Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Van:

Afgestemd met:

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 030 274 91 11
info@rivm.nl

memo

DPV_187 Technische Aansluitvoorwaarden CIMS

Datum
15 december 2020

Ons kenmerk

Uw kenmerk

Behandeld door

Kopie aan

Bijlage(n)

1.1 Doel memo

In dit memo worden de manieren beschreven zoals de gegevensuitwisselingen met CIMS gepland zijn. Op volgorde van voorkeur zijn de volgende manieren van uitwisseling voorzien:

1. Uitwisseling via het Landelijk Schakelpunt (LSP)[1].
2. Automatische uitwisseling via een besloten netwerk naar een SFTP server.
3. Automatische uitwisseling via het internet naar een SFTP server.
4. Uitwisseling via zorgmail (onder voorbehoud)[2].

1.2 Uitwisseling middels LSP

Dit is voor CIMS de preferente manier van gegevensuitwisseling. Dit om de volgende redenen: LSP is een zorginfrastructuur dat speciaal ontwikkeld en beveiligd is om medische gegevens van patiënten digitaal met elkaar uit te wisselen. LSP is een gesloten netwerk waarvan de deelnemers bekend zijn.

Uitwisseling middels LSP is momenteel nog niet mogelijk.

1.3 Automatische uitwisseling via een besloten netwerk naar een SFTP server

Indien uitwisseling middels LSP/VZVZ niet mogelijk is kan de gegevensuitwisseling geautomatiseerd plaats vinden door het aanleveren

[1] Nog niet mogelijk, zie paragraaf 1.2
[2] Afstemming vindt momenteel plaats met leverancier zorgmail

van de data[3] bestanden naar de SFTP (FTP over SSH) server via een besloten netwerk. Op het moment van schrijven wordt dit ondersteund via E-Zorg en Diginetwerk.

Voor de uitwisseling gelden de volgende uitgangspunten:

1. Het betreft een push mechanisme vanuit de leverancier naar een SFTP server van CIMS.
2. Per leverancier zal een unieke username worden verstrekt.
3. De authenticatie vindt bij voorkeur plaats via keypair (public/private key). Zie ook paragraaf 2.3 en 2.4.
4. Het systeem van de leverancier zal op IP-adres basis toegang worden verschaft.

1.4 Automatische uitwisseling via het internet naar een SFTP server

Indien een leverancier niet is aangesloten op een besloten netwerk zal de uitwisseling via het internet gaan plaatsvinden. Het betreft hier wederom een automatische uitwisseling van de data bestanden met de SFTP server.

Voor de uitwisseling gelden de dezelfde uitgangspunten als bij transport over een besloten netwerk (zie paragraaf 1.3), met uitzondering van het feit dat authenticatie middels een wachtwoord niet beschikbaar is. Zie voor details paragraaf 2.4.

1.5 Uitwisseling via CIMS mailbox bij zorgmail

Indien automatische aanlevering via de SFTP niet mogelijk is kan de gegevensuitwisseling van het data bestand ook via het zorgmail netwerk, hetzij automatisch of handmatig, plaats vinden.

Voor de uitwisseling gelden de volgende uitgangspunten:

1. De leverancier dient aangesloten te zijn op het zorgmail netwerk.
2. De data bestanden worden als bijlage verstuurd naar de mailbox van CIMS bij zorgmail.
3. RIVM haalt de data bestanden uit de mailbox bij zorgmail op en verwerkt deze in de CIMS database.

[3] Voor het formaat van de data bestanden verwijzen we naar de betreffende documentatie van RIVM/DVP

2. Technische configuratie SFTP

2.1 Inleiding

Dit hoofdstuk beschrijft de technische configuratie van het SFTP pad naar de RIVM server waar de gegevens verzameld worden.

2.2 Protocol

De server is bereikbaar via het SFTP protocol (FTP over SSH) op TCP poort 22. Het publieke IP adres is afhankelijk van de koppeling tussen de leverende partij en het RIVM, en is op aanvraag verkrijgbaar. Het IP adres waarmee de verbinding opgezet wordt dient aan RIVM doorgegeven te worden in verband met IP whitelisting op de firewalls.

2.3 Beveiliging

De voorkeur gaat uit naar beveiliging door middel van keypairs. Hierbij wordt er bij de leverende partij een public/private keypair gegenereerd, en wordt het publieke deel daarvan naar RIVM gezonden. RIVM neemt deze op in de 'authorized keys' lijst van het betreffende account. Voor de versleuteling van de key kunnen verschillende methoden gebruikt worden, aangeraden wordt een RSA key tussen de 2048 bits en 4096 bits.

De ondersteunde ciphers (toegestane encryptie-methoden) van de SFTP server bij RIVM zijn 'aes128-ctr', 'aes192-ctr' of 'aes256-ctr'. Dit betreft de versleuteling van het transport. Mogelijk worden er in de toekomst meerdere ciphers aan de lijst toegevoegd.

Hoe deze zaken aan de kant van de leverende partij geconfigureerd en gegenereerd moeten worden hangt af van het Operating System en de gekozen software voor het opzetten van de SFTP verbinding.

2.4 Wachtwoord authenticatie

Authenticate door middel van een wachtwoord wordt uitsluitend toegestaan indien de keypair methode niet kan worden gebruikt, bijvoorbeeld doordat de software bij de leverende partij dat niet ondersteunt. In dat geval levert RIVM een automatisch gegenereerd wachtwoord aan, dat tevens periodiek vervangen wordt, afhankelijk van het beveiligingsbeleid.

Wachtwoord-authenticatie wordt niet toegestaan indien het transport over internet plaatsvindt, maar alleen voor transport over een besloten netwerk.

2.5 Aanlevering

Na inloggen op de SFTP server dient de betreffende file in de submap 'incoming' geplaatst te worden. Let wel: het is niet mogelijk om bestanden te plaatsen in de homedirectory (map waar men initieel binnenkomt).