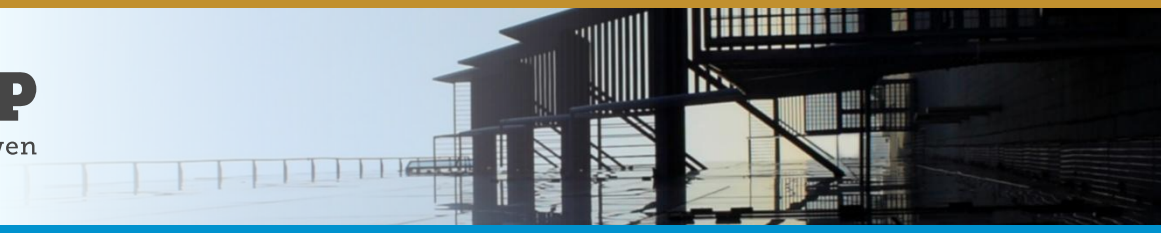
ZorgTTP
Privacy & vertrouwen



API Documentatie Wkkgz

Handhaven vertrouwelijkheid gegevens

Voor de aanlevering van gegevens aan kwaliteitsregistraties kunt u gebruik maken van de pseudonimisatiedienstverlening van ZorgTTP. U kunt door middel van twee technieken gegevens aanleveren, te weten via een webgebaseerde techniek of via een lokale client. Deze handleiding beschrijft hoe u de webgebaseerde techniek kunt gebruiken voor het aanleveren en ontvangen van gegevens. Wanneer u de lokale client gebruikt, raadpleeg dan de documentatie welke bij deze techniek hoort (installatiehandleiding en berichtspecificaties).

Deze API wordt gebruikt voor zowel de omkeerbare als onomkeerbare pseudonimisering van persoonsgegevens, waaronder mogelijk persoonlijke gezondheidsinformatie. Door het toepassen van Privacy Enhancing Technologies wordt de herleidbaarheid naar natuurlijke personen zoveel mogelijk beperkt.

Voor een correcte en veilige werking van deze API is het essentieel dat de aanlevering voldoet aan de afgesproken specificaties. Een aanlevering die niet conform de specificaties is, kan ertoe leiden dat gegevens niet of niet correct worden verwerkt.

Gezien het vertrouwelijke karakter van de persoonsgegevens die via deze API worden verwerkt, is het van groot belang om zorgvuldig om te gaan met de gegevensaanlevering en de ontvangen pseudoniemen. Test bij een eerste verwerking met de API daarom altijd eerst met fictieve persoonsgegevens. Pas na succesvolle validatie mogen daadwerkelijke persoonsgegevens worden verwerkt.

Inhoud

© copyright ZorgTTP 2026

De rechten van intellectuele en industriële eigendom, waaronder het auteursrecht, op alle informatie in dit document berusten bij ZorgTTP of diens licentiegevers. Verveelvoudiging en/of commercieel gebruik van deze informatie anders dan voor het doel waarvoor dit document is bestemd is niet toegestaan, tenzij hiervoor uitdrukkelijk schriftelijke toestemming is verleend. Alle rechten worden voorbehouden.

1. Inleiding

Dit document beschrijft de technische details van de Pseudonimisatie API van ZorgTTP.

De eindgebruikers van de API zijn te verdelen in twee te onderscheiden categorieën:

1. **Aanbieders** van persoonsgegevens, zoals zorgaanbieders
2. **Afnemers** van pseudoniemen, zoals dataverwerkers en kwaliteitsregistraties

De API ondersteunt twee soorten pseudonimisatie;

1. **Onomkeerbare pseudonimisatie**, voor aanbieders en afnemers, waarbij de oorspronkelijke persoonsgegevens niet kunnen worden herleid
2. **Omkeerbare pseudonimisatie**, waarbij pseudoniemen terug te vertalen zijn naar de oorspronkelijke gegevens

Beide vormen van pseudonimisatie kunnen tegelijkertijd worden toegepast via het algemene endpoint. Voor speciale toepassingen kan elke vorm van pseudonimisatie apart toegepast worden via specifieke endpoints.

De API biedt voor elke categorie, aanbieders of afnemers, specifieke functies. In deze documentatie is één deel bedoeld voor de aanbieders en een ander deel voor de afnemers. Ga bij het raadplegen van deze documentatie dus eerst na welk deel van toepassing is.

1.1 Documenteigenschappen

Dit document wordt regelmatig geüpdatet om wijzigingen en verbeteringen in de API nauwkeurig weer te geven. De meest recente versie is altijd beschikbaar via onze website: https://www.zorgttp.nl.

Versie:	**0.1**
Datum:	**25-3-2026**
Auteur:	**Marnix Bindels**
Co:	**Jaïr van Eer**

1.2 Contact ZorgTTP

Heb je vragen over deze documentatie, ervaar je problemen bij het gebruik van de API, of wil je toegang aanvragen tot de API? Neem dan contact op met de Servicedesk van ZorgTTP. We helpen je graag verder.

Servicedesk ZorgTTP
E-mail: servicedesk@zorgttp.nl
Telefoon: 030-63 60 649
Website: https://www.zorgttp.nl

De Servicedesk is bereikbaar op werkdagen tussen 08:30 en 17:00 uur.

