VALTIOVARAINMINISTERIÖ

Kansallisen palveluväylän viitearkkiteh-tuuri

2.9.2013

Versio: 0.95

Sisällys

Dokumentin versiohistoria

Versio	*Päiväys*	*Laatija*	*Muutoksen kuvaus*
0.11	26.4.2013	J.T.	Ensimmäinen luonnos, arkkitehtuurin runko
0.8	6.6.2013	MK/JT/PN/OK	Ohjausryhmälle kommentoitavaksi tarkoitettu versio
0.9	16.6.2013	MK	Ohjausryhmän ja projektiryhmän kommenttien perusteella muokattu versio
0.92	26.6.2013	JT	Tarkennuksia, muutoksia kommenttien perusteella
0.93	27.6.2013	JT	Teknisten osien siirto liitemateriaaliksi
0.94	26.8.2013	MK	Täsmennetty kommentointikierrokselta saatujen kommenttien pohjalta
0.95	2.9.2013	JT/PK	Ohjausryhmän palautteen mukaiset täsmennykset

1. Johdanto

1.1. Dokumentin tarkoitus

Tässä dokumentissa kuvataan **kansallisen palveluväylän (=Palveluväylä)** viitearkkitehtuuri hyödyntäen ns. kokonaisarkkitehtuurimenetelmää. Kyseinen tavoitearkkitehtuuri ohjaa kansallisesti tietojen ja palvelujen yhdistämisen ratkaisukokonaisuuksia ja tiedonvälityksen välineiden kehittämistä.

Viitearkkitehtuurilla tarkoitetaan määritetyn kohdealueen yleistasoista tavoitetilan arkkitehtuurikuvausta (tavoitearkkitehtuuria). Viitearkkitehtuuri jäsentää ja määrittää ratkaisukokonaisuuden keskeisimmät rakenneosat ottamatta tarkasti kantaa esimerkiksi toteutusteknologiaan tai muihin suunnittelun tai toteutuksen yksityiskohtiin. Viitearkkitehtuuri määrittää puitteet, jonka sisällä kansallinen palveluväylä, sen komponentit, tietojen hallinta, tietojärjestelmät sekä ylläpito ja hallinta tulee toteuttaa.

Tämä viitearkkitehtuuri kuvaa kokonaisuutena miten eri toimijoiden palvelujen ja tietojen yhdistämisen prosessit, tietorakenteet, toimijat, roolit sekä tietojärjestelmäpalvelut toimivat kansallisesti tavoitetilassa yhteen. Viitearkkitehtuurin tarkoituksena on jakaa toiminnot ja teknologiset komponentit loogisiin kokonaisuuksiin, joissa samaan asiaan toteutetaan vain yksi ratkaisu ja jotka kytkeytyvät saumattomasti muihin kansallisiin palveluihin ja olemassa oleviin toteutuksiin.

Kansallisen palveluväylän teknologiaratkaisut tulee sovittaa tähän tavoitearkkitehtuuriin. Palveluväylän kehittäjän tulee teknologiaa ja kansallisen tiedonvaihdon infrastruktuuria kehittäessään verrata potentiaalisia ratkaisumalleja tähän tavoitearkkitehtuuriin ja pyrkiä hankkimaan tai toteuttamaan ratkaisuja, jotka parhaiten sopivat tässä kuvattuihin arkkitehtuuritavoitteisiin.

Kansallisen palveluväylän arkkitehtuurin suunnittelu –hankkeen (VM008:00/2013) tehtävänä on ollut suunnitella ja kuvata kokonaisarkkitehtuurimenetelmän mukaisesti kansallisen palveluväylän viitearkkitehtuuri (= loogisen tason ratkaisumalli) ja sitä tarkentavat ratkaisun kuvaukset.

Palveluväylällä tuetaan hallitusohjelmassa, ICT-strategiassa sekä ICT-klusteri 2015 -työryhmän raportissa asetettujen tavoitteiden toteuttamista. Viimeksi mainitussa palveluväylän käyttäjäkuntaa on laajennettu ottamalla mukaan yksityissektori, jonka vuoksi palveluväylää kutsutaan kansalliseksi palveluväyläksi.

Kansallisen palveluväylän viitearkkitehtuuri on osa julkisen hallinnon yhteistä kokonaisarkkitehtuuria. Julkisen hallinnon yhteinen kokonaisarkkitehtuuri (JHKA) sisältää mm. viitearkkitehtuurien kuvauksia, joilla ohjataan tietyn rajatun ratkaisukokonaisuuden suunnittelua ja toteutusta julkisen hallinnon organisaatioissa halutunlaiseen yhtenäiseen toteutusrakenteeseen.

1.2. Kenelle tämä dokumentti on tarkoitettu

Tämä viitearkkitehtuurikuvaus on tarkoitettu kansallisen tiedonvaihdon infrastruktuurin ja palveluiden kehittämisestä ja toteuttamisesta vastaaville organi-

saatioille sekä koosteisia, usean organisaation tietoja ja palveluja hyödyntävien loppuasiakaspalvelujen kehittäjäorganisaatioille ja sen yhteistyökumppaneille. Tämä viitearkkitehtuuri toimii myös päätöksenteon tukena tiedonvaihdon ratkaisuista päätettäessä.

Keskeisiä kansallisen palveluväylän viitearkkitehtuurin kohderooleja ovat:

- Valtiovarainministeriön kansallisen yhteentoimivuuden lainsäädäntöä valmistelevat avainhenkilöt erityisesti tietohallintolain valtiovarainministeriölle antaman asetusmandaatin näkökulmasta
- Valtiovarainministeriö ja JulkICT-toiminnon avainhenkilöt. Viitearkkitehtuuria voidaan käyttää erityisesti päätöksenteon tukena määriteltäessä tulevaisuuden tiedonvaihdon ja sähköisten palvelujen kehittämisen strategisia suuntauksia ja resursointia
- Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA tietojen vaihdon JHS-suositusten ja standardien valmistelun näkökulmasta.
- Julkisen hallinnon kokonaisarkkitehtuurissa kuvattujen kansallisen arkkitehtuurin Kohdealueiden kokonaisarkkitehtuurityöstä vastaavat vastuuhenkilöt
- Kansallisen tietojenvaihdon infrastruktuurin ratkaisuja ja palveluja kehittävät avainhenkilöt ja kehittämisprojektien vastuuhenkilöt, projektipäälliköt sellaisissa asiakkuudenhallintaa ja sen välineitä kehittävissä projekteissa, joissa toiminnan kehittämiseen liittyvät suoraan tai välillisesti tietoteknisen ympäristön palvelut.
- Yritysten, kuntien, valtionhallinnon ja kolmannen sektorin substanssi- ja liiketoimintapalvelujen kehittäjät ja innovaattorit palveluväylän ja siihen kytkettyjen palvelujen hyödyntämismahdollisuuksien näkökulmasta
- Yritysten, kuntien, valtionhallinnon ja kolmannen sektorin kokonaisarkkitehtuurityöstä vastaavat avainhenkilöt
- Yritysten tiedonvaihdon ratkaisuja kehittävät avainhenkilöt
- Kuntien tiedonvaihdon ratkaisuja kehittävät avainhenkilöt
- Valtion virastojen tiedonvaihdon ratkaisuja kehittävät avainhenkilöt
- Organisaation ulkopuolisia tietoja ja palveluja hyödyntävien tietojärjestelmien ja ratkaisujen kehittämisen avainhenkilöt ja hankinnoista vastaavat henkilöt
- ICT-projektien suunnittelijat ja tekniset vastuuhenkilöt yhteentoimivuuden varmistamisen näkökulmasta
- Yritysten, kuntatoimijoiden, valtion virastojen ja kolmannen sektorin organisaatioiden tietohallintojohto, erityisesti tietojen vaihdon ja integraatioratkaisujen kehittämisen näkökulmasta

Edellisten lisäksi tämän viitearkkitehtuurin kohderyhmään kuuluvat tietojen vaihdon ja palvelujen yhdistämisen tietojärjestelmiä, ICT-palveluja, konsul-

tointi- ja asiantuntijapalveluja tai kehittämispalveluja tarjoavat julkishallinnolliset ja yksityissektorin palveluntuottajat.

1.3. Tämän kuvauksen rajaukset ja reunaehdot

Tämän viitearkkitehtuurityön yleisiä rajauksia ovat:

- Tässä dokumentissa suunniteltu kansallisen palveluväylän viitearkkitehtuuri hyödyntää ja soveltaa täysimääräisesti julkisen hallinnon kokonaisarkkitehtuuria. Tässä viitearkkitehtuurissa noudatetaan kyseisiä linjauksia.
- Tässä viitearkkitehtuurissa keskitytään määrittämään erityisesti kansallisen tiedonvaihdon infrastruktuurin ja sen teknisten ja hallinnollisten palvelujen kokonaisuutta. Tässä työssä ei tarkasti määritetä, mitä substanssi- ja liiketoimintapalveluja kansalliseen palveluväylään tullaan kytkemään. Palveluväylä pyritään toteuttamaan siten, että palvelujen liittäminen siihen on mahdollisimman helppoa ja turvallista.
- Tämä kuvaus ei ole yksityiskohdiltaan riittävä hankintojen edellyttämään vaatimusmäärittelyyn. Tämän kuvauksen perusteella voidaan kuitenkin pilotoida ja arvioida tässä kuvatun arkkitehtuurin mukaisia ratkaisuja. Tämän viitearkkitehtuurin pohjalta voidaan määrittää hankinnoissa ja tarkemmassa toteutussuunnitelmassa tarvittava vaatimusmäärittely suhteellisen suoraviivaisesti.
- Kansallisen palveluväylän viitearkkitehtuuri ei ota tarkasti kantaa varsinaisen tiedonsiirtokerroksen (tietoliikenneverkko) teknisen toteutuksen yksityiskohtiin. Palveluväylään tulee kuitenkin voida liittyä ilman, että on kytkeytynyt tiettyyn fyysiseen tietoliikenneverkkoon.
- Tämä viitearkkitehtuuridokumentti ei sisällä kuvausta kansallisen palveluväylän liiketoiminta- ja hallintamallista, kustannus-hyötyarviosta eikä kansallisen palveluväylän toimeenpanon kehittämispolusta. Nämä kuvataan omissa dokumenteissaan.
- Tämä kansallisen palveluväylän viitearkkitehtuuri on kokonaisarkkitehtuurimenetelmällä kuvattu kansallisen yhteentoimivuuden infrastruktuurin tavoitetilakuvaus, joka ottaa huomioon tasapainoisesti sekä toiminnan, tiedon, tietojärjestelmäpalvelujen että teknologian näkökulmat. Sitä tulee tarkentaa sanomanvälityksen tarkemmilla kuvauksilla sekä täsmällisemmällä ratkaisusuunnittelulla.

Varsinaiset kuvattavan kohteen rajaukset on listattu tarkemmin jäljempänä arkkitehtuurin rajauksissa ja reunaehdoissa.

Huom. Viitearkkitehtuuri toimii ylätason suunnitteluna ja runkona tarkemmalle ratkaisu- ja toteutussuunnittelulle. Viitearkkitehtuuri ei korvaa tätä tarkempaa suunnitteluvaihetta vaan jää suunnitellusti ylemmälle tasolle.

2. Kansallisen palveluväylän terminologia

Tässä viitearkkitehtuurissa käytetään seuraavaa kansallista palveluväylää koskevaa terminologiaa:

Kansallinen palveluväylä	Joukko tietoliikenneverkon (internetin tai rajatun alueen verkon kautta) yhteen liitettyjä palveluväylän liityntäpisteitä ja keskitetyt palveluväylän palvelut kaikissa vyöhykkeissä yhteensä.
Keskuspalvelin	Palveluväylän keskitettyjen palvelujen palvelinkokonaisuus. Voi koostua joukosta palvelimia, mutta näkyy palveluväylään yhtenä loogisena palvelimena.
Liiketoiminta / substanssisovellus	Palveluväylän toimijan liiketoimintasovellus, joka sisältää toimintalogiikan tietojen ja palvelujen käsittelystä. Tarjoaa palvelun palveluväylään.
Palvelukatalogi	Palveluväylän keskitetty palvelu: Sisältää tiedon palveluväylään kytketyistä palveluista, rajapinnoista ja niiden hyödyntämisessä tarvittavista tiedoista
Palveluväylän keskitetyt palvelut	Palveluväyläoperaattorin omassa hallinnassa olevien Palveluväylän palvelujen (primääripalvelut ja muut kansallisesti keskitetyt palvelut) joukko. On koottu loogiselle Keskuspalvelimelle.
Palveluväylän liityntäpalvelin	Yksittäiselle palveluväylään liittyneelle organisaatiolle sen liityntäpisteeseen asennettu "liityntälaite", joka sisältää myös palveluväylän Sanomasiirron sovelluskomponentin. Laite on tyypillisesti virtuaalipalvelin, mutta se voidaan toteuttaa myös fyysisenä palveluna
Palveluväylän liityntäpiste	Looginen kytkentäpiste, josta palvelut kytketään palveluväylään. Koostuu palveluväylän verkko-osoitteesta sekä tähän liitetyistä liityntäpalvelimista (yksi tai useampi). Peittää palveluväylältä varsinaiset siihen kytketyt substanssijärjestelmät sekä tietovarannot ja päinvastoin
Palveluväylän lokipalvelu	Kuhunkin liityntäpalvelimeen kytketty lokipalvelu, joka tallentaa sekä muodostetut yhteydet (yhteysloki) että varsinaiset sanomat (sanomaloki). Sekä lähettävä että vastaanottava pää lokittaa ko. tiedot. Näistä muodostetaan keskitettyyn palveluun md5-tiiviste (tai muuten luotettavasti toteutettu vastaava tiiviste) jäljitettävyyttä ja kiistämättömyyttä varten.
Palveluväylän rajapinta	Määritelty rajapinta, jota palveluväylään kytketyt tietojärjestelmäpalvelut noudattavat. Palvelua käytetään käytännössä siihen määritetyn rajapinnan läpi. Rajapinta peittää varsinaisen Palvelun sisäisen rakenteen sitä hyödyntäviltä tietojärjestelmiltä ja muilta palveluilta.
Palveluväylän sanoma	Varsinainen sanoma (tyypillisesti XML-viesti), jonka liityntäpalvelimet välittävät toisilleen.
Palveluväylän sanomanvälityspalvelu	Palveluväylän liityntäpalvelimeen asennetun perustoiminnallisuuden sovelluskomponentti, joka tarjoaa sovelluspalvelun, joka välittää sanomia liityntäpalvelimilta toisille.

