Handleiding pseudonimisatie

Behorend bij pseudonimisatietool Versie 3.01

Inhoud

1. Inleiding

Voor de uitvoer van het DDD-partnership verwerkt i2i grote hoeveelheden privacy- en marktgevoelige informatie van zowel verzekeraars als zorgverleners. Met behulp van deze data mag het op geen enkele manier mogelijk zijn om individuen te identificeren. Daarnaast moet de data beveiligd verstuurd worden. Hiertoe heeft SBPDDDP een pseudonimisatietool ontwikkeld. Dit document is de handleiding behorend bij die pseudonimisatietool. Voor een functionele beschrijving van de tool kunt u terecht op de website van i2i support: https://www.i2i.eu/data-aanleveringen/pseudonimisering/.

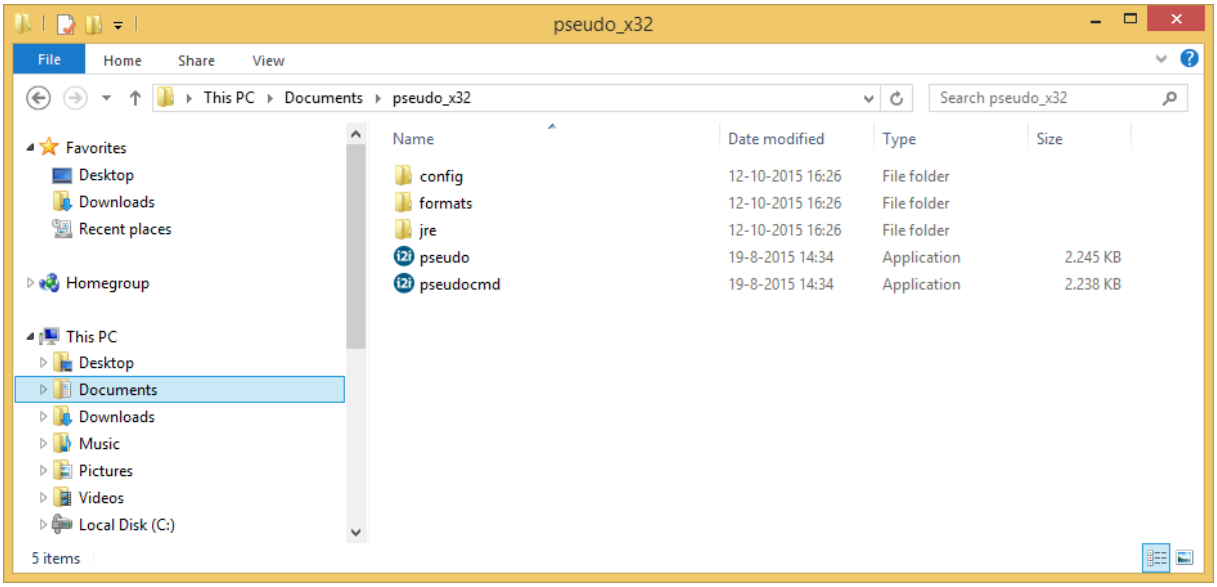
2. Systeemeisen

Voor de uitvoer van de pseudonimisatie met de pseudonimisatietool is een computer nodig met de volgende requirements:

- RAM: minimaal 3 GB vrij bruikbaar geheugen
- Windows XP / 7 / 8
- Permissie om executable uit te voeren (installatie is niet nodig)

3. Benodigde software

De software hoeft niet geïnstalleerd te worden. Nadat u een account bij Zivver heeft aangemaakt ontvangt u via het Zivverportaal van support@i2i.eu een zipbestand met daarin de pseudonimisatietool. **Let op: verstuur nooit data met persoonsgegevens naar support@i2i.eu, maar altijd via de link op https://veilig.doelmatigdirectdeclareren.nl/.** Pak dit zipbestand uit in een map waar u executerechten heeft. De mappenstructuur ziet er nu als volgt uit, de naam van de hoofdmap maakt niet uit:



Verder ontvangt u van SBPDDDP uw publieke sleutel. Hernoem dit bestand indien nodig tot *provider.xml* en plaats het in de map *config*. U bent nu klaar om bestanden te pseudonimisatie en te versleutelen voor verzending.

