afnemer komt volgens onderstaande stappen in het bezit van gepseudonimiseerde gegevens

1. De aanbieder gebruikt de API en zet persoonsgegevens om in tijdelijke pseudoniemen
2. De aanbieder vervangt in de gegevens alle persoonsgegevens door de pseudoniemen
3. De aanbieder draagt de gepseudonimiseerde gegevens over aan de afnemer

4. De afnemer gebruikt de API om de tijdelijke pseudoniemen om te zetten naar definitieve pseudoniemen
5. De afnemer vervangt in de gegevens alle tijdelijke pseudoniemen door de definitieve pseudoniemen

De term tijdelijke pseudoniemen slaat op de one-time tokens uit figuur 1. Vluchtig pseudoniemen zijn slechts tijdelijk bruikbaar omdat ze zowel bij aanbieder als afnemer bekend worden in het proces om tot definitieve pseudoniemen te komen. Als ze geen tijdelijk karakter zouden hebben dan zou de pseudonimisering doorbroken kunnen worden en kan niet voldaan worden aan de eis om zodanig te pseudonimiseren dat de relatie tussen pseudoniem en oorspronkelijk gegeven slechts door tussenkomst van technische en organisatorische maatregelen gelegd kan worden. Afnemers moeten de tijdelijke pseudoniemen daarom niet permanent opslaan.

De API geeft steeds wisselende tijdelijke pseudoniemen af voor dezelfde persoonsgegevens. De levensduur van de tijdelijke pseudoniemen is instelbaar. Een aanbieder kan tijdelijke pseudoniemen bijvoorbeeld een dag lang gebruiken voor interacties met diverse afnemers.

Definitieve pseudoniemen zijn voor dezelfde persoonsgegevens steeds gelijk en maken volgen en koppelen van personen mogelijk. Afnemers kunnen tijdelijke pseudoniemen met de API omzetten naar definitieve pseudoniemen.

4.2.2 Samenwerken

Twee afnemers kunnen hun gepseudonimiseerde gegevens niet zonder meer koppelen. De definitieve pseudoniemen zijn gebonden aan een domein en voor dezelfde persoon bij de twee afnemers verschillend. Om samen te werken en de gegevens te koppelen moet een gezamenlijk domein worden gecreëerd. De voorwaarden daarvoor vallen buiten de beschrijving van dit document. Beide afnemers kunnen via de API hun definitieve pseudoniemen omzetten in tijdelijke pseudoniemen. De gegevens worden vervolgens aan de dataverwerker van het nieuwe gezamenlijke domein beschikbaar gesteld. Die dataverwerker gebruikt de API voor afnemers om definitieve pseudoniemen te krijgen in het gezamenlijke domein waarna de gegevens gekoppeld kunnen worden. Geen van de afnemers moeten de tijdelijke pseudoniemen langdurig opslaan.

4.2.3 Beschikbaar stellen API functies

De pseudonimisatie dienstverlener stelt de API beschikbaar op een aantal end points waarvoor URL's gegeven worden. Via verbinding met deze URL's wordt gebruik gemaakt van de functies in de API.

De functies in de API zijn gespecificeerd in [Open API versie 3](#). Gangbare tooling stelt de gebruiker in staat de API te ontdekken en ontsluiten via deze *machine readable* specificatie.

4.2.4 Identificatie en autorisatie

De API is slechts beperkt toegankelijk. De dienstverlener verleent gebruikers toegang op basis van een moderne Single Sign On voorziening met ondersteuning voor openbare standaarden op dit gebied. Voorbeelden zijn Bearer token, OAuth2.0, OpenID connect en SAML. Daarbij wordt steeds gecontroleerd of de gebruiker nog gerechtigd is. Hierbij:

- Wordt voor de API worden twee rollen onderscheiden: **afzender** en **afnemer**.
- Is het afzenders alleen toegestaan tijdelijke pseudoniemen te verkrijgen.
- Mogen afnemers tijdelijke pseudoniemen omzetten in definitieve en andersom. Dit wordt alleen toegestaan op de domeinen in beheer van die afnemer.

4.2.5 Pseudoniemen

De API wordt gebruikt om persoonsgegevens te pseudonimiseren. De onomkeerbare pseudoniemen die de API produceert voldoen aan de [openbare specificatie](#) voor onomkeerbare pseudonimisatie.

Voor omkeerbare pseudonimisatie wordt gebruik gemaakt van een methode vergelijkbaar met de openbare beschrijving van de [encryptieservice](#). De omkeerbare versleuteling moet voorzien in het volgende beoogde gebruik:

1. Versleutelen en ontsleutelen; een gebruiker kan informatie versleutelen (Encrypt) en deze vervolgens weer ontsleutelen (Decrypt).
2. Versleutelen namens een andere gebruiker; een gebruiker kan namens een andere gebruiker informatie ver- of ontsleutelen (On-behalf).
3. Rechten en rollen; gebruikers kunnen per registratie verschillende rollen en rechten hebben. Bijvoorbeeld wel het recht om de informatie van eigen patiënten te ver- en ontsleutelen, maar niet het recht om de informatie van een collega in te zien. Terwijl een collega wel van alle patiënten de informatie mag ontsleutelen.

4.2.6 Basis aanroep API

De request dient als volgt te worden opgebouwd:

```

1  {
2    "pseudonymTypes": [
3      "C",
4      "MRN"
5    ],
6    "records": [
7      {
8        "GD": "19721005",
9        "PC": "5121SC",
10       "G": "M",
11       "MRN": "BIN197210050001"
12     },
13     {
14       "GD": "19780613",
15       "PC": "4056GH",
16       "G": "M",
17       "MRN": "12927257"
18     }
19   ]
20 }

```

Waarbij middels de API de volgende typen pseudoniemen kunnen worden gemaakt:

variabele	Toelichting
pseudonymTypes	Selecteer de gewenste pseudoniemtypen. Kies uit: - PHH, NGGV, NGG, MRN, B, BG, PGG, P4GG, GG
Records	Een array van records, elk record bevat de te pseudonimiseren persoonsgegevens. Records mogen verschillen in welke soort persoonsgegevens erin opgenomen zijn
PHH	Postcode, huisnummer, huisnummertoevoeging. Nederlandse postcode. NL-4056GH (zonder landaanduiding wordt NL aangenomen) <i>1200JC</i> Huisnummer van een adres, cijfers <i>26</i> Eventuele toevoegingen achter een huisnummer <i>A</i> <i>1200JC 26 A</i>
NGGV	Naam, geboortedatum, geslacht, voorletter Geboortenaam, achternaam. Met of zonder tussenvoegsels <i>van Binsbergen</i> Geboortedatum; 13 juni 1978, Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. <i>V</i>

	Voorletter <i>W</i> <i>Van Binsbergen 19780613 V W</i>
NGG	Naam, geboortedatum, geslacht Geboortenaam, achternaam. Met of zonder tussenvoegsels <i>van Binsbergen</i> Geboortedatum; 13 juni 1978, <i>19780613</i> Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. <i>V</i> <i>Van Binsbergen 19780613 V</i>
MRN	Lokaal patiëntnummer, ook wel medisch registratienummer genoemd, unieke tekenreeks voor persoon, patiënt of client in het systeem van de aanbieder <i>EPC-43201</i>
B	Burgerservicenummer <i>11 proef en 9 cijferig</i>
BG	Burgerservicenummer, geboortedatum <i>11 proef en 9 cijferig</i> Geboortedatum; 13 juni 1978, <i>19780613</i> <i>000000000 19780613</i>
PGG	Postcode, geboortedatum, geslacht Nederlandse postcode. NL-4056GH (zonder landaanduiding wordt NL aangenomen) <i>1200JC</i> Geboortedatum; 13 juni 1978, <i>19780613</i> Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. <i>V</i> <i>1200JC 19780613 V</i>
P4GG	Postcode, geboortedatum, geslacht Nederlandse postcode. NL-4056 (zonder landaanduiding wordt NL aangenomen) <i>1200</i> Geboortedatum; 13 juni 1978, <i>19780613</i> Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. <i>V</i> <i>1200JC 19780613 V</i>
GG	Geboortedatum; 13 juni 1978, <i>19780613</i> Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders.

	V 19780613 V
G	Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. V
PC	Nederlandse postcode. NL-4056GH (zonder landaanduiding wordt NL aangenomen) 1200JC Als een postcode voor het land wordt ondersteund wordt de postcode gevalideerd volgens de nationale specificatie. Indien correct/plausibel dan gaat hij (onder vermelding van het land) mee in het pseudoniem.
NM	Geboortenaam, achternaam. Met of zonder tussenvoegsels van Binsbergen
VL	Voorletter W
HNR	Huisnummer van een adres, cijfers 26
GG	Geboortedatum; 13 juni 1978, Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. 19780613V
REF	Elk ander referentiegegeven, een niet lege string A8765-34.2

4.2.7 Decryptie aanroep API

Met decrypteren wordt bedoeld het ontsleutelen van een omkeerbaar pseudoniem. Om pseudoniemen te kunnen decrypteren wordt de URL aangeroepen voor een decryptie request. Daarbij wordt het volgende proces doorlopen:

1. De geëncrypteerde string wordt conform de specificatie voor decryptie aangeboden;
2. De applicatie bepaalt middels welk account gebruiker is ingelogd;
3. De applicatie bepaalt of het encryptieresultaat niet corrupt is door de signature van het encryptieresultaat te valideren. Indien het encryptieresultaat corrupt is, zal er een foutmelding geretourneerd worden naar de gebruiker en is decryptie niet mogelijk;
4. De applicatie bepaalt of de gebruiker mag decrypteren op basis van de gespecificeerde sleutel in het encryptieresultaat;
5. De applicatie zoekt de sleutel op waaraan gerefereerd wordt in het encryptieresultaat;
6. De applicatie decrypteert de geëncrypteerde string;
7. De gedecrypteerde waarde wordt geretourneerd naar gebruiker.