Palveluväylän sovelluskomponentti	Liityntäpalvelimeen asennettava sovelluskokonaisuus, joka sisältää palveluväylän keskeiset hajautetut palvelut. Perustoiminnallisuuden sisältävän kaikille toimijoille automaattisesti tulevan komponentin lisäksi voidaan määrittää sektori- tai vyöhykekohtaisia sovelluskomponentteja.
Palveluväylän vyöhyke	Palveluväylän internetin yli toimivaan Palveluväylän ytimeen kytketty SLA-taattu tai korkeamman tietoturvatason rajattu osaverkko. Vyöhykkeen sisällä tiedonvaihdon infrastruktuuri voidaan rakentaa palveluväyläratkaisun mukaisesti tai siellä voidaan käyttää sektorikohtaisia ratkaisuja. Vyöhykkeen ja Palveluväylän ytimen reunalla olevan Palveluväylän liityntäpisteen tulee pystyä muuntamaan mahdollinen vyöhykkeen sisäinen viestinvälitys Palveluväylän välitettäväksi viestiliikenteeksi ja päinvastoin
Palveluväylän ydin	Palveluväylän internetin yli tapahtuvan tiedonvälityksen kokonaisuus, joka noudattaa kaikilta osin palveluväylän rajapintoja ja määrityksiä ja toteutetaan palveluväylän toteutuksilla. Koostuu ytimeen liitetyistä liityntäpisteistä, mutta ei muiden eri palveluväylän vyöhykkeiden sisäisistä liityntäpisteistä.
Palveluväyläosoite	IP-osoite tai DNS-nimi, josta palveluväylään kytketty palvelu löytyy
Palveluväylään kytketty palvelu	Palveluväylän toimijan palveluväylään kytketty tietojärjestelmäpalvelu, joka tuottaa varsinaisen substanssipalvelun. Substanssipalvelu voi olla esim. tietovarantopalvelu, laskentapalvelu tai muu tietojärjestelmäpalvelu. Palvelu peitetään palveluväylän määritykset täyttävän rajapinnan taakse.
Primääripalvelu / node	Palveluväylän keskeiset osat on rakennettu hierarkkisesti siten, että niihin on määritetty ns. keskitetysti ylläpidettävä ja operoitava keskuspalvelimeen sijoitettu **pääpalvelu (primääri)**, joka jakaa omat toimintonsa ja tietonsa hajautettuihin sekundääripalveluihin tai -nodeihin. Esimerkiksi palvelukatalogin primääripalvelu on keskitetty Palveluväyläoperaattorin hallintaan ja sen tiedot levitetään kaikkiin liityntäpalvelimiin. Näin kiistämättömin tietolähde palveluista on koko ajan primääripalvelussa, mutta sitä ei tarvita reaaliaikaisesti liityntäpalvelimien väliseen yhteydenmuodostukseen, koska tiedot ovat jatkuvasti ajan tasalla myös sekundäärinodeissa paikallisesti.
Sekundääripalvelu / node	Ks. Primääripalvelu / node -yllä
Sertifikaattipalvelu	Sertifikaattipalvelun tuottaja, käytetään palveluväylän palveluiden autentikointiin
Tiedonvaihtosopimus	Kahden palveluväylätoimijan keskinäinen sopimus tietojen vaihdosta. Toteutetaan rakenteisen, yhteisen mallin mukaan. Tallennetaan keskitetysti palveluväylään, voidaan hyödyntää one-to-many ja many-to-one sanomavälityksessä.

Turvanimipalvelu	Keskitetty palvelu: Palveluväylään kytketyt liityntäpalvelimet sijoitetaan yhteisen varmennetun nimipalvelun piiriin.

Edellä olevaa sanastoa ja synonyymeja on kuvattu tarkemmin *Liitteessä 1, KA-taulukot*.

3. Kokonaisarkkitehtuurimenetelmän hyödyntäminen

Kokonaisarkkitehtuurilla (KA) tarkoitetaan toiminnan, tietotarpeiden, tietojärjestelmien ja teknologiaratkaisujen mallintamista, kuvaamista ja suunnittelemista yhtenäisen mallin mukaisesti. Kokonaisarkkitehtuuri on suunnitelma kohteena olevan toiminnan muodostaman kokonaisuuden ja sen osien rakenteesta ja osien välisistä suhteista. Kokonaisarkkitehtuuri on strategisen johtamisen väline, jonka avulla yhtenäistetään toiminnan ja ratkaisujen kehittämistä. Kokonaisarkkitehtuurimenetelmän kautta tämä viitearkkitehtuuri kuvaa, kuinka kansallisesti yhteentoimivat palvelut kytketään toisiinsa. Siinä kuvataan, miten palveluväylän tekniset komponentit, siihen kytkettävät palvelut, näiden toimintamallit, tekniset valvontatiedot ja järjestelmät toimivat kokonaisuutena. Sen avulla palvelujen kytkemisestä toisiinsa tulee ennakoivaa ja se saadaan sidotuksi strategiseen kehittämiseen – sekä kansallisella tasolla että yksittäisissä organisaatioissa.

Kokonaisarkkitehtuuri varmistaa eri osa-alueiden ja erityisesti toiminnan tarpeiden yhdenmukaisen huomioimisen kaikessa toiminnan ja ICT-ratkaisujen kehittämisessä. Kokonaisarkkitehtuuri ulottaa näkökulmansa pelkkien tietojärjestelmien ulkopuolelle kuvatakseen ne substanssitoiminnan syyt ja tarpeet, joita varten tietojärjestelmiä tehdään sekä tässä tarvittavat tiedot.

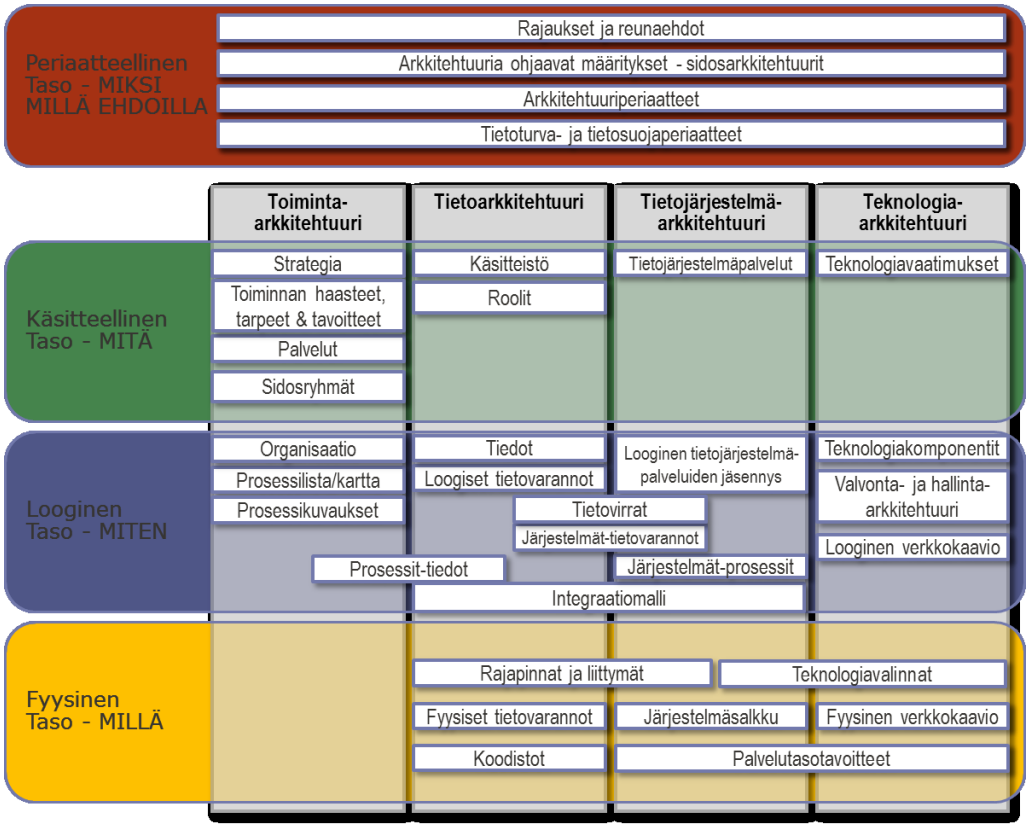
Varmistaakseen toteutettavien ratkaisujen kattavuuden ja tarkoituksenmukaisuuden kokonaisarkkitehtuurimenetelmä jäsentyykin **näkökulmiin** ja **käsitteellisiin tasoihin** (abstraktiotasoihin).

- **Näkökulmat:**
  - Toiminta: *liiketoiminnan ja asiakkuuksien näkökulma*
  - Tieto: *tietoa, käsitteitä ja tietovarantoja tarkasteleva näkökulma*
  - Järjestelmä: *järjestelmien näkökulma*
  - Teknologia: *tekniikan, laitteiden ja teknisten ratkaisujen sekä ylläpidon näkökulma*
- **Abstraktiotasot:**
  - Periaatteellinen taso – MIKSI, missä rajoissa
  - Käsitteellinen taso – MITÄ
    - *esim. mitä tietoa taltioidaan, mitä tarkoitusta varten, mitkä ovat toiminnan keskeiset käsitteet*
  - Looginen taso – MITEN

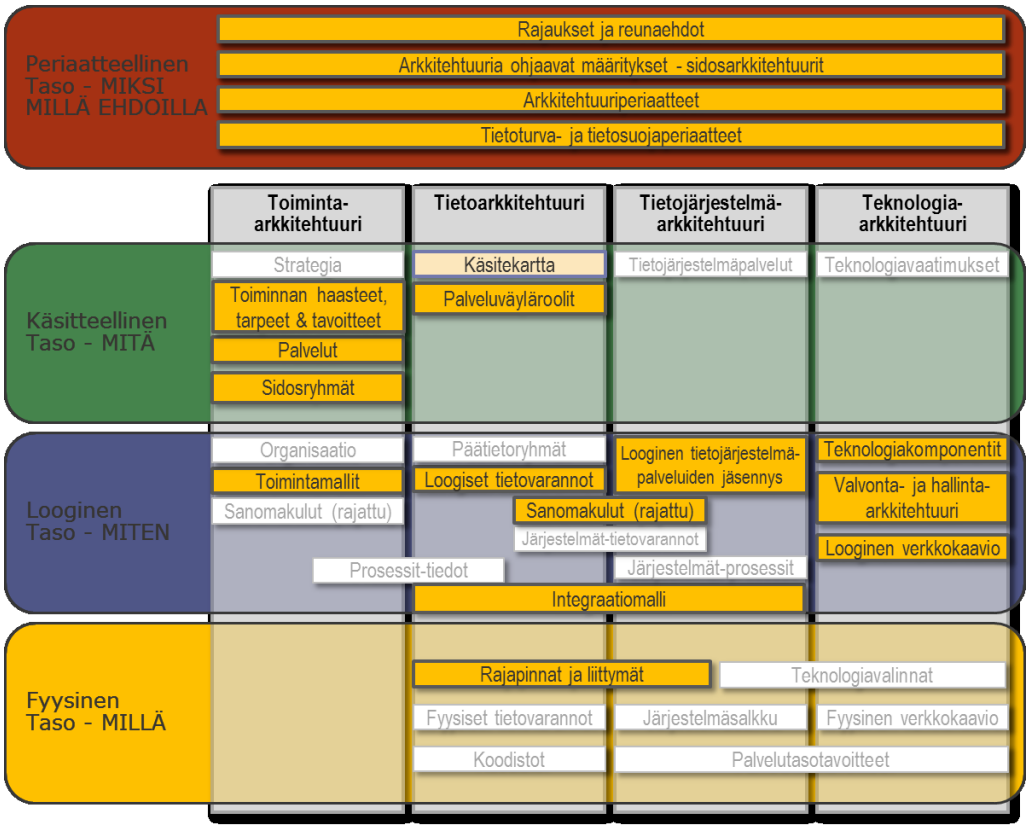
- *esim. tietovarantojen looginen jäsennys ja tietojen sijoittuminen eri kokonaisuuksiin*

- Fyysinen taso – MILLÄ
  - *esim. mihin fyysisiin tietokantoihin eri loogiset tietovarannot sijoitetaan, mitkä toteutetaan tiedostoina tai dokumenttienhallintajärjestelmän avulla*

Tässä työssä on soveltaen hyödynnetty alla kuvattua opetustoimen Kartturi-kokonaisarkkitehtuurimenetelmää, joka on yhteensopiva laajennus JHS 179 kokonaisarkkitehtuurimenetelmään:



Kokonaisarkkitehtuurimenetelmän mukaisesti arkkitehtuurityö käynnistettiin määrittämällä, mitä KA-kuvauksia tässä nimenomaisessa kohteessa hyödynnetään. Tässä työssä kokonaisarkkitehtuurikuvauksen kohteena on tavoitetilaa kuvaava viitearkkitehtuuri, joten kuvaaminen painottui kokonaisarkkitehtuurifilosofian mukaisesti kaavion yläosan tavoitteita kuvaaviin osiin. Tässä kuvauksessa on mallinnettu soveltaen seuraavat keltaisella kuvatut kokonaisarkkitehtuurin osakuvaukset.



Tavoitetilan lisäksi koottiin ja arvioitiin keskeisimpiä lähtötilanteen integraatioratkaisuja.

4. Periaatetason arkkitehtuurilinjaukset

4.1. Kansallisen palveluväyläarkkitehtuurin yleiskuva; rajaukset ja reunaehdot

4.1.1. Yleiset reunaehdot ja rajaukset

Ensimmäinen tehtävä tavoitearkkitehtuuria kuvattaessa on rajata selkeästi ja tarkasti kuvattava kohde. Samalla tunnistetaan ne reunaehdot, jotka joko kuvaamistyössä tai varsinaisissa kohdearkkitehtuurilinjauksissa on otettava huomioon.

