ZorgTTP
Privacy & vertrouwen

Technische plaat pseudonimisatie ZorgTTP

Auteur:
Joost Verduijn
Datum:
9 december 2019
Versie:
2.0

Inleiding

Persoons-identificerende kenmerken zoals naam en BSN worden bij pseudonimisatie vervangen door een pseudoniem, zodanig dat voor ieder persoonsgegeven steeds hetzelfde pseudoniem wordt gegenereerd. Individuen worden op deze wijze koppelbaar in tijd en over verschillende bronnen heen zonder dat daartoe de oorspronkelijke persoonsgegevens verstrekt hoeven te worden. Door tussenkomst van de TTP zijn bron en doel niet in staat om persoonsgegeven en het daar uit resulterende pseudoniem aan elkaar te relateren.

De inzet van pseudonimisatie via ZorgTTP werkt via een gelaagd model. Hierin worden een aantal vormen van beveiliging gehanteerd. Het gaat om maatregelen op de volgende niveaus:

1) Pseudonimisatie op recordniveau
2) Versleuteling op bestandsniveau
3) Transportbeveiliging
4) Controle afzender middels certificaat

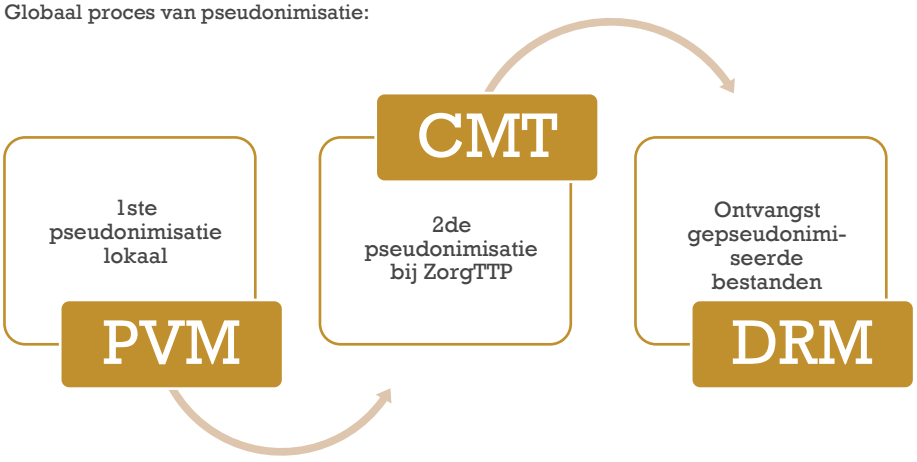
Op de volgende pagina worden de werking van de pseudonimisatiesoftware en de getroffen beveiligingsmaatregelen toegelicht.

Pseudonimisatie

De pseudonimisatieketen bestaat uit drie onderdelen:

1. Privacy- en Verzend Module (PVM) wordt door de informatiebron gebruikt om de bestanden te pseudonimiseren en te verzenden;
2. Centrale Module TTP (CMT) wordt door ZorgTTP gebruikt;
3. Doel- en Receive Module (DRM) wordt door het informatiedoel gebruikt om de bestanden vanaf de server van ZorgTTP te downloaden.

Globaal proces van pseudonimisatie:



Werking PVM

ZorgTTP is als Trusted Third Party verantwoordelijk voor de pseudonimisatie van persoonsgegevens. De eerste stap naar een pseudoniem wordt gezet bij de bron, in de Privacy- en Verzend Module (PVM). De PVM kent de volgende stappen:

1. Validatie van het aangeboden bestand op technische verwerkbaarheid;
2. Inhoudelijke validatie van het aangeboden bestand, bijvoorbeeld de 11-proef op het BSN;
3. Aanmaken van pre-pseudoniemen: persoonsgegevens waar een eerste onomkeerbare versleuteling op basis van hashing heeft plaats gevonden;
4. Verwijderen van de persoonsgegevens, bijvoorbeeld het originele BSN;
5. Splitsing van het bestand in een pseudoniemendeel en een deel met enkel inhoudelijke data;
6. Aanmaken van een kwaliteitsrapportage;
7. Versleuteling (RSA) van pseudoniemen-deel met publieke sleutel van ZorgTTP;
8. Versleuteling (AES) van data-deel met publieke sleutel van het informatiedoel;
9. Transport met daarin een meegeleverd 'adres'. Dit geeft ZorgTTP inzicht in de databron, de oorspronkelijke bestandsnaam maar ook het doel waar het bestand voor is bestemd;
10. Het versleutelde bestand wordt over een HTTPS (TLS) verbinding naar ZorgTTP verstuurd.

Verwerking ZorgTTP

Na verwerking in de PVM worden de versleutelde bestanden automatisch verzonden naar de Centrale Module TTP (CMT), de centrale verwerkingsomgeving die onder beheer van ZorgTTP valt en verantwoordelijk is voor het produceren van de definitieve pseudoniemen.

1. CMT opent het deel met pre-pseudoniemen met de private sleutel van ZorgTTP;
2. De pre-pseudoniemen worden voor de tweede maal versleuteld. Onderdeel van de tweede versleuteling is een domein specifieke versleuteling (AES) op het pseudoniemen deel. Deze versleuteling is enkel door ZorgTTP om te keren.
3. Het bestand met pseudoniemen wordt versleuteld met de publieke sleutel van het informatiedoel.