5 Bestandsformaten en inputvalidatie

5.1 Bestandformaten

De pseudonimiseringsdienst moet input kunnen verwerken in de volgende formats voor batch georiënteerde aanleveringen:

- CSV (zie Bijlage E: CSV dictionaire)
- XML (zie Bijlage F: XML-aanlevering)
- HL7-FHIR en Jason (zie Bijlage G: HL7-FHIR-aanlevering)

Communicatie met de webservice vindt plaats op basis van een op basis van OpenAPI v3.0 specificatie die door de dienstverlener wordt gepubliceerd. De feitelijke verantwoordelijkheid voor het beheer van de input en output specificaties ligt bij de Opdrachtgever.

5.2 Omgang met en rapportage over fouten in aangeleverde bestanden

De aanleversoftware voert slechts heel beperkte controles uit op de aangeleverde bestanden.

Gecontroleerd wordt of:

1. De bestandsnamen en -indelingen *structureel* in lijn zijn met de specificaties.
2. De gegevens structureel in lijn zijn met de specificaties (zoals postcode is opgebouwd conform format NNNNAA)
3. De gegevens inhoudelijk in lijn zijn met de specificaties (zoals postcode is een valide postcode)

Gegevens die niet zijn gespecificeerd door de registratiehouder (en/of de aanbieder) worden niet gecontroleerd op het eventueel bevatten van persoonsgegevens.

Resultaten van controles kunnen fataal of niet fataal zijn.

- Bij een fatale fout wordt de verwerking niet afgerond. Fatale fouten corresponderen met controles van type 1. De input is niet interpreteerbaar waardoor de verwerking wordt afgebroken.
- Bij niet fatale fouten wordt de verwerking verder uitgevoerd maar wordt een waarschuwing in een verwerkingsverslag opgenomen. Het verwerkingsverslag bevat de naam van het aangeboden bestand, tijdstip van verwerking, aantal verwerkte records, detailinformatie over validatiefouten en contactgegevens van de servicedesk.

Bij falende controles 2 of 3 wordt de gespecificeerde uitwis operatie wel uitgevoerd maar wordt geen voorlopig pseudoniem opgeleverd in Tussenbestand1. In het uiteindelijk gepseudonimiseerde bestand wordt een dummy pseudoniem opgeleverd dat altijd op dezelfde manier is opgebouwd en dat de afnemer waarschuwt bij de verwerking van het afgeleverde bestand. Vergelijk Sectie 4.3.2 in [NEN] die integraal is opgenomen in Bijlage D.

Het verwerkingsverslag wordt gepresenteerd aan en beschikbaar gesteld (en te bewaren) voor de gebruiker door de aanleveringssoftware na de verwerkingen. Het verwerkingsverslag bevat geen persoonsgegevens maar doet wel verslag van het type geconstateerde fout op en de regel waar deze is geconstateerd is. De gebruiker wordt in de gelegenheid gesteld het insturen van het Tussenbestand1 (zie Sectie 4.1.1) naar de pseudonimiseringsdienst af te breken op basis van dit verslag.

Een geconsolideerde versie van het verwerkingsverslag wordt ook meegezonden voor de afnemer. Dit is gelijk aan het verslag gepresenteerd aan de aanbieder met dit verschil dat dit detail informatie (regelnummers) verstrekt over validatiefouten.

6 Gevraagde pseudonimisering dienstverlening

De onderstaande opsomming beschrijft de eisen die worden gesteld aan de gevraagde pseudonimisering pseudonimiseringsdienstverlening. In enkele gevallen wordt een aanbieder van deze dienstverlening om een toelichting gevraagd. De eisen/vragen zijn opgedeeld in de volgende onderwerpen:

- Kernfunctionaliteit van de pseudonimiseringsdienst (Sectie 6.1)
- Conformiteit met de Algemene Verordening Gegevensbescherming (Sectie 6.2)
- Beheer van de pseudonimiseringsdienst (Sectie 6.3)
- Informatiebeveiliging van de pseudonimiseringsdienst (Sectie 6.4)
- Dagelijkse ondersteuning van de pseudonimiseringsdienst (Sectie 6.5)
- Incident management rond de pseudonimiseringsdienst (Sectie 6.6)
- Rapportage over de pseudonimiseringsdienst (Sectie 6.7)
- Request(s) for change (Sectie 6.8)

Bij sommige eisen wordt verwezen naar de detailbeschrijvingen in Secties 3, 4 en 5.

6.1 Kernfunctionaliteit van de pseudonimiseringsdienst

Waar in dit document wordt verwezen naar normen of standaarden wordt daarmee de actuele versie bedoeld; indien de norm/standaard wijzigt, dient de opdrachtnemer deze wijziging te volgen in zijn dienstverlening. Bijlage A: Referenties bevat een overzicht van normen en standaarden waarnaar in dit document verwezen wordt.

- Eis 1. De dienstverlening bevat een technische pseudonimiseringsdienst beschikbaar vanaf het internet waarmee gebruikers van de dienst pseudoniemen kunnen aanvragen of aanbieden conform de beschrijvingen in Sectie 3. De dienstverlening omvat behalve een webservice gebaseerde interface ook een interface voor het verwerken van gegevensbatches middels aanlever en afhaal software. Daarbij omvat de dienstverlening pseudonimisering, her-pseudonimisering (domeinconversie) en sleutelconversie (roteren van sleutels).*
- Eis 2. De dienst moet om kunnen gaan met de in dit document beschreven interfaces en vormen van input.*
- Eis 3. De dienstverlening omvat ook sleutelconversie zoals beschreven in Sectie 3.1.5. De aanbieder (=afnemer) kan daarbij aangeven in de aanleversoftware of er nieuwe sleutels moeten worden gegenereerd of dat naar een andere sleutelversie moet worden geconverteerd. Daarbij mag conversie naar (oude) sleutelversies niet meer mogelijk zijn.*
- Eis 4. De pseudonimiseringsdienst moet de pseudonimiseringsmethode toepassen zoals gespecificeerd in Bijlage D: specificatie van de VWS-pseudonimiseringsmethode.*
- Eis 5. De technische pseudonimiseringsdienst moet zijn ingericht conform de richtlijnen gespecificeerd in Bijlage C: Richtlijnen rond pseudonimisering.*

- Eis 6. *Het cryptografisch sleutelmateriaal dat gebruikt wordt voor de omzetting van persoonsgegevens is eigendom van de Opdrachtgever met dien verstande dat de Opdrachtnemer dit nooit in onversleutelde vorm mag overhandigen aan de Opdrachtgever zelf maar slechts op diens verzoek moet overhandigen aan een andere, door Opdrachtgever aangewezen, opdrachtnemer.*
- Eis 7. *De pseudonimiseringsdienst moet gebruik maken van Hardware Security Module (HSM's). Deze HSM's moeten gecertificeerd zijn conform Federal Information Processing Standards (FIPS) 140-2 Level 3 [FIPS140-2]. Noot: de certificatie is een kwaliteitsgarantie voor de HSM, de HSM's hoeven niet in "FIPS mode" geconfigureerd te worden.*
- Eis 8. *De pseudonimiseringsdienst waakt over de continuïteit van de gebruikte HSM's binnen de pseudonimiseringsdienst. Dit omvat het betrouwbaar maken van back-ups van de sleutels in de HSM's alsmede het testen van het terugzetten van de back-ups. Dit omvat ook het monitoren of de HSM's bij het einde van hun levensduur kunnen worden gemigreerd naar een nieuwe HSM. Deze laten toe dat de Opdrachtnemer een versleutelde back-up van de Advanced Encryption Standard (AES) sleutels uit de HSM maken die kunnen worden geïmporteerd in een HSM van een andere leverancier. Zie ook eis 6.1.*
- Eis 9. *De dienstverlening, waaronder de aanlever- en afhaal software moet in staat zijn (grote) bestanden te verwerken tot en met 500 miljoen regels.*
- Eis 10. *Na aflevering vanuit de aanleversoftware aan de verwerkingsmodule is de verwerkte data gegarandeerd binnen 8 uur beschikbaar voor de afhaal software. Hierbij wordt door de Opdrachtnemer ook rekening gehouden met de pieken.*
- Eis 11. *De pseudonimiseringsdienst (aanleverservice, verwerkingsmodule, afhaalservice zie Sectie 3) is 7 * 24 uur operationeel.*
- Eis 12. *De beschikbaarheid van de pseudonimiseringsdienst (aanlever service, verwerkingsmodule, afhaal service, zie Sectie 3) is minimaal 98% op jaarbasis. Hierbij wordt door de Opdrachtnemer ook rekening gehouden met de pieken.*
- Eis 13. *De dienstverlening omvat het betrouwbaar beschikbaar stellen van aanlever software aan aanbieders, al dan niet via de Opdrachtgever. Deze software moet het pseudonimiseringsproces faciliteren in lijn met de beschrijvingen in Secties 3, 4 en 5. Zie ook Eis 43 (validatie gebruik meest recente versie).*
- Eis 14. *De dienstverlening omvat het betrouwbaar beschikbaar stellen van afhaal software aan afnemers. Deze software moet het pseudonimiseringsproces faciliteren in lijn met de beschrijvingen in Secties 3, 4 en 5.*
- Eis 15. *De pseudonimiseringsdienst moet in staat zijn om bij het verwerken van batches met behulp van de aanleversoftware één inputbestand naar meerdere afnemers te versturen ('multi-destination'). Dit betekent dat de naamgeving van de inputbestanden bijvoorbeeld toelaat om hierin meerdere afnemers op te nemen. Daarnaast moet het ook mogelijk zijn om verschillende pseudonimisatie bewerkingen toe te laten passen op dezelfde identificerende gegevens binnen het inputbestand binnen de aanleversoftware en de centrale verwerkingsmodule voor verschillende afnemers. Het moet bijvoorbeeld mogelijk zijn dat op basis van gegevens als Naam, Adres en geboortedatum in het input bestand de ene afnemer een pseudoniem met de volledige geboortedatum ontvangt en de andere afnemer een pseudoniem met alleen het geboortjaar ontvangt.*

