Tekninen Ohje

Palveluväyläliitäntöjen valmistelun tueksi

V0.92

6.2.2015

AKUSTI

Alueiden ja kuntien sosiaali- ja terveydenhuollon
tietohallintoyhteistyöfoorumi

Kuntaliitto
Kommunförbundet

Versio	Muutos	Tekijä	pvm
0.1	Dokumentin alustava rakenne	Tiera (Janne Ollenberg, Mikael Puusa ja Jaana Siitari)	27.11.2014
0.2	Tekninen tarkistuslista	Tiera	28.11.2014
0.3-0.5	PSOP-projektiryhmä haastattelu, KaPA-seminaarin pohjalta dokumentin täydennys	Tiera, PSOP-projektiryhmä	28.11 - 10.12.2014
0.6	VRK haastattelut ja Kela kommentit	Tiera, VRK (Eero Kontta-niemi, Petteri Kivimäki)	10.12 - 15.12.2014
0.7	AKUSTI ja Kuntasektori KA-ryhmä kommentit	Tiera	19.12.2014
0.8	Kommenttien pohjalta viimeistely	Tiera	19.12.2014
0.9	Siirto AKUSTI-pohjalle ja johdannon täydennys	Tiera	12.1.2015
0.91	Kommentit VM ja VRK huomioitu	Tiera	15.1.2015
0.92	Palveluväylä viimeisin tiedote huomi-oitu	Tiera	6.2.2015

Sisällysluettelo

1. Johdanto 3

2. Sanasto 4

3. Yleistä 4

4. Väylän rakenne ja periaatteellinen toteutus 5

4.1. Lokitus ja tietoturva 6
4.2. Keskuspalvelin 6
4.3. Liityntäpalvelin 7
4.4. Liityntäpalvelimen toteutuksen vaihtoehdot 7
4.4.1. Jaetun liityntäpalvelimen käyttö 7
4.4.2. Oma liityntäpalvelin 7
4.4.3. Kahdennettu liityntäpalvelin 8
4.4.4. Toimialueittain jaettu liityntäpalvelin 8
4.5. Palveluväylien välinen federointi 8
4.6. Turvamoduuli 8
4.7. Rajapintakuvaukset 9
4.8. Käyttäjätunnisteet 9
4.9. Sanomanvälityksen periaatteita 9

5. Liityntäpalveluiden toteutus 10

5.1. Tietoturva 10
5.2. Toiminnallinen toteutus 11
5.3. Tuetut käyttöjärjestelmät ja liittymien auditointi 11
5.3.1. Tuetut käyttöjärjestelmät 11
5.3.2. Liittymien auditointi palveluväylään 11
5.4. Palvelukatalogin rakenteellinen hallinta 11
5.5. Palvelun tuottaminen palveluväylään 12
5.6. Version 6 testaaminen ja käyttöönotto 12
5.7. Tulevia kehityskohteita 12
5.8. V5 ja V6 erot sanomarakenteessa 13
5.9. Tekniset vaatimukset 13
5.10. Palveluväylään liittymisen työmäärät ja läpimenoajat 13

1. Johdanto

Tämän dokumentin tarkoituksena on koota hyödynnettäväksi ajantasainen ja tiivis ohjeistus kansallisen palveluväylän teknisen yhteensopivuuden varmistamiseksi valmisteltaessa väyläliitäntöjä ja vaiheittaisia toteutuksia niin sosiaali- ja terveydenhuollon kärkihankkeiden kuin laajemminkin kuntasektorin kokonaisuudessa.Kansallinen palveluväylä on siirtymässä versioon 6.0. Tuotantoversion oletettu käyttöönotto tulee tapahtumaan vuoden 2015 viimeisen neljänneksen aikana. Tuotantokäyttöä jouduttiin siirtämään puuttuvien ominaisuuksien takia. Suurimmat toiminnalliset puutteet liittyvät sanomien lokitukseen sekä valvontaominaisuuksiin. Lisäksi tukea Red Hat - käyttöjärjestelmälle ei ollut saatavissa. Ajantasaista tilannetietoa kansallisen palveluväylän ja kansallisen palveluarkkitehtuurihankkeen etenemisestä on saatavissa e-suomi.fi – sivustolta.

Uuden version (6.0) merkittävimmät erot verrattuna aiempaan liittyvät organisaatiotietojen hallintaan, liittymäkuvausten käsittelyyn ja tiedon hallintaan. Lisätietoa ja tarkempaa ohjeistusta kansalliseen palveluväylään liittymisestä löytyy **palveluvayla.fi** – sivustolta.

Ohjeistus on jatkoa **Kansallisen palveluväylän käyttöönoton esiselvitykselle sosiaali- ja terveydenhuollossa**. Esiselvitys tuotti 1) ehdotukset kansallisen palveluväylän ensimmäisen vaiheen käyttöönotosta sosiaali- ja terveydenhuollossa, 2) arvioi kansallisesti Suomessa käyttöön valittujen tiedonvälitysstandardien ja määritysten yhteensopivuutta kansallisen palveluväylän pohjaratkaisuna toimivan X-ROAD:n kanssa, sekä 3) tuotti tietoa kehittämistarpeista kansallisen palveluväylän jatkokehittämissuunnitelmien laatimisen tueksi.