2. Algemene kenmerken van de API

In dit hoofdstuk wordt een aantal kenmerken van de pseudonimisatie API beschreven die zowel bij aanbieders als afnemers van toepassing zijn. De onderwerpen hebben betrekking op de techniek, gebruikte standaarden, benodigde infrastructuur, gebruiksmodellen, randvoorwaarden, beperkingen en beveiliging.

2.1 Gebruiksmodel

De API wordt gebruikt voor het pseudonimiseren van gegevens. De gegevens hebben betrekking op personen. De gegevens zijn in bezit van een aanbieder en worden gepseudonimiseerd beschikbaar gesteld aan een afnemer. De afnemer gebruikt de gegevens zonder de identificerende gegevens van de personen waar de gegevens betrekking op hebben. De afnemer is dankzij de pseudonimisatie in staat te bepalen welke gegevens bij dezelfde persoon horen, ongeacht van welke aanbieder ze afkomstig zijn en ongeacht op welk moment die gegevens beschikbaar zijn gesteld. We noemen dit ongeacht plaats en tijd volgen van personen zonder de identiteit te hoeven kennen.

2.1.1 Gegevens leveren – Pseudonimisatie

Voor de pseudonimisatie biedt ZorgTTP een API die gebruikt wordt 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 pseudoniemen
2. De aanbieder vervangt in de aan te leveren gegevens alle persoonsgegevens door de pseudoniemen
3. De aanbieder draagt de gepseudonimiseerde gegevens over aan de afnemer

De onomkeerbare pseudoniemen zijn maar tijdelijk bruikbaar, de aanbieder kan deze bijvoorbeeld een dag lang gebruiken voor interacties met diverse afnemers. De omkeerbare pseudoniemen zijn geschikt voor decryptie die alleen is toegestaan voor de aanbieder die ze heeft versleuteld.

2.1.2 Gegevens ontvangen – Definitieve pseudonimisatie

De API geeft steeds wisselende tijdelijke pseudoniemen af voor dezelfde persoonsgegevens. Ze zijn dus niet geschikt voor het volgen van een persoon. Afnemers moeten tijdelijke pseudoniemen met de API omzetten naar definitieve pseudoniemen, daar is bijvoorbeeld een week de tijd voor.

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

De definitieve pseudoniemen zijn voor dezelfde persoonsgegevens steeds gelijk en maken volgen en koppelen van personen mogelijk. Afnemers moeten de tijdelijke pseudoniemen niet voor lange termijn opslaan.

2.2 Open API

De technische invulling van de API is als volgt. ZorgTTP 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. De specificatie is te vinden op deze url:

Productieomgeving:

https://api.zorgttp.nl/v3/openapi.json

Testomgeving:

https://api.test.zorgttp.nl/v3/openapi.json

De functies van de API worden benaderd met HTTP functies, met name POST en GET. De input voor een functie wordt in de body aangeleverd als JSON (RfC 8259) en gebruikt dus altijd UTF-8 encoding. Het escapen van Unicode karakters wordt ondersteund.

2.3 Identificatie en autorisatie

De API is slechts beperkt toegankelijk. ZorgTTP beveiligt met de pseudonimisatie persoonsgegevens en dat moet zorgvuldig gebeuren. Om gebruik te kunnen maken van de API, zal ZorgTTP de gebruikers toegang verlenen op basis van rechten en rollen en steeds controleren of de gebruiker nog gerechtigd is:

- Voor de API worden twee rollen onderscheiden: **aanbieders** zowel om als onomkeerbare pseudonimisatie en **afnemer** voor onomkeerbare pseudonimisatie
- De afnemers mogen tijdelijke pseudoniemen omzetten in definitieve en andersom. Dit wordt alleen toegestaan op de domeinen in beheer van die afnemer.
- **Aanbieders** mogen omkeerbare pseudoniemen die aangemaakt zijn voor dezelfde zorgaanbieder ontsleutelen.

Het identificeren en authenticeren van gebruikers kan op verschillende manieren plaats vinden. Hierbij wordt een groeiend palet van mogelijkheden geboden. Op dit moment ondersteunt de API:

- BEARER TOKEN
- OAuth2.0
- OIDC

2.3.1 OAuth 2.0

Deze autorisatiemethode kan afhankelijk van de situatie in verschillende flows worden gebruikt. Kies hierbij de wenselijke flow voor machine-to-machine of gebruikersinteractie.

Gebruikersinteractie (Webbrowser en multifactor-authenticatie)

ZorgTTP voorziet u van een zogenaamd *resource ID* en maakt gebruik van grant type **authorization code (with PKCE)**. De volgende scopes zijn noodzakelijk: **openid urn:zitadel:iam:org:project:id:zitadel:aud urn:zitadel:iam:user:metadata**

Voor het verkrijgen van tokens via gebruikersinteractie is aan uw kant een front-end-applicatie vereist die deze flow ondersteunt. Wij registreren uw front-end applicatie in ons ZorgTTP Identity Provider (IDP) platform. Het *resource ID* dat u ontvangt is het registratienummer van uw applicatie. Om deze registratie te kunnen voltooien dient u een callback URL (redirect URL) aan te leveren.