Eis 16. De pseudonimiseringsdienst moet de input- en outputbestand specificaties ondersteunen beschreven in Sectie 5. De Opdrachtnemer moet specificatie documentatie opstellen en onderhouden voor aanbieders en afnemers die hen gedetailleerd informeert over de te verwachten formaten van input- en output bestanden.

Noten:

- *dit betreft met name de opbouw van de bestandnamen, format en de invulling van de veld namen,*
- *deze eis heeft als doel dat de pseudonimiseringsdienst zonder aanvullende ontwikkeling (en kosten) alle input- en outputbestand specificaties moet ondersteunen zoals beschreven in Sectie 5. Er is slechts sprake van extra ontwikkeling als deze ondersteuning nader op maat moet worden gemaakt.*

Eis 17. De Opdrachtnemer ontwikkelt en onderhoudt een routeoverzicht zoals beschreven in Sectie 3.1.6 en zoals geïllustreerd in Tabel 2.

Eis 18. De aanleverservice moet de validaties uitvoeren op het inputbestand zoals beschreven in Sectie 5.2.

Eis 19. De aanleverservice moet een fatale fout geven (waarbij de verwerking wordt stopgezet) in de volgende gevallen:

- *de aanroep / bestandsnaam voldoet niet aan de afgesproken opbouw, dit omvat een controle tegen de afgesproken input specificaties,*
- *de opbouw van de aanroep / het bestand wijkt af van de afgesproken input specificaties; .*
- *er geen geldige tokens, (publieke) sleutels of certificaten beschikbaar zijn voor de voorziene bewerkingen;*
- *de input bevat zowel direct identificerende gegevens (woonadres, postcode, geboortedatum) als pseudoniemen (zie Sectie 3.2).*

Bovenstaande lijst zal interactief tussen de Opdrachtgever en de Opdrachtnemer verder worden gefinaliseerd als onderdeel van de totstandkoming van de dienst.

Eis 20. Het verwerkingsverslag (Sectie 5.2) wordt gepresenteerd aan en beschikbaar gesteld (en te bewaren) voor de gebruiker door de aanleverservice na de verwerkingen. Het verwerkingsverslag geeft meer visueel gewicht aan controle types 2 en 3 dan aan type 4 (zie Sectie 5.2).

Eis 21. Bij gebruik van de lokale aanleverservice wordt de gebruiker in de gelegenheid gesteld het insturen van het Tussenbestand¹ (zie Sectie 3.1) naar de pseudonimiseringsdienst af te breken op basis van het verwerkingsverslag.

Eis 22. Indien er sprake is van regel- of recordvolnummers (record-id), zoals bij domein-conversies, zal ergens binnen de pseudonimisering dienstverlening de regel ordening van het aangeboden bestand moeten worden verwijderd. De regel ordening kan worden verwijderd in de aanlever software of in de centrale verwerkingsmodule, waarbij de laatste plaats de voorkeur heeft. Vergelijk de discussie aan het einde van Sectie 4.1.1.

Eis 23. De aanleverservice biedt voor aanbieders en afnemers behalve een Graphical User Interface (GUI) ook een Command Line Interface (CLI). De CLI biedt dezelfde functionaliteit als de GUI maar is bedoeld voor de automatisering afdelingen om vanuit een script gegevens aan te leveren of op te halen.

- Eis 24. De pseudonimiseringsdienst moet aanbieders via email notificeren nadat de door hen aangeboden gegevens (Tussenbestand1, zie Sectie 4.1.1) zijn verwerkt door de Centrale Verwerkingsmodule. De notificatie bevat slechts een verwijzing naar de aanlevering en de door de aanleversoftware geproduceerde rapportage en of deze succesvol of niet. De notificatie bevat geen detail informatie en geen URL's waarop geklikt kan worden. Noot: de notificatie voorziet ook in een behoefte van aanbieders inzake interne en externe verantwoording.*
- Eis 25. De lokale aanleverservice moet afnemers notificeren als er output voor hen beschikbaar is. Na initiële notificatie via email volgt handmatige notificatie (opbellen) als er niet binnen 2 werkdagen gestart wordt met het ophalen van de deze bestanden. De email notificatie bevat geen detail informatie en geen URL's waarop geklikt kan worden.*
- Eis 26. De lokale aanleverservice moet na de verwerking een verslag beschikbaar stellen over de uitgevoerde verwerking op basis waarvan de gebruiker kan vaststellen in hoeverre de verwerking correct is uitgevoerd.*
- Eis 27. Als de verwerking door de lokale aanleverservice is geslaagd (realisatie Tussenbestand1, Sectie 4.1.1) maar door netwerk problemen de verzending niet, dan moet dienstverlening een mechanisme hebben om de te verzenden informatie nogmaals te sturen zonder dat de verwerking weer van voren af aan moet starten.*
- Eis 28. De beschikbaar gestelde software voor de lokale aanleverservice aan aanbieder en afnemers dient de volgende besturingssystemen te ondersteunen: Windows, Linux en OS X (Apple).*

6.2 Conformiteit met de Algemene Verordening Gegevensbescherming

Zoals blijkt uit Secties 3, 4 en 5 verwerkt de Opdrachtnemer zogenaamde *hashes* van persoonsgegevens. Deze *hashes* worden gezien als persoonsgegevens omdat deze persoonsgegevens middels een brute-force kunnen worden teruggehaald. Mede omdat de pseudonimiseringsdienst alleen voorziet in een kortdurende verwerking van persoonsgegevens, zal de Opdrachtnemer niet worden gevraagd te assisteren bij de inwilliging van de AVG eisen rond recht van inzage, correctie en verwijdering.

- Eis 29. De Opdrachtnemer bevestigt dat deze een Verwerker van persoonsgegevens is in de zin van de Algemene Verordening Gegevensbescherming (AVG) afkomstig van de aanbieders. De Opdrachtnemer zal de verplichtingen uit de AVG naleven voor zover van toepassing op hem als Verwerker, als bijlage bijgesloten bij het Beschrijvend document.*
- Eis 30. De Opdrachtnemer verplicht zich om passende technische en organisatorische maatregelen ten uitvoer te leggen zoals bedoeld in AVG Artikel 32 om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. De Opdrachtnemer verplicht zich er op toe te zien dat deze maatregelen een passend beveiligingsniveau garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen. Daarbij verplicht de Opdrachtnemer de principes van "minimale gegevensverwerking" (AVG Artikel 5) en "privacy by design" toe te passen (AVG artikel 25).*

Noot: deze principes zijn ook al toegepast in de beschrijving van de dienstverlening in Sectie 6.2.