- **Rajaus** = kuvataan vain tähän asti, ei mennä tämän rajan yli, ei suunnitella tai kuvata tätä asiaa lainkaan tässä vaiheessa (rajaus ulos) tai käsitellään vielä ainakin tämä asia (rajaus sisään)
- **Reunaehto** = tavoitearkkitehtuurin tulee täyttää tämä ehto, tavoitetilan tulee olla tämän reunaehdon mukainen, tavoitetilan tulee sisältää tämä asia

Tähän viitearkkitehtuuriin kuuluu erityisesti kansallisen tiedonvaihdon infrastruktuurin loogisen tason ylätason määrittely sekä liitettävien palvelujen ja palveluväylän ytimeen kuuluvien palvelujen keskinäinen jäsennys. Tämän

arkkitehtuurin piiriin katsotaan kuuluvan myös palveluväylän hallintaan ja jatkuviin palveluihin tarvittavat peruskomponentit ja kokonaisuudet.

Kansallisen palveluväylän viitearkkitehtuurin kuvaamisen on rajattu seuraavasti:

Kehittämistä koskeva rajaus tai reunaehto	Reunaehto/ rajaus	Vaikutukset
Palveluväylän tietojen välittämistä tarkastellaan kaikkien toimialojen ja organisaatioiden tarpeista	Rajaus - sisään	Kehittämisen alussa ei rajata vielä mitään palveluja pois palveluväylän palveluista
Palveluväylä on kansallinen ratkaisu, joka sisältää sekä julkisen hallinnon, yksityissektorin että kolmannen sektorin tietojen ja palveluiden vaihdon.	Rajaus - sisään	Kansallisen palveluväylän avulla voidaan yhdistää kaikkien toimijoiden palvelut saumattomiksi ja asiakaslähtöisiksi kokonaisuuksiksi hallinnollisista rajoista riippumatta
Palveluväylän kehittämiseen sisältyy tarkastelu sen kytkemisestä kansaivälisiin palveluihin ja tietolähteisiin	Rajaus - sisään	Vähintään palveluväylän "reunaan" tulee voida liittää palveluja, jotka kytkevät sen kansainvälisiin kohteisiin
Palveluväylä keskittyy eri osapuolten tietojen tehokkaaseen ja helppoon välittämiseen. Siinä ei vielä määritetä kaikkia mahdollisia sen kautta saatavia palveluja.	Rajaus - ulos	Palveluväyläarkkitehtuurissa ei kuvata kaikkia yksittäisiä palveluja, joita siihen voidaan tuottaa. Työssä otetaan kuitenkin huomioon keskeisimmät yleiset palvelut, joita tarvitaan palveluväylän tehokkaaseen käyttöön.
Palveluväylän tavoitearkkitehtuurissa hyödynnetään olemassa olevia ratkaisumalleja	Rajaus - ulos	Palveluväylän toteutustason ratkaisussa käytetään mahdollisuuksien mukaan jo olemassa olevia ratkaisuja ja toteutuksia
Palveluväylä keskittyy siirtämään tietoja vain **palveluiden** välillä	Rajaus - ulos	Palveluväylä ei sisällä merkittävästi loppukäyttäjän asiointipalvelukokonaisuuksia, joilla tuotetaan tietoa. Palveluväylä kytkeytyy lähinnä palveluihin.
Palveluväylä on loppukäyttäjälle läpinäkyvä kokonaisuus	Reunaehto	Palveluväylä ei sellaisenaan näy loppukäyttäjille muuten kuin välillisesti - joukkona parempia toisiinsa kytkettyjä ja kehittyviä palveluja
Palveluväylä tulee määritellä sille tasolle, että sen toteuttaminen voidaan käynnistää heti viitearkkitehtuurityön jälkeen	Reunaehto	Palveluväylätyössä tulee löytää yhteinen näkemys toteutettavasta palvelusta ja sen keskeisistä ratkaisuista. Kehittäminen tulee pystyä vaiheistamaan

Viitearkkitehtuuri kattaa laajasti kaikki olennaiset ylätason eri organisaatioiden ja kansalaisten palvelujen tietojen vaihtoon ja eri toimijoiden sähköisten palvelujen hyödyntämiseen liittyvät kokonaisuudet. Erityisesti viitearkkitehtuuri käsittelee kokonaisarkkitehtuurin keinoin tasapuolisesti kaikkia kokonaisarkkitehtuurinäkökulmia – toimintaa, tietoa, tietojärjestelmäpalveluita ja loogisella tasolla teknologiaa. Toteutettavan palveluväyläratkaisun tulee olla monipuolisesti hyödynnettävissä ja kaikkien toimijoiden käytettävissä.

Tässä viitearkkitehtuurissa on keskitytty erityisesti kokonaisvaltaiseen tietojen vaihdon tarkasteluun – ottamatta tarkasti kantaa, mitkä palvelut palveluväylään tullaan kytkemään. Palveluväylän tulee myös pystyä hyödyntämään jo olemassa olevia ja muilla sektoreilla määriteltyjä (esim. EU-tasolla tai tietyllä toimialalla) rajapintoja ja integraatiomalleja. Viitearkkitehtuuri keskittyy erityisesti kokonaisvaltaiseen kansalliseen tietojenvaihdon yhteentoimivuuteen sekä laajennettavuuteen. Rajausten perusteella tavoitteeksi määrittyi tavoite laatia sekä ylätason yhtenäinen kokonaiskuva eri toimijoiden palvelujen hyödyntämisestä että erityisesti jäsentää, mistä komponenteista palveluväylä koostuu.

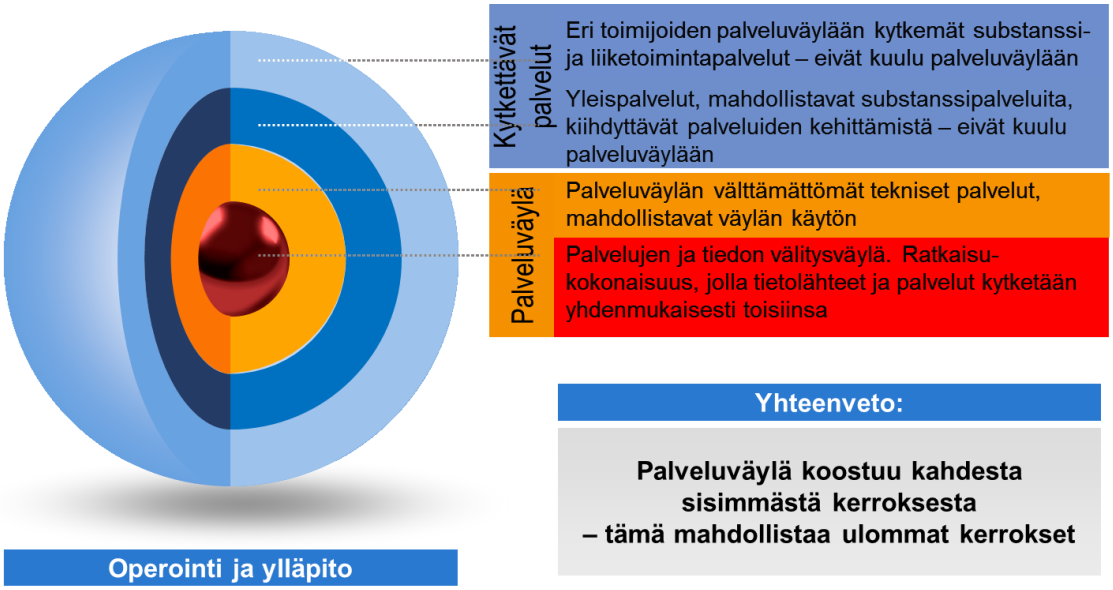
Kuvauksen rajaukset ja reunaehdot on listattu tarkemmin *Liitteessä 1, KA-taulukot*.

4.1.2. Kansallinen palveluväylä konseptina

Edellä kuvatun perusteella kansallinen palveluväylä voidaan määritellä laajennettavana konseptina, joka katalyytin tavoin kiihdyttää yhteentoimivien ja innovatiivisten sähköisten palvelujen kehittämistä ja tätä kautta parempia ja kustannustehokkaampia palveluita

Kansallinen palveluväylä tuo helpon ja turvallisen tavan kytkeytyä sekä julkisen hallinnon että yritysten ja kolmannen sektorin tarjoamiin tietovarantoihin ja sähköisiin palveluihin kustannustehokkaalla tavalla.

Kansallinen palveluväylä toimii eri toimijoiden välisten palvelujen yhdistävänä ytimenä:



Kansallinen palveluväylä on tiedonvälityskokonaisuus, joka itsessään ei tarjoa uusia tietoja palvelujen käytettäviksi eikä tarjoa olemassa olevien tietolähteiden avulla uusia palveluja. Kukin palveluväylään liitetty järjestelmä hallitsee omia tietojaan sekä vastaa siitä, että muiden tarvitsemat tiedot ovat saatavissa välitysalustan kautta ottaen huomioon tietojen käyttöön liittyvät mahdolliset rajoitukset.

Palveluväylä itsessään ei tarjoa loppukäyttäjäpalveluita. Palveluväylä on tietojärjestelmien välillä oleva komponentti, joten se on täysin läpinäkyvä kansalaiselle, yrityksen työntekijälle, viranhaltijalle ja muille tietojärjestelmiä hyödyntävälle loppukäyttäjälle.

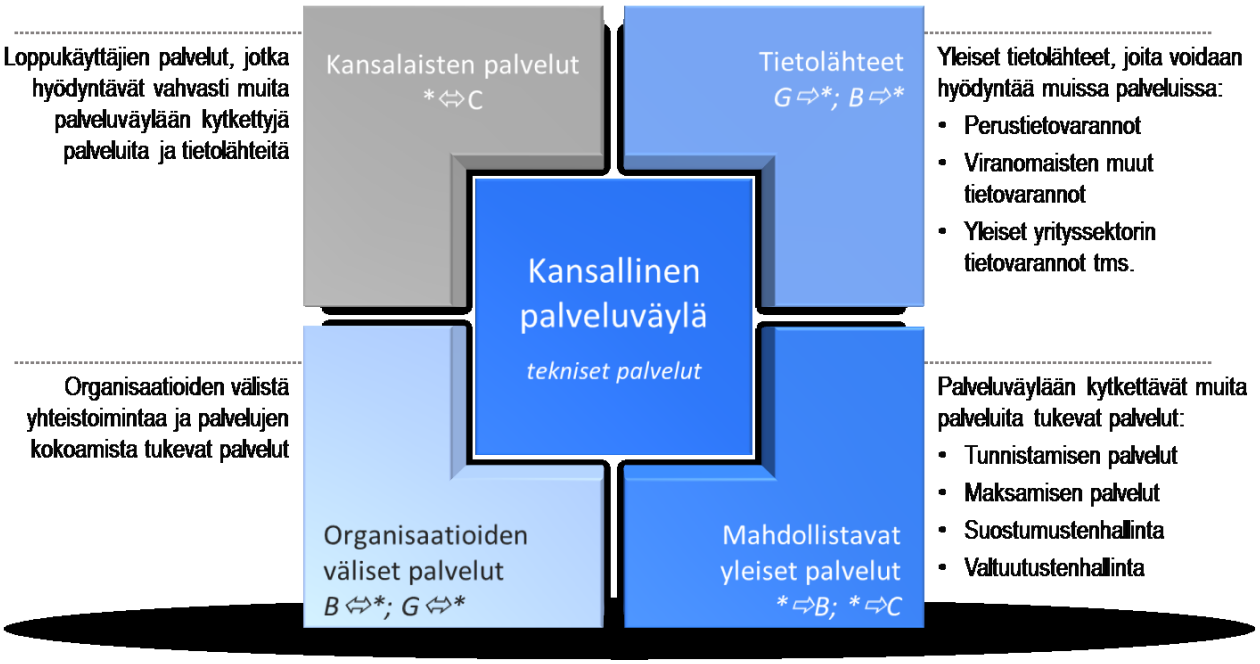
Kansallinen palveluväylä luo kansallisten tietovarantojen ja palvelujen sekä näitä tarjoavien toimijoiden ekosysteemin, joka pystyy luomaan helposti ja nopeasti kansalaisten käyttämiä lisäarvopalveluita hyödyntämällä eri ratkaisuihin tallennettuja tietoja.

Palveluväylä ei itsessään muuta tai luo uusia toiminnallisia palveluprosesseja. Mikäli kaikki nykyiset palvelut ja tietovarannot muutettaisiin kommunikoi-

maan palveluväylän kautta, palvelujen loogiset tietovirrat säilyisivät samanlaisina. Palveluväylän käyttöönotto ei vaikuta palveluihin loogisella tasolla.

Palveluväylä ei tarjoa substanssipalveluita. Palveluväylän loppukäyttäjähyödyt syntyvät palveluväylään kytketyistä tiedoista ja palveluista, ei väylästä itsestään. Palveluväylän arvo on sen muodostamassa standardoidussa tietojen vaihdon ratkaisumallissa.

Palveluväylä voi kytkeä toisiinsa erilaisia palveluja ja palveluketjuja[1]:



Yllä oleva kuva havainnollistaa palveluväylän roolia osana kansallista palveluarkkitehtuuria.

Kansallinen palveluväylä muodostaa ekosysteemin, joka voi sujuvasti ja nopeasti tuottaa yhteentoimivia kansalaisten, yritysten ja julkisen hallinnon lisäarvopalveluja.

Tekniset palvelut

Palveluväylän ytimessä olevat tekniset palvelut sisältävät väylän toiminnan kannalta välttämättömimmät osat ja tekniset palvelut, joita ilman palveluväylä ei voi täyttää tehtäväänsä eikä varsinaisia palveluväylään liitettäviä palveluja ja tietovarantoja pystytä palveluväylän avulla luotettavasti käyttämään. Palveluväylän ydinpalveluihin kuuluvat teknisen toiminnallisuuden lisäksi mm. operatiiviset ja toiminnalliset määritykset ja kuvaukset, palveluväylän käyttöehdot, sekä toimijoilta edellytettävien kyvykkyyksien listaus, jotka voivat olla erilaisia toimijan roolista riippuen (esim. yleispalveluilta voidaan edellyttää väylän näkökulmasta eri asioita kuin niitä hyödyntäviltä kansalais- ja yhteisöpalveluilta). Palveluväylän omistaja ja operaattori vastaa kaikista.