Een gebruiker start in uw front-end applicatie de authenticatie met een call naar het **auth endpoint**. Dit endpoint genereerd een **authorization code** na succesvolle authenticatie en stuurt deze terug naar de aangeleverde redirect URL. Vervolgens kan deze **authentication code** door uw frontend worden uitgewisseld voor een token bij het **token endpoint.**

Machine-to-Machine

ZorgTTP voorziet u van zogenaamde credentials: *client ID* en *client secret* en maakt gebruik van grant type **client credentials**. De volgende scopes zijn noodzakelijk: **openid urn:zitadel:iam:org:project:id:**[vul hier het project ID in]**:aud urn:zitadel:iam:user:metadata**. Met deze credentials maakt u een POST call rechtstreeks naar het token endpoint. De response bevat het token dat u vervolgens kunt gebruiken voor uw data aanlevering.

Voor de autorisatie op basis van OAuth 2.0 zijn de volgende end points van toepassing:

Productieomgeving (project ID 345491965879517345):

End Point	Type	Url
Auth	Gebruikersinteractie	https://auth.zorgttp.nl/oauth/v2/authorize
Token	Machine-to-Machine & Gebruikersinteractie	https://auth.zorgttp.nl/oauth/v2/token

Testomgeving (project ID **284743580386328579**):

End Point	Type	Url
Auth	Gebruikersinteractie	https://auth.test.zorgttp.nl/oauth/v2/authorize
Token	Machine-to-Machine & Gebruikersinteractie	https://auth.test.zorgttp.nl/oauth/v2/token

2.4 Pseudoniemen

De API wordt gebruikt om persoonsgegevens te pseudonimiseren. De onomkeerbare pseudoniemen die de API produceert voldoen aan de openbare specificatie. ZorgTTP hanteert hierbij de TTP ID waarde 3101.

De onderstaande typen pseudoniemen kunnen met de API worden gemaakt:

Pseudoniemen	Variabelen
ENCRYPT:MRN	Patiëntnummer (omkeerbaar)
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
A-pseudoniem	Postcode (6), huisnummer, huisnummertoevoeging
REFKEY-pseudoniem	Referentienummer zoals bijvoorbeeld tussen medicijn en recept
B-pseudoniem	BSN

Voor deze pseudoniemen zijn de genoemde persoonsgegevens als input noodzakelijk. Deze worden opgevoerd onder verkorte unieke labels zoals hieronder vermeld:

Label	Persoonsgegeven	Format of datatype
MRN	Medisch registratienummer of patiëntnummer	Vrije tekenreeks
G	Geslacht	0129, M, V, F of O
GD	Geboortedatum	19690923
NM	Naam	Lettertekens, spatie, punt of streepje
VL	Voorletter	Letter
PC	Postcode	NL-1200JC (landcode optioneel)
HNR	Huisnummer	Cijferreeks
XHNR	Huisnummertoevoeging	Tekenreeks
BSN	BSN	9 (of 8) cijfers
REF	Referentiesleutel	Vrije tekenreeks

3. Aanbieder API functies

Voor de API-functies wordt gebruik gemaakt van een OpenAPI v3.0 specificatie. Alle interacties vinden plaats voor een geautoriseerde gebruiker met de rol **aanbieder**.

De specificatie bevindt zich op:

https://api.zorgttp.nl/v3/openapi.json (Productieomgeving)

https://api.test.zorgttp.nl/v3/openapi.json (Testomgeving)

3.1 Volatile-encrypt

3.1.1 Basis aanroep - POST

De request kan op verschillende manieren opgesteld worden, maar kan uit maximaal drie elementen bestaan.

Variabele	Toelichting
careProvider	Optioneel, object met gegevens over de aanbieder, waarvan thans één item wordt toegestaan: AGB
pseudonymTypes	Optioneel, array van peudonymtypes, waaronder omkeerbare types (ENCRYPT)
records	Een array van records, elk record bevat de te pseudonimiseren persoonsgegevens. Records mogen verschillen in welke soort persoonsgegevens erin opgenomen zijn

3.1.2 Eenvoudige aanroep

De aanbieder kan de optionele elementen careProvider en pseudonymTypes achterwege laten om de pseudonimisatie API het standaardantwoord op basis van de in de request aanwezige persoonsgegevens te laten produceren. Hierbij zullen alle mogelijke pseudoniemtypes, eerder benoemd in 2.4, worden aangevraagd. De aanwezige persoonsgegevens per records-element zullen bepalen welke pseudoniemen er aangemaakt kunnen worden voor dat record. Het omkeerbare pseudoniem wordt in dit geval standaard aangemaakt over het WKKGZ-domein.

Bijvoorbeeld dit request voor twee patiënten:

```
{
  "records": [
    {
      "MRN": "BIN19721333",
      "G": "M",
      "GD": "19930515",
      "PC": "1234AA",
      "REF": "1"
    },
    {
      "MRN": "BIN18632222",
      "G": "V",
      "GD": "19971122",
      "PC": "9876BB",
      "NM": "Binsbergen"
    }
  ]
}
```

Levert voor beide patiënten alle mogelijke pseudoniemen op basis van de PII-gegevens in het record.
Voor de eerste patiënt:

Pseudoniem	Toelichting
MRN	Omkeerbaar, op basis van domein WKKGZ
MRN	Onomkeerbaar, op basis van waarde veld MRN
C	Onomkeerbaar, op basis van waarde velden PC(6)-GD-G
GG	Onomkeerbaar, op basis van waarde velden GD-G
RGG	Onomkeerbaar, op basis van waarde velden PC(4)-GD-G
REF	Onomkeerbaar, op basis van waarde veld REF