- Eis 31. De Opdrachtnemer informeert Opdrachtgever over de inzet van eventuele sub-verwerkers binnen de dienstverlening voor en tijdens de totstandkoming van de overeenkomst en gedurende de looptijd van de overeenkomst. Verandering van een sub-verwerker is grond voor de heronderhandeling/ beëindiging van de overeenkomst. Alle eisen gesteld vanuit Opdrachtgever aan de Opdrachtnemer zijn integraal van toepassing op de sub-verwerker en dienen contractueel tussen de Opdrachtnemer en diens sub-verwerkers te zijn vastgelegd.*
- Eis 32. De Opdrachtnemer zal geen gegevens van de pseudonimiseringsdienst geleverd aan de Opdrachtgever buiten de Europese Economische Ruimte brengen zonder voorafgaande schriftelijke toestemming van de Opdrachtgever.*
- Eis 33. Wanneer de AVG wordt aangepast of opgevolgd door een andere wet of verordening gedurende de looptijd van de overeenkomst verplicht de Opdrachtnemer zich proactief mee te werken en rekening te houden met de consequenties die de aanpassingen op opvolging heeft voor de pseudonimiseringsdienstverlening.*
- Eis 34. De Opdrachtnemer zal proactief en in interactie met de Opdrachtgever rekening houden met de opinies van de European Data Protection Board (EDPB).*
- Eis 35. De Opdrachtnemer committeert zich aan toepassing van en conformiteit met de norm NEN 7524:2019 getiteld "Health Informatics-Pseudonymization services" voor zover deze niet strijdig is met de eisen in dit document.*

6.3 Beheer van de pseudonimiseringsdienst

- Eis 36. Aan de pseudonimiseringsdienstverlening moet een Service Level Agreement ten grondslag liggen die in lijn is met Information Technology Infrastructure Library (ITIL) V4.*
- Eis 37. De dienstverlening omvat aan- en afsluitprocessen voor nieuwe aanbieders en afnemers van de dienst alsmede voor nieuwe pseudonimisering en pseudoniem conversie routes. Deze processen zijn gedocumenteerd en voorzien in een formele accordering vanuit Opdrachtgever voor de aansluiting van nieuwe partijen en routes. Dit betekent aldus dat er voor elke pseudonimisering of pseudoniemconversie van een bestand van een aanbieder naar een afnemer een gedocumenteerde grondslag moet zijn inclusief een accordering vanuit de Opdrachtgever. De Opdrachtnemer dient hiervoor een efficiënt en effectief accordering proces in te regelen.*
- Noten:*
- er wordt voorzien dat er reguliere en niet-reguliere pseudonimiserings zijn. Voor de reguliere pseudonimiserings zal dan een eenmalig akkoord volstaan. Niet reguliere pseudonimiserings zullen vaak pseudoniem conversies betreffen.*
 - er zal een contactpersoon binnen de opdrachtgever beschikbaar zijn die gerechtigd is deze accorderingen te verlenen.*
- Eis 38. De aan- en afsluitprocessen van de dienstverlening voorzien in de betrouwbare registratie van email adressen van contactpersonen bij de aanbieders en afnemers, deze zijn immers essentieel bij zowel het aanlever- als afnameproces. Bij de aan- en afsluitprocessen van de dienstverlening moet hier zo goed mogelijk in worden voorzien.*

Eis 39. Binnen diens webdiensten maakt de Opdrachtnemer zelf gebruik van digitale certificaten afkomstig van een Certificate Service Provider die onderdeel uitmaken van de trustlists in de gangbare internet browsers. Hoewel dat niet de voorkeur heeft vanuit beveiliging mogen de drie digitale certificaten (versleuteling, TLS server, ondertekening) gecombineerd worden tot één. Noot: deze eis betreft dus niet de certificaten die worden gebruikt door de aanbieders en de afnemers.

Eis 40. De aan- en afsluitprocessen van de dienstverlening voorzien in het betrouwbaar verstrekken van digitale certificaten aan nieuwe aanbieders of ter vervanging. Indien de afnemer/aanbieder geen vertraging introduceert, moet dit proces binnen 5 werkdagen afgerond zijn. Tenzij de private sleutels van aanbieders afgegeven worden op een smartcard, moeten deze door de aanbieders zelf worden gegenereerd en niet beschikbaar zijn bij voor anderen. De certificaten hebben een maximale levensduur van 5 jaar.

Noot: een opzet die in beginsel volstaat, bestaat eruit dat de Opdrachtnemer een nieuwe afnemer op betrouwbare wijze voorziet van een activatiecode. De activatiecode wordt dan gebruikt vanuit de aanlever software om over een verbinding met de Opdrachtnemer on-the-fly een certificaat af te geven op basis van een publieke sleutel gegenereerd in de software. De verbinding is beveiligd met een TLS verbinding vanuit de Opdrachtnemer en geauthentiseerd met de activatiecode vanuit de (nieuwe) aanbieder.

Eis 41. Het management systeem op basis waarvan certificaten worden afgegeven aan afnemers moet gecertificeerd zijn door een audit organisatie die daarvoor geaccrediteerd is door een Europese accreditatie instelling tegen de Lightweight Certificate Policy (LCP) uit de norm ETSI TS 102 042 [ETSI] of equivalent.

Noot: een opzet die in beginsel volstaat, bestaat eruit dat de Opdrachtnemer een certificaat dienstverlener inzet die (nieuwe) afnemers op betrouwbare wijze voorziet van een activatiecode. De activatiecode wordt dan gebruikt vanuit de afhaal software om over een verbinding met de Opdrachtnemer on-the-fly een certificaat af te geven op basis van een publieke sleutel gegenereerd in de software. De verbinding is beveiligd met een TLS verbinding vanuit de Opdrachtnemer en geauthentiseerd met de activatiecode vanuit de (nieuwe) afnemer.

6.4 Informatiebeveiliging van de pseudonimiseringsdienst

Eis 42. De aanlever en afhaal software moet vrij van kwaadaardige code, e.g. virussen trojans, zijn en moet digitaal ondertekend zijn door de pseudonimiseringsdienst. De digitale handtekening moet door de gebruiker met standaard middelen aanwezig op zijn computer kunnen worden geverifieerd voor de installatie van de software. Noot: dit betekent dat het gebruikte handtekening certificaat deel uit maakt van de standaard trust ketens.

Eis 43. Geïnstalleerde aanlever en afhaal software moet bij opstarten valideren dat zij de van de meest recente versie zijn en als dit niet het geval is de gebruiker assisteren bij het verkrijgen daarvan.

Eis 44. De pseudonimiseringsdienst moet gebruik maken van enkelzijdige TLS (zie [TLS]) tussen de aanleversoftware en de aanleverservice. De opzet van de TLS opzet moet in lijn zijn met good practices zoals beschreven in [NCSC-TLS]. Daarbij moet de pseudonimiseringsdienst de volgende twee risico's mitigeren (cf. Sectie 4.1.1):

Eis 45. het risico van Denial of Service (DOS) op de aanleverservice

Eis 46. het risico van replay van aanleveringen.

Noot: het gebruik van tweezijdige TLS is een mogelijkheid om deze risico's te mitigeren, in Sectie 4.1.1 wordt een andere mogelijkheid op basis van enkelzijdige TLS genoemd.

Eis 47. De pseudonimiseringsdienst moet gebruik maken van tweezijdige TLS (zie [TLS]) tussen de afhaal software en de afhaalservice. De opzet van de TLS opzet moet in lijn zijn met good practices zoals beschreven in [NCSC-TLS].

Eis 48. De pseudonimiseringsdienst moet gebruik maken van cryptografische primitieven die zijn gestandaardiseerd door het National Institute of Standards and Technology (NIST). Zie <http://csrc.nist.gov>. De cryptografische primitieven moeten ook worden toegepast volgens deze standaarden. De veilige (random) generatie van cryptografische sleutels binnen de pseudonimiseringsdienst moet conform [NIST-KEY] zijn. Cryptografische sleutels binnen de pseudonimiseringsdienst moeten zo beheerd worden dat zij niet beschikbaar kunnen komen buiten de Opdrachtnemer. Zie ook eis 53-2 (beveiligingsregime back-ups pseudoniem sleutels).

Eis 49. De aanlever- en afhaal software moet de gebruiker de mogelijkheid geven om diens private sleutel te versleutelen met een wachtwoord; dit betekent dat de gebruiker bij elk gebruik van deze software eerst dit wachtwoord moet ingeven waarna de software over de private sleutel kan beschikken na een ontsleuteling. De versleuteling van de private sleutel moet conform [PKCS12] zijn of vergelijkbaar.

Eis 50. De pseudonimisering methode moet voldoen aan de specificaties in Bijlage D.

Eis 51. De cryptografische sleutels die worden gebruikt binnen de pseudonimiseringsdienst dienen cryptografisch random gegenereerd te zijn en beheerd te worden in lijn met [NIST].

De pseudonimisering pseudonimiseringsmethode gespecificeerd in Bijlage D die verplicht moet worden toegepast, onderkent cryptografische sleutels die de vertrouwelijkheid van gehashte persoonsgegevens (Geboortedatum, Geslacht, Naam, Voorletter en Postcode) beschermen en van cryptografische sleutels die de authenticiteit van de pseudoniemen beschermen.

Eis 52. Per combinatie van een afnemer en een pseudoniem type (bijvoorbeeld Naam, Geboortedatum, Geslacht, Voorletter) dient een unieke vertrouwelijke sleutel te worden gehanteerd. Eenzelfde vertrouwelijke sleutel mag dus niet worden gebruikt voor de generatie van Postcode-Geboortedatum-Geslacht pseudoniemen, ook niet bij dezelfde afnemer. Het heeft de voorkeur om ook unieke authenticiteit sleutels te hanteren voor elke combinatie en pseudoniem type. Minimaal wordt vereist dat authenticiteit sleutels niet worden gedeeld door de pseudonimiseringsdienst over afnemers, dit met name om de portabiliteit niet te bemoeilijken. Met andere woorden: verschillende afnemers hebben verschillende authenticiteit sleutels. Opgemerkt wordt dat bovenstaande sleutel eigenschappen efficiënt kunnen worden ingericht middels sleutel diversificatie technieken, cf. [KDF].