[1] Kuvassa: C=consumer, kuluttaja tai kansalainen; B=Business, yksityinen sektori, liike-elämä, G=Government, julkinen hallinto.

Yleispalvelut

Palveluväylän hyödyntämistä helpottaa joukko kansallisen palveluarkkitehtuurin yleispalveluja, jotka eivät ole välttämätön osa palveluväylää, mutta ne merkittävästi helpottavat palveluväylään kytkettyjen muiden palvelujen käyttöä ja kiihdyttävät palveluväylän hyödynnettävyyttä. Yleispalvelut eivät sisällä varsinaisia substanssi- tai liiketoimintapalveluja vaan ovat luonteeltaan näitä tukevia. Tyypillisiä yleispalveluja ovat esimerkiksi kansalaisen ja yritysten tunnistamiseen liittyvät palvelut tai tietojen käytön suostumuksiin ja sähköisiin valtuutuksiin liittyvät palvelut. Yleispalveluita voidaan kehittää ja hankkia useilta osapuolilta.

Organisaatioiden väliset palvelut

Organisaatiot pystyvät kytkemään palvelujaan toisiinsa kansallisen palveluväylän avulla. Kansallinen palveluväylä helpottaa eri organisaatioiden välisten prosessien kytkemistä toisiinsa liiketoiminnan ja loppukäyttäjän näkökulmasta saumattomiksi kokonaisuuksiksi.

Tietolähteet

Palveluväylään voidaan liittää eri organisaatioihin ja palveluihin tallennettua tietoa käytettäväksi muissa palveluissa. Keskeisimpiä kytkettäviä tietolähteitä ovat seuraavat kansalliset perustietovarannot:

- väestötietojärjestelmä
- yhdistysrekisteri
- kaupparekisteri
- säätiörekisteri
- kiinteistötietojärjestelmä
- yritys- ja yhteisötietojärjestelmä
- Maanmittauslaitoksen ja Geodeettisen laitoksen ylläpitämä maastotietoja koskeva tietojärjestelmä

sekä

- todennetun osaamisen rekisteri TOR (valmisteilla SADe-ohjelman Oppijan palvelukokonaisuudessa)
- terveydenhuollon potilastietopalvelu KanTa ja vastaava tuleva sosiaalihuollon asiakastietopalvelu KanSa.

Muut palvelut voivat käyttää sovittujen käyttöehtojen ja tietosuojalainsäädännön puitteissa perustietovarantoihin ja muihin julkisen hallinnon tietovarantoihin taltioitua tietoa helposti ja turvallisesti. Tämä ei välttämättä kokonaan poista tietojen kokoamista useaan paikkaan, mutta tällä vältetään tarpeeton saman tiedon moneen kertaan tallentaminen ja vältetään pyytämästä loppukäyttäjältä sellaista tietoa, jonka viranomaiset ovat jo itse taltioineet tai jonka loppukäyttäjä on jo toiselle viranomaiselle antanut.

Yllä lueteltujen julkisen hallinnon perustietovarantojen lisäksi tietolähteiksi voidaan luonnollisesti kytketä muita julkisen hallinnon ja yksityisen sektorin sekä kolmannen sektorin tietovarantoja.

Kansalaisten palvelut

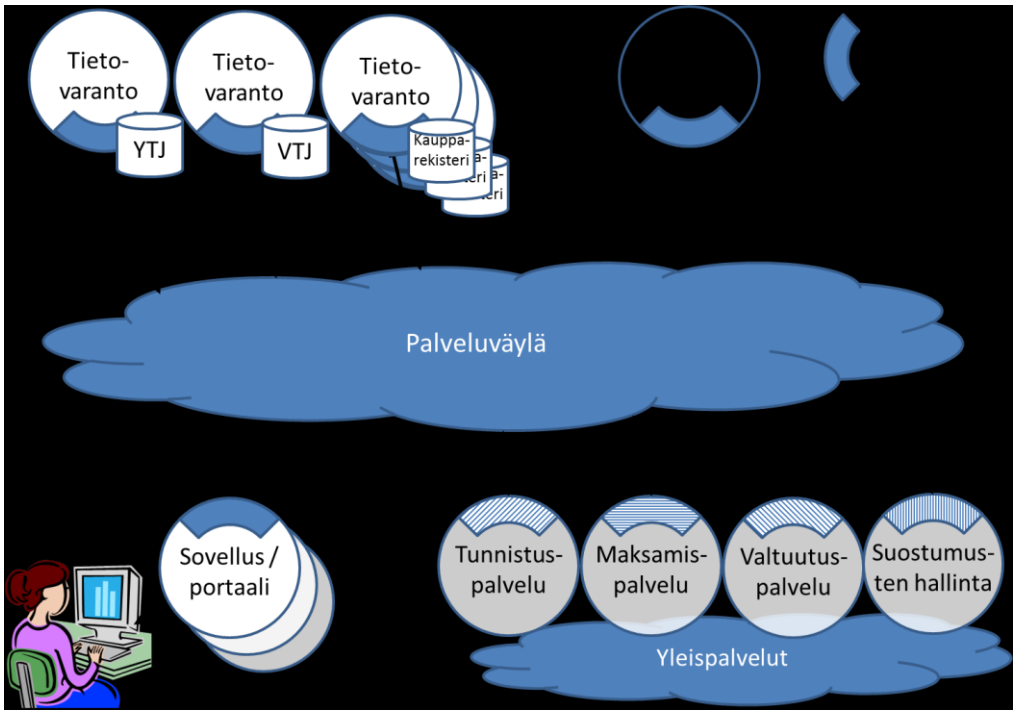
Kansalaisten palvelut syntyvät pääosin välillisesti. Eri organisaatiot voivat kansallisen palveluarkkitehtuurin yleispalvelujen, organisaatioiden välisen tiedonvaihdon sekä tietovarantojen avulla luoda luovia ja hyödyllisiä kansalaisille ja yrityksille sekä yhteisöille tarkoitettuja substanssipalveluja.

Näiden lisäksi itse kansalliseen palveluväylään voidaan haluttaessa kehittää loppukäyttäjäpalveluja, kuten esimerkiksi palvelu, jonka avulla kansalainen voi seurata, mitä tietoja hänestä on eri tietovarantoihin tallennettu tai mihin hänen tietojaan on käytetty.

Palveluiden ja tietolähteiden kytkeminen toisiinsa

Palveluväylä, sen rajapinnat ja väylään oleellisesti kuuluvat infrastruktuuripalvelut sekä kansallisen palveluarkkitehtuurin yleispalvelut mahdollistavat uusien tietolähteiden avaamisen palvelujen käytettäväksi yhdenmukaisilla tavoilla sekä uusien palvelujen helpomman toteuttamisen luomalla eri tietolähteille yhtenevän rajapintamallin, kuten alla oleva kuva havainnollistaa. Kuvassa toimijat ovat:

- Loppukäyttäjä, joka voi olla yksityinen kansalainen, yrityksen edustaja, virkamies jne. joka käyttää palveluväylään liitettyä sovellusta. Loppukäyttäjä voi olla myös tietojärjestelmä, mikä on normaali toimintatapa automatisoiduissa prosesseissa.
- Käyttöliittymäsovellus, joka on loppukäyttäjän näkymä palveluun. Mikäli kyseisen sovelluksen käyttö edellyttää käyttäjän tunnistuksen, sovellus tekee sen kansallisen palveluarkkitehtuurin yleispalveluna olevan tunnistuspalvelun avulla. Tunnistuspalvelu (joita voi olla useampia) kykenevät erilaisiin tunnistustapoihin.
- Tietovarantosovellus, joka tarjoaa palveluväylään tietoja. Tyypillisinä esimerkkeinä julkishallinnon tietovarannoista ovat YTJ, Väestörekisteri ja Kaupparekisteri.
- Lisäarvopalvelu, joka voi esim. yhdistää useamman rekisterin tietoja ja tarjota yhdisteltyjä tietoja muille sovelluksille. Lisäarvopalvelu voi myös olla prosessimoottori tms. joka huolehtii palveluprosessin tai sen osan läpimenosta.
- Kansalliseen palveluarkkitehtuuriin kuuluvat yleispalvelut, jotka eivät ole palveluväylän sisäisiä palveluita, mutta edesauttavat palveluväylän hyödyntämistä.
- Palveluväylä, joka tarjoaa rajapintamääritysten lisäksi palveluhakemiston, tietoturvaan liittyvät palvelut (mm. liittymisen edellytykset), tapahtumalokipalvelut jne.



Kansallisen palveluväylän viitearkkitehtuurin määrityksessä huomioidaan olemassa olevat määritykset ja ratkaisut sekä on pyritty pitämään niihin kohdistuvien muutoksien määrää mahdollisimman pieninä.

Palveluväylän hyödyntäminen siten, että luodaan uusia lisäarvopalveluita, suurella todennäköisyydellä edellyttää lainsäädännöllisiä muutoksia. Väylän menestyksellisen käyttöönoton edellytyksenä voidaan pitää, että palveluiden rakentamisen kannalta oleelliset tietopalvelut ja tietovarannot ovat sen kautta hyödynnettävissä. Tämä tarkoittaa lainsäädännön, tietovarantojen käyttöehtojen ja käytön hinnoittelun tarkistamista sekä tietovarantojen tarjoamien rajapintojen toteuttamista yhteisten määritysten mukaisiksi.

Palveluväylän liiketoimintamallin tulee mahdollistaa palveluväylän palvelujen ja niiden käytön nopea laajentaminen. Väylään liittymisen edellytykset palveluja tarjoaville sovelluksille on mahdollistettava ja väylästä aiheutuvien kustannuksien kattaminen saatava tasolle, joka tekee väylän käyttämisestä houkuttelevan.

Palveluväylä kokonaispalveluna

Palveluväyläkokonaisuus sisältää teknisten komponenttien lisäksi jatkuvan palvelun komponentit, joilla varmistetaan kansallisen palveluväylän toimivuus ja kehittyminen tarpeen mukaan:

Palveluväylä on konsepti

- Palveluväylä sisältää tekniset tiedon- ja sanomanvälitysratkaisun lisäksi palvelut, joilla varmistetaan ratkaisun toimivuus, kapasiteetti, turvallisuus ja ajanmukaisuus
- Palveluväylä sisältää välttämättömät tekniset tukipalvelut palveluväylän käytölle kansallisesti (esim. järjestelmävarmenteet)
- Palveluväyläkonseptiin määritetään myös selkeä toimintamalli ja palvelujen kytkemistä ja kehittämistä tukevat asiantuntijapalvelut – tarkoituksenmukaisessa laajuudessa

Kansalliselle palveluväylälle määritetään palveluväyläoperaattori, joka järjestää palveluväylän keskitettyjen palvelujen käyttö-, kapasiteetti- ja ylläpitopalvelut. Näillä palveluilla varmistetaan riittävä suorituskyky, tietoturvallisuus ja palvelun jatkuvuus. Palveluväyläoperaattori voi joko itse tuottaa nämä jatkuvat palvelut tai se hankkii nämä erikseen toiselta taholta, joka toimii käytännön tasolla palveluväylän ylläpitäjänä.

Kansallinen palveluoperaattori kehittää Palveluväylän omistajan ja ohjausorganisaation sekä asiakkaiden tarpeiden pohjalta kansallisten palveluväylän ominaisuuksia ja käytettävyyttä jatkuvan kehittämisen prosessin mukaisesti.

4.2. Sidosarkkitehtuurit, -hankkeet ja –ratkaisut

Kehittämisen kohteena olevaan alueeseen liittyy useita sidosratkaisuja ja –hankkeita sekä lainsäädäntöä ja sidosarkkitehtuureja, jotka tulee ottaa huomioon kansallista palveluväylää kehitettäessä.

4.2.1. Ohjaava lainsäädäntö

Kansallista palveluväylää ohjaavat erityisesti tiedonvaihtoa sekä henkilötietojen käsittelyä koskevat lait. Tässä työssä ei ole koottu näitä lakeja kattavasti, mutta seuraavaan on listattu tyypillisimpiä kansallisen palveluväylän kehittämistä ja siihen kytkettäviä palveluja ohjaavaa lainsäädäntöä.

Yleinen tiedonhallintaa ja tietojen käyttöä koskeva lainsäädäntö

Tiedonhallintaa koskeva yleislainsäädäntö		
Laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki),	**Velvoittava**	Ks.Finlex. Yleinen tiedonhallintaa koskeva perussäännös
Arkistolaki (831/1994)	**Velvoittava**	Ks.Finlex. Yleinen tiedonhallintaa koskeva perussäännös
Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011, tietohallintolaki)	**Velvoittava**	Ks.Finlex. Yleinen tiedonhallintaa koskeva perussäännös
Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010, tietoturvallisuusasetus)	**Velvoittava**	Ks.Finlex
Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)	**Velvoittava**	Ks.Finlex

Sähköisiä palveluja koskevia lakeja

Sähköisiä palveluja koskevia lakeja		
sähköisestä asioinnista viranomaistoiminnassa annettu laki (13/2003)	**Velvoittava**	Ks.Finlex
tietoyhteiskunnan palveluiden tarjoamisesta annettu laki (458/2002)	**Velvoittava**	Ks.Finlex
sähköisen viestinnän tietosuojalaki	**Velvoittava**	Ks.Finlex
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)	**Velvoittava**	Ks.Finlex
viestintämarkkinalaki (393/2003)	**Velvoittava**	Ks.Finlex
verkkotunnuslaki (228/2003),	**Velvoittava**	Ks.Finlex
eräiden suojauksen purkujärjestelmien kieltämisestä annettu laki (1117/2001),	**Velvoittava**	Ks.Finlex
osittain julkisuuslaki- ja asetus (viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta annettu asetus 1030/1999, julkisuusasetus, JulkA)	**Velvoittava**	Ks.Finlex
laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)	**Velvoittava**	Ks.Finlex
henkilökorttilaki (829/1999)	**Velvoittava**	Ks.Finlex
valtioneuvoston asetus julkisen hallinnon yhteisistä sähköisistä asioinnin ja hallinnon tukipalveluista (393/2009)	**Velvoittava**	Ks.Finlex
henkilötietolaki ja kansainvälisistä tietoturvallisuusvelvoitteista annettu laki (588/2004)	**Velvoittava**	Ks.Finlex
rikoslaki (39/1889, muun muassa 34 luku 9 a–b §)	**Velvoittava**	Ks.Finlex

Yllä kuvatut lait tulee ottaa huomioon palveluväylään kytkettävien palvelujen yhteydessä.