Esiselvityksen lopputuotoksen pohjalta Sote-alue / organisaatiokohtainen suunnittelutyö ja tätä tukevat kansalliset tukitoimenpiteet on käynnistetty. Tarkoituksena on, että alueellisessa yhteistyössä sovitaan tapa ja palveluiden liittämiselle Kansalliseen palveluväylään.

VAKAVA-projektin (kuntien, sairaanhoitopiirien ja kansallisten toimijoiden yhteistyönä laadittu sosiaali- ja terveydenhuollon alueellisen tiedonhallinnan ja tietojärjestelmäratkaisujen kehittämistä ohjaavan viitearkkitehtuurin tavoitetilan 2020 kuvaus) suositusten mukaisesti kansalliseen palveluväylään ja tietoliikenneratkaisuun kytkeytyminen kannattaa tehdä sosiaali- ja terveydenhuollossa mahdollisimman hallitusti. Liityntäpisteiden suunnittelu Kansalliseen palveluväylään tulee toteuttaa Sote-alueen laajuisessa yhteistyössä. Yksi mahdollinen ja suositeltava vaihtoehto on, että saman Sote -alueen sisällä olevat toimijat järjestävät yhteisen vikasietoisuuden saavuttamiseksi kahdennetun alueellisen liitynnän kansalliseen palveluväylään kaikkien alueen sovellusten- ja palveluiden liittämisen mahdollistamiseksi. Palveluväylään liityttäessä tulee kiinnittää huomiota myös tietoliikenneyhteyksien järjestämiseen. Alueelliset tietoverkot ja kansallinen, kuntien yhteinen KY-verkko -ratkaisu mahdollis-

tavat osaltaan ehdotetun kansallisen palveluväylän liityntäpisteiden toteutuksen alueellisessa yhteistyössä. Suosimalla keskitettyä liikennöintiä ja reititystä voidaan hyödyntää yhteisiä panostuksia ja turvata korkeampi käytettävyys kaikille osapuolille pienemmällä kustannusrakenteella.

Tätä ohjeistusta kehitetään eteenpäin yhdessä Kansallisesta palveluväylästä vastaavien tahojen, sote-kärkihankkeiden sekä kuntien kansallinen palveluväylä projektitoimiston (KUKAPA) kanssa. Dokumentin ensimmäisen julkaistun (0.93) version työstämiseen on osallistunut Kuntaliiton, PSOP-projektiryhmän, VRK:n, Kelan ja Kuntien Tieran henkilöitä.

2. Sanasto

Täydennetään tarvittaessa dokumentin päivityksen yhteydessä:

Toimija	Kuntaorganisaatio, palvelun tuottaja valtiollinen toimija tai muu yhteisö, joka on liittyy omalla sopimuksellaan palveluväylään tuottaakseen tai hyödyntääkseen väylään liitettävää tietoa

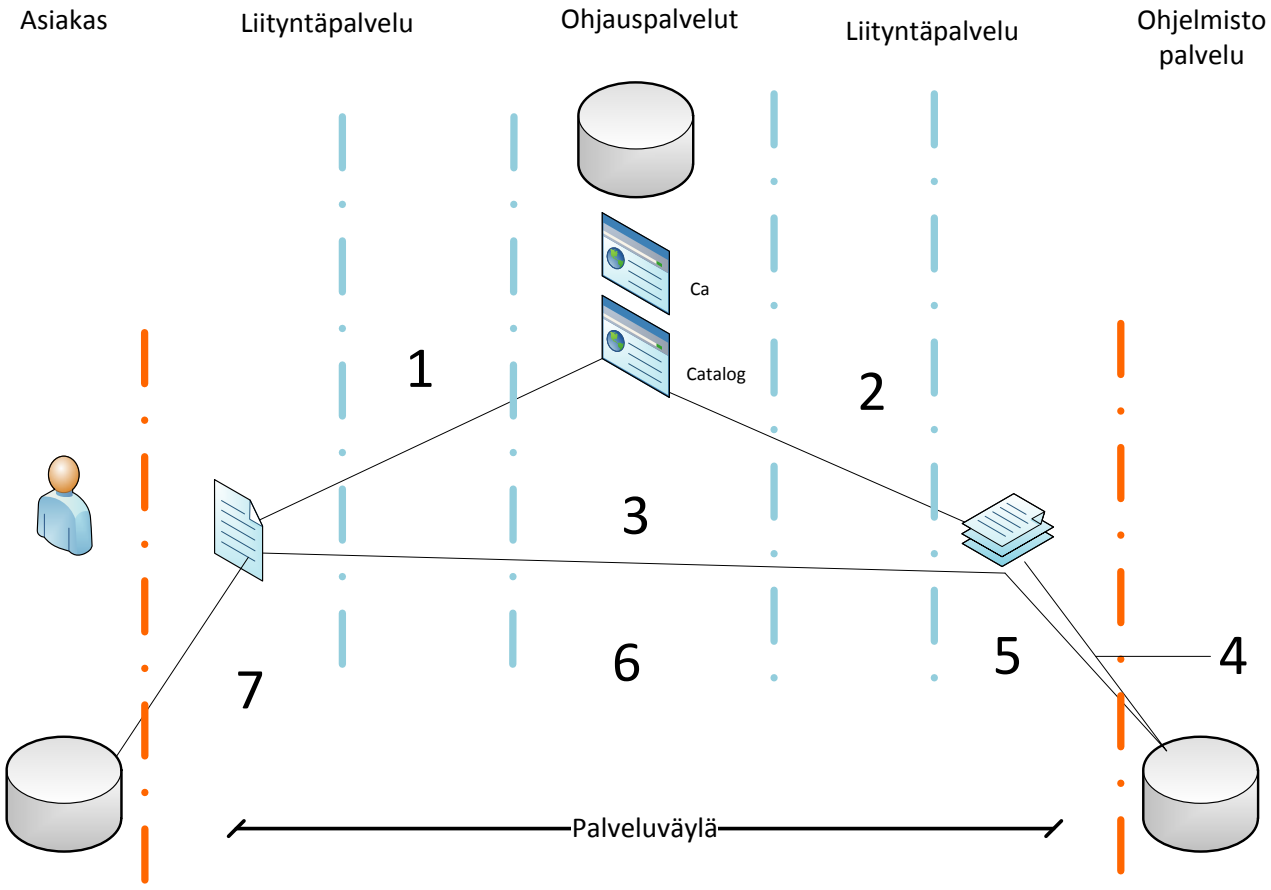
Kansallisen palveluväylän sanasto on työn alla osoitteessa:
https://confluence.csc.fi/display/Palveluvayla/Sanasto

