Reactie VZVZ op consultatie Health Tools Interoperability (HTI) als (kandidaat) bouwsteen voor het duurzaam informatiestelsel in de zorg

Geachte Informatieberaad Zorg,

VZVZ heeft met interesse het voorstel doorgelezen en reageert hierbij op de open consultatie rond HTI.

Samenvatting

Wij adviseren HTI niet op te nemen als (kandidaat)bouwsteen voor het DIZ. Het is op dit moment niet duidelijk welke meerwaarde HTI biedt boven internationale standaarden en profielen.

De functionaliteit van HTI is beperkt tot het starten van applicaties. HTI is daarmee eigenlijk geen protocol maar een beschrijving van een gesigneerde JSON Web token dat naar één lancerende partij wordt verstuurd. HTI zou als toolkit meer bouwstenen moeten bevatten, voordat het ingezet zou kunnen worden als een volwaardig Health Tools Interoperability component. Ter vergelijking wordt verwezen naar SMART App Launch, dat nauw geïntegreerd is met FHIR en gebruik maakt en refereert naar de IETF-standaarden en het Oauth2 (Open Autorisatie) protocol. Dit raamwerk verbindt applicaties van derden met EPD-gegevens, waardoor eHealth modules van binnen of buiten de gebruikers interface van een (EPD) systeem kunnen worden gestart. Na het lanceren van een eHealth module, kan deze eHealth module m.b.v. een context parameter de context bij een autorisatie server ophalen, als de eHealth module daarvoor de juiste autorisatie rechten voor heeft gekregen. Daarmee biedt Smart App Launch vergelijkbare functionaliteit als HTI.

Scope, context en mogelijkheden van gebruik van HTI is moeilijk vast te stellen op basis van beschikbare documentatie. De documentatie (GIDS Open Standaarden) lijkt incompleet. Wij missen referenties naar technische en inhoudelijke standaarden en de documentatie loopt achter in vergelijking met de huidige LTI en internationale standaarden waarop HTI is gebaseerd. LTI is inmiddels uitgebreid waarmee allerlei interacties tussen partijen ondersteund en de documentatie beschrijft deze in detail. Deze uitwerking van LTI-ontwikkelingen zou ook in HTI meegenomen moeten worden .

HTI wordt nu beproefd in Koppeltaal 2.0. In het (aanpalende) toepassingsgebied van HTI zijn de standaarden/profielen SMART on FHIR en het IHE IUA profiel, met de onderliggende standaarden zoals Oauth2.0 en OpenID Connect (allen op basis van JWT) nog in ontwikkeling, gezien er regelmatige nieuwe RfC's voor Oauth2.0 uitkomen. Nu al een keuze maken voor HTI met, 1) een beperkt toepassingsgebied en 2) als extensie op een standaard die zich ook nog niet bewezen heeft (SMART on FHIR) is daarom voorbarig. Indien de toegevoegde waarde van HTI is bewezen zou het logischer zijn dat het eerst wordt toegevoegd wordt aan de internationale SMART on FHIR-specificaties, waarna het geheel (HTI en Smart on FHIR) als potentiële bouwsteen zou kunnen worden ingediend. Hier loopt ook al een traject voor.

Inleiding

HTI staat voor Health Tools Interoperability, en beschrijft zichzelf als een open technisch protocol, waarmee eHealth- en portal-leveranciers zonder persoonsgegevens aan elkaar te verstrekken, met elkaar kunnen integreren. Bijvoorbeeld “vanuit een digitaal wijkplatform opent een bezoeker direct een eHealth-module. Het verstrekken van een e-mailadres of persoonsgegevens is daarbij niet nodig. HTI helpt om het gedoe op de achtergrond tussen ICT-leveranciers en aanbieders van techniek of concurrentie voor de gebruiker relatief onzichtbaar te maken."

Integratie is het bij elkaar brengen van diverse (internationale) componenten/subsystemen om ervoor te zorgen dat alle subsystemen met elkaar functioneren als een systeem. Op het vlak van informatietechnologie is systeemintegratie het proces dat verschillende systemen en applicaties fysiek of functioneel aan elkaar koppelt. Bedrijfsmatig moeten de juiste mensen op het juiste moment beschikken over de juiste informatie die nodig is om hun werk te doen.

Wat is HTI eigenlijk voor component?

HTI wordt gebruikt voor het kunnen opstarten van een module met een specifieke taak vanaf een portaal (browser). HTI is een protocol dat peer-to-peer tussen de portaal en module aanbieders wordt geïmplementeerd.

Module aanbieders kunnen in aanvulling op HTI profielen gebruiken om de gebruiker nader te identificeren en om verdere dataverwerking aan de gebruiker te 'koppelen'. Hoe dat precies in zijn werk gaat, is niet uit de documentatie te halen. Welk HTI-profiel men tot bouwsteen wil verheffen wordt niet duidelijk in de Gids Open Standaarden.