Voor de tweede patiënt:

Pseudoniem	Toelichting
MRN	Omkeerbaar, op basis van domein WKKGZ
MRN	Onomkeerbaar, op basis van waarde veld MRN
C	Onomkeerbaar, op basis van waarde velden PC(6)-GD-G
GG	Onomkeerbaar, op basis van waarde velden GD-G
RGG	Onomkeerbaar, op basis van waarde velden PC-GD-G
NGG	Onomkeerbaar, op basis van waarde velden NM-GD-G
sNGG	Onomkeerbaar, op basis van waarde velden NM(4)-GD-G

De response bevat een lijst van records die in dezelfde volgorde staan als de request en een samenvattende statistics sectie. Elk record geeft de gevraagde pseudoniemen terug in het item pseudonyms. Elk record geeft in het item **pseudonyms** de gevraagde pseudoniemen terug voor de aanwezige persoonsgegevens. Eventuele problemen bij het verwerken van een record, bijvoorbeeld ontbrekende velden of ongeldige invoer, worden gemeld in het item diagnostics.

De statistics geven inzicht in het resultaat van de pseudonimisaties. Onder **encryptions** staat het aantal geslaagde en mislukte omkeerbare encrypties, terwijl onder **volatile pseudonyms** het aantal tijdelijke pseudoniemen dat geslaagd of mislukt is weergeeft. Deze indeling maakt het eenvoudig om in één oogopslag te zien of de pseudonimisatie volledig is uitgevoerd en waar eventueel aanvullende aandacht nodig is. Referentievelden (REF) blijven altijd behouden in de response, zodat ze als sleutel kunnen dienen om response-records te koppelen of te identificeren.


```
{
    "statistics": {
        "volatile pseudonyms": {
            "pseudonymTotal": 11,
            "errorTotal": 0,
            "speed": 61
        },
        "encryptions": {
            "encryptTotal": 2,
            "errorTotal": 0
        }
    },
    "records": [
        {
            "pseudonyms": {
                "GG": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-GG-A/PjAAAAAdDRCSulAhTjkF585G5xBu77Ccdf55q3Vg==",
                "C": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-C-A/PjAAAAAfOkG6YUxnWultKQ9CSHk3XhqDa9oiwCEQ==",
                "RGG": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-RGG-A/PjAAAAAfW0oVVZw780/zeaSl0vfqRBW8Ot8qzVIQ==",
                "REFKEY": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-REFKEY-A/PjAAAAAU26UuT4hpWsb9cYZH1AuCFi2fZYYbViUg==",
                "MRN": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-MRN-A/PjAAAAAee6GogRueWjnqU1ElqMJ7tkSpKAonhnNA==",
                "ENCRYPT:WKKGZ:MRN": "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:E+RB1Po3gseyeVidnJ/W
                    +BPqvf6ncr3IPacrfJNXi1w=::::pYPlxx8Bm+8OYU9r+l+29V9XtUn0Th8FNKUb5sDxY50="
            },
            "diagnostics": [],
            "ref": "1"
        },
        {
            "pseudonyms": {
                "GG": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-GG-A/PjAAAAAe8yK8OO5GdCQz2oMDyj5lWu4PJNxFT0cQ==",
                "C": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-C-A/PjAAAAAZHwJ6v0dZCOhcPdmZEx6BYpAKmYjA3a0Q==",
                "RGG": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-RGG-A/PjAAAAAa0VpSyoljnDA1THXu3p5MW53cP2dHbpVQ==",
                "MRN": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-MRN-A/PjAAAAAZlhi2qDXznun+lpFwUqt2Le17zAw7yu2Q==",
                "sNGG": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-sNGG-A/PjAAAAAUfB0YGuwHFTmMb9lDDAHdvBJgXY+z34BA==",
                "NGG": "WSabzzzzzzOSdACCIDrABAEJsCDECDE-P-NGG-A/PjAAAAAaoMqg0wYh2FGhvFzWNCrDbG6OGS+EE48Q==",
                "ENCRYPT:WKKGZ:MRN": "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:BxMCj0U5UurYeV7Fvzm
                    +o1psCgeVubZNVhVmwWvtjHg=::::XdWfVKmiUippj6ZYoCRLXVi6PBlPnSkY24e/W1HzYbE="
            },
            "diagnostics": []
        }
    ]
}
```

3.1.3 Aanvullende pseudonimisatie mogelijkheden

Het **pseudonymTypes** element geeft controle over de exacte pseudonimisatie van de request. Dit kan worden toegepast als er in de response op een eenvoudige aanroep teveel of niet alle gewenste – omkeerbare- pseudoniemen aanwezig zijn.

De hierboven in sectie 2.4 uiteengezette lijst met pseudonymtypes hierbij van toepassing. Zo kan er een encryptie met alleen onomkeerbare pseudoniemen uitgevoerd worden, door geen ENCRYPT actie te specificeren:

```
{
  "pseudonymTypes": [
    "C",
    "MRN"
  ],
  "records": [
    {
      "GD": "19721005",
      "PC": "5121SC",
      "G": "M",
      "MRN": "BIN197210050001"
    }
    ,{
      "GD": "19780613",
      "PC": "4056GH",
      "G": "M",
      "MRN": "12927257"
    }
  ]
}
```

De pseudonymTypes kunnen zowel onomkeerbare types bevatten zoals C of MRN, als omkeerbare types in de vorm ACTION:DOMAIN:FIELD.

