

Handleiding anonimisatie

Behorend bij anonimisatietool

Versie 3.01

Inhoud

1. Inleiding.....	1
2. Systemeisen	2
3. Benodigde software.....	2
4. Stappenplan / instructie	3
4.1 Klaarzetten bestanden	3
4.2 Anonimiseren en versleutelen	3
4.3 Beveiligd verzenden van bestanden	4

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 anonimisatietool ontwikkeld. Dit document is de handleiding behorend bij die anonimisatietool. Voor een functionele beschrijving van de tool kunt u terecht op de website van i2i support: <http://www.i2i.eu/anonimisering/>.

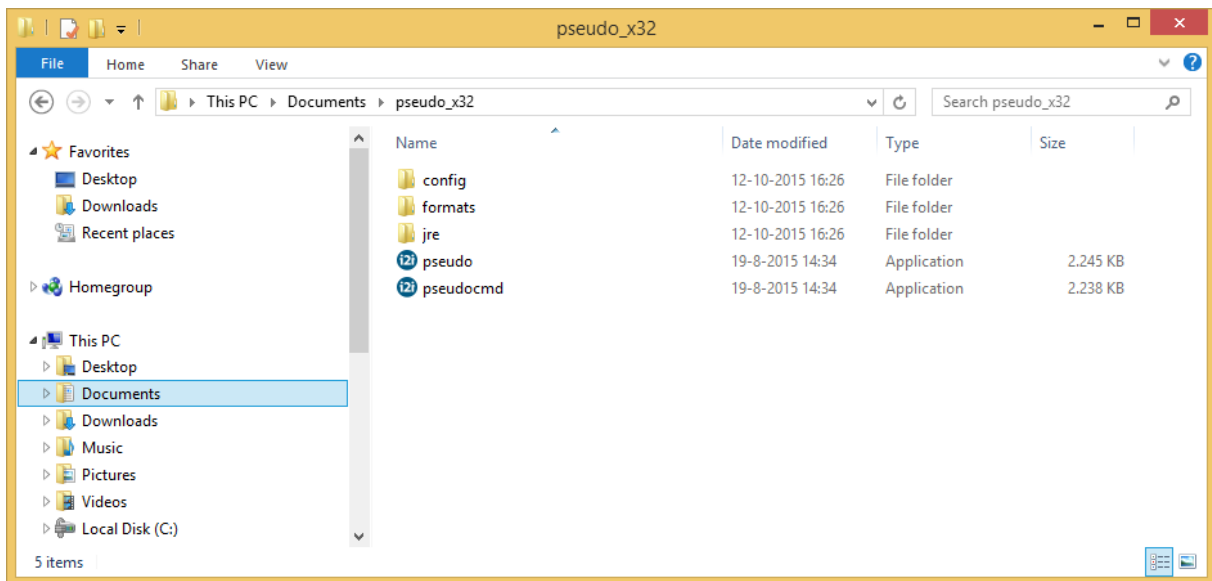
2. Systemeisen

Voor de uitvoer van de anonimatie met de anonimatiETOOL 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. U hebt per e-mail een set configuratiebestanden toegezonden gekregen. Pak deze uit in een map waar u permissie heeft om executables uit te voeren. Download vervolgens de tool via de support website van i2i: <http://www.i2i.eu/anonimisering/>. Pak de voor u gewenste versie uit (32 of 64 bit, afhankelijk van uw systeem) naar de map die u zojuist heeft uitgepakt, waarin ook de mappen "Config" en "Formats" staan. De mappenstructuur ziet er nu als volgt uit, de naam van de hoofdmap maakt niet uit:



Om een nieuwe versie van de anonimeringstool in gebruik te nemen kunt u al deze stappen opnieuw uitvoeren. Let er wel op dat u het bestand provider.xml uit de map "Config" verplaatst van de locatie van de oude versie naar de locatie van de nieuwe versie.