Sektorikohtaiset tietojärjestelmäratkaisuja ohjaavat lait

Sektorikohtaiset tietojärjestelmäratkaisuja ohjaavat lait			
	rekisterihallintolaki (166/1996)	**Velvoittava**	Ks.Finlex
	yritys- ja yhteisötietolaki (244/2001, YtL)	**Velvoittava**	Ks.Finlex
	yritys- ja yhteisötietojärjestelmästä annettu laki (288/2001)	**Velvoittava**	Ks.Finlex
	pientyönantajien maksu- ja ilmoituspalvelujärjestelmästä annettu laki (658/2004)	**Velvoittava**	Ks.Finlex
	henkilötietojen käsittelystä poliisitoimessa annettu laki (761/2003)	**Velvoittava**	Ks.Finlex
	tie- ja katuverkon tietojärjestelmästä annettu asetus (991/2003)	**Velvoittava**	Ks.Finlex
	ajoneuvoliikennerekisteristä annettu laki (541/2003), työhallinnon asiakaspalvelun tietojärjestelmästä annettu laki (1058/2002)	**Velvoittava**	Ks.Finlex
	henkilötietojen käsittelystä rangaistusten täytäntöönpanossa annettu laki (422/2002)	**Velvoittava**	Ks.Finlex
	maaseutuelinkeinohallinnon tietojärjestelmästä annettu laki (284/2008)	**Velvoittava**	Ks.Finlex
	ulosottokaari (705/2007, 24–35 §)	**Velvoittava**	Ks.Finlex
	yrityspalvelujen asiakastietojärjestelmästä annettu laki (240/2007),	**Velvoittava**	Ks.Finlex
	sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (159/2007)	**Velvoittava**	Ks.Finlex
	sähköisestä lääkemääräyksestä annettu laki (61/2007)	**Velvoittava**	Ks.Finlex
	rakennerahastolaki (1401/2006, 65 §)	**Velvoittava**	Ks.Finlex
	vesikulkuneuvorekisteristä annettu laki (976/2006)	**Velvoittava**	Ks.Finlex
	ympäristönsuojelulaki (86/2000, 27 §)	**Velvoittava**	Ks.Finlex
	hätäkeskuslaki (157/2000, 7 §)	**Velvoittava**	Ks.Finlex
	lainhuuto- ja kiinnitysrekisteristä annettu laki (353/1987, LkL)	**Velvoittava**	Ks.Finlex
	kiinteistörekisterilaki (392/1985, KrL)	**Velvoittava**	Ks.Finlex
	yhdistysrekisteriasetus (506/1989, YrA)	**Velvoittava**	Ks.Finlex
	säätiölaki (109/1930) ja -asetus (1045/1989)	**Velvoittava**	Ks.Finlex
	verotililaki (604/2009)	**Velvoittava**	Ks.Finlex
	Laki hallinnon turvallisuusverkkotoiminnasta	**Velvoittava**	Ks.Finlex
	Laki potilaan asemasta ja oikeuksista (785/1992), 4 luku;	**Velvoittava**	Ks.Finlex
	Terveydenhuoltolaki, 9 §;	**Velvoittava**	Ks.Finlex
	Laki sähköisestä lääkemääräyksestä (61/2007);	**Velvoittava**	Ks.Finlex
	Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000), erityisesti 3 ja 4 luvut	**Velvoittava**	Ks.Finlex
	Laki sosiaali- ja terveydenhuollon asiakastietojen sähkoisestä käsittelystä 9.2.2007/159 muutoksineen	**Velvoittava**	Ks.Finlex. Esim. "Kansaneläkelaitos ei saa antaa valtakunnallisten tietojärjestelmäpalvelujen järjestämiseen liittyvien potilasrekistereiden tai niihin liittyvien lokirekistereiden käsittelyä tai säilyttämistä toimeksiantotehtävänä ulkopuolisille"
	Perusopetuslaki (628/1998) erityisesti 31a §	**Velvoittava**	Ks.Finlex
	Laki opiskelijavalintarekisteristä ja ylioppilastutkintorekisteristä (1058/1998);	**Velvoittava**	Ks.Finlex
	Kiinteistörekisterilaki (392/1985);	**Velvoittava**	Ks.Finlex
	Laki Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009), erityisesti 22 §;	**Velvoittava**	Ks.Finlex
	Laki maaseutuelinkeinohallinnon tietojärjestelmästä (284/2008)	**Velvoittava**	Ks.Finlex
	Henkilotietolaki 22.4.1999/523	Velvoittava	Ks.Finlex

Edellisten lisäksi on olemassa toimiala- ja virastojen erityistoimintaa koskevaa erityislainsäädäntöä.

Kunkin kansalliseen palveluväylään palveluja tuovan organisaation tulee ottaa huomioon omaa toimintaansa ja kyseistä palvelua / tietolähdettä ja sen tietojen vaihtoa koskeva lainsäädäntö. Kansallisessa palveluväylässä tietojen vaihtoa voidaan rajoittaa kahdenvälisin sopimuksin.

4.2.2. Sidosarkkitehtuurit

Seuraavaan on koottu palveluväylän kehittämiseen kytkeytyvät keskeiset sidoshankkeet ja –ratkaisut. Velvoittavuus –sarake kuvaa, onko kyseisessä kehittämisessä huomioitava vai noudatettava kyseisen ratkaisun määrityksiä.

Tyypillisiä toimialakohtaisia olemassa olevia kansainvälisiä tiedonvaihdon ohjaavia arkkitehtuureja ovat mm.:

Integraatiopalvelujen toimialakohtaisia sidosarkkitehtuureja			
EU:n EMCS-arkkitehtuuri	Ohjaava	Tätä täydentää Finseed-arkkitehtuuri. Excise Movement and Control System. Se on sähköinen järjestelmäkokonaisuus, jonka avulla valvotaan koko EU:ssa yhdenmukaistetun valmisteveron alaisten tuotteiden eli alkoholin, alkoholijuomien, tupakan ja nestemäisten energiatuotteiden verottomuusjärjestelmässä tapahtuvia siirtoja	EU-komissio
EMEA EudraVigilance gateway	**Velvoittava**	The EudraVigilance Gateway. EudraVigilance is EMEA's new European data-processing network and database management system for the exchange, processing and evaluation of expedited Individual Case Safety Reports (ICSRs) in pharmacovigilance related to all medicinal products authorized in the European Union.	EMEA
epSOS	**Velvoittava**	epSOS aims to design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. **In a first phase:** - Patient Summary: access to important medical data for patient treatment - Cross-border use of electronic prescriptions ("ePrescription" - or "eMedication" systems) **In a second phase** (epSOS enlargement phase): - Integration of the 112 emergency services - Integration of the European Health Insurance Card (EHIC) - Patient access to their data	EU-komissio
Pankkien sanomastandardit	**Velvoittava**	Pankkisanomastandardit rahasiirroille	
Sähköiset laskustandardit	**Velvoittava**	eInvoice-standardit	
eReseptin integraatioarkkitehtuuri	Ohjaava	ks. Kunta-IT:n tuotokset 2011	VM / Kuntaliitto

Olemassa olevia kansallisia ohjaavia tai huomioitavia ratkaisuja sekä käynnissä olevia ja käynnistyviä tietojen vaihtoon keskittyviä hankkeita ovat mm.:

Olemassa olevat kansalliset toteutukset			
Valtionhallinnon integraatiopalvelu (VIA)	Huomioitava	Valtion IT-palvelukeskuksen ylläpitämä palvelu, jonka avulla palvelua käyttävät asiakkaat voivat siirtää digitoituja tietoja (sanomia) eri tietojärjestelmien ja tietolähteiden välillä – joko asiakakkaan omien tietojärjestelmien välillä tai omien tietojärjestelmien ja muiden organisaatioiden tietojärjestelmien välillä. Integraatiopalvelu on turvallinen, luotettava ja tehokas tapa yhdistää tietojärjestelmät ja varmistaa niiden välinen tiedonsiirto.	Valtiokonttori / VIP
KanTa	Ohjaava	KANTA-integraatiomäärittely. Huom. Laajenee mahdollisesti sosiaalihuollon tietojen vaihtoon (KanSa)	Kela, ohjaus STM ja THL
Käynnissä olevat tai käynnistyvät tietojen vaihtoon suoraan liittyvät hankkeet			
Perustietovarantojen viitearkkitehtuuri	Ohjaava	Kansallisten perustietovarantojen käytön ja toteutuksen viitearkkitehtuuri. Tekeillä kesällä 2013	VM/JulkICT
Kansallinen sähköinen identiteettihanke, kansalaisen tunnistaminen	Huomioitava	Suunnitteluvaiheessa kesällä 2013	VM/JulkICT

Näistä erityisesti perustietovarantojen tietojen vaihdon ratkaisukokonaisuus sekä mahdollinen kansalaisen tunnistamisen palvelu kytkeytyvät suoraan kansallisen palveluväylän ja siihen kytkettävien palvelujen suunnitteluun ja toteutukseen.

Muita erityisesti integraatiopalveluita ja tiedon vaihdon ratkaisuja ohjaavia sidosratkaisuja ovat mm.:

Muut integraatiopalveluita koskevat sidosarkkitehtuurit			
STM:n Kanta-välittäjätahon auditointikriteeristö	Ohjaava	Sisältää potilastietoja ja sähköisiä lääkemääräyksiä välittävän välittäjätahon turvallisuusvaatimukset	
Sote-sektorin alueelliset integraatioratkaisut ja liityntäpisteet	Huomioitava	Useita. Esim. HUS-alueen Alli/Navitas-palvelu	Useita
Organisaatioiden sisäiset integraatio- ja palveluväyläratkaisut	Huomioitava	Useita, organisaatiokohtaisia. Ks. Esim. Kunnan sähköisen asioinnin arkkitehtuuri	Useita
Kuntien KY-verkko	Huomioitava	Kuntien yhteisen tietoliikenneinfrastruktuurin kehittämisprojekti	Kuntaliitto
Viron X-road -palveluväyläratkaisu	Huomioitava	Kansallinen palveluväyläratkaisu Virossa. Perustuu hajautettuun verkostoon.	
Ruotsin SHS-palveluväyläratkaisu	Huomioitava	Kansallinen palveluväyläratkaisu Ruotsissa. Perustuu hajautettuun verkostoon.	Försakringkassan
Belgian Federal Service Bus	Huomioitava	Kansallinen palveluväyläratkaisu Belgiassa. Perustuu keskitettyyn integraatiovälineeseen.	

Yllä mainittuja eri toimialojen ja eri maiden integraatioratkaisuja voidaan hyödyntää kansallisen palveluväylän viitearkkitehtuurin suunnittelussa. Sosiaali- ja terveydenhuollossa tiedonvälityksen toimijoiden tulee täyttää yllä mainitut STM:n Kanta-välittäjätahon lähinnä tietoturvallisuutta koskevat auditointikriteerit.

Kansallista palveluväylää kehittävien tahojen ja tietojärjestelmätoimittajien tulee arvioida kehittämisen aikana tarkemmin yllä kuvattuja sidosarkkitehtuureja ja kehittämisprojekteja ja tarpeen mukaan päivittää tätä viitearkkitehtuuria sidosarkkitehtuurien huomioon ottamisen osalta.

Kansallisen palveluväylän viitearkkitehtuuriin kytkeytyvät luonnollisesti muut julkisen hallinnon kokonaisarkkitehtuuriin ja muihin kansallisiin ratkaisuihin liittyvät sidosarkkitehtuurit ja määritykset, joista keskeisimmät ovat:

Julkisen hallinnon kokonaisarkkitehtuuri			
JHKA	**Velvoittava**	Julkisen hallinnon kokonaisarkkitehtuuri	VM / JulkICT
Sähköisen asiakaspalvelun viitearkkitehtuuri	Ohjaava	Kuvaa yleisen asiakaspalvelumallin, laajentaa sähköisen asioinnin arkkitehtuuria	VM / JulkICT
Tiedolla johtamisen arkkitehtuuri	Ohjaava	Johtamisen ja sen järjestelmäkokonaisuuden viitearkkitehtuuri	VM / JulkICT
Tietoarkkitehtuuri	Ohjaava	Kansallisen tietoarkkitehtuurin kuvaus	VM / JulkICT
Tiedon hallinnan viitearkkitehtuuri	Ohjaava	Tiedon ja ydintietojen hallinnan viitearkkitehtuuri	VM / JulkICT
Yhteisten ICT-palvelujen viitearkkitehtuuri	Ohjaava	Yhteisten ICT-palvelujen (esim. palvelinten käyttöpalvelut, työasemapalvelut tms.) viitearkkitehtuuri	VM / JulkICT

Kansalliset, yhteiset perustietovarannot			
Väestötietojärjestelmä, VTJ	**Velvoittava**	Väestötietojärjestelmä on valtakunnallinen atk-rekisteri, jossa on perustiedot Suomen kansalaisista ja Suomessa vakinaisesti asuvista ulkomaalaisista. Järjestelmässä on tietoa myös rakennuksista, rakennushankkeista ja huoneistoista sekä kiinteistöistä. Väestötietojärjestelmä on maamme eniten käytetty perusrekisteri.	Väestörekisterikeskus
Yhdistysrekisteri	**Velvoittava**	Sisältää suomessa toimivat rekisteröidyt yhdistykset ja uskonnolliset yhdyskunnat	Patentti- ja rekisterihallitus
Kaupparekisteri	**Velvoittava**	Kaupparekisteri on virallinen ja julkinen rekisteri yrityksistä. Enemmistön yrityksistä muodostavat osakeyhtiöt ja yksityiset elinkeinonharjoittajat. Yritysten lisäksi kaupparekisteriiin merkitään myös eräät muut yhteisöt, kuten asunto-osakeyhtiöt ja asumisoikeusyhdistykset.	Patentti- ja rekisterihallitus
Säätiörekisteri	Ohjaava	Sisältää tiedot rekisteröidyistä säätiöistä	Patentti- ja rekisterihallitus
Yritys- ja yhteisötietojärjestelmä	Ohjaava	Hakupalvelu, jonka kautta voi hakea tietoa yrityksistä, joilla on Y-tunnus	Patentti- ja rekisterihallitus
Kiinteistötietojärjestelmä	Ohjaava	Kiinteistötietojärjestelmään kuuluu kaksi rekisteriä: •kiinteistörekisteri; sekä •lainhuuto- ja kiinnitysrekisteri	Maanmittauslaitos
Maastotietokanta, paikkatiedot	Ohjaava	Maastoa ja rakennettua ympäristöä esittävät tiedot on kerätty Maastotietokantaan. Se sisältää tarkimman koko Suomen kattavan maastoa ja sen yksityiskohtia kuvaavan tiedon. Tietosisältö on yhteen sovitettua ja tietoja voidaan yhdistellä käyttötarpeen mukaan	Maanmittauslaitos
Todennetun osaamisen rekisteri	Ohjaava	Sisältää jatkossa (käynnistyy 2015, SADe-hanke) julkisen rahoituksen kautta hankitut luvanvaraisen koulutuksen tutkinnot ja myöhemmin opintosuoritukset.	OKM