Eis 53. De pseudonimisering sleutels binnen de verwerkingsmodulen dienen zodanig beschermd te worden door de Opdrachtnemer dat deze alleen onder dual control (vier ogen principe) kunnen worden beheerd. In het bijzonder kunnen zij niet onder een single control worden geëxporteerd. Conform eis 7 moeten de AES sleutels worden beheerd in een HSM. De AES sleutels mogen alleen als back-up exporteerbaar zijn uit de HSM onder de volgende drie condities:

- 1. in aanwezigheid van het management van de Opdrachtnemer en van Opdrachtgever, hetgeen technisch dient te worden afgedwongen,*

2. *in versleutelde vorm van hetzelfde cryptografische beveiligingsniveau als dat van de sleutel zelf*
3. *import van de AES sleutels mag alleen in een andere HSM plaatsvinden en dit mag alleen kunnen in aanwezigheid van het management van de Opdrachtnemer en van Opdrachtgever; dit dient technisch te worden afgedwongen.*

- Eis 54. Om de beschikbaarheid en continuïteit van de pseudonimiseringsdienst te garanderen, dienen de pseudonimisering sleutels binnen de verwerking geback-up't te zijn onder een beveiligingsregime dat vergelijkbaar is met die in de productieomgeving op een andere fysieke locatie op minimaal 15 kilometer afstand.*
- Eis 55. Opdrachtnemer wist op verzoek van de Opdrachtgever de pseudonimisering sleutels (en alle kopieën, e.g. in back-up, daarvan), met name na de overgang naar een andere Opdrachtnemer. Die termijn waarbinnen verwijdering moet plaatsvinden ligt vast in de dienstverleningsovereenkomst.*
- Eis 56. Bij de ontwikkeling van de software (aanlever- en afleversoftware en de centrale software) en het onderhoud wordt rekening gehouden met informatiebeveiliging conform de eisen uit hoofdstuk 8 uit de norm ISO 27001:2022. Opdrachtnemer toont jaarlijks schriftelijk aan Opdrachtgever aan dat zij voldoet aan deze norm, en dat zij "in control is" van haar informatiebeveiligingsrisico's.*
- Eis 57. De Opdrachtnemer ziet erop toe dat beschikbare security patches worden toegepast op de aanlever- en afleversoftware en de centrale infrastructuur. Voor kritische⁷ patches binnen een termijn van 4 weken nadat deze security patches beschikbaar komen. De Opdrachtnemer informeert aanbieders en afnemers over het beschikbaar komen van gepatchte software.*
- Eis 58. De Opdrachtnemer meldt informatiebeveiligingsincidenten aan de Opdrachtgever, conform de procedure zoals opgenomen in de Verwerkersovereenkomst. Onder een informatiebeveiligingsincident wordt verstaan een "inbreuk in verband met persoonsgegevens" in de zin van Artikel 4 van de AVG of elke gebeurtenis of een serie gebeurtenissen die een risico vormen of hebben gevormd voor de informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid van informatie) van de pseudonimisering dienstverlening.*
- Eis 59. De dienstverlening dient af te dwingen dat alleen die pseudonimiserings, pseudoniem domeinconversies en sleutelconversies kunnen plaatsvinden waarvoor een formele accordering bestaat vanuit de Opdrachtgever.*
- Eis 60. De Opdrachtnemer dient te beschikken over een werkend management systeem conform de ISO 27001 norm waarmee het management van de Opdrachtnemer de beveiligingsrisico's rond de geleverde dienst aantoonbaar onder controle heeft. Onafhankelijk van de risico inschatting van de Opdrachtnemer dient de BBN2 maatregelen gespecificeerd in de 2017 versie van de Baseline Informatiebeveiliging Overheid (BIO) te hebben geïmplementeerd en op te nemen in de Statement of Applicability vereist vanuit de ISO 27001 norm. Zie [BIO-2020]. De implementatie van het management systeem dient gecertificeerd te zijn door een audit organisatie die daarvoor geaccrediteerd is door een Europese accreditatie instelling.*
-

- Eis 61. Opdrachtgever heeft het recht, voor eigen kosten, een register EDP-auditor een controle te laten doen van de naleving door Opdrachtnemer van de eisen gesteld in dit Programma van Eisen. Opdrachtnemer verplicht zich hieraan zijn medewerking te verlenen. Opdrachtgever verplicht zich de controle te laten uitvoeren in overeenstemming met de gedrags- en beroepsregels van de beroepsorganisatie van register EDP-auditors NOREA. Opdrachtnemer is gerechtigd te verlangen dat de register EDP-auditor een geheimhoudingsverklaring tekent ten gunste van Opdrachtnemer (waarvan Opdrachtnemer een exemplaar krijgt). De geheimhoudingsverklaring dient die voorwaarden te bevatten die gebruikelijk zijn voor dit soort verklaringen. Het tijd periode waarop een controle zal plaatsvinden wordt in onderling overleg bepaald. Opdrachtgever zal erop toezien dat controles de bedrijfsvoering van Opdrachtnemer zo min mogelijk verhinderen.*
- Eis 62. De Opdrachtnemer dient software en een procedure te hebben voor de migratie van pseudonimisering sleutels naar een andere pseudonimisering sleutels (sleutelconversie) in geval van compromittering, van een geplande vervanging daarvan of in het geval van HSM continuïteit problemen (vergelijk eis 8 **Fout! Verwijzingsbron niet gevonden.**). Deze procedure dient getest te zijn. Zie ook Sectie 4.*
- Eis 63. De Opdrachtnemer meldt beveiligingszwakheden en-tekortkomingen in de pseudonimisering methode in Bijlage D aan Opdrachtnemer zodra deze hier van op de hoogte is.*
- Eis 64. De Opdrachtnemer dient een procedure te hebben voor de migratie naar een andere pseudonimisering methode, bijvoorbeeld in het geval dat zich beveiligingszwakheden voordoen in de pseudonimisering methode in Bijlage D.*

6.5 Dagelijkse ondersteuning van de pseudonimiseringsdienst

Dagelijkse ondersteuning betreft het beantwoorden van vragen van gebruikers omtrent de functionaliteit van de pseudonimiseringsdienst en het gebruik van de beschikbare software. Gebruikers zijn in dit geval werknemers van de aanbieder of afnemende organisatie.

- Eis 65. De Opdrachtnemer beschikt over een Nederlandstalige service desk die telefonisch en via email bereikbaar is en aan de volgende eisen voldoet:*

Onderwerp	Beschikbaarheid	Norm
Vragen over functionaliteit en ondersteuning bij het gebruik daarvan.	08:30 – 17:00 uur op werkdagen.	95% bereikbaarheid Indien niet direct te beantwoorden geldt een reactietijd en van twee werkdagen
Vragen over functionaliteit en ondersteuning bij het gebruik daarvan.	Buiten openingstijden	Uiterlijk de volgende werkdag contact. Daarna treedt de norm voor meldingen tijdens werkdagen in werking.

- Eis 66. De (eerste lijn) service desk voor de pseudonimiseringsdienst bestaat uit een vaste groep van mensen met kennis en ervaring rond de pseudonimisering dienstverlening. Daarbij beschikt de Opdrachtnemer over een vaste accountmanager richting de Opdrachtgever.*

6.6 Incident management rond de pseudonimiseringsdienst

Er is sprake van een incident als een gebruiker van de pseudonimiseringsdienst geen (volledig) gebruik kan maken van de onderscheiden functionaliteiten. Incidenten worden door de gebruikers gemeld aan de eerstelijns ondersteuning van Opdrachtnemer maar kunnen ook door de Opdrachtnemer zelf worden geconstateerd.

Eis 67. De telefonische aanmelding van incidenten moet aan de volgende eisen voldoen:

Onderwerp	Beschikbaarheid	Norm
Melding incident	08:30 – 17:00 uur op werkdagen.	95% bereikbaarheid voor aannames melding.
Melding incident	Buiten openingstijden	Uiterlijk de volgende werkdag contact.

De Opdrachtgever gaat uit van een onderscheid tussen incidenten. Dit onderscheid wordt hieronder gegeven:

Onderwerp	Omschrijving
Prioriteit 1 Storingsmelding	Die incidenten waarbij de technische pseudonimiseringsdienst in het geheel niet meer functioneert of waardoor de functionaliteit zodanig is afgenomen dat dit als zodanig wordt ervaren. Een <i>workaround</i> is niet mogelijk.
Prioriteit 2 Storingsmelding	Die incidenten waarbij de technische pseudonimiseringsdienst gedeeltelijk niet meer functioneert maar waarbij het bij de overgebleven functionaliteit toch redelijk mogelijk blijft om te kunnen functioneren. Een <i>workaround</i> is mogelijk. Problemen die zo spoedig mogelijk opgelost dienen te worden. De applicatie werkt, echter deze problemen hebben tot gevolg dat gebruikers minder efficiënt kunnen werken.