Hierbij is de actie ENCRYPT, DOMAIN het project waarvoor geëncrypteerd wordt, en FIELD staat voor de waarde in het record dat geëncrypteerd moet worden, zoals ENCRYPT:WKKGZ:MRN. Hierin is ENCRYPT:WKKGZ de actie die uitgevoerd moet worden voor alle MRN-waarden in de records.

Het is mogelijk om meerdere waarden gegroepeerd te laten encrypten tot 1 omkeerbaar pseudoniem, door deze met een plus-teken (+) samen te voegen, zoals het MRN en de AGB-code samen te voegen zijn door ENCRYPT:WKKGZ:MRN+AGB aan te geven. De speciale variabele AGB kan zowel in een record aanwezig zijn als in het **careProvider** element. De AGB waarde in een record gaat altijd voor, anders wordt de careProvider waarde gebruikt.

Wanneer er geen domein is opgegeven in de ENCRYPT pseudonymtype wordt standaard het WKKGZ-domein gebruikt.

De request body dient een JSON-object te bevatten dat op deze manier wordt opgebouwd:

```
1  {
2    "careProvider": [
3        {
4            "AGB": "87654321"
5        }
6      ],
7    "pseudonymTypes": [
8      "C",
9      "MRN",
10     "ENCRYPT:MRN",
11     "ENCRYPT:MRN+AGB",
12     "ENCRYPT:ZORGTTP_DEMO:PC+MRN+GD"
13     ],
14   "records": [
15     {
16       "MRN": "BIN19721333",
17       "G": "M",
18       "GD": "19930515",
19       "PC": "1234AA",
20       "AGB": "12345678"
21     },
22     {
23       "MRN": "BIN18632222",
24       "G": "V",
25       "GD": "19971122",
26       "PC": "9876BB"
27     }
28   ]
29 }
```

Waarbij te zien is dat er zowel een algemene AGB-code in careProviders is toegevoegd aan de request, alswel in één van de records door toevoeging van de variabele AGB (line 20). In dit geval zal de omkeerbare encryptie waarbij MRN en AGB worden samengevoegd in het ene record gedaan worden over value “BIN19721333+12345678” (AGB uit record) en in het andere records over value “BIN18632222+87654321” (AGB uit careProvider).

Niet alle variabelen hoeven in elk record aanwezig te zijn; alleen als de variabelen die nodig zijn voor het opgegeven pseudonymType aanwezig zijn, wordt het pseudoniem geleverd in de response. Als er een C pseudoniem (postcode, geboortedatum, geslacht) wordt gevraagd, maar een specifiek record mist één of meerdere van deze velden, dan wordt voor dit record geen C-pseudoniem aangemaakt.

De response van de service heeft de volgende vorm:


```
{
    "statistics": {
        "volatile pseudonyms": {
            "pseudonymTotal": 4,
            "errorTotal": 0,
            "speed": 667
        },
        "encryptions": {
            "encryptTotal": 6,
            "errorTotal": 0
        }
    },
    "records": [
        {
            "pseudonyms": {
                "C": "WSabzzzzzzOSdACCICrAECIGsCDECDE-P-C-A/PjAAAAAVAmu1pPkv0hPsQ249cRpMAsgaKL4+5CXA==",
                "MRN": "WSabzzzzzzOSdACCICrAECIGsCDECDE-P-MRN-A/PjAAAAAb6GcWFpCf6v7DanNXRilJ
                    +Ph8mUqY2teQ==",
                "ENCRYPT:WKKGZ:MRN": "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:uc/
                    U4HgL2d45yZ2UZpUMgPngCg+6sbDrcylyb2aWKCooiEn09MnlH6muG/9ebRP0::::xmCCUj/QM/
                    gzI4iYF21I8PDhuMKJyT3N+o9zSy3ssQk=",
                "ENCRYPT:WKKGZ:MRN+AGB":
                    "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:UG8nmRlzUb2P0IQqQQtAXEudvxz0mfWhmkYdB5igL
                    28MICAkbrPhXCAOoxc8CxHioAcvvSE60r5Fcc6UEgf2bQ==::::zHCC+SqfvKFEvS9lDjWfU/
                    WGTBTzZwnrxhaS5zcfns0=",
                "ENCRYPT:ZORGTTP_DEMO:PC+MRN+GD": "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:24fS1T2
                    +Np6B8VUAuApwPVPy9Kta7qF4xI0MKbvnpz46r3kHR1atlYcgpJ6FJ/
                    I1IkIj76AEIqebQAeZt6AYwg==::::ihg9r3kxrVsO1BNkcRfDqG782VjU6x14S4JaLMdTcvY="
            },
            "diagnostics": []
        },
        {
            "pseudonyms": {
                "C": "WSabzzzzzzOSdACCICrAECIGsCDECDE-P-C-A/PjAAAAAXTt9Ic48PhBtnRULmVlIQx8JK/XSVAxcw==",
                "MRN": "WSabzzzzzzOSdACCICrAECIGsCDECDE-P-MRN-A/
                    PjAAAAAbCkJGNzwNJggJ0vsBXTyR13O6PTA2ZIkg==",
                "ENCRYPT:WKKGZ:MRN": "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:QnBNBc2e3TQ/wumwFN/
                    i4EImpEeX+7p8wR61etZkMkAB0+9pU5RD79a4eVzJQTT1::::ZW58BtS3Eqe5ni6pm/YDOd
                    +yPy26PIuJOg9aC5tmw0I=",
                "ENCRYPT:WKKGZ:MRN+AGB": "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:uz9z9x3gDprftYNMqy/
                    MdwS5wCEokKLE7ZxH0Igd7zWGsOL8E0gjfMQKP0cIFCgfW5KtoTygNO52LnETLsjaLg==::::BEA/
                    JAwtO4gajOmUhrNQAtdsWLge7bnEOBH8rzHw8Ww=",
                "ENCRYPT:ZORGTTP_DEMO:PC+MRN+GD":
                    "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:gEg8Tz2VyWTH+87bOJXydZBCghP/
                    7VDWgELSxDkBhUb+fjLpvjmIcifwZOd1OKBUe5MhKp+/
                    190kNDrnhXTH7w==::::Ucj2oZDUHqwct8AxrYWIf/0V73LW7lidoHnAWRxRuQE="
            },
            "diagnostics": []
        }
    ]
}
```