3. Yleistä

Kansallisen palveluväylän versio 6 tuo uuden sovellusympäristön. Merkittävin palveluväylän sisäinen muutos on ympäristön ohjelmointikielen vaihtuminen.

Periaatteelliset ratkaisut ovat monilta osin aiempien kehitysversioiden kaltaisia. Merkittävimmät käsitteelliset erot liittyvät turvapalvelimen (Security Server) käytettävän suomenkielisen termin vaihtamiseen liityntäpalvelimeksi ja organisaatiohierarkioiden tukeminen. Organisaatioilla voi olla useita eri liityntäpalvelimia, jonka lisäksi käyttöoikeuksien myöntäminen voidaan nyt tehdä yksittäisten järjestelmien tasolla, kun aiemmin oikeudet oli aina myönnettävä organisaatiotasolla. Väylien väliseen federointiin on tulossa tuki ja KaPa-ohjelmassa toteutettavan kansallisen tunnistusratkaisun hyödyntäminen väylän kautta tulee olemaan mahdollista.

4. Väylän rakenne ja periaatteellinen toteutus



Kuva 1 Väylän toimintaperiaate yleisellä tasolla

Asiakkaan liityntäpalvelin hakee vastaanottajan tiedot käyttäen omaa paikallista kopiotaan keskuspalvelimelta määräajoin noudettavista konfiguraatiotiedoista. Suoraa yhteyttä keskuspalvelimeen ei sanomien lähettämisen yhteydessä tarvita. Liityntäpalvelin allekirjoittaa lähetettävän sanoman, ja liikenne salataan liityntäpalvelinten välisen yhteyden osalta palveluväylän varmennepalvelun (CA) tuottamilla sertifikaateilla (3). Sertifikaattien voimassaolo tarkistetaan molempien liityntäpalvelinten toimesta ennen varsinaisen sanoman lähettämistä. Vastaanottajan liityntäpalvelin aikaleimaa ja lokittaa sanoman, jonka jälkeen se tarkistaa asiakkaan oikeutuksen kutsua palvelua ja joko välittää pyynnön eteenpäin kohdejärjestelmälle tai palauttaa suoraan takaisin asiakkaalle oikeuksien puuttuessa (4). Kohdejärjestelmä palauttaa vastaussanoman omalle liityntäpalvelimelleen (5), joka ensin allekirjoittaa sanoman ja sitten lähettää sen salattua yhteyttä käyttäen takaisin asiakkaan liityntäpalvelimelle (6). Asiakkaan liityntäpalvelin aikaleimaa ja lokittaa vastauksen ja välittää vastaussanoman alkuperäisen sanoman lähettäneelle asiakkaan järjestelmälle (7).

On hyvä huomioida, että yhteyksien salaaminen ja käyttöoikeuksien hallinta koskevat automaattisesti kaikkea palveluväylän kautta siirrettävää tietoa tiedon luonteesta riippumatta (esim. avoin data). Palvelukohtaisesti ei ole siis mahdollista määritellä käytetäänkö salattua yhteyttä ja edellytetäänkö käyttöoikeuksien määrittelyä.

Väylässä on kaksi kriittistä osaa. Suora yhteys keskuspalvelimeen tarvitaan aina uusia liityntäpalvelimia, organisaatioita tai organisaatioiden yksittäisiä järjestelmiä lisättäessä tai poistettaessa. Liityntäpalvelinten välinen viestinvälitys sen sijaa toimii myös ilman keskuspalvelinta niin kauan, kuin liityntäpalvelimilla sijaitsevat paikalliset kopiot väylään liitetyistä liityntäpalvelimista ja niitä käyttävistä organisaatioista ovat voimassa. Tietojen voimassaolojan ollessa yhden viikon ja päivityksen tapahtuessa päivittäin voi palveluväylä siis toimia ilman keskuspalvelinta jopa kuuden vuorokauden ajan ennen kuin liityntäpalvelinten paikalliset kopiot tiedoista vanhenevat. Aikaleimapalvelu ja varmennepalvelu ovat sen sijaan huomattavasti kriittisempiä, sillä aikaleimojen ja sertifikaattien voimassaolotarkistusten voimassaoloajat ovat minuutteja.