Als er meerdere incidenten tegelijk in behandeling zijn wordt hiervan de prioriteit vastgesteld. De prioriteit is afhankelijk van de urgentie en de impact. Indien dit voorkomt neemt de ondersteunende afdeling contact op met de Opdrachtgever. De Opdrachtgever stelt de prioriteit van de individuele incidenten vast.

Eis 68. De Opdrachtnemer houdt een rapportage bij van alle geconstateerde/gemelde incidenten, hun prioriteit en de afhandeling daarvan.

Voor de afhandeling van incidenten gaat de Opdrachtgever uit van de volgende betekenis van Reactietijd en Hersteltijd.

Term	Betekenis
Reactietijd	Tijd die verstrijkt vanaf de eerste melding/constatering van het incident tot het moment waarop de Opdrachtnemer reageert met een melding over de aard van de storing en de te nemen maatregelen.

Hersteltijd	Tijd die verstrijkt vanaf de eerste melding/constatering van het incident tot het moment waarop een geconstateerd en gemeld probleem is opgelost.
-------------	---

De afhandeling van incidenten moet aan de volgende eisen voldoen:

Onderwerp	Norm
Melding/constatering incident, prioriteit niveau 1	Reactietijd: Tijdens kantooruren twee uur. Buiten lokale kantooruren uiterlijk de eerste twee kantooruren van de volgende werkdag.
	Hersteltijd: Uiterlijk één werkdag met een norm van 90%
Melding/constatering incident prioriteit niveau 2	Reactietijd: Tijdens kantooruren dezelfde werkdag. Buiten lokale kantooruren uiterlijk de volgende werkdag.
	Hersteltijd: Uiterlijk twee werkdagen met een norm van 90%

6.7 Rapportage over de pseudonimiseringsdienst

- Eis 69. De lokale pseudonimisatiesoftware) stelt verwerkingsverslagen ter beschikking aan de gebruiker in lijn met Sectie 5.2.*
- Eis 70. Maandelijks rapporteert de Opdrachtnemer aan de Opdrachtgever over de uitgevoerde pseudonimiseringen over de voorgaande maand waaronder:*
- Eis 71. Aantallen succesvol verwerkte pseudoniemen en bestanden, verdeeld in het type verwerking (pseudonimisering, domeinconversie) dat heeft plaatsgevonden. Zowel totaal als onderverdeeld per bestemming;*
- Eis 72. Aantallen niet succesvol verwerkte bestanden en aanbieder en afnemers daarvan en een summiere oorzaak analyse daarvan*
- Eis 73. Overzicht van alle prioriteit 1 en 2 incidenten waaronder de reactietijd en hersteltijd (toelichting indien langlopend)*
- Eis 74. Excepties in de verwerkingen en analyses daarvan (zie Sectie 4.1.2)*
- Eis 75. Beveiligingsincidenten.*
- Eis 76. Beschikbaarheid van het pseudonimisatieplatform*
- Eis 77. Jaarlijks, op nader af te stemmen moment in het jaar, rapporteert de Opdrachtnemer aan de Opdrachtgever over de uitgevoerde pseudonimiseringen over het afgelopen jaar waaronder:*
- Eis 78. Aantallen succesvol verwerkte pseudoniemen en bestanden, verdeeld in het type verwerking (pseudonimisering, domeinconversie) dat heeft plaatsgevonden. Zowel totaal als onderverdeeld per bestemming;*
- Eis 79. Aantallen niet succesvol verwerkte bestanden en aanbieder en afnemers daarvan en een summiere oorzaak analyse daarvan;*
- Eis 80. Overzicht van alle prioriteit 1 en 2 incidenten waaronder de reactietijd en hersteltijd;*

- Eis 81. Beveiligingsincidenten;*
- Eis 82. Beschikbaarheid van het pseudonimisatieplatform;*
- Eis 83. Een lijst met actieve geautoriseerde gebruikers van de dienst binnen de dienstverlening, zowel totaal als onderverdeeld per bestemming;*
- Eis 84. Analyse en evaluatie van de dienstverlening over het voorafgaande jaar.*
- Eis 85. Naar aanleiding van de jaarlijkse rapportage aan de Opdrachtgever belegt de Opdrachtnemer een vergadering om deze rapportage te bespreken. Bij deze vergadering kan de dienstverlening ook plannen voor het komende jaar voorstellen.*

6.8 Request(s) for change

- Eis 86. Als beantwoording van een wijzigingsverzoek vanuit de Opdrachtgever verstrekt de Opdrachtnemer een inzichtelijke opgave van de kosten en inspanning die daarmee verbonden zijn. Noot: het betreft hier functionele wijzigingen aan de pseudoniseringssoftware.*
- Eis 87. De Opdrachtnemer beschikt over een standaard opzet voor de beantwoording van wijzigingsverzoeken die inzichtelijkheid van kosten, inspanning en impact nastreeft. De kosten, inspanning en impact betreffen zowel die van de Opdrachtnemer zelf als van de betrokken partijen (aanbieders, afnemers, Opdrachtgever).*
- Eis 88. De dienst moet zodanig schaalbaar zijn dat gebruikers snel kunnen worden aangesloten en afgesloten. Daarnaast moet de software om kunnen gaan met data elementen die niet van belang zijn voor de pseudonimisering. Met andere woorden; de software mag geen onnodige impact op de datalogistiek hebben.*
- Eis 89. De opdrachtgever beschikt over een gescheiden ontwikkel-, test- en acceptatieomgeving om wijzigingen aan de dienstverlening op gecontroleerde wijze door te voeren en richting productie te brengen.*

De Opdrachtnemer beschikt over een procedure om de Opdrachtgever (en namens hem aanbieders of afnemers) wijzigingen in de aanleversoftware, centrale verwerkingsmodule of afhaalsoftware te laten testen en te accepteren in de vooraleer deze worden toegepast in bedrijfsomstandigheden.

- Eis 90. De Opdrachtnemer informeert betrokken partijen over de doorvoer van wijzigingen in de centrale verwerkingsmodule, één week voorafgaand daaraan.*

Bijlage A: Referenties

#	Document
[AES]	Specification for the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, 26 November, 2001. Zie http://csrc.nist.gov/publications/PubsSPs.html .
[BIO-2020]	Baseline Informatiebeveiliging Overheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2020.
[CSV]	URI Fragment Identifiers for the text/csv Media Type, Request for Comments 4180, January 2014. Zie https://tools.ietf.org/html/rfc7111 .
[ETSI]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI, TS 102 042 V2.4.1 (2013-02).
[FIPS140-2]	Security requirements for cryptographic modules, FIPS PUB 140-2, May 25, 2001.
[NEN]	Voorstel voor cryptografische specificatie pseudonimisering aan het Nederlands Normalisatie Instituut (NEN), Eric Verheul (namens het Ministerie van Volksgezondheid, Welzijn en Sport), 26 september 2014. Dit voorstel is integraal opgenomen als Bijlage D.
[NIST-KEY]	Recommendation for Key Management – Part 1: General (Revision 5), NIST Special Publication 800-57, National Institute of Standards and Technology, May 202. Zie https://csrc.nist.gov/publications/sp800 .
[NCSC-TLS]	ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS), NCSC, 19 januari 2021. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
[PKCS12]	PKCS #12: Personal Information Exchange Syntax v1.1, Internet Engineering Task Force (IETF), Request for Comments 7292. Zie https://tools.ietf.org/ .
[TLS]	The Transport Layer Security (TLS) Protocol Version 1.3, Request for Comments 8446, August 2018. Zie https://tools.ietf.org/html/rfc8446 .
[WIS]	G.F. Hughes, D.M. Commins, and T. Coughlin, Disposal of disk and tape data by secure sanitization, IEEE Security and Privacy, Vol. 7, No. 4, (July/August 2009), pp. 29-34.

Bijlage B: Begrippenlijst

In onderstaande tabel zijn de belangrijkste begrippen opgetekend die worden gebruikt in dit document en is aangegeven waar zij zijn geïntroduceerd.

