Memo

Nictiz Betere gezondheid door betere informatie

Van	**:**	Lisanne van der Molen
Datum	**:**	16 mei 2019
Onderwerp	**:**	Terugkoppeling sessie 2 infrastructuur eOverdracht

---

In navolging van de deelsessies 'infrastructuur eOverdracht' tijdens de leveranciersbijeenkomst voor het programma InZicht op 18 april, heeft op 16 mei een tweede sessie plaatsgevonden. Tijdens deze sessie zijn we nader ingegaan op de punten 1 t/m 5 uit de eerste memo: identiteit/authenticatie, adressering, logging, metadata en technisch uitwisselprotocol. Zoals in de eerste sessie besproken blijven toestemming en versiebeheer buiten beschouwing voor de afspraken die we met elkaar maken voor de korte duur van de proeftuinen.

Gedurende de sessie zijn over de volgende (minimale) onderwerpen afspraken gemaakt:

1. **Identificatie en authenticatie**
   Gedurende de proeftuinen kiezen we voor een simpele oplossing: server-server uitwisseling, waarbij er één aansluiting (technisch adres) is per geadresseerde. Identificatie vindt plaats aan de hand van hostnames, authenticatie aan de hand van X.509-servercertificaten. Partijen vertrouwen elkaars certificaten, zolang deze aan de ICT-beveiligingsrichtlijnen voor TLS voldoen (zie punt 5).

   Voor het ondertekenen van certificaten kan gebruik worden gemaakt van een derde partij (certificaatdienstverlener), of kan self-signing worden toegepast. Als informatie moet worden uitgewisseld om een certificaat te kunnen vertrouwen, zorgen partijen er samen voor dat deze informatie zodanig wordt uitgewisseld dat de authenticiteit van de andere partij afdoende zeker wordt gesteld.

2. **Adressering**
   Adresuitwisseling vindt onderling plaats. Het technische adres bestaat uit een URL van het FHIR-endpoint, waarbij de hostname uit de URL moet matchen met het certificaat.

3. **Logging**
   Onverminderd bestaande wet- en regelgeving en afspraken tussen leverancier en zorgaanbieder of derden, loggen verzender en ontvangen in de proeftuin ten minste:
   a. Welke FHIR-operatie heb je op welk end point gedaan (met timestamp)?
   b. Welke response code kreeg je terug (met timestamp)?
   c. Wat was het ID van het bericht?

   Voor A, B en C is het niet nodig persoonsgegevens te loggen; de afspraken in deze proeftuin leggen dus geen verplichting daartoe op.

4. **Metadata uitwisselen**
   Veel FHIR-elementen zijn relevant als metadata. Zie https://informatiestandaarden.nictiz.nl/wiki/vpk:V3.1_FHIR_eOverdracht voor het technisch ontwerp behorende bij het bericht dat voor de proeftuinen eOverdracht is gedefinieerd. Op dit moment zijn er geen additionele behoeften ten aanzien van metadata.

5. **Technisch interacteren**
   FHIR zegt veel over interactie. Ten aanzien van de FHIR-profielen is afgesproken om ten minste JSON te gebruiken. Dat betekent dat een partij altijd JSON moet ondersteunen wanneer dit door de wederpartij wordt gevraagd, en geen XML hoeft te ondersteunen wanneer de wederpartij dat vraagt.

   Er is afgesproken gedurende de proeftuinen te werken met de zibs uit zib publicatie 2017 en de daarbij behorende FHIR profielen.

   Ten aanzien van de beveiliging van het transportkanaal wordt gebruik gemaakt van TLS. Hierbij is gekeken naar de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC (https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html), versie april 2019. Ten aanzien van de proeftuinen eOverdracht volgen we het scenario 'alleen controle over de servers' waarbij we alleen niveau 'goed' hanteren. In aanvulling op de richtlijn gebruiken we alleen TLS v1.3 (en niet v1.2, ook al is die als 'goed' gekwalificeerd). De verplichte OCSP-stapling geldt niet gedurende de termijn van de proeftuinen, omdat er geen gebruik hoeft te worden gemaakt van certificaatdienstverleners. OCSP-stapling is echter wel toegestaan.

   Partijen zijn vrij in de keuze van een netwerk voor datacommunicatie. Daarbij mag een partij niet forceren dat er gebruik wordt gemaakt van een netwerk dat bij een andere partij niet aanwezig is. Elk van de partijen heeft daarom het recht gebruik te maken van het Internet en van de andere partij te verlangen dat hij daar voor de betreffende uitwisseling ook gebruik van maakt.

Bovenstaande uitwerking is een weergave van de discussie zoals deze heeft plaatsgevonden tussen de aanwezige leveranciers, en is gebaseerd op gemeenschappelijke kennis. Ten aanzien van de uitwerking is geen specifieke expertise ingeroepen. Bij de uitwerking is ervoor gekozen om in technische termen op te schrijven wat is besproken en in enkele gevallen een platformvoorstel gedaan (zodat er op iets concreets gereageerd kan worden) naar aanleiding van een uitzoekpunt. Review door de leveranciers is noodzakelijk. Leveranciers moeten altijd aan de relevante eisen (wet- en regelgeving en overige verplichtingen) blijven voldoen, deze afspraken doen daar niet aan af. Vanuit Nictiz hebben we bemiddeld in de discussie, waarbij bovenstaande geen advies vanuit Nictiz of andere partijen is. De uiteindelijke verantwoordelijkheid blijft bij de leveranciers.