

20.9.2013

Valtionvarainministeriö
Julkisen hallinnon ICT-toiminto

VIITE: Lausuntopyyntö VM008:00/2013

LAUSUNTO**Kansallisen palveluväylän viitearkkitehtuurista sekä sen alustavasta toteutussuunnitelmasta.****Yleistä**

Medi-IT Oy on kahdeksan sairaanhoitopiirin omistama yhtiö, joka tuottaa sote-ict-sektorin hyvinvoinnin ratkaisuja ja järjestää omistajien toimintaa tukevia ict-palveluja. Lausunnossamme tarkastelemme kansallista palveluväylää pääasiassa sote-sektorin näkökulmasta. Lähtökohtana on huolehtia nykyisten tietojärjestelmäkokonaisuuksien kehittämisestä samaan aikaan, kun kansallista palveluväylää rakennetaan. Toinen painotus on kansallisen palveluväylän mahdollisuudet kansalaisen sähköisen asioinnin kehittämisen kannalta. Sähköisessä asiointissa on meneillään ylimaakunnallinen yhteistyö Hyvis.fi-palveluiden kehittämisessä ja käytössä.

Medi-IT:n näkemys on, että kansallisen palveluväylän arkkitehtuuri kuvatulla tasolla luo mahdollisuuksia erityisesti kansalaiselle tarjottavien palveluiden kehittämiseen. Organisaatioiden välinen yhteistoiminta on toinen osa-alue, mutta sekin linkittyy lopulta kansalaisen kokemaan palveluun. Mitä sujuvampaa on organisaatioiden välinen yhteistoiminta, sitä helpommin ja vaivattomammin voidaan kansalaiselle tarjota palveluja, jotka eivät ilman kansallisen palveluväylän yhtenäistä tapaa kytkeä toimijoita toisiinsa olisi niin helposti saavutettavissa.

Oleellista on hahmottaa palveluväylän mahdollistama palvelujen verkosto (ekosysteemi) riittävän erillään teknisestä toteutuksesta.

Kansallisen palveluväylän arkkitehtuurissa ja toteutussuunnitelmassa on huomioitu peruspalvelut ja perustietolähteet, jotka ovat ehdottomia edellytyksiä väylän täysimittaiselle hyödyntämiselle. Tällainen on esimerkiksi tunnistamispalvelu. Medi-IT on kuitenkin tunnistanut mahdollisuuksia suorittaa teknisiä kokeiluja niin, että peruspalvelut liitetään myöhemmin mukaan. Kansallista palveluväylää on mielestämme mahdollista alkaa kokeilemaan nopeastikin.

Lausuntopyyntö koskee kansallisen palveluväylän viitearkkitehtuuria ja alustavaa toteutussuunnitelmaa. Näitä on tarkoitus tarkentaa jatkotyössä. Lausunnossamme on kuitenkin jo viittauksia teknisiin ja muihin käytännön toteutuksiin, koska ne voivat auttaa jatkotyön suunnittelussa. Näiden yksityiskohtien kautta olemme samalla arvioineet alustavan toteutussuunnitelman realistisuutta. Yhteenvetona voi todeta, että viitearkkitehtuuri sinänsä on riittävän kattava jatkotyön aloittamiseksi. Jatkotyössä tehtävissä teknisissä kokeiluissa tulee kuitenkin esiin ratkaistavia käytännön kysymyksiä, joiden selvittämiseen pitää varata riittävästi resursseja.

20.9.2013

Tärkeää on huolehtia siitä, että palveluväylän toteuttamiseen ja hallintaan liittyvä päätöksenteko pystyy vastaamaan teknisten kokeilujen esiin tuomiin asioihin nopeasti.

SOTE-sektorin osalta merkittävä kysymys liittyy olemassa olevien vyöhykkeiden liittämiseen kansalliseen palveluväylään. Käytännössä tämä tarkoittaa KanTa-palveluiden ja kansallisen palveluväylän roolitusta, josta ei selvittäne ilman lainsäädännöllisiä muutoksia. Lakimuutokset vievät aikaa, joten mielestämme on järkevää aloittaa SOTE-sektorin kytkeminen palveluväylään sellaisista palveluista, joissa KanTa-yhteensopivuus ei ole ehdoton edellytys.

Kaiken kaikkiaan palveluväylän mahdollisuuksien täysimittainen hyödyntäminen vaatii käyttäjä- ja kehittäjäorganisaatioissa ajattelutavan muuttamista. Perinteisesti potilaan on esimerkiksi pitänyt muistaa, mitä kaikkea hoitoa hänen vapaaehtoinen sairausvakuutuksensa kattaa. Voisiko terveydenhuollon organisaatio kysyä tuon tiedon suoraan vakuutusyhtiöltä potilaan suostumuksella? Palveluväylän rakentamisen ja käyttöönoton yhteydessä on tuettava teknisen toteutuksen lisäksi myös toimintatapojen uudelleen miettimistä.