4.1. Lokitus ja tietoturva

Jokaisesta sanomasta jää tiiviste, aikaleima ja sanoma kokonaisuudessaan sanomaliikenteen välisille liityntäpalvelimille. Kaikki lokitukset säilytetään liityntäpalvelimilla (ei enää tallennusta keskuspalvelimille).

Liityntäpalvelinten hallinnoijilla on vastuu tietosuojavelvoitteiden täyttämisestä. Ohjeistusta menettelyjen osalta tullaan vielä tarkentamaan (esim. lokitiedoston salaaminen, automaattinen tyhjentäminen, sanomasisällön droppaukset, tiukennetut ylläpitovelvoitteet jne.).

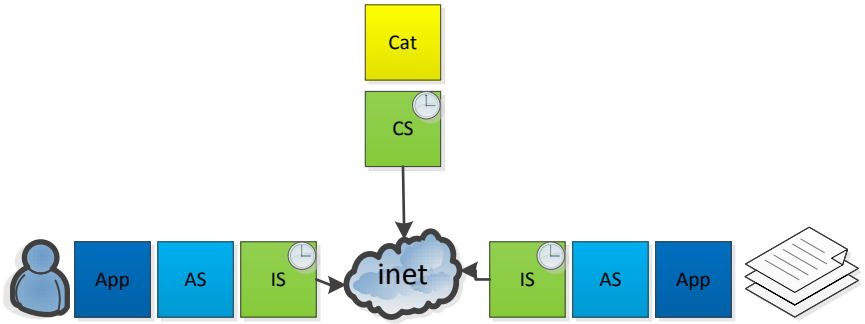
4.2. Keskuspalvelin

Väestörekisterikeskus (VRK) vastaa toteutuksesta, CSC toteuttaa alkuvaiheessa, myöhemmin (arviolta n. 2 vuoden kuluessa) palvelut siirtyvät Valtorille. VRK tarjoaa varmenne- ja aikaleimapalvelut.

Data voi olla avointa tai tietoluvan edellyttämää. Palveluista laaditaan erillinen sopimus, jossa määritellään datan ominaisuudet tarkemmin. Tiedon tuottaja määrittää ehdot. Tavoitteena on tietolupien yhdenmukaistaminen sekä asiakkaiden, että laajemmin kaikkien toimijoiden osalta.

Käyttöoikeuksien hallinta tapahtuu paikallisesti liityntäpalvelimella palveluväylään liittyneiden organisaatioiden omasta toimesta. Liityntäpalvelin tarjoaa käyttöoikeuksien hallinnointiin web-pohjaisen käyttöliittymän, jonka kautta käsiteltävät tiedot tallennetaan liityntäpalvelimen omaan tietokantaan. Keskuspalvelin ei sisällä keskitettyä tietokantaa eri palveluiden käyttöoikeuksista.

4.3. Liityntäpalvelin



Kuva 2: Palveluväylän komponentit

Kuvassa palveluväylän komponentit. Loppukäyttäjä hyödyntää applikaatiota (app), joka löytää palvelukatalogin (cat) ohjaamana kohdeympäristön liityntäpalvelimen (is). Väylä avataan ja suojataan asiakkaan ja tiedon tuottajan liityntäpalvelimien (is) välille. Kohdeympäristön liityntäpalvelin tarkistaa, onko asiakkaalle luvitettu ao. palvelu ja välittää sanoman eteenpäin kohdejärjestelmälle, jos luvitus on kunnossa. Sovellusten tieto muutetaan palveluväylän sanomarakenteiksi sovitinpalvelussa (as = Adapter Server).

4.4. Liityntäpalvelimen toteutuksen vaihtoehdot

Liityntäpalvelimen toteutus voi olla rakenteellisesti monipuolinen. Kuntatoimijan kannalta vaihtoehdot ovat seuraavat:

4.4.1. Jaetun liityntäpalvelimen käyttö

Toimija voi hankkia palveluntuottajalta liityntäpalvelun organisaationsa tai sen osan liittymätarpeisiin. Tämä tarkoittaa sitä, ettävalintansa mukaan tiedon tuottaja voi ulkoistaa palveluväylän tuotannon halutessaan osin tai kokonaan, huomioiden tietosuoja- ja turvavaateet esim. lokien suhteen käyttöpalveluvaatimuksissa. Hajautettaessa palveluväylän tuottamista usean kumppanin kesken tulee huolehtia, että jakelumallit ja organisaatiohierarkiat tukevat tavoiteltavaa jakelutapaa. Samalla organisaatiotasolla tulee esimerkiksi liityntäpalvelimien rakenteiden olla symmetriset. Mikäli palvelutuotanto halutaan hajauttaa, pitää palveluväylää varten muodostaa tätä tukeva organisaatiorakenne. (ks. myös kappale ”Toimialueittain jaettu liityntäpalvelin”).

4.4.2. Oma liityntäpalvelin

Toimija voi perustaa tai hankkia oman liityntäpalvelimen. Ympäristövaatimukset on esitetty kappaleessa 5.3.