Te zien is dat bij het in de request opgegeven pseudonymtype ENCRYPT:WKKGZ het default domein WKKGZ is toegevoegd, en er in de response dus de volledige waarde ENCRYPT:WKKGZ:MRN wordt geretourneerd.

3.1.4 Foutsituaties

Elke aanroep van de service levert een HTTP-statuscode die aangeeft of de request correct is verwerkt. De tabel hieronder geeft de mogelijke situaties weer waarbij het resultaat anders is dan HTTP 200 – OK:

HTTP code	Toelichting
400	Bad request: De request kan door een syntax error niet correct verwerkt worden
400	**errorCode 1001** - Onbekend pseudoniemtype bij ZPS-validatie. Het type staat niet in de lijst van toegestane irreversibele pseudoniemen.
400	**errorCode 1002** - Ongeldig format van een ENCRYPT-type. Het moet de vorm ACTION:DOMAIN:FIELDS hebben.
400	**errorCode 1003** - Ongeldig actie-type in ENCRYPT. Alleen actie ENCRYPT wordt ondersteund.
400	**errorCode 1004** - Onbekend domein in een ENCRYPT-type. Het opgegeven domein komt niet voor in de mapping
400	**errorCode 1005** - Veld in de ENCRYPT-specificatie ontbreekt in het record. Als een veld nodig is voor de encryptie, maar niet aanwezig is, wordt dit gemeld.
400	**errorCode 1006** – Onbekend veld in careProvider. Alleen key "AGB" is toegestaan
400	**errorCode 1007** – careProvider is geen list
401	Unauthorized: token niet meer geldig of u heeft niet de juiste rol voor deze aanroep
412	De service is nog niet geïnitialiseerd na herstart, ZorgTTP moet dit nog doen
422	De request is niet in orde: een onbekend pseudoniemtype, hetzelfde type twee keer
500	Server error: de service is niet in staat een response te geven

variabele	Toelichting
pseudonymTypes	Selecteer de gewenste pseudoniemtypes. Kies uit: - A, B, BG, C, GG, MRN, NGG, NGGV, REFKEY, RGG, sNGG, sNGGV - Voor encryptie kiest u een van onderstaande record types in het volgende format: ENCRYPT:DOMAIN:FIELD{+FIELD}
records	Een array van records, elk record bevat de te pseudonimiseren persoonsgegevens. Records mogen verschillen in welke soort persoonsgegevens erin opgenomen zijn
BSN	Burgerservicenummer 123456782
GD	Geboortedatum; 13 juni 1978 19780613
MRN	Medisch registratienummer, unieke tekenreeks voor persoon, patiënt of client in het systeem van de aanbieder EPC-43201
G	Geslacht: M, m of 1 voor mannelijk, V, F, 2: voor vrouw, 0, O voor onbekend, 9 voor anders. V
PC	Nederlandse, Duitse of Belgische postcode. NL-4056GH (zonder landaanduiding wordt NL aangenomen) 1200JC
NM	Geboortenaam, achternaam. Met of zonder tussenvoegsels van Binsbergen
VL	Voorletter W
HNR	Huisnummer van een adres, cijfers 26
AGB	Zorgaanbieder AGB code, 8 cijfers
XHNR	Eventuele toevoegingen achter een huisnummer A
REF	Elk ander referentiegegeven, een niet lege string (de waarde wordt als referentie overgenomen in de response) A8765-34.2

De response van de service heeft de volgende vorm:


```
{
    "records": [
        {
            "pseudonyms": {
                "MRN": "WSaadABGEDrAGEAFsCDECDE-P-MRN-AwwdAAAAAaZLHWJUhSOEA98VRBnfeynG0Kjq12CLcA=="
            },
            "diagnostics": [],
            "ref": "1"
        },
        {
            "pseudonyms": {
                "MRN": "WSaadABGEDrAGEAFsCDECDE-P-MRN-1----------------------------------------"
            },
            "diagnostics": [
                {
                    "code": 3070,
                    "field": "MRN",
                    "errorMsg": "MRN is leeg",
                    "content": ""
                }
            ],
            "ref": "2"
        }
    ],
    "statistics": {
        "pseudonymTotal": 1,
        "errorTotal": 1,
        "speed": 500
    }
}
```


Waarbij de lijst van records even lang is als die van de request en dezelfde volgorde kent, gevolgd door een samenvattende statistiek. In die laatste is eenvoudig na te gaan of de pseudonimisatie volledig is geslaagd.