Kansalliset palvelujen ohjauspalvelut			
Kansalaisen asiointitili	Ohjaava	Asiointitili on viranomaisen ja asiakkaan välisen sähköisen vuorovaikutuksen yhdenmukainen, helppokäyttöinen ja turvallinen keskitetty ratkaisu, joka on liitettävissä jo olemassa oleviin sähköisiin asiointipalveluihin. Asiointitilin asiakkaita ovat kansalaiset, yritykset ja yhteisöt.	Valtiokonttori / VIP
Suomi.fi	Ohjaava	Suomi.fi on julkishallinnon verkkopalveluiden yhteinen osoite. Portaaliin on koottu kansalaisten arkielämässä tärkeitä tietoja, jotka ovat julkishallinnon organisaatioiden tai niiden toimintaa täydentävien järjestöjen tuottamia. Suomi.fin sisältö koostuu tekstien ja linkkien lisäksi asiointipalveluista ja lomakkeista, laeista sekä uutisista.	Valtiokonttori / VIP

Kansalliset tekniset tukipalvelut			
Vetuma	Ohjaava	Julkishallinnon yhteinen verkkotunnistamisen ja -maksamisen palvelun (VETUMA) avulla kansalaisen on mahdollista tunnistautua ja maksaa sähköisesti kaikissa niissä asiointipalveluissa, joihin palvelu on liitetty. (Vetuma on tarkoitettu henkilöiden tunnistautumiseen, Verohallinnon toteuttama KATSO on tarkoitettu yritysten ja yhteisöjen tunnistautumiseen).	Valtiokonttori / VIP
Virtu	Huomioitava	Federoituun luottamusverkostoon perustuva virkamiehen tunnistamiseen liittyvä yhteinen palvelu, jota käytetään organisaatiorajojen ylitse käytettävien palveluiden käyttäjätunnistukseen. Virtun käyttöönotto vaatii organisaatiolta iPD-roolin. Virtulla saavutettavissa oleva hyöty on loppukäyttäjän näkökulmasta kertakirjautuminen (=muistettavien tunnusten+salasanojen määrä vähenee). Järjestelmän ylläpidon näkökulmasta välttää käyttäjien salasanojen unohtumiseen / lukkiutumiseen liittyvä työ. Mutta järjestelmien varsinaista käyttäjätietojen ja käyttöoikeuksien ylläpitotyötä ei Virtun käyttöön siirtyminen poista.	Valtiokonttori / VIP
Yleinen karttakäyttöliittymä	Huomioitava	Yleisen karttakäyttöliittymän avulla on helppo käyttää useita julkisia taustakarttapalveluja sekä liittää omia paikkatietoja karttakäyttöliittymään. Karttakäyttöliittymä sisältää hakupalvelut pai-kannimen ja osoitteen perusteella. Karttakäyttö-liittymä voidaan integroida osaksi sisällönhallin-tajärjestelmää.	YM / Rakennetun ympäristön ja asumisen palvelukokonaisuus
Katso (jatkossa Rova)	Huomioitava	Rooli- ja valtuutuspalvelu RoVa on yritysten ja yhteisöjen sähköisessä asioinnissa tarvittavien rooli- ja valtuutustietojen hallintaan tarkoitettu palvelu. RoVa-palvelun ensisijaisena tarkoituksena on tarjota julkishallinnon sähköisille asiointipalveluille ajantasainen, tarkka ja kattava tieto yrityksen tai muun tahon edustajana asioivan henkilön rooleista palveluissa. Korvaa Katso-palvelun.	Nyt: Vero ja Kela yhdessä, jatkossa TEM ja Vero

Edellisiä täydentävät vielä seuraavat sidosarkkitehtuurit:

Muut kansalliset sidosarkkitehtuurit ja määräykset				
	Arkistolaitos - sähköinen arkistointi	**Velvoittava**	Sähke 2 -normi. Sähköisen arkistoinnin vaatimukset	Arkistolaitos
	Yhteentoimivuus.fi	Ohjaava	Julkisen hallinnon yhteentoimivuuden aineistot (esim. KA-aineistot) kokoava kansallinen verkkoportaali	VM/JulkICT
	JHS-suositukset yleisesti	Ohjaava	JHS-järjestelmän mukaiset suositukset koskevat valtion- ja kunnallishallinnon tietohallintoa. Sisällöltään JHS voi olla julkishallinnossa käytettäväksi tarkoitettu yhtenäinen menettelytapa, määrittely tai ohje	Juhta
	JHS-152	Ohjaava	Suositus kuvaa prosessien kuvaamisen mallin.	Juhta
	Julkishallinnon XML-skeemojen määrittäminen	Ohjaava	JHS 170, Suosituksessa kuvataan julkisen hallinnon XML-skeemojen muodostamisen yhteisiä periaatteita.	Juhta
	JHS-174	Ohjaava	Suositus kuvaa sähköisissä palveluissa käytettävän palvelutasoluokituksen	Juhta
	JHS-179	Ohjaava	Suositus kuvaa julkisen hallinnon yleisen kokonaisarkkitehtuurimenetelmän	Juhta
	Metatietopalvelu	Huomioitava	Osa kansallisen tietoarkkitehtuurin jalkauttamista. Tulossa oleva palvelu.	VM/JulkICT

Yllä kuvatut sidosarkkitehtuurit on otettu huomioon tätä viitearkkitehtuuria kehitettäessä ja ne tulee arvioida tarkemmin kansallisen palveluväylän tarkemman ratkaisusuunnittelun yhteydessä. Kyseiset sidosarkkitehtuurit, sidoshankkeet ja ohjaava lainsäädäntö tulee käydä läpi myös yksittäisiä palveluväylään kytkettäviä palveluja ja niiden käyttöehtoja kehitettäessä.

Sidosarkkitehtuurit ja -hankkeet sekä ohjaava lainsäädäntö on listattu tarkemmin *Liitteessä 1, KA-taulukot.*

4.3. Arkkitehtuuriperiaatteet

Kansallisen palveluväylän ja siihen liittyvien palvelujen keskeiset suunnittelun ja toteutuksen sekä jatkuvien palvelujen peruskivinä toimivat linjaukset on koottu seuraaviksi arkkitehtuuriperiaatteiksi:

Nimi	Prioriteetti	Kuvaus
Palveluväylä muodostaa hallitun kokonaisuuden, jonka kautta organisaatioiden tietoaineistoja voidaan jakaa ja hyödyntää	✪✪✪✪✪	Palveluväylä on konsepti, joka sisältää teknisen tiedonvälityksen lisäksi välttämättömät tekniset palvelut sekä ylläpidon ja valvonnan, joiden avulla sitä kautta voidaan välittää kaikkea kansallista tietoa.
Palveluväylä tukee organisaatioiden välisten saumattomien palveluprosessien kehittämistä	✪✪✪✪✪	Palveluväylää voidaan hyödyntää kytkemään prosesseja saumattomasti toisiinsa. Palveluväylä toimii prosessien edellyttämällä laadulla ja tasolla.
Kaikki kansalliset organisaatiot voivat hyödyntää palveluväylään kytkettyjä palveluja ja tietolähteitä tietosuojan ja tietoturvan reunaehtojen puitteissa	✪✪✪✪✪	Kaikki julkisen hallinnon ja yksityisen ja kolmannen sektorin toimijat voivat julkaista tietovarantojaan ja hyödyntää muiden palveluja sovittujen käyttöperiaatteiden mukaisesti. Tämä sisältää myös Sote-palvelujen tiedonvaihdon.
Palveluväylä on vikasietoinen ja sen palvelutasotavoitteet voidaan sovittaa sitä käyttävien prosessien tarpeisiin	✪✪✪✪✪	Palveluväylä toteutetaan palvelutavoitteisiin sovitetulla korkean käytettävyyden alustalla ja vikasietoisesti. Palvelutasotavoitteiden lähtökohtana ovat toiminnan tarpeet.
Palveluväylää voidaan laajentaa ja skaalata kysynnän ja palvelujen kehittyessä	✪✪✪✪✪	Palveluväyläratkaisu voidaan käynnistää tiiviillä ytimellä, jota on helppo laajentaa. Alkupanostus ei ole tarpeettoman suuri. Tekninen arkkitehtuuri tarjoaa helpon suorituskyvyn lisäämisen.
Palveluväylään kytkeytyvät osapuolet voidaan tunnistaa luotettavasti	✪✪✪✪✪	Palveluväylään kytketyt tunnistamista edellyttävät toimijat tunnistetaan kiistämättömästi ja luotettavasti
Palveluväylän kautta välitettävät tiedonsiirrot voidaan jäljittää luotettavasti	✪✪✪✪✪	Palveluväylä sisältää ratkaisumekanismin, jonka avulla voidaan kiistämättömästi jäljittää palveluväylän kautta välitetty tieto.
Palveluväylälle määritetyt palvelut noudattavat yhteisiä, dokumentoituja rajapintamäärityksiä	✪✪✪✪	Palveluväylän palvelut ovat helposti saatavissa ja ne on määritetty ja toteutettu yhteisten sääntöjen mukaisesti.
Palveluväylä rakentuu moduuleista	✪✪✪✪	Palveluväylä rakentuu loogisista komponenteista / moduuleista, joita voidaan tarpeen mukaan vaihtaa toisiin eri aikaan. Tämä parantaa kokonaishallittavuutta ja riippumattomuutta.
Palveluväylä kestää muutosta	✪✪✪✪	Palveluväylä on toteutettu rakenteisesti siten, että siihen voidaan hallitusti tuoda uusia ominaisuuksia ja ratkaisuja vaiheittain - sen arkkitehtuuri on pitkäikäinen. Kansallisen aplveluväylän rakenteet on jäsennetty sellaisiin kokonaisuuksiin, joissa muutokset voidaan kohdistaa rajattuihin osiin.
Palveluväylä tukee erilaisia sovellustason sanomamuotoja.	✪✪✪✪	Palveluväylä tukee kaikkia yleisesti käytössä olevia sovellustason sanomamuotoja käärimällä eri sovellussanomat palveluväylän yhtenäiseen sanomamuotoon ja välittämällä ne yhdenmukaisen tiedonvälitystekniikalla.
Kansallinen palveluväylä on erillisiä ratkaisuja kustannustehokkaampi tiedonvälitysratkaisu	✪✪✪✪	Palveluväylän suunnittelussa ja toteutuksessa otetaan huomioon sen kustannukset. Palveluväylä toteutetaan sekä teknisesti että palvelujen näkökulmasta kustannustehokkaasti siten, että sitä voidaan laajentaa kysynnän kasvaessa. Alkupanostus ei ole tarpeettoman suuri.
Palveluväylän liiketoimintamalli mahdollistaa palveluväylän palvelujen ja niiden käytön nopean laajentamisen	✪✪✪✪	Liiketoimintamalli ja rahoitusmalli on suunniteltu siten, että ensimmäisten asiakkaiden ei tarvitse maksaa merkittävää osaa alkuinvestoinnista. Palveluun on jo alkuvaiheessa hyvin helppo kytkeytyä.
Palveluväylän teknologia on toimittajariippumatonta	✪✪✪	Palveluväylän tekninen ratkaisu ei perustu yhden toimittajan yksinoikeuden alaiseen teknologiaan, ja siihen on saatavissa usean toimittajan tukea kehittämiseen ja ylläpitoon
Palveluväylän tulee mahdollistaa eri suojaustason tietoaineistojen välittäminen	✪✪✪	Palveluväylään voidaan rakentaa eri suojaustason palveluosia.
Palveluväylä edistää palveluinnovaatioita ja avoimen datan hyödyntämistä	✪✪✪	Palveluväylä tarjoaa tai se voidaan laajentaa edistämään avoimen datan välittämistä
Palveluväylään voidaan tuottaa kansalliset kytkentäpisteet kansainvälisiin palveluihin	✪✪	Esim. lääketurvallisuuden EU-tasoinen valvonta, epSOS-mallin mukainen potilastietojen EU-tasoinen vaihto.

Arkkitehtuuriperiaatteet korostavat kokonaisvaltaista ja kattavasti eri toimijoiden tarpeisiin soveltuvaa tietojen vaihdon infrastruktuuria, jossa tietojen välittäminen käsittely on hallittua ja turvallista.

Ratkaisukokonaisuuden tulee olla joustava ja tarpeiden mukaan kehittyvä. Arkkitehtuuriperiaatteissa on kuitenkin huomioitu myös tuki uusille asiakas- ja käyttäjäkeskeisille prosesseille sekä uusille palveluinnovaatioille. Kansallisen palveluväylän ratkaisun tulee myös olla kustannustehokas.

Kansallisen tietojenvaihdon ratkaisun ja organisaatiorajat ylittävien prosessien sekä tietojärjestelmien kehittäjien tulee ottaa huomioon kaikessa kehittämisessä yllä kuvatut arkkitehtuuriperiaatteet.

Arkkitehtuuriperiaatteet on listattu tarkemmin *Liitteessä 1, KA-taulukot.*

4.4. Tietoturvaperiaatteet

Seuraavassa kuvatut tietoturvaperiaatteet ovat alustavia ja koskevat erityisesti kansallisen palveluväylän keskitettyjä palveluja ja niiden ylläpitoa.