4.4.3. Kahdennettu liityntäpalvelin

Toimija voi peilata liityntäpalvelimensa useammalle saitille. Tällöin jokaisella liityntäpalvelimella tulenee olemaan symmetrinen sisältö (suunnittelu on kuitenkin vielä kesken tuotantoon otettavan version osalta). Mikäli liityntäpalvelimet halutaan jakaa itsenäisillä sisällöillä useille saiteille, esimerkiksi liityntäpalvelin/palveluntuottaja, tulee jako suorittaa organisaatiohierarkian avulla. Katso kappale 3.7

VAKAVA-projektin suositusten mukaisesti Sote –alueen sisällä toimijoiden pitäisi järjestää yhteisen vikasietoisuuden saavuttamiseksi kahdennettu alueellinen liityntä kansalliseen palveluväylään kaikkien alueen sovellusten- ja palveluiden liittämisen mahdollistamiseksi.

4.4.4. Toimialueittain jaettu liityntäpalvelin

Kunta voi jakaa liityntäpalvelimensa loogisesti esim. toimialoittain tai palvelun tuottajittain, jolloin kukin kokonaisuus ylläpidetään sopimuskumppanin toimesta. Mallia voidaan käyttää esim. tilanteissa, joissa kuntatoimija on jakanut palvelunsa useamman palveluntuottajan kesken. Katso kappale 3.7.

4.5. Palveluväylien välinen federointi

Tuki väylien väliseen integraatioon on tulevassa version 6.0 julkaisussa. Tämä tarkoittaa ensisijaisesti kansallisten palveluväylien välistä federointia tässä vaiheessa. Toistaiseksi ei ole luvassa erillistoteutuksien välistä tukea. Tämä tarkoittaa sitä, että alusta ja ympäristö tukevat versiosta 6 asti luottamusketjuja palveluväylien välillä, jolloin yhdestä palveluväylästä voidaan luvittaa palveluita toisen väylän järjestelmille ja käyttäjille, jotka ovat kirjautuneet omaan väyläänsä ja joille on luvitettu ao. väylässä palveluita. Toimintoa tuetaan aluksi ensisijaisesti kansallisella tasolla, esimerkiksi Viron ja Suomen kansallisten palveluväylien välisessä liikenteessä.

4.6. Turvamoduuli

Versio 6 tukee organisaatioiden allekirjoitusvarmenteisiin liittyvien yksityisten avainten tallentamista erilliseen turvamoduuliin (Hardware security module, HSM). Turvamoduuli voidaan toteuttaa laitteisto- (hardware) tai ohjelmisto- (software) pohjaisena. Laitteistoon perustuva toteutus on turvallisempi, mutta siitä aiheutuvat kustannukset ovat ohjelmistopohjaista toteutusta korkeammat. Turvamoduuli voidaan toteuttaa myös keskitettynä verkon yli käytettynä palveluna, jolloin monet järjestelmät voivat käyttää saman turvamoduulin tarjoamia palveluita.

Virossa on päädytty määräämään turvamoduulin käyttö pakolliseksi kaikille palveluväylään liittyneille organisaatioille. Suomessa tehdään turvamoduulin käyttöön ja sen perusteisiin liittyvä selvitys ennen kansalliseen palveluväylään liittyvän linjauksen antamista. Linjaus tullaan antamaan vuoden 2015 ensimmäisellä neljännekselle ennen tuotantokäyttöön siirtymistä.

4.7. Rajapintakuvaukset

Versio 6 tukee useaa rajapintakuvausta per organisaatio. Aiemmissa versioissa jokaisella organisaatiolla oli yksi rajapintakuvaus, jonka tuli sisältää kaikkien organisaation tarjoamien rajapintojen kuvaukset. Useamman rajapintakuvauksen käyttö mahdollistaa usean eri sovitinpalvelun käyttämisen ja tekee uusien rajapintojen liittämisestä palveluväylään aiempaa yksinkertaisempaa. Rajapintakuvauksen tarjoaminen liityntäpalvelimelle on sovitinpalvelun vastuulla.

4.8. Käyttäjätunnisteet

Hierarkiset organisaatio-, järjestelmä- ja palvelintunnisteet:

instance/memberclass/organizationCode/subsystem/service/version

jossa Operaattori (=VRK) määrittää polun: instance/memberclass/organizationCode/

ja jossa Organisaatio (=väylään liittyvä toimija) määrittää: subsystem, service, version.

Organisaatiohierarkioiden avulla voidaan vaikuttaa esimerkiksi palveluiden näkyvyyteen ja oikeustasoihin. Organisatiotasot eivät palveluväylän suhteen tarkoita välttämättä julkaisijan sisäistä organisaatiohierarkiaa, vaan tasot kannattaa alusta lähtien suunnitella siten, että julkaisukohteiden hallinta on tasojen avulla järkevää ja mahdollista.

Esimerkiksi subsystem tasolla määritellään Toimijan palveluntuottaja 1, palveluntuottaja 2 ja palveluntuottaja 3. Tällöin eri palveluntuottajille sijoitetut liityntäpalvelimet voivat muodostaa kukin oman itsenäisen sisältönsä.

X-Roadin versiossa 6 jokaiselle palveluväylään liittyneelle organisaatiolle sekä sen palveluväylään liittämälle järjestelmälle ja palvelulle annetaan globaalisti uniikki tunniste. Globaalisti uniikin tunnisteen tarkoituksena on tukea X-Roadin federaatio-ominaisuutta, joka mahdollistaa useiden eri X-Road-instanssien liittämisen toisiinsa. X-Roadin sisäinen viestinvälitys ja käyttöoikeuksien hallinta perustuu organisaatioiden, järjestelmien ja palveluiden uniikkeihin tunnisteisiin sekä yksittäisen instanssin, että monesta eri instanssista muodostuvan kokonaisuuden sisällä.