ZorgTTP heeft geen toegang tot het datadeel. Dit is beveiligd en kan enkel door het informatiedoel worden ontsleuteld.

Werking DRM

De ontvanger kan de gepseudonimiseerde gegevens vanaf CMT downloaden met een Doel- en Receive Module (DRM). De DRM wordt gebruikt door de ontvangende partij. De DRM kent de volgende stappen:

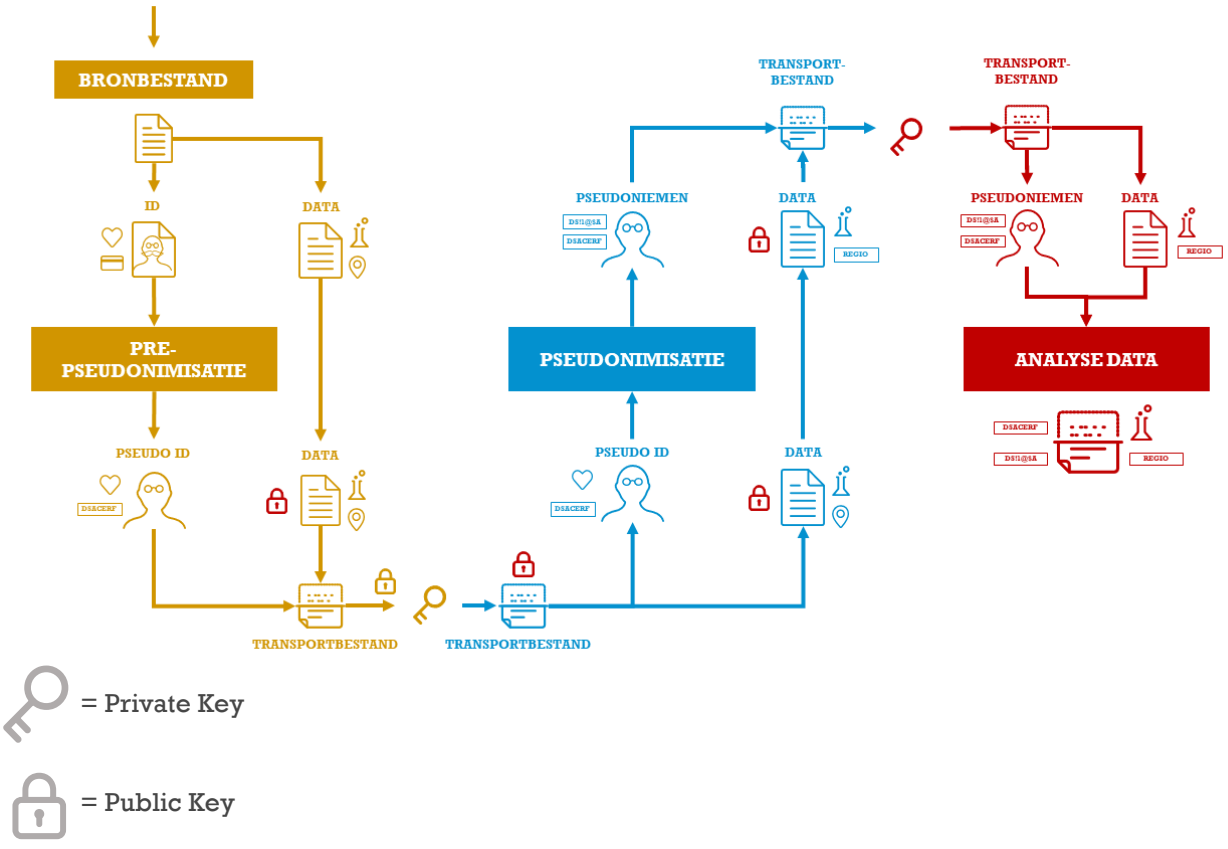
1. De DRM legt contact met de server van ZorgTTP;
2. Als er bestanden beschikbaar zijn, worden deze gedownload;
3. De bestanden worden ontsleuteld met de private sleutel van het informatiedoel;
4. De bestandsdelen – deel met pseudoniemen én deel met inhoudelijke gegevens – worden samengevoegd;
5. Het bestand wordt omgezet naar het gewenste opleverformaat.

Beveiliging van informatie

ZorgTTP stelt de databron software ter beschikking voor de eerste bewerking. Daarbij worden persoonsgegevens omgezet naar pseudoniemen, ook wordt het bestand geanonimiseerd. Bijvoorbeeld door het omzetten van een geboortedatum naar een leeftijdscategorie. De medisch inhoudelijke informatie wordt vervolgens versleuteld, deze informatie is voor ZorgTTP gedurende het transport ontoegankelijk. Vanwege logistieke voordelen worden de pseudoniemen én inhoudelijke data in één levering via ZorgTTP aan de ontvanger aangeboden.

Uitwisseling van gegevens tussen de diverse partijen vindt plaats over beveiligde internetverbindingen (TLS). De identiteit van partijen wordt gevalideerd middels digitale certificaten (Public Key Infrastructure (PKI)).

Overzicht berichtstromen:



= Private Key

= Public Key