Kansallisen palveluväylän viestinvälityksen tietoturvallisuuden ja tietosuojan ratkaisuja on kuvattu tarkemmin jäljempänä kansallisen palveluväylän loogisen ratkaisukuvauksen yhteydessä.

Kansalaisen ja hänen tietojensa käsittelyn ja tietojen vaihdon ratkaisujen ja toiminnan tietosuojaan ja tietoturvaan liittyvät haasteet kohdistuvat erityisesti kansalaisten tietojen lainmukaiseen välittämiseen, tietojen ja osapuolten kiistämättömyyteen sekä palveluissa käsiteltävien tietojen käytön rajoittamiseen sekä käytön valvontaan. Lähdetietojen eheys ja kiistämättömyys ovat tietoturvallisuuden kohteita, joiden hallinnan ja varmistamisen suunnitteluun tulee kiinnittää erityishuomiota.

Kansallisen palveluväylän tietoturvaperiaatteissa hyödynnetään Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) tuottamia ohjeita ja linjauksia soveltaen. Ne luovat hyvän perustan tietoturvallisuustyölle julkisen hallinnon ratkaisuissa.

Yleisiä kansallisen palveluväylän tietoturvallisuuden suunnittelua ohjaavia VAHTI-määrityksiä ovat mm:

- Tietoturvallisuusasetus (681/2010)
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010
- Verkkopalvelut (VAHTI 12/2006)
- Salauskäytännöt (VAHTI 3/2008)
- Tietoturvasanasto (VAHTI 8/2008)
- Hankkeen tietoturvaohje (VAHTI 9/2008)
- Lokien käsittelyohje (VAHTI 3/2009)

Näiden lisäksi kansallisen palveluväylän ja sen kehittämisen tietoturvan varmistamiseen sovelletaan, milloin tarkoituksenmukaista, seuraavia yleisiä tietoturvamalleja:

- ISO/IEC 27001
- Kansallinen turvallisuusauditointikriteeristö, versio 2 (Katakri II)
- Valtion tietoturvatasot (Vahti)
- Julkisen hallinnon varautuminen

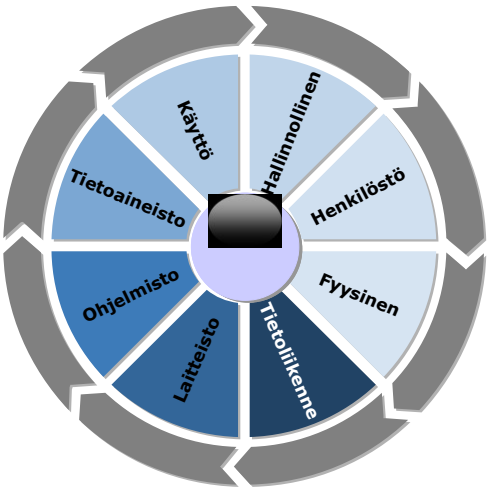
- Huoltovarmuuskeskuksen Sopiva-vaatimukset
- Vahti 1/2013: tietojärjestelmän kehittämisen tietoturvaohje

Kansallista palveluväyläratkaisukokonaisuutta koskevat keskeisimmät tietoturvaperiaatteet ovat:

Palveluväylä todentaa siihen liittyvät toimijat luotettavasti	**Kriittinen**	Palveluväylän kautta kommunikoitaessa voidaan olla varmoja siitä, minkä tahon kanssa kommunikointi tapahtuu.
Palveluväylä välittää viestit perille luotettavasti	**Kriittinen**	Kun viesti liirtyy pallveluväylään, voidaan olla varmoja viestin perillemenosta.
Palveluväylä sietää tietoliikenneyhteyksissä esiintyviä katkoja	**Kriittinen**	Palveluväylän toiminta ei halvaannu yksittäisen tietoliikennekomponentin vikaantuessa.
Palveluväylän käytettävyystaso on korkea	tärkeä	Palveuväylän hyödynnettävyyteen voidaan luottaa. Palveluväylälle vaihtoehtoisia viestinvälitysmekanismeja ei ole tarpeen rakentaa.
Palveluväylä ei heikennä siihen liittyvien järjestelmien tietoturvaa	**Kriittinen**	Ratkaisun tarjoamien tiedonsiirtomekanismien tulee noudattaa valtionhallinnon tietoturvavaatimuksia (Valtionhallinnon tietoturvaohjeistukset) riippumatta siitä, onko kyseessä valtionhallinnon sisäinen sanomaliikenteenne vai sanomaliikenne ulkoisiin sidosryhmiin. Tietoturva tulee ottaa huomioon jokaisessa vaiheessa määrittelystä käyttöönottoon.
Palveluväylä säilyttää viestien sisällön luottamuksellisuuden lähettäjän ja vastaanottajan välillä	**Kriittinen**	Palveluväylän kautta tapahtuva viestien välitys ei näy ulkopuolisille toimijoille
Palveluväylä takaa kuljettamiensa viestien muuttumattomuuden	**Kriittinen**	Viestin vastaanottaja voi luottaa vastaanottamansa viestin paikkansapitävyyteen.
Palveluväylä mahdollistaa viestien välityksen kiistämättömyyden tarkistamisen	tärkeä	Jälkeenpäin on mahdollista vahvistaa että tietty viesti on lähetetty

Keskeiset kansallisen palveluväylän tietoturvaperiaatteet voidaan jäsentää yleisen tietoturvallisuuden viitekehyksen mukaan, jossa tietoturvallisuutta tarkastellaan kahdeksan osa-alueen näkökulmasta:

- Hallinnollinen turvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus



Seuraavat tästä alaspäin kuvatut tietoturvaperiaatteet koskevat **erityisesti keskitetysti tuotettuja palveluväyläpalveluita** (keskuspalvelin ja sen ylläpitopalvelut), kuten palvelukatalogi, turvanimipalvelu, keskitetty lokipalvelu, so-

pimuspalvelu ja varmennepalvelu[2]. Keskitettyjen palvelujen tulee täyttää seuraavat tietoturvamääritykset:

Tietoturvatasot: Korkean tason vaatimukset	**Kriittinen**	Palveluväylän keskitetty ratkaisukokonaisuus ja sen käyttöympäristö sekä ylläpito täyttävät VAHTI 3/2011 tietoturvatasojen **korkean tason** vaatimukset
Varautuminen: korotettu taso	**Kriittinen**	Palveluväylän keskitetty ratkaisukokonaisuus ja sen käyttöympäristö sekä ylläpito täyttävät VAHTI 2/2012 varautumisen **korotetun tason** vaatimukset
Katakri II: Korotettu taso	**Kriittinen**	Palveluväylän keskitetty ratkaisukokonaisuus ja sen käyttöympäristö sekä ylläpito täyttävät Katakri II **korotetun tason** vaatimukset

Kansallisen palveluväylän keskitettyjen palvelujen tietoturvaperiaatteet on listattu edellä mainittujen kahdeksan tietoturvanäkökulman mukaisesti tarkemmin *Liitteessä 1, KA-taulukot.*

5. Käsitteellisen tason arkkitehtuurilinjaukset

5.1. Kehittämisvaatimukset ja tavoitteet

Kansallisen palveluväylän arkkitehtuurin kehittämisvaatimukset ja suunnittelun tavoitteet on johdettu seuraavista asiakirjoista:

- Hallitusohjelma
- Ehdotus julkisen hallinnon ICT:n hyödyntämisen strategiaksi
- Suomen ICT-klusteri 2015 työryhmän tavoitteet

Lisäksi tavoitteita on tarkennettu hankkeen ohjausryhmältä ja hankkeen työryhmältä saadulla evästyksellä.

Tärkeimpinä kansallista palveluväylää koskevat tavoitteet ovat:

- Tiedonvälityksen edellytyksien luominen
- Tietojen yhteiskäytön lisääminen
- Yhtenäiseen kokonaisarkkitehtuuriin perustuvien tietoalustojen käyttöönoton edistäminen
- Tiedonvälityksen (tiedonvaihdon) kehittäminen
- Joustavan infrastruktuurin luominen
- Innovaatiohalukkuuden lisääminen

Palveluväylä ei itse tuota substanssipalveluja, se mahdollistaa substanssipalvelujen ja tietovarantojen kytkemisen yhtenäiseen kokonaisuuteen, josta palveluväylään kytkettyjä palveluja on helppoa ja turvallista hyödyntää.

Alle on listattu vielä yksittäisiä kansallisen palveluväylän tavoitteita ja yleisiä vaatimuksia:

[2] Yksittäisille Palveluväylään liittyville Palveluille tai Liityntäpisteille ei aseteta tässä tarkkoja tietoturvavaatimuksia. Liittyvien palvelujen tulee lähinnä täyttää Palveluväylän käyttösopimuksen turvallisuusvaatimukset.

Yleiset vaatimukset		
Palveluväylä on tietoturvallinen	Välttämätön	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylä tukee tietosuojan turvaamista ja valvontaa	Välttämätön	Palveluiden käyttäjät, kansalaiset
Palveluväylä tukee useita tietoturvamenetelmiä	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät
Palveluväylä voidaan kytkeä olemassa oleviin integraatioratkaisuihin	Hyödyllinen	Nykyisten ratkaisujen tuottajat, rahoittajat, palvelujen hyödyntäjät.
Palveluväylä on kaikkien organisaatioiden hyödynnettävissä	Toivottu	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylä voidaan liittää erilaisiin verkkoihin	Toivottu	Eri toimialojen toimijat
Palveluväylään voidaan liittää kaikki sellaiset palvelut, jotka täyttävät sen tietoturvavaatimukset ja käyttöehdot	Hyödyllinen	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylä on vikasietoinen	Välttämätön	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylä on käytössä 24/7	Välttämätön	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylä tulee voida toteuttaa korkean käytettävyyden ratkaisuksi	Välttämätön	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylän tulee skaalautua kuormituksen mukaan	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät
Palveluväylän läpi voidaan kuljettaa erilaisia sanomia sovellustason sanomamuodosta riippumatta	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Palveluväylä varmistaa siihen liitettyjen palvelujen kiistämättämyyden	Hyödyllinen	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Palveluväylä pitää kirjaa siihen liittyneistä palveluista ja organisaatioista	Välttämätön	Palveluiden tuottajat ja hyödyntäjät
Palveluväylän toteutusmalli on sellainen, että siihen on helppo liittyä	Toivottu	Palveluiden tuottajat ja hyödyntäjät
Palveluväylässä voi hyödyntää olemassa olevia sovelluskohtaisia rajapintoja	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Palveluväylän sanomaliikenne on jäljitettävissä	Välttämätön	Palveluiden tuottajat, hyödyntäjät ja käyttäjät
Kaikille liittyville toimijoille käytetään samoja käyttöehtoja	Toivottu	Palveluiden tuottajat ja hyödyntäjät
Palveluväylä tukee sekä synkronista että asynkronista tiedonvälitystä	Välttämätön	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Palveluväylä tukee SOAP-palvelurakenteita ja rajapintoja	Välttämätön	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Palveluväylä tukee REST-palvelurajapintaa	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Palveluväylän palveluja tulee voida kehittää hajautetusti	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät
Palveluväylän osateknologioita tulee voida vaihtaa tarvittaessa toisiin ilman, että tämä edellyttää koko ratkaisuteknologian vaihtamista	Välttämätön	Palveluiden tuottajat ja hyödyntäjät
Palveluväylään voidaan lisätä uusia toiminnallisuuksia hallitusti ja systemaattisesti - suuret kokonaisuudet kootaan sovellusmoduuleihin, jotka voidaan asentaa hallitusti liityntäpalvelimiin tarpeen mukaisesti	Välttämätön	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Yksittäiseen liityntäpalvelimeen voidaan asentaa useita palveluväylän yhteisiin palveluihin hyväksyttyjä sovellusmoduuleja.	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät, eri toimialat
Palveluväylä sisältää kokonaispalveluna myös sen tuki- ja ylläpitopalvelut sekä keskitettyjen ratkaisujen kapasiteettipalvelut	Hyödyllinen	Palveluiden tuottajat ja hyödyntäjät

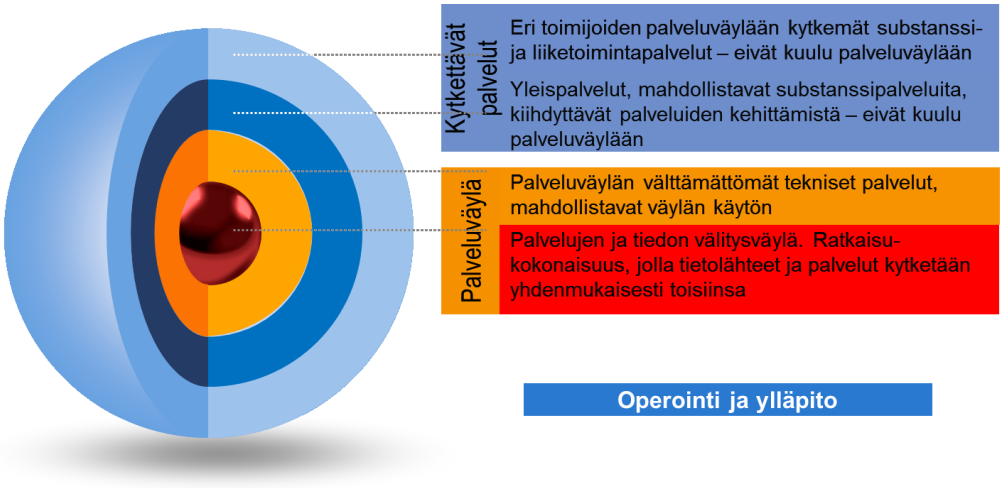
Yllä olevat vaatimukset ovat ns. käsitteellisen tason yleisvaatimuksia, jotka eivät vielä ole riittävät varsinaiselle toteutukselle tai hankinnalle. Varsinainen vaatimusmäärittely tulee toteuttaa myöhemmässä vaiheessa tämän viitearkkitehtuurin pohjalta.