Wanneer in de request een record is voorzien van een REF input-waarde, is deze waarde ook onderdeel van de response – ongeacht of er een REF-pseudoniem is aangemaakt. Met behulp van deze REF input kan een referentiesleutel worden gebruikt in plaats van of als aanvulling op de record-volgorde.

Elk record in de response levert de gevraagde pseudoniemen voor zover de input daarvoor aanwezig én correct was. Als de controles op de input een probleem met een persoonsgegeven constateren, wordt daarvan melding gemaakt in het diagnostics deel.

3.1.5 Foutsituaties

Elke aanroep leidt tot een response met een HTTP reponse code. De tabel hieronder geeft de mogelijke situaties weer waarbij het resultaat anders is dan HTTP 200 – OK:

HTTP code	Toelichting
401	Unauthorized: token niet meer geldig of u heeft niet de juiste rol voor deze aanroep
412	De service is nog niet geïnitialiseerd na herstart, ZorgTTP moet dit nog doen
422	De request is niet in orde: een onbekend pseudoniemtype, hetzelfde type twee keer
500	Server error: de service is niet in staat een response te geven

4. Afnemer API functies

Voor de API functies wordt gebruik gemaakt van een OpenAPI v3.0 specificatie. Alle interacties vinden plaats voor een geautoriseerde gebruiker met de rol **afnemer**.

De specificatie bevindt zich op:

https://api.zorgttp.nl/v3/openapi.json (Productieomgeving)

https://api.test.zorgttp.nl/v3/openapi.json (Testomgeving)

4.1 Pseudonymizations

4.1.1 Basis aanroep - POST

De request dient op deze manier te worden opgebouwd:

```
{
  "pseudonyms": [
   "WSabzzzzzzOSdABJCFrAHEGDsCDECDE-P-C-A/PjAAAAAUqYC/WyxQRaO1kmJUDDodKjmspI7JPhig==",
   "WSabzzzzzzOSdABJCFrAHEGDsCDECDE-P-RGG-A/PjAAAAAcrZMFVXfkvxKNZWOev3Wx4jHtj8WSaXhA==",
   "WSabzzzzzzOSdABJCFrAHEGDsCDECDE-P-MRN-A/PjAAAAAYQT78Bn/NqdMHzKbg0fIj/hKWNNyDMZGg=="
   ],
  "targetDomain": "SSHA1"
}
```

variabele	Toelichting
pseudonyms	Een array van pseudoniemen, elk item is een tijdelijk pseudoniem ontvangen van een databron.
targetDomain	Het pseudonimisatiedomein voor de definitieve pseudoniemen

De response van de service heeft de volgende vorm:


```
{
    "records": [
        {
            "pseudonym": "SHASOFT-P-C-AwABAAAAAbPguDbURkj09+A6CQSEUDTz/yiUb4PTDg==",
            "diagnostics": []
        },
        {
            "pseudonym": "SHASOFT-P-C-AwABAAAAAbKXiz+KCbCTu7wJndU5fsEhgLoLk41CqQ==",
            "diagnostics": []
        },
        {
            "pseudonym": "SHASOFT-P-MRN-AwABAAAAAVTFnNevKEW0ALP4mZsOywSB/4FWrfYB1Q==",
            "diagnostics": []
        }
    ]
}
```


Waarbij de lijst van records even lang is als die van de request en dezelfde volgorde kent. Elk element in de array is een paar van definitief pseudoniem en diagnostische meldingen.

Elk record in de response levert het definitieve pseudoniem voor zover de input correct en niet verlopen is.

Tijdelijke pseudoniemen moeten binnen beperkte tijd worden omgezet in definitieve pseudoniemen, wanneer de termijn is overschreden wordt dit gemeld en bevat de response geen pseudoniem.

4.1.2 Foutsituaties

Elke aanroep leidt tot een response met een HTTP reponse code. De tabel hieronder geeft de mogelijke situaties weer waarbij het resultaat anders is dan HTTP 200 – OK:

HTTP code	Toelichting
401	Unauthorized: token niet meer geldig of u heeft niet de juiste rol voor deze aanroep
412	De service is nog niet geïnitialiseerd na herstart, ZorgTTP moet dit nog doen
500	Server error: de service is niet in staat een response te geven

5. Decrypt API functie

Van de decrypt API-functie kan gebruik gemaakt worden door gebruikers met de rol **aanbieder** met de aanvullende rechten om tekst strings decrypteren. Voor het uitvoeren van de decryptie hoeft u enkel de geëncrypteerde waarden door te geven.