Begrip	Waar gebruikt	Definitie
Aanbieder	Sectie 0	Zorgaanbieder, die de data aanlevert.
Aanlever Software	Sectie 3.2	Software van de pseudonimiseringsdienst waarin de te encrypteren informatie aangeleverd moet worden door de aanbieder.
Afhaal Software	Sectie 3.2	Software van de pseudonimiseringsdienst waarin de geëncrypteerde data in opgehaald kan worden door de afnemer.
Afnemer	Sectie 0	Kwaliteitsregistratie, die de data ontvangt.
Centrale Verwerkingsmodule	Sectie 3.2	De software van de pseudonimiseringsdienst waarin de encryptering plaatsvindt.
Cryptografische operaties	Sectie 2.2	Het versleutelingsproces, die herhaalbaar is.
Cryptografische sleutel	Sectie 3.1	Met een cryptografische sleutel worden de direct identificerende gegevens omgezet naar een pseudoniem, de sleutel wordt beheerd door de TTP.
CSV bestand	Bijlage E: CSV dictionaire	Type bestandsformat.
Conversie (operatie)	Sectie 3.1	Het proces om een pseudoniem om te zetten naar een ander domein wordt een conversie operatie genoemd.
Datarecord	Sectie 5.1	Een cel in een databestand.
Domein	Sectie 3.1	Technische specificaties van de afnemer.
Domeinconversie	Sectie 3.1	Het proces om een pseudoniem om te zetten naar een ander domein wordt een <i>domeinconversie (operatie)</i> genoemd
Gebruiker	Eis 26	Natuurlijke persoon die de aanleverservice bedient.
Hardware Security Module (HSM)	Sectie 4.1.4	In een Hardware Security Module (HSM) kunnen cryptografische sleutels beschermd worden gegenereerd, gebruikt en opgeslagen.
Inputbestand	Sectie 3.2 E en F	Het bestand wat door de (zorg)aanbieder wordt aangedragen voor pseudonimisering.
Meta gegevens	Sectie 3.1	Aanvullende gegevens die karakteristieken van (de gegevens in) een bestand omschrijven.
Operatie	Sectie 3.1	Dit proces wordt een <i>pseudonimisering (operatie)</i> genoemd van het persoonsgegevens.
Opdrachtgever	Sectie 3.1	Juridische entiteit die de contractuele relatie aangaat met de opdrachtnemer voor de pseudonimiseringsdienst
Opdrachtnemer	Sectie 0	In deze context de pseudonimiseringsdienst (TTP)

Outputbestand	Sectie 3.2	Het bestand wat beschikbaar wordt gesteld voor de afnemer.
Payload data	Sectie 3.1	De zorgdata, zijnde niet de data die persoonsgegevens bevatten.
Pseudoniem	Sectie 3.1	Versleuteld persoonsgegeven.
Pseudonimisering (operatie)	Sectie 3.1	Het proces waarin identificerende gegevens omgezet worden naar een pseudoniem.
Sleutelconversie	Sectie 0	Hierbij worden de pseudoniemen van de aanbieder omgezet naar nieuwe sleutels zodat ook nieuwe pseudoniemen ontstaan. Dit wordt typisch gedaan als een sleutel niet langer als veilig wordt beschouwd.
Tussenbestand	Sectie 3.2	De pseudonimiseringsdienst zet een gespecificeerd inputbestand aangeboden door een aanbieder om in een gespecificeerd outputbestand voor de afnemer. Deze omzetting gebeurt in drie stappen uitgevoerd door de aanleversoftware, de verwerking module en de afhaal software en levert twee tussenbestanden op
X.509 certificaten		De verwerkingsmodule beschikt over de X.509 certificaten van afnemers. Met dergelijke certificaten is de verwerkingsmodule in staat om informatie te versleutelen zodanig dat alleen de eigenaar van de private sleutel behorende bij het certificaat deze kan ontsleutelen.

Bijlage C: Richtlijnen rond pseudonimisering

Deze bijlage bevat een aanvulling op de methodebeschrijving zoals beschreven in bijlage D. Deze beschrijving is (ook) in opdracht van het ministerie van VWS opgesteld ten behoeve van de aanbesteding van gegevensverwerkingen voor de Risicoverevening en het DBC-informatiesysteem.

De pseudonimisering houdt rekening met de richtlijnen opgesteld door het College Bescherming Persoonsgegevens in 2007⁸. Deze richtlijnen hadden een officiële status in Nederland, tot de introductie van de Algemene verordening gegevensbescherming (AVG) in 2016. Deze status omvatte dat bij toepassing van deze richtlijnen er geen sprake was van de verwerking van persoonsgegevens. Vanuit deze aanbesteding wordt conformiteit met deze richtlijnen als eis gesteld, zonder dat sprake is van de oorspronkelijke status. Met name bij criterium c. in onderstaande tabel met voorwaarden moet rekening houdend met de huidige stand der techniek gelezen worden als het zo veel mogelijk beperken van de indirecte herleidbaarheid.

"Bij toepassing van pseudonimisering moet aan de volgende voorwaarden worden voldaan:

- Er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens
- Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ("replay back") te voorkomen;
- De verwerkte gegevens zijn niet indirect identificerend;
- In een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden a, b en c is voldaan;
- De pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt."

Met betrekking tot pseudonimisering voor kwaliteitsregistraties zijn de aanvullende eisen opgenomen in het wijzigingsvoorstel voor de Wet kwaliteit, klachten en geschillen in de zorg dat momenteel in behandeling is. Het gaat om de volgende eisen:

1. De registratiehouder verwerkt uitsluitend gepseudonimiseerde gegevens

Artikel 11p, lid 2: *"De registratiehouder, of een onder diens verantwoordelijkheid werkzame verwerker, verwerkt slechts persoonsgegevens als daarop pseudonimisering is toegepast en vervolgens ten aanzien van deze verwerkingen onafgebroken is gecontinueerd."*

2. Een zorgaanbieder pseudonimiseert gegevens voor verstrekking

Artikel 11q lid 3: *"Een zorgaanbieder als bedoeld in het eerste lid, past op de in dat lid bedoelde gegevens pseudonimisering toe, alvorens de gegevens te verstrekken."*

Ook de Memorie van Toelichting⁹ stelt aanvullende eisen;

3. Pseudonimisering zo vroeg mogelijk in het proces (aan de bron)

"Op grond van de AVG dient pseudonimisering plaats te vinden in combinatie met andere maatregelen die erop gericht zijn de herleidbaarheid van de gegevens te beperken. Daarom verdient het de voorkeur om de pseudonimisering zo vroeg mogelijk in het proces, liefst aan de bron, te laten plaatsvinden."

4. Koppelbaarheid in de tijd en over locaties heen (herhaalbaarheid en koppelbaarheid)

⁸ Bijvoorbeeld in 'Pseudonimisering risicoverevening', College Bescherming Persoonsgegevens, 6 maart 2007. Zie ook <https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-pseudonimisering-persoonsgegevens-bij-risicoverevening>.

⁹ <https://www.tweedekamer.nl/downloads/document?id=2022D55107>

'Zoals al is aangegeven, moeten behandeltrajecten en waar mogelijk ook verschillende elementen van een behandeling aan een unieke cliënt gekoppeld kunnen worden en dubbelingen in de registratie van unieke cliënten zoveel mogelijk worden tegengegaan. Pseudonimisering van gegevens over dezelfde cliënt maakt het alleen mogelijk om deze gegevens uit verschillende bronnen te koppelen indien gebruik wordt gemaakt van hetzelfde pseudoniem.'

5. State of the art (kwaliteit van de pseudonimisering)

Waar in dit wetsvoorstel gesproken wordt over de verplichte en ononderbroken toepassing van pseudonimisering, zullen alle betrokken partijen zich dienen te richten naar de eisen in die ministeriële regeling die voldoen aan de actuele stand van de techniek. Daarmee wordt een heldere en objectieve standaard geboden voor het (door)ontwikkelen van het kader waaraan alle uitwisselingen van persoonsgegevens tussen kwaliteitsregistraties en zorgaanbieders en kwaliteitsregistraties onderling moeten voldoen, wanneer zij binnen de kaders van dit wetsvoorstel gegevens verwerken.'

Tot slot staat in de Ministeriële regeling en het aanvraagformulier voor opname in het register de eis:

6. Gestandaardiseerde methode.

De ministeriële regeling verwijst naar het aanvraagformulier voor opname in het register waarin voorgaande eisen deels herhaald worden. Aanvullend wordt gesteld dat gepseudonimiseerde gegevens uit verschillende registraties koppelbaar zijn op basis van een gestandaardiseerde methode.

Bijlage D: specificatie van de VWS- pseudonimiseringsmethode

Uitgangspunt voor specificatie van de pseudonimisering is de methodebeschrijving die is opgesteld ten behoeve van de aanbesteding door het ministerie van VWS, de NZa en het Zorginstituut van de gegevensverwerkingen voor de risicoverevening en het DBC-Informatiesysteem (DIS). Deze methode is oorspronkelijk gebruikt om redelijkerwijs niet herleidbare gegevens te verkrijgen door uitspraken van de EDPB.

Dit document, zie onderstaande link, is nog steeds relevant als vertrekpunt. Zo kan gedegen voortgeborduurd worden op de kennis en inzichten die in de loop der jaren in eerder werk en ervaring in de praktijk zijn opgedaan. Daarnaast zijn er de nodige ontwikkelingen geweest waar uiteraard rekening mee gehouden moet worden en rekening mee gehouden wordt.

Separaat bijgesloten als [NEN].



Bijlage J bij PvE NEN pseudonimisering s

Uitbreiding van de specificaties van de VWS-pseudonimiseringsmethode met omkeerbare pseudonimisering

Een belangrijk verschil in context tussen de verwerkingen waarvoor bovenstaande methodebeschrijving is opgesteld en de vereisten voor de kwaliteitsregistraties is de noodzaak om terug te kunnen naar het oorspronkelijke identificerende gegeven. Omdat dit een handeling is die risico met zich meebrengt is deze mogelijkheid in deze specificatie enkel voor het lokale patiëntnummer voorzien.