De Gids Open Standaarden

In de open consultatie voor HTI wordt er verwezen naar de "Gids Open Standaarden". In deze "Gids Open Standaarden" staat HTI beschreven als "protocol". De gids somt een verzameling aan voordelen van HTI op waarbij een aantal kanttekeningen geplaatst kunnen worden:

- Het gebruik van JWT in plaats van OAuth 1.x.
    - JWT is een beschrijving van het formaat van een JSON Web token en OAuth is een autorisatie protocol beschrijving. Er zijn echter geen referenties naar RFCs van de IETF-standaarden, IMS Global Learning Consortium (LTI) of de samenwerking met (open) standaarden
- Alignen met de HL7 FHIR standaarden.
    - HTI geeft een (FHIR) Task resource in een token mee, maar er is verder geen alignment met FHIR beschreven. Onduidelijk is wie de FHIR Task resource beheert, hoe de originele FHIR Task resource geupdate kan worden en hoe andere resources geraadpleegd kunnen worden die in de FHIR Task resource worden gerefereerd.
- Er is geen persoonlijke data, tijdens een launch aanwezig.
    - Dit is standaard onderdeel van het OAuth2/OpenID Connect protocol (Single Sign-On). Bij een SSO-protocol (in een JWT) wordt geen persoonlijke data meegestuurd, alleen een issuer id en subject id. In die zin is dat niet een specifiek voordeel van HTI. De gebruiker dient ook geauthenticeerd en geautoriseerd te worden, wat met dezelfde technologie kan worden gedaan. Daarom zou je het geheel ervan moeten bezien en niet slechts een klein stukje ervan tot bouwsteen te verheffen.
- Beperkingen op beveiliging, privacy en delen van data.

- Bij berichtenuitwisseling, bij launching via een webbrowser, moeten berichten getekend worden om de integriteit van de berichten te kunnen waarborgen. Dit is niet specifiek een voordeel van HTI, maar wordt zou in zijn algemeen toegepast moeten worden.

Is HTI als component bruikbaar in de zorg

"HTI helpt om het gedoe op de achtergrond tussen ICT-leveranciers en aanbieders betreffende techniek of concurrentie voor de gebruiker relatief onzichtbaar te maken."

Een aantal opmerkingen hierover:

- De architectuur die door HTI wordt beschreven, is een Non-Web services gebaseerde architectuur. Zie voorbeeld van HTML-form dat gepost wordt.
- De authenticatie en autorisatie is gebaseerd op OAuth2/OpenID Connect. Zie de vorige opmerking over SSO. Er moet dus ook een component zijn, die een gebruiker authentiseert.
- HTI maakt alleen gebruik van de FHIR Task resource, maar maakt niet gebruik van de FHIR-koppelvlaktechnologie dat op (FHIR) REST APIs gebaseerd is om gegevens uit te kunnen wisselen. Niet beschreven wordt hoe de referenties, van de FHIR Resource Task gecontroleerd of gevalideerd kunnen worden. Bij FHIR is er sprake van een aanbieder die volgens specificaties (informatie) diensten aanbiedt aan afnemers. Er wordt dus gedacht en ontworpen in termen van diensten, niet in termen van (lanceer) berichten. Dit wordt niet nader beschreven in de "Gids Open Standaarden".
- HTI maakt geen gebruik van een autorisatie dienst. Het is niet duidelijk hoe de lancerende partij kan valideren dat de FHIR Task resource uitgevoerd mag worden of wie x de lancerende partij authentiseert en autoriseert.
- HTI biedt geen bi-directionele communicatie tussen partijen, maar eenzijdige communicatie. Er worden gesigneerde tokens (JWT) gebruikt bij het lanceren van applicaties.
- Alle partijen die HTI gebruiken, zouden minimaal kennis moeten hebben van de IETF-standaarden (niet beschreven in de "Gids Open Standaarden"). Op deze standaarden is namelijk HTI gebaseerd, zie:
    - JWS (JSON Web Signature RFC7515)
    - JWE (JSON Web Encryption RFC7516)
    - JWK (JSON Web Key RFC7517)
    - JWA (JSON Web Algorithms RFC7518)
    - JWT (JSON WEB Tokens RFC7519)
- De gelanceerde module moeten verschillende JWS-algoritmes ondersteunen, moet de publieke sleutel van de issuer (lancerende partij) hebben, moet de issuer id weten en moet via een beveiligde verbinding de launch URL kunnen doorgeven. Dit geldt voor elke partij die HTI wil gaan gebruiken. Het is niet duidelijk hoe de FHIR Task resource in sync blijft, tussen de aanbiedende en afnemende partijen indien er meer dan 1 portaal wordt gebruikt.

HTI is niet meer dan een protocol dat peer-to-peer tussen één portal en één module aanbieder een lanceerbericht uitwisselt. Er is verder geen sprake van informatie-uitwisseling, na het lancering of starten van een module. Over het beheer en de manier van uitwisseling van de (geheime en publieke) sleutels wordt niet gerept.

Is HTI als nationale standaard noodzakelijk?

DIZRA benoemt als uitgangspunt het gebruik van internationale standaarden. De reden hiervan is de kleine reikwijdte van Nederland in de zorg en de slagkracht op internationaal gebied. HTI is geen (internationale) standaard, terwijl er voor dit soort toepassingen er wel internationale standaarden zijn, zoals het SMART App Launch van HL7 FHIR. Het SMART App Launch biedt ons inziens meer mogelijkheden. SMART zorg voor identiteit- en toegangsmanagement, toegangscontrole tot informatie en geeft de launch context door aan een geautoriseerde module die opgestart wordt. Verder kan het SMART App Launch Framework een app in de context van een EPD, portaal of stand-alone opstarten. Daarnaast biedt IHE IUA profiel voor dit soort toepassingen ook een optie.