4. Stappenplan / instructie

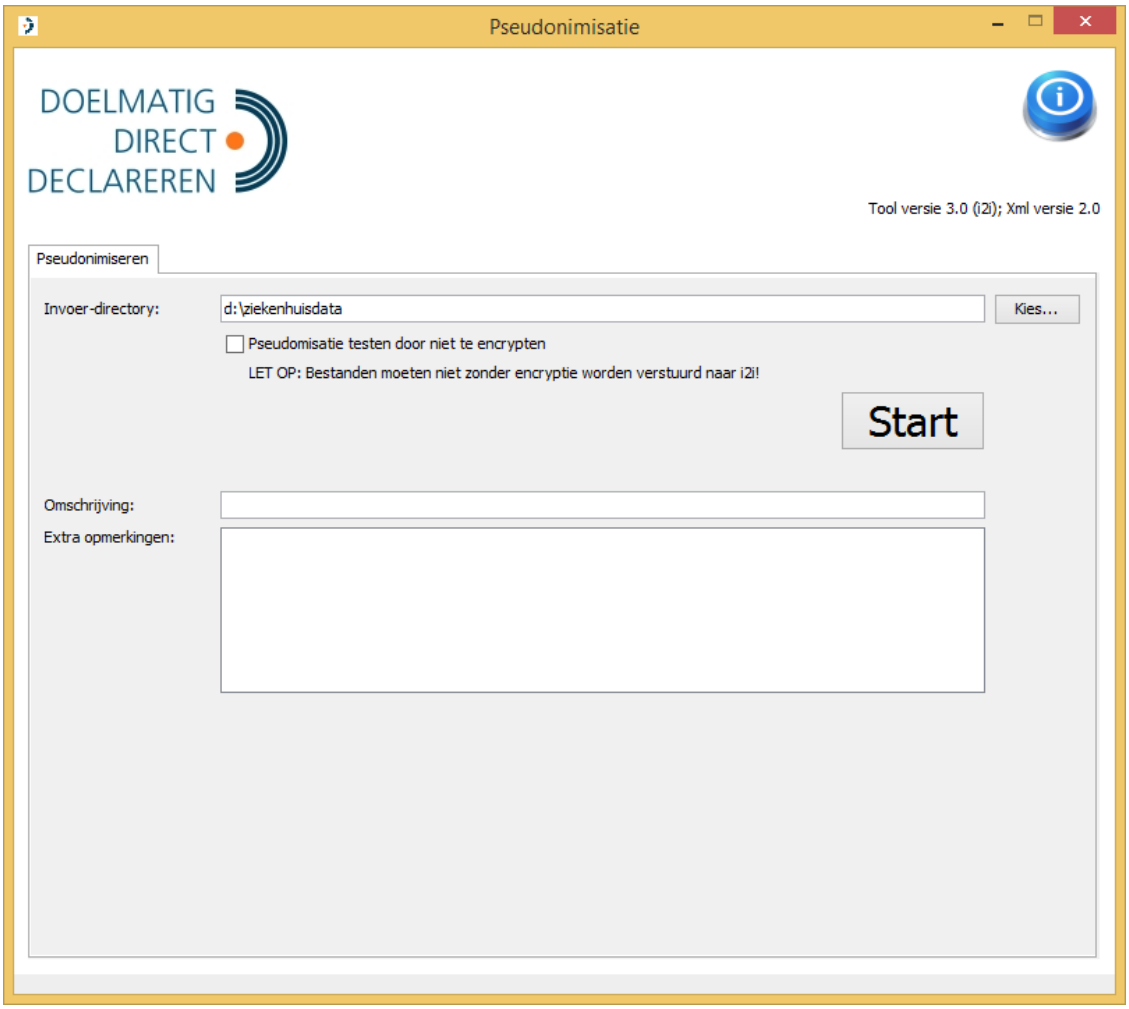
Hieronder volgt de stapsgewijze instructie voor het hele pseudonimsatie- en aanleverproces.

4.1 Klaarzetten bestanden

- Per formaattype alle te pseudonimiseren bestanden klaar te zetten in een folder met lees en schrijfrechten (bijv. folder d:\ziekenhuisdata, d:\farmaciedata). Eventuele subfolders worden ook verwerkt.
- Bestanden kunnen zowel zips zijn als uitgepakte bestanden, maar dienen wel uniform in de folder te staan (alleen zips of alleen uitgepakte bestanden).
- Zip-bestanden moeten niet gecomprimeerd zijn met de DEFLATE64-compressiemethode. Windows gebruikt deze methode standaard als er bestanden groter dan 2 GB worden gecomprimeerd. Daarom moeten bestanden groter dan 2 GB gecomprimeerd worden met het aparte programma *7-zip* (gratis te downloaden op http://www.7-zip.org/).

4.2 Pseudonimiseren en versleutelen

- Start de pseudonimisatietool door te dubbelklikken op pseudo.exe of door de commandlineversie aan te roepen via pseudocmd.exe. De syntax voor pseudocmd.exe is op te roepen door `pseudocmd -help` uit te voeren in de console.



- Selecteer de folder met te pseudonimiseren files.
- Geef via de omschrijving aan welke gegevens worden aangeleverd en voor welke tijdvlak(ken). Extra opmerkingen kunnen ook worden ingevuld.
- Klik op de knop “Start”. De tool herkent automatisch om wat voor type bestanden het gaat.
- Indien alles correct verlopen is, krijgt u een melding dat de tool klaar is. De gezipte verwerkte bestanden staan in een subfolder van de folder met originele files (bijv. d:\ziekenhuisdata\gepseudonimiseerd). Klik op de knop “Ga naar de directory met de gepseudonimiseerde bestanden..” om de Windows verkenner deze directory automatisch te laten openen.
- Indien er fouten opgetreden zijn die u waarschijnlijk zelf kunt oplossen, verschijnen deze op het scherm.
- Indien er complexe fouten opgetreden zijn, maakt de tool hier ook melding van. Gedetailleerde error logging staat op het scherm en in de folder van het programma onder de bestandnaam “log.txt”. We verzoeken u deze samen met een screenshot van de inputmap naar support@i2i.eu te mailen.
- Om de werking van de pseudonimisatie zonder versleuteling te kunnen zien – bijvoorbeeld voor auditing of troubleshooting - kunt u de optie “Pseudonimisatie testen door niet te encrypten” aanzetten. De ZIP-bestanden waarin de gepseudonimiseerde bestanden geplaatst worden zijn dan te openen zonder wachtwoord. Normaliter zijn de gepseudonimiseerde bestanden beveiligd en enkel te openen door SBPDDDP.

4.3 Beveiligd verzenden van bestanden

- De gepseudonimiseerde en versleutelde bestanden kunt u beveiligd uploaden naar SBPDDDP via Zivver, te breieken via de volgende link: https://veilig.doelmatigdirectdeclareren.nl/.