Organisaatiokohtaiset tunnisteet muodostuvat kolmesta, järjestelmäkohtaiset neljästä ja palvelukohtaiset kuudesta erillisestä osasta. Tunnisteet ovat hierarkkisia ja järjestelmien tunnisteet sisältävät aina ne omistavan organisaation tunnisteen. Palveluiden tunnisteet sisältävät vastaavasti aina sekä järjestelmän, että organisaation tunnisteet.

4.9. Sanomanvälityksen periaatteita

Sovitinpalvelu: käsitemalli JSON/XML/SOAP

REST rajapinnan osalta on käynnistetty joulukuun 2014 lopussa yhteinen kehitystyö. Kehitystyötä tehdään täysin avoimesti, ja kaikki materiaali on saatavilla REST gateway –työtilassa GitHub:issa. REST Gateway –komponentista on tähän mennessä julkaistu versiot 0.0.1 ja 0.0.2.

REST Gateway –työtila GitHub:issa: https://github.comeducloudalliance/xroad-rest-gateway

SOAP-pohjaisten järjestelmien liittäminen palveluväylään on periaatteessa yksinkertaista. Yksikertaisimmillaan järjestelmän liittäminen palveluväylään tarkoittaa liityntäpalvelimen pystyttämistä sekä sovitinpalvelun toteuttamista tarvittavien SOAP-otsikkotietojen lisäämiseksi. Lisäksi sovitinpalvelun on myös tarjottava liitettävien palveluiden rajapintakuvaukset (WSDL). Rajapintakuvausten tarjoaminen tosin koskee vain palveluväylään tietoa tarjoavia järjestelmiä. Palveluväylän kautta tietoa käyttävien järjestelmien ei tarvitse tarjota rajapintakuvauksiaan palveluväylään.

5. Liityntäpalveluiden toteutus

Liityntäpalvelimen tulee aina sijaita omalla sekä liitettävästä tietojärjestelmästä, että sovitinpalvelusta erillisellä palvelinalustalla. Liityntäpalvelimen kokoonpano tullaan vakioimaan jakelijan toimesta (joka on ensivaiheessa VRK) ja kokoonpanolle tullaan hankkimaan Viestintäviraston hyväksyntä. Tietojärjestelmä (IS), ja sovitinpalvelu (as) voivat sijaita samassa tai erillisissä instansseissaan. Laajemmassa tuotantoympäristössä suositellaan palveluiden hajauttamisesta eri alustoille.

Sisäisen sanomanvälityksen toteutus väylällä on periaattessa mahdollista, mutta ei välttämättä tehokasta. Palveluväylän käyttö sisäiseen sanomanvälitykseen johtaa tavallisesti sanomien kierrättämiseen tarpeettomasti verkon ulkolaidan kautta, jolloin tetoliikenteellisesti ei saavuteta parasta suorituskykyä ilman erityisjärjestelyitä.

Palveluväylän käytölle sinällään ei ole teknisiä esteitä sisäiseen liikenteeseen. Erityistarkoituksissa voi olla järkevää käyttää palveluväylään kertaalleen laadittua rajapintaa myös sisäisten järjestelmien käyttöön. Asian kannattavuus tulee kuitenkin ratkaista tapauskohtaisesti.

5.1. Tietoturva

6.0 version muodossa palveluväylän sanomarakenne ja lokikäsittely on VAHTI tietoturvallisuuden korotetun tason vaatimusten näkökulmasta puutteellista. Ainakaan alkuvaiheessa palveluväylä ei täytä korotetun tason asettamia vaatimuksia. Perusratkaisuna palveluväylä tarjoaa VAHTI perustason mukaisen kokonaisuuden, joka mahdollistaa suojaustason IV (ST4) mukaisen aineiston siirtämisen väylän kautta.

Merkittävimmät puutteet nykytoteutuksessa liittyvät lokitietueiden käsittelyyn ja salaukseen. Tämän johdosta kriittisen ympäristön liityntäpalvelimien sijoitus ja seuranta (ml. lokitiedostojen säilytys ja siirto) pitää suunnitella huolella, jotta voidaan varmistaa yhteyden luottamuksellisuuden säilyminen.

5.2. Toiminnallinen toteutus

Kansalliseen palveluväylään liittyviltä edellytetään ammatillista otetta liittymien laatimiseen. Lähtökohtaisesti uudet liittymät liitetään aina ensintestiympäristöön ja sitten vasta tuotantoon. Palveluvayla.fi sivustolla on määritelty tarkemmin voimassa olevat liityntä- ja tuotantoperiaatteet.

5.3. Tuetut käyttöjärjestelmät ja liittymien auditointi

5.3.1. Tuetut käyttöjärjestelmät

Ubuntu + red hat linux tuettuina Suomessa (huom. ei muita linux jakeluita).

Versio 6 tukee lähtökohtaisesti Ubuntu 14.04 LTS – käyttöjärjestelmää. Suomessa tullaan toteuttamaan tuki Red Hat (RHEL 6 tai 7) – käyttöjärjestelmälle vuoden 2015 toisen puolikkaan aikana.

Ubuntu-pohjaisen liityntäpalvelimen version saa testikäyttöön JULKICT labin kautta. Yhteydenotot palveluvayla@vrk.fi osoitteeseen.