Yksityiskohtaisemmat kommentit

Viitearkkitehtuuri

Viitearkkitehtuurin kohderoolit ja kuvaileva materiaali

Kohderooleissa on kuvattu, kenelle viitearkkitehtuuri on suunnattu. Kansallisen palveluväylän mahdollistama palveluiden verkosto (ekosysteemi) on käsitteenä sellainen, että viitearkkitehtuuridokumentti ei saa olla ainut palveluväyläajatteluun johdettava dokumentti. Luetelluille kohderooleille sekä erityisesti muulle asiasta kiinnostuneelle yleisölle on tuotettava myös kuvailevampaa tukimateriaalia, josta esimerkkinä on *Kansallinen palveluväylä - konsepti, tavoitteet ja ratkaisumalli* – dokumentti. Tällaisessa tukimateriaalissa tulisi kuvata, miten palveluväylään kytketyistä palveluista muodostetaan aitoja arvoketjuja, esimerkiksi palveluseteli - miten julkinen / yksityinen sektori liitetään prosessi / palveluväylä - informaatio näkökulmasta yhteen.

Vyöhykemalli

”Vyöhykemallia tulee hyödyntää vain niissä erityiskohteissa, joissa ei ulkoisista reunaehdoista tai aikaisempien investointien takia voida käyttää kansallisen palveluväylän tiedonvaihtoinfrastruktuuria.”

- Edessä on jonkinlainen siirtymäaika. Nopeasti tarvitaan näkemystä ja kokemusta siitä, mitkä olisivat mahdollisesti nk. kiellettyjä käyttötarkoituksia...

20.9.2013

Toteutussuunnitelma

Käsitteet

Toteuttamissuunnitelmassa puhutaan välityspalvelinohjelmistosta (5.4.15, s. 26, 6.1.5, s.30) ja liityntäpalvelinohjelmistosta (5.4.3, s.19). Tässä on ilmeisesti samalla asialla kaksi eri nimeä?

Sivulla 30 lukee *"Keskuspalvelin tarkistaa välityspalvelimen IP-osoitteen perusteella sen DNS-nimen ja käyttää sitä palveluväylän sisäisen DNS-nimen muodostamisessa (sovellus.firma.fi muotoon sovellus.firma.palveluvayla.fi)." Kyseessä lienee esimerkki – käytännössä ei voida olettaa, että organisaatioilla on aina .fi -domain? Sulkujen sisään voisi selvyiden vuoksi lisätä 'esimerkiksi'.*

Teknologiakokeilut

Medi-IT:n kannalta mahdollisia kokeilukohteita löytyy kahdentyyppisiä:

- Ratkaisut, joilla *korvataan jokin olemassa oleva palvelu suoraan*. Esimerkkinä VTJ-päivitys.
- Ratkaisut, joissa *toteutetaan samalla uusi palvelu, tai tapa toteuttaa jokin palvelu*. Esimerkkeinä potilaan vakuutustietojen kysely vakuutusyhtiöstä, B-lausunto sähköisessä asiointissa, tai yhteenvetotietojen tuottaminen uudesta, tiettyä potilassegmenttiä tukevasta palveluportaalista.

Näistä ensimmäisillä tapauksilla (korvataan suoraan) on kaikkein suoraviivaisinta kokeilla palveluväylän toteutusta, mutta uutta lisäarvoa ei vielä juurikaan synnytetä. Tällaiset tapaukset sopisivat esimerkiksi palveluväylän perusrakenteiden (sanomakehys, sopimuskäytännöt, palvelukatalogi) testaamiseen.

Terveystietojenhuollossa olemassa olevan vyöhykemallin purkaminen vaatii muutoksia lainsäädäntöön. Vähintään niiltä osin, kuin KanTa-palvelut liitetään palveluväylään.

Teknologiakokeiluiksi tulisi valita sopivan pieniä kohteita, mutta kuitenkin sellaisia, joilla olisi mahdollisuuksia jatkaa suoraan varsinaiseen tuotantovaiheeseen.

Kun teknologiakokeiluissa tarvitaan ongelmanselvitystä palveluita rakennettaessa, saadaan kokemusta myös palveluväylän operaattori- ja hallintatoiminnan kehittämiseksi.

Samanaikaisesti teknologiakokeilujen kanssa tulisi varmistaa, että tieto käytännön kokemuksista ja ratkaisuista leviää eri osapuolille riittävästi. Tämä ei kuitenkaan saisi jäädä teknologiakokeiluissa mukana olevien käytännön toteuttajien vastuulle. Kansallinen palveluväylä on konseptina jokseenkin hankalasti käsitettävä, joten ymmärryksen kasvattaminen *käytännön toteutusten* kautta olisi tärkeää.

Riskeistä

"Organisaatiot eivät valmistaudu ajoissa väylän käyttöönottoon."

Medi-IT Oy haluaa vaikuttaa tämän riskin hallintaan osallistumalla aktiivisesti teknologiakokeiluihin, joiden kautta tuotetaan käytännön tietoa palveluväylään liittymisestä ja siihen valmistautumisesta, erityisesti SOTE-sektorin osalta.

20.9.2013

Valmistautumisessa on huomioitava aiemmat kokemukset vastaavantyyppisten kansallisten tai muuten laajojen hankkeiden läpiviennistä.