De specificatie bevindt zich op:

https://api.zorgttp.nl/v3/openapi.json (Productieomgeving)

https://api.test.zorgttp.nl/v3/openapi.json (Testomgeving)

5.1 Decryptie - omkeerbaar

5.1.1 Basis aanroep - POST

De request dient op deze manier te worden opgebouwd:

```
{
  "texts":[
     "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:76FPyf5UHIRixRfgoqXYqcR8jm5NB4zqlhs/wi/IIOQ=:::Q
      +47CB6yDaaDKBcjRN+tJd4L1Wk5yd5kXEc2h7XrWFY=",
     "3::a807d22a-2f45-43e8-8160-4080d5ef0130::2:Mi5alCywpovj4GbK/FBjQWdLUbGrHQ5FO7eojA772/
      p6lgBwbIAKvB0Xfmj2Czgl:::yYtSVow4ggTb1oFIzeiD5ntH6nNNbgrk6Kofj8p0umc="
  ]
}
```

In dit geval zal aangenomen worden dat het domein waarmee de waardes geëncrypteerd zijn het WKKGZ-domein is, en zal over dit domein getracht worden te decrypteren. Als er waarden worden toegevoegd die niet over dit domein geëncrypteerd zijn, zal decryptie falen voor deze specifieke waarde.

```
[
    {
        "responseCode": 0,
        "responseMessage": "BIN19721333",
        "apiVersion": "V5"
    },
    {
        "responseCode": 0,
        "responseMessage": "BIN19721333+12345678",
        "apiVersion": "V5"
    },
    {
        "responseCode": 303,
        "responseMessage": "You are not allowed to decrypt this text. You are not the owner and do not
            have group permission to decrypt.",
        "apiVersion": "V5"
    }
]
```

Waarbij de lijst van records in de response is even lang als die van de request en dezelfde volgorde kent. Elk element in de list bestaat uit een response-code, gedecrypteerde waarde en diagnostische melding.

De response van de service heeft de volgende vorm:

```
[
    {
        "responseCode": 0,
        "responseMessage": "BIN19721333",
        "apiVersion": "V5"
    },
    {
        "responseCode": 0,
        "responseMessage": "BIN19721333+12345678",
        "apiVersion": "V5"
    }
]
```

Waarbij te zien is dat de eerste waarde was opgesteld uit één enkele waarde, en het tweede uit twee waardes, samengevoegd met een plus-teken (+).

Alternatieve manieren om

5.1.2 Foutsituaties

Elke aanroep leidt tot een response met een HTTP reponse code. De tabel hieronder geeft de mogelijke situaties weer waarbij het resultaat anders is dan HTTP 200 – OK:

HTTP code	Toelichting
400	Bad Request: de syntax van de request is incorrect
401	Unauthorized: token niet meer geldig
500	Server error: de service is niet in staat een response te geven

Aanvulllend zijn er ook API-endpoint response codes. Deze kunnen voorkomen als u weliswaar geauthenticeerd bent, maar een actie probeert uit te voeren waar u niet de juiste rechten voor heeft:

responseCode	Toelichting
100	The user name or password is incorrect, or the user does not belong to the selected project:
222	The authentication failed for the user: Token niet geldig voor de actie die u wilt uitvoeren
303	"You are not allowed to decrypt this text. You are not the owner and do not have group permission to decrypt."
310	The plain text that should be encrypted was not specified
999	Unknown error: de service is nog niet geïnitialiseerd na herstart, ZorgTTP moet dit nog doen

6. Algemene API functies

Voor de API functies wordt gebruik gemaakt van een OpenAPI v3.0 specificatie.

De specificatie bevindt zich op:

https://api.zorgttp.nl/v3/openapi.json (Productieomgeving)

https://api.test.zorgttp.nl/v3/openapi.json (Testomgeving)

6.1 Health

6.1.1 Basis aanroep - GET

De request heeft geen parameters of body.

De response heeft de volgende vorm:


```
{
    "pseudonymTypes": [
        "A",
        "B",
        "C",
        "BG",
        "RGG",
        "GG",
        "NGG",
        "NGGV",
        "sNGG",
        "sNGGV",
        "MRN",
        "REFKEY",
        "ENCRYPT:DOMAIN:FIELD"
    ],
    "requestSize": {
        "volatileCreate": 10000,
        "psCreate": 25000
    },
    "endpoints": {
        "/pseudonymizations/": true,
        "/pseudonymizations/volatile": true,
        "/volatile-pseudonymizations/": true,
        "/volatile-pseudonymizations/from-hash": true,
        "/encrypt": true,
        "/decrypt": true,
        "/translate": true,
        "/wkkgz/decrypt": true,
        "/wkkgz/encrypt-volatile": true,
        "/fhir/pseudonymizations": true,
        "/fhir/volatile-pseudonymizations": true
    }
}
```

De response bevat enkele aanwijzingen over het gebruik van de API en de status van de service als geheel. Ga voor gebruik van een end point na of deze beschikbaar is, de waarde bij de betreffende url is dan true.

6.1.2 Foutsituaties

Elke aanroep leidt tot een response met een HTTP reponse code. De tabel hieronder geeft de mogelijke situaties weer waarbij het resultaat anders is dan HTTP 200 – OK:

HTTP code	Toelichting
401	Unauthorized: token niet meer geldig of u heeft niet de juiste rol voor deze aanroep
500	Server error: de service is nog niet geïnitialiseerd na herstart