5.3.2. Liittymien auditointi palveluväylään

Hyväksymisen proseduurit ja hyväksymiskriteerit ovat työn alla ja ne julkaistaan palveluvayla.fi portaalissa.

Palveluväylään liitettävälle tiedolle määritellään aina myös turvaluokitus. Tietoturvatasot liittyvät kansallisiin tietoturvatasovaatimuksiin, kuten VAHTI-ohjeistukset.

Liittyjien velvollisuuksista ja oikeuksista: Velvoitteet ja oikeudet määritellään tarkemmin palvelusopimuksessa. Lähtökohtaisesti liityntäpalvelimen tietoturvataso on VAHTI-ohjeistuksen tarkoittama perustaso.

Tiedon tuottaja antaa liittyessään palvelulupauksen tarjoittavalle tiedolle, väylään liittyvä toimija ilmoittaa mm. milloin tieto on saatavilla. (esim. 24/7 jne)

5.4. Palvelukatalogin rakenteellinen hallinta

Palvelukatalogiin liittyessään tiedontuottaja on hyväksynyt liittymisen ehdot. Tällöin teknisen liittymisen edellytyksenä ovat sekä väylän palvelimien hyväksyntä tuotantoon että liittymärajapintojen testaus testiympäristössä ennen varsinaisen tuotantokäytön aloitusta.

Lopuksi palvelu julkaistaan katalogissa haku- ja laatusanastonsa kanssa. Katalogin hallinta edellyttää yhtenäistä ja yleistä semantiikkaa. Jokainen toimiala ja toimija vastaavat siitä, että heidän käyttämänsä sanasto ja tietomalli ovat yhteensopivaa toimialan yleisesti käytettyjen mallien mukaisesti.

5.5. Palvelun tuottaminen palveluväylään

Palveluväylään saataville tuotava tieto edellyttää aina sopimusta tuotettavan tiedon saatavuudesta ja rakenteesta.

Sopimuksessa määritellään liitettyvän järjestelmän

- elinkaari
- esimerkkisanomat
- vastuuhenkilöt
- yhteyshenkilöt (yksi yhteystaho/asiakas, ei palvelukohtaisia yhteyshenkilöitä)
- saatavan tiedon hinta
- lupakäytännöt, lisenssi
- tiedon luokittelu

5.6. Version 6 testaaminen ja käyttöönotto

CA ja TSA osana kehitysympäristöä

Halukkaat organisaatiot pääsevät liittymään kehitysympäristöön Q3/2015

Auditoinnit Q3/15 -

- arkkitehtuurin katselmointi
- keskuspalvelin
- liityntäpalvelimen referenssitoteutus
- lähdekoodi

Tuotantoympäristön käyttöönotto Q4/15

5.7. Tulevia kehityskohteita

- Liityntäpalvelimen lähdekoodi avataan ja julkaistaan käyttöönoton yhteydessä.
- Avoimen kehittämisen mallin suunnittelu ja käyttöönotto valmisteilla.
- Hallintamallin käyttöönotto liittyen ylläpitoon ja käyttöön kansallisella tasolla.
- Keskeisten tietovarantojen liittämisen tukeminen (tekninen ja taloudellinen tuki).
- Muita tulevia kehityskohteita:
    - RHEL – tuki
    - valvontatyökalut
    - lokitukseen liittyvät käytännöt (salaus etc)
    - rajapintakuvausten WSDL validointi

5.8. V5 ja V6 erot sanomarakenteessa

X-Roadin protokollassa versioiden 5 ja 6 välillä tapahtuneet muutokset keskittyvät pääasiassa SOAP-sanomien otsikkotietoihin (*SOAP header*) ja X-Roadin edellyttämiin metapalveluihin. SOAP-sanomien body-osa säilyy sen sijaan täysin ennallaan. Ajantaiset tiedot löytyvät osoitteesta palveluvayla.fi (sisältäen mm.v6 sanomarakennekuvaukset).

5.9. Tekniset vaatimukset

Palvelinalusta Ubuntu tai Rhel, virtuaalinen tai fyysinen, minimivaatimukset 64-bittinen 2-ytimen Intel, AMD tai yhteensopiva suoritin. AES käskykannan tuki on suositeltavaa. Muisti minimi 2 Gt, suositus vähintään 4 Gt, Levytila 7 Gt. Java 8.

Liityntäpalvelimen sijoituspaikaksi suositellaan DMZ-aluetta ja toimijan valinnan mukaan liityntäpalvelimet segmentoidaan DMZ:n sisällä.

Tiedonsiirron osalta palveluratkaisun tulee täyttää julkisen hallinnon toiminnalle asetetut tietoturvavaatimukset. Erityisesti sosiaali- ja terveydenhuollon sektoriin kohdistuu lainsäädännön vaatimuksia, jotka tulee huomioida tiedonsiirron tietoturvavaatimuksissa. Palveluväylä toimii Kanta-palvelun näkökulmasta tietoliikenteen reitittäjän roolissa.

Käyttöönoton suunnittelun muistilista

- Tarkista ajoalustan yhteensopivuus käyttöjärjestelmän kanssa.
- Olemassa olevien prosessien tarkistus.
- Varmista että liityntäpalvelimen ja taustajärjestelmän välinen tietoliikenneyhteys on käytettävyydeltään ja tietoturvatasoltaan riittävä.
- Varaa tarvittava määrä ip-osoitteita sekä verkkoliityntöjä ajoalustalle.
- Suunnittele varmennehakemukset.
- Suunnittele varmistus sekä palautus palvelun vaatimustason mukaisesti.
- Dokumentoi suunnitelma

Listaa ollaan tarkentamassa VRK:n toimesta vähitellen 1/2015 lähtien.