4. Stappenplan / instructie

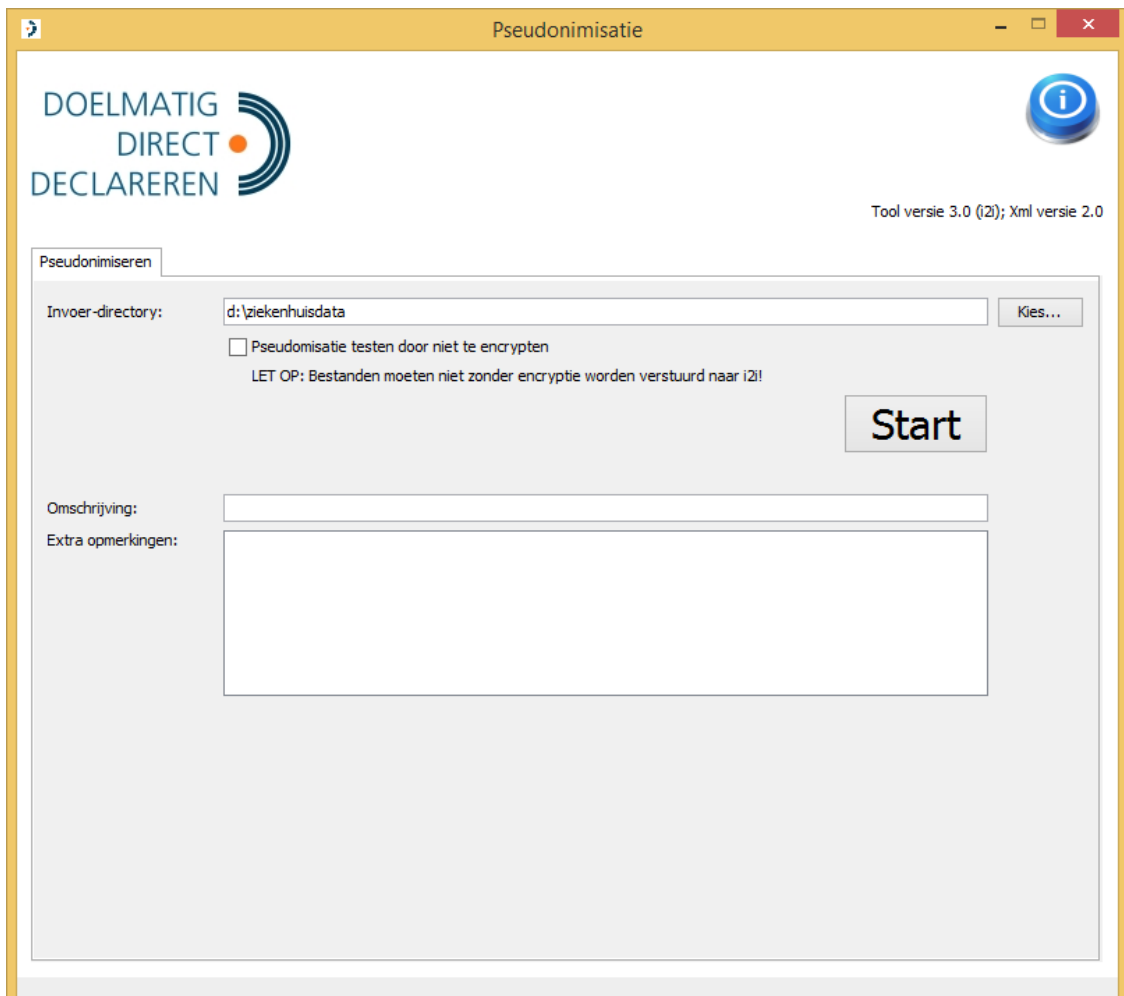
Hieronder volgt de stapsgewijze instructie voor het hele anonimisatie- en aanleverproces.

4.1 Klaarzetten bestanden

- Per formaattype alle te anonimiseren 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 Anonimiseren en versleutelen

- Start de anonimisatietool 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.



The screenshot shows the 'Pseudonimisatie' application window. The title bar reads 'Pseudonimisatie'. The interface features the logo 'DOELMATIG DIRECT DECLAREREN' on the left and a version indicator 'Tool versie 3.0 (i2); Xml versie 2.0' on the right. The main area is titled 'Pseudonimiseren' and contains the following elements:

- An 'Invoer-directory:' field with the text 'd:\ziekenhuisdata' and a 'Kies...' button to its right.
- A checkbox labeled 'Pseudomisatie testen door niet te encrypten' which is currently unchecked.
- A warning message: 'LET OP: Bestanden moeten niet zonder encryptie worden verstuurd naar i2!'.
- A large 'Start' button.
- An 'Omschrijving:' field with a text input area.
- An 'Extra opmerkingen:' field with a larger text input area.

- Selecteer de folder met te anonimiseren 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 gezippte 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 anonimisatie 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 geanonimiseerde bestanden geplaatst worden zijn dan te openen zonder wachtwoord. Normaliter zijn de geanonimiseerde bestanden beveiligd en enkel te openen door SBPDDDP.

4.3 Beveiligd verzenden van bestanden

- De geanonimiseerde en versleutelde bestanden kunt u beveiligd uploaden naar SBPDDDP via de onderstaande link met uw login en password:
<https://secure.doelmatigdirectdeclaren.nl/>.