Bijlage E: CSV dictionaire

In deze bijlage is beschreven aan welke eisen een CSV-bestand van de (zorg)aanbieder moet voldoen om verwerkt te kunnen worden met de aanleversoftware.

Vormvereisten input

Onderwerp	Eis
Bestandstype	Comma Separated Values (CSV)
Scheidingsteken	Puntkomma ";"
Character set	UTF-8
Kolomlabels	De eerste regel van het bestand bevat kolomlabels
Verplichte labels	Eén of meerdere van de volgende variabelen zijn verplicht aanwezig, maar mogen leeg zijn ten behoeve van de pseudonimisering: <i>Geboortedatum, Geslacht, Postcode, Huisnummer, Naam, Voorletter, PatientID, BSN</i>
Overige labels	Overige inhoudelijke variabelen: vrij & toegestaan.

Notatiewijze verplichte kolomlabels

Kolomlabel	Notatiewijze
Geboortedatum	jjjjmmdd
Geslacht	M/m/1 (man), V/v/F/f/2 (vrouw), 9/0/O/o (onbekend)
Postcode	NNNN[AA]
Huisnummer	XXX-AA
Naam	Geboortenaam
Voorletter	H.J.S., h.j.s., HJS of hjs. Eerste letter wordt gepseudonimiseerd
PatientID	Patiëntnummer
BSN	Burgerservicenummer, 11 proef en 9 cijferig.

Validaties kolomlabels

Headernaam	Notatiewijze	Input voor pseudonym type(s)	Output na pseudonimiseren
Geboortedatum	jjjjmmdd	C, RGG, NGGV, NGG, GG, G, BG	Aggregatieniveau afhankelijk van de noodzaak voor de registratie ¹⁰ .
Geslacht	M/V/F, m/v/f, 1/2/9/0 (nul) of O/o (Onbekend)	C, RGG, NGGV, NGG, GG	Doorgeven
Postcode	NNNAA of NNNN	C, RGG	Coderen of aggregeren. Aggregatieniveau afhankelijk van de noodzaak voor de registratie.
Huisnummer	XXX (123) met optionele toevoeging -AA (cijfers en letters).	PHH	Leeg

¹⁰ Het aggregatieniveau is uitkomst van de door de KR uitgevoerde DPIA.

Naam	Dijk, DIJK of van Dijk (normalisatie op voorvoegsels)	NGGV, NGG	Leeg
Voorletter	H.J.S., HJS, h.j.s, hjs. Alleen letters en punten, eerste letter wordt gebruikt voor pseudonimisatie	NGGV	Leeg
PatientID	A00123	MRN onomkeerbaar en MRN omkeerbaar	Leeg
BSN11	Elfproef & 9 cijfers	B	Leeg
Inhoudelijke data	Vrij	-	Inhoudelijke data wordt 1-op-1 doorgeven

De volgende pseudoniemen kunnen op basis van de aangeboden input worden aangemaakt:

Pseudoniemen	Variabelen
C-pseudoniem	Geboortedatum, geslacht, postcode (6)
GG-pseudoniem	Geboortedatum, geslacht
sNGGV-pseudoniem	Naam (4 karakters), geboortedatum, geslacht, voorletter
sNGG-pseudoniem	Naam (4 karakters), geboortedatum, geslacht
RGG-pseudoniem	Geboortedatum, geslacht, postcode (4)
NGGV-pseudoniem	Naam (8 karakters), geboortedatum, geslacht, voorletter
NGG-pseudoniem	Naam (8 karakters), geboortedatum, geslacht
MRN-pseudoniem	Patiëntnummer
B-pseudoniem	BSN

Bestandsnaamconventie

¹¹ Technisch verwerkbaar, maar op dit moment niet toegestaan voor kwaliteitsregistraties.

Er geldt een verplichte bestandsnaamconventie. Deze is van belang voor de correcte verwerking van het bestand. De bestandsnaamconventie is als volgt:

Format:

Domein_data_NaamKwaliteitsregistratie_aanleverendeOrganisatie_datum_volgnummer.csv

Voorbeeld:

DomeinA_data_DHFA_UMCU_20240529_001.csv

De elementen Domein_data_NaamKwaliteitsregistratie_ (inclusief underscores) zijn essentieel voor het correct verwerken van het bestand.

Element	Beschrijving
Domein	Route waarover het bestand moet worden verzonden
NaamKwaliteitsregistratie	Nnaam van de kwaliteitsregistratie waaraan wordt aangeleverd
AanleverendeOrganisatie	naam aanleverende organisatie
Datum	Datum van verzending in jjjjmmdd
Volgnummer	Volgnummer van bestand bestaande uit 3 karakters, startend met 001

Specificatie van de output

De opbouw van de output na pseudonimisatie is vergelijkbaar met de opbouw van de input. Het verschil is dat de toegevoegde pseudoniemen als eerste kolom(men) zijn toegevoegd.

Bijlage F: XML-aanlevering

In deze bijlage is beschreven aan welke eisen een XML-bestand moet voldoen om verwerkt te kunnen worden met de aanleversoftware.

Bestandsindeling (input)

De databronnen zullen de bestanden aanleveren conform de XML-structuur zoals beschreven in de XSD. Alle registraties worden op een generieke wijze afgehandeld. Er wordt gebruik gemaakt van de volgende specificaties:

- XML bestand;
- Er geldt een verplichte bestandsnaamconventie (zie hieronder);
- De opbouw van de XML is als volgt:

```
<export>
```

```
  <exportheader projectname=" " projectversion="" />
```

```
  <patient>
```

```
    <upn></upn>
```

```
    <tussen></tussen>
```

```
    <naam></naam>
```

```
    <voorletter></voorletter>
```

```
    <gebdat></gebdat>
```

```
    <geslacht></geslacht>
```

```
    <pcode></pcode>
```

```
    <bsn></bsn>
```

```
  </patient>
```

```
</export>
```

Validaties

Verplichte headernaam	Omschrijving	Verplicht?	Voorbeeld notatie	Aangemaakt pseudoniem	Output na pseudonimiseren
Gebdat	Geboortedatum	Nee	jjjjmdd	C, RGG, NGGV, NGG, G, BG	Aggregatie afhankelijk van de noodzaak voor de desbetreffende registratie ¹² .
Geslacht	Geslacht	Nee	M/V/F, m/v/f, 1/2/9/0 (nul) of O/o(Onbekend)	C, RGG, NGGV, NGG, G	Aggregatie afhankelijk van de noodzaak voor de desbetreffende registratie.
Pcode	Postcode	Nee	NNNAA of NNNN	C, RGG	Aggregatie afhankelijk van de noodzaak voor de desbetreffende registratie.
Huisnr	Huisnummer	Nee	XXX (123) met optionele toevoeging -AA (cijfers en letters).	PHH	Leeg
Naam	Geboortenaam	Nee	Dijk, DIJK of van Dijk (normalisatie op voorvoegsels)	NGGV, NGG	Leeg
Voorletter	Voorletter	Nee	H.J.S., HJS, h.j.s, hjs. <i>Alleen letters en punten, eerste letter wordt gebruikt voor pseudonimisatie</i>	NGGV	Leeg
Upn	PatientID	Nee	A00123	MRN onomkeerbaar en MRN omkeerbaar	Leeg
bsn ¹³	BSN	Nee	Elfproef & 9 cijfers	B	Leeg
Inhoudelijke data	-	-	Vrij	-	Inhoudelijke data wordt 1-op-1 doorgegeven

¹² Deze afweging is afhankelijk van het resultaat van de voor de KR uitgevoerde DPIA. Een aggregaat of behoud van de oorspronkelijke waarde dient noodzakelijk te zijn.

¹³ Technisch verwerkbaar, maar op dit moment niet toegestaan voor kwaliteitsregistraties.

Specificatie output

Na pseudonimisatie wordt een bestand opgeleverd (ter download klaargezet) voor de afhaal software. Het bestand heeft de volgende kenmerken:

XML bestand;

De eerste attributen betreffen de pseudoniemen;

De opbouw van de XML is als volgt:

```
<export>
<exportheader />
<patient>
  <pseudonyms>
    <pseudonym type = "C" > </pseudonym>
    <pseudonym type = "NGGV" > </pseudonym>
    <pseudonym type = "NGG" > </pseudonym>
    <pseudonym type = "sNGGV" > </pseudonym>
    <pseudonym type = "sNGG" > </pseudonym>
    <pseudonym type = "RGG" > </pseudonym>
    <pseudonym type = "MRN" > </pseudonym>
    <pseudonym type = "B" > </pseudonym>
    <pseudonym type = "GG" > </pseudonym>
  </pseudonyms>
  <geslacht></geslacht>
</patient>
</export>
```

Bijlage G: HL7-FHIR-aanlevering

Pseudonimisatie vindt plaats op in de patient resource aanwezige elementen.

Zie <https://simplifier.net/nictizstu3-zib2017/nl-core-patient>