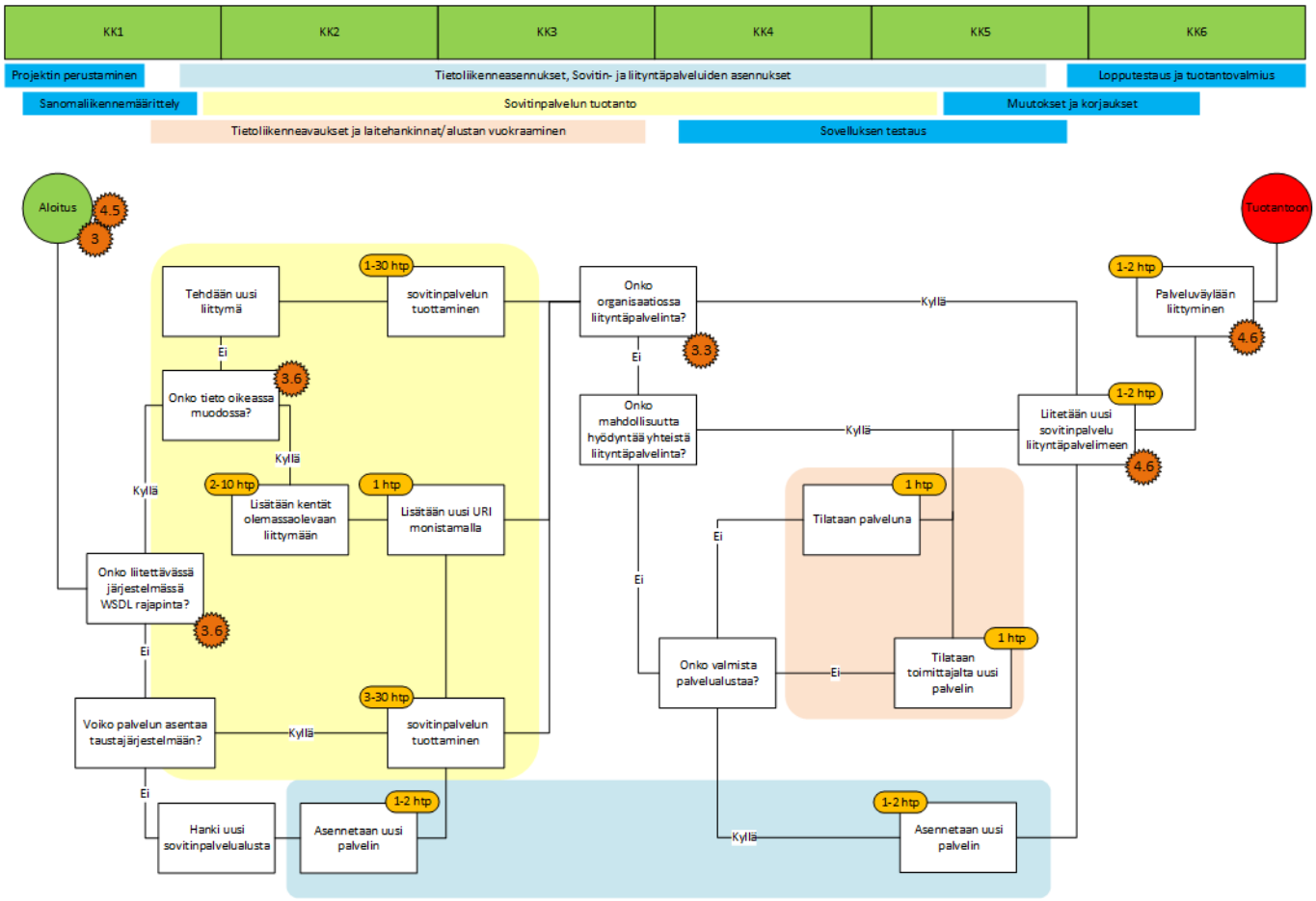
5.10. Palveluväylään liittymisen työmäärät ja läpimenoajat

Kappaleessa on kuvattu aiempien pilotointien perusteella odotettavissa olevia työmääriä ja läpimenoaikoja palveluväylän ensikertaiselle käyttöönotolle.

Liityntäpalvelimen asennuksen työvaiheet

- Asenna tai tilaa palvelimen asennus

- Tee tai tilaa palomuuriavaukset turvapalvelimen ja taustajärjestelmän, keskuksen ja kumppanien järjestelmiin
- Tee varmennehakemukset
- Asenna varmenteet ja testaa toimivuus
- Liitä taustajärjestelmä
- Testaa järjestelmän toimivuus sekä varmistus ja palautus.
- Päivitä dokumentointi
- Siirrä tuotantoon



Kuva 4: Aiempiin toteutuksiin perustuva aikatauluhahmotelma tuotannossa olevan järjestelmäliittymän muuntamisesta palveluväylään. Kuvan numerot (esim. 3.6) viittaavat tämän dokumentin otsikkonumeroihin. Työmäärät (esim. 1-2 htp) ovat suuntaa-antavia ko. vaiheeseen vaadittavan työmäärän osalta.