Kustannukset

Kustannusten synty- ja jakoperusteet tulee olla mahdollisimman selkeästi määritelty mahdollisimman aikaisesti. Julkisten organisaatioiden ja palvelujen kehittäjien ensimmäisiä kysymyksiä on: "Mitä tämä maksaa meille?"

Suunnitelman mukaan organisaatioiden tulee hankkia itse riittävän korkeakapasiteettinen ja korkealaatuinen internetliittymä. Tämä linkittyy palvelutasokysymyksiin ja liittyjälle asettaviin vaatimuksiin. Tulevaisuudessa koosteiset palvelut tullevat olemaan riippuvaisia hyödyntämiensä osa-palveluiden kapasiteeteista ym. palvelutasotekijöistä. Ovatko palveluväylään liittyneet palveluntuottajat tällöin vastuussa riittävästä palvelutasosta palveluväylälle vai toisilleen? Tukeeko palveluväylän sopimushallintapalvelu/Tiedovaihtosopimus myös näitä eri toimijoiden välisiä sopimuksia?

Aikataulusta

Esitetty aikataulu on kovin tiukka. Myös lievennetty vaihtoehto. Tämä ei kuitenkaan tarkoita, että aikataulusta pitäisi heti joustaa. Päinvastoin, jatkokehityssuunnitelmaa pitää työstää ja konkretisoida mahdollisimman aikaisessa vaiheessa, jotta uskottavuus säilyy ja toimijat sitoutuvat tähän. Aikataulujen realistisuus selviää lopullisesti vasta tekemällä.

Yleisellä tasolla optimistisen aikataulun toteutus vaatii uudenlaista ja innovatiivista työskentelytapaa organisaatioille - lisää dynaamisuutta ja ketteryyttä.

SOTE-sektorilla oman haasteensa tuo eArkiston yhtälailla tiukka aikataulu. Osa todennäköisistä kansalliseen palveluväylään liittymisen toteuttajista osallistuu tiivistä myös eArkiston käyttöönottoon.

Muita yksityiskohtia, jotka liittyvät lähinnä käytännön toteutukseen

Viitearkkitehtuurin ja toteutussuunnitelman pohjalta laadimme alustavia suunnitelmia erilaisten palveluiden toteuttamisesta kansallisen palveluväylän arkkitehtuurin mukaisesti. Seuraavassa on listattu joitakin käytännön kysymyksiä, jotka nousivat esiin. Yksityiskohtaiset vastaukset eivät kuulu viitearkkitehtuurin piiriin, joten nämä on koottu omaksi kokonaisuudekseen.

- Organisaatioiden verkot ovat vielä IPv4-maailmassa ja osittain joudutaan käyttämään privaattiosoitteita ja NATia, jolloin liityntäpalvelimien näkyvyys palveluväylän keskuspalvelimelle ja toisille liityntäpalvelimille on rajattu; liityntäpalvelimella pitänee olla julkinen IP-osoite, mutta edelleenkin organisaatio sijoittaa sen liittymän palomuurin taakse, jolloin tarvitaan tiedot palomuriavauksista vai kuinka tämä on ajateltu?
- Pitäisikö tässä ottaa kantaa jo IPv6:seen?

20.9.2013

- Organisaatiolla on käytössä palomureja, joten selvitettäväksi jää, miten liikennöinti hajautetussa palveluväylässä toteutetaan eri liityntäpalvelimien ja keskuspalvelimen välillä.
- Liityntäpalvelimen ohjelmisto on käytännössä virtuaalipalvelin, jonka organisaatio asentaa verkkoonsa. Onko tämän sijoittelussa organisaation verkossa merkitystä palveluväylän tai organisaation näkökulmasta? DMZ tai joku muu?
- Voisiko toteuttamissuunnitelman protokollat koota taulukkoon tyyliin HTTP Over TLS/HTTPS, NTP, DNSSEC jne. ja niiden kaavailut käyttötarkoitukset? Lisäksi olisi syytä ymmärtää, mitä nämä protokollat tarkoittavat palveluväylässä tietoliikenteen osalta esim. organisaation palomuriin tarvittavat konfiguraatiot liityntäpalvelimien osalta.
- Varmennepalveluissa pitäisi huomioida CA-varmenteet jotenkin, osana liityntäpalvelimen ohjelmistoa?
- Itseprovisioinnissa voi mahdollisesti aiheuttaa poikkeuksen kirjaamalla DNS:n reverse zone:en jonkin toisen liityntäpisteen DNS-nimen. Tämän tyyppiset poikkeukset pitäisi käsitellä jotenkin.
- Liityntäpalvelimia valvoo ja varmistaa ilmeisesti organisaatio itse. Tähän tarvitaan joku rajapinta.
- Onko lokitiedot mahdollista tallentaa paikallisen ratkaisun lisäksi erilliseen lokipalveluun organisaation sisällä? Esim. syslog -tyylinen palvelu organisaation hallinnoimalle lokipalvelimelle?

Kotkassa, 20.9.2013

Timo Koivu
ToimitusjohtajaMedi-IT Oy
Tel. +358 (0)44 223 1514
timo.koivu@medi-it.fi
Heikinkatu 7, 48210 Kotka