5.2. Kansallisen palveluväylän palvelut

Palveluväylän palvelut voidaan jakaa:

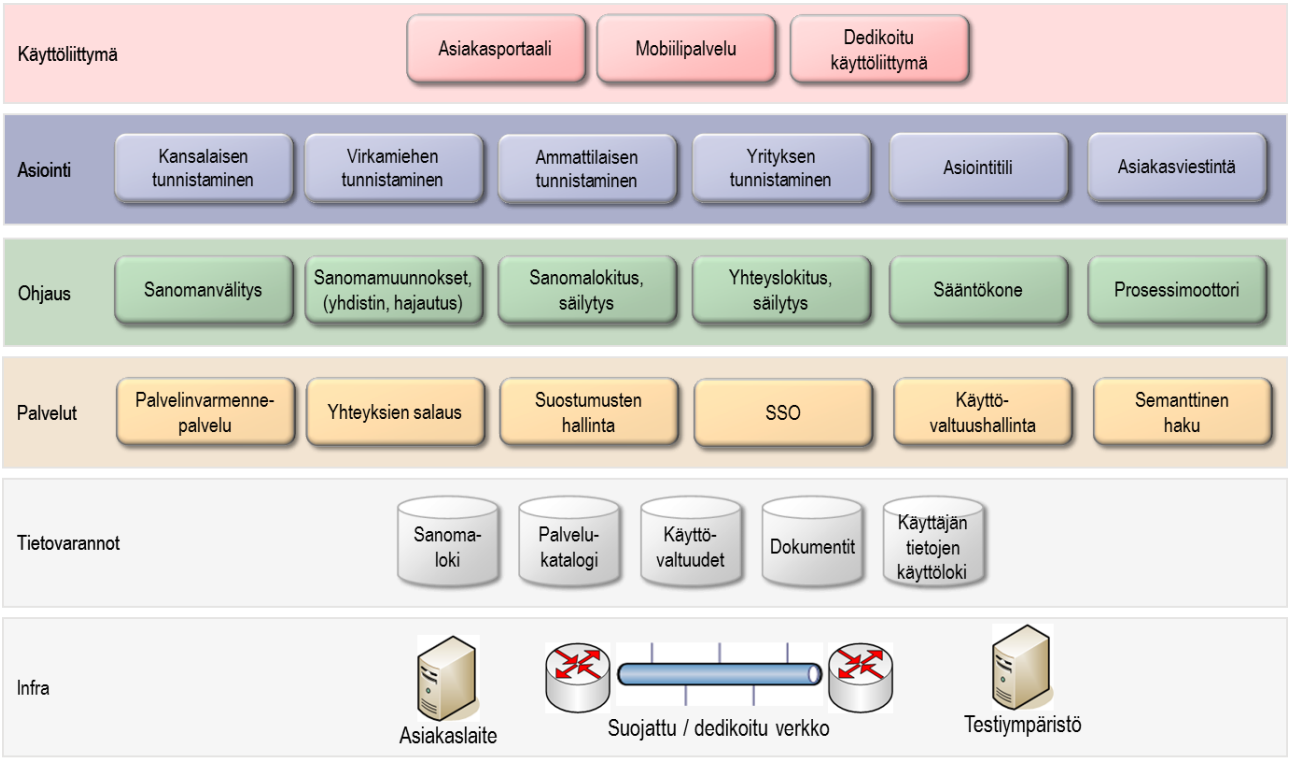
- Palveluväylä tiedonvälitysväylään ja teknisiin ydinpalveluihin
- Palveluväylään kytkettäviin sähköisiin tietojärjestelmäpalveluihin ja
- Palveluväylän operointiin ja ylläpitoon liittyviin jatkuviin palveluihin

Tekniset ja kytkettävät tietojärjestelmäpalvelut jäsentyvät edellä kuvatun mallin mukaisesti kerroksittain:



Kansallinen palveluväylä sisältää yllä olevan kuvan punaisen ytimen ja oranssin teknisen kerroksen.

Tyypillisesti viestinvälityksen ratkaisut koostuvat erilaisista yhdistelmistä alla jäsennetyistä teknisistä ja tietojärjestelmäpalveluista:



Edellä oleva kuva visualisoi tyypillisimpiä viestinvälityksen ratkaisujen tietojärjestelmäpalveluja sijoittamalla ne kerroksellisen järjestelmäarkkitehtuurin tyypillisiin kerroksiin. Kuvassa on selvyyden vuoksi mukana tiedonvälityksen tietojärjestelmäpalveluiden lisäksi myös varsinainen tiedonvälitysinfrastruktuurikerros.

Edellä kuvattu tietojärjestelmäpalvelukartta on yleistys, johon on listattu erilaisista viestinvälitysratkaisuista (vrt. lähtötilanteen arviointi) löytyviä tietojärjestelmäpalveluita. Yksittäinen tiedonvälitysratkaisu harvoin sisältää kaikkia yllä kuvattuja tietojärjestelmäpalveluita. Kansallisen palveluväylän rooli on yleisiä yritysten, virastojen ja kuntien käytössä olevia integraatioratkaisuja kohdennetumpi ja sisältää ainakin ensivaiheessa pienemmän joukon tietojärjestelmiä.

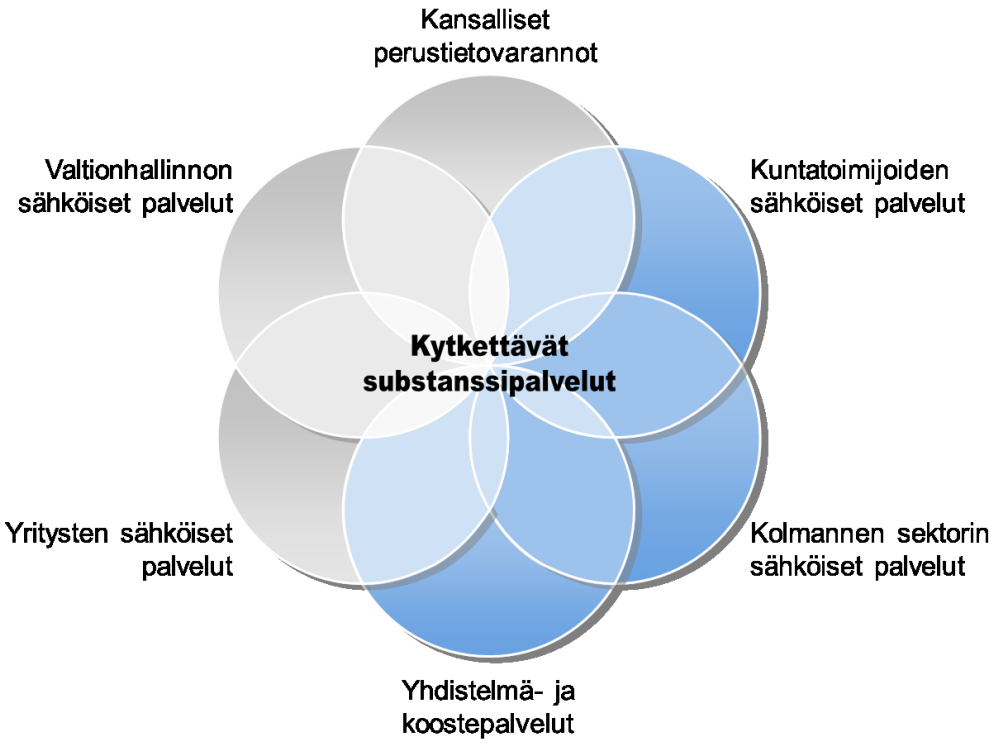
Palveluväylän ytimessä olevat tekniset tietojärjestelmäpalvelut ja alustava näkemys kansallisen palveluarkkitehtuurin keskeisimmistä yleispalveluista on kuvattu jäljempänä loogisen arkkitehtuurin kuvauksissa.

5.2.1. Kansalliseen palveluväylään kytkettävät palvelut

Kansalliseen palveluväylään voidaan kytkeä lähes rajattomasti eri toimijoiden tarjoamia ja hyödyntämiä tietovarantoja ja palveluja. Kytkettävien palveluiden on täytettävä palveluväylään määritettävät tekniset rajapintavaatimukset. Sen lisäksi palvelujen tuottajien on sitouduttava erikseen listattuihin kansallisen palveluväylän käyttöehtoihin ja tietoturvavaatimuksiin, joiden noudattaminen voidaan milloin tahansa auditoida.

Kukin palveluväylään kytkeytyvä toimija (palveluväyläorganisaatio) solmii kahdenvälisen sopimuksen niiden palvelujen omistajien kanssa, joita kyseinen kytkeytyvä organisaatio haluaa hyödyntää. Nämä sopimukset määrittävät, mitä palveluja kyseinen Hyödyntäjä voi Tuottajan liityntäpisteestä käyttää ja mihin tarkoituksiin. Nämä käyttösopimukset tallennetaan myös sähköiseen muotoon siten, että palveluväylän sanomanvälityspalvelu voi automaattisesti varmistaa, että hyödyntäjällä on aina oikeus käyttää kyseistä tuottavaa palvelua (esim. tietovarantopalvelua). Jotkut tuottavat palvelut voidaan määritellä sellaisiksi, että ne ovat vapaasti kansallisen palveluväylän kautta käytettävissä ilman erillisiä kahdenvälisiä sopimuksia.

Mikä tahansa edelliset ehdot täyttävä palvelu, voidaan jatkossa kytkeä kansalliseen palveluväylään. Kytkettävät substanssi- ja liiketoimintapalvelut voidaan jakaa seuraaviin ryhmiin:



Viitearkkitehtuuri ei ota tarkasti kantaa, mitä substanssi- ja liiketoimintapalveluja kansalliseen palveluväylään voidaan kytkeä.

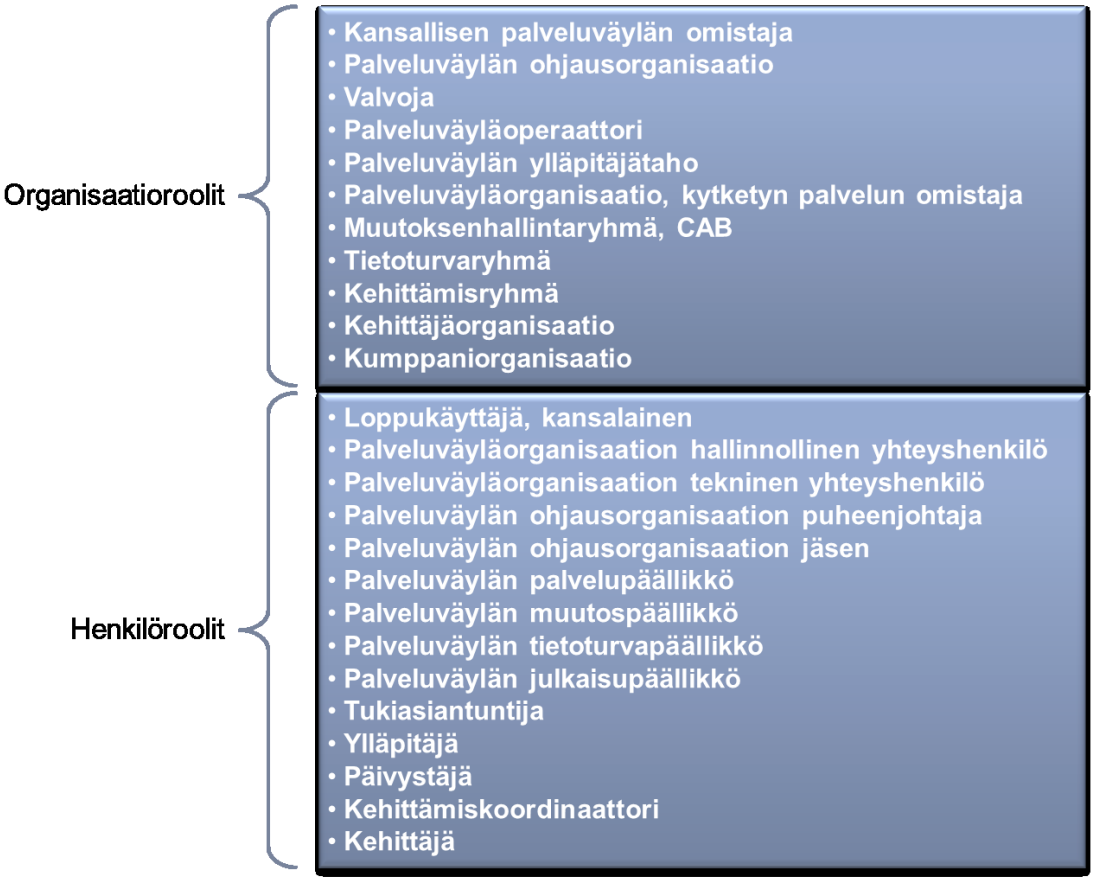
Viitearkkitehtuurissa suositellaan erityisesti, että kaikki kansalliset perustietovarannot kytketään heti ensimmäisessä kehitysvaiheessa kansalliseen palveluväylään.

Julkisen hallinnon on hyvä näyttää esimerkkiä ja liittää yleisimmin eri toimijoiden välillä välitettävien tietojen tietovarannot ja palvelut kansalliseen palveluväylään.

Palveluväylän omistajan ja palveluväyläoperaattorin tulee kannustimin ja viestinnän sekä julkisen hallinnon palveluväylään liitettävien tietovarantojen kautta kannustaa yrityksiä ja kolmatta sektoria liittämään ja kehittämään uusia palveluja kansalliseen palveluväylään.

5.3. Kansalliseen palveluväylään liittyvät keskeiset toimijat ja roolit

Palveluväylän ohjauksen, ylläpidon, käytön ja kehittämisen keskeiset roolit voidaan jakaa organisaatiorooleihin ja henkilörooleihin seuraavasti:



Roolituksessa on otettu huomioon sekä kansallisen palveluväylän ohjauksen ja johtamisen että sen operatiivisen toiminnan sekä kehittämisen keskeisimmät roolit.

Keskeisimmät kansallisen palveluväylän toiminnan organisaatioroolit ovat:

Organisaatiorooli	Kuvaus
Kansallisen palveluväylän omistaja	*Taho, joka vastaa kansallisen palveluväylän toiminnasta ja tarkoituksenmukaisuudesta kansallisiin yhteentoimivuuden infrastruktuurivaatimuksiin nähden, yksi vastuuorganisaatio.* *Omistaja vastaa kansallisen palveluväylän rahoitusmallista ja rahoituksesta.*
Palveluväylän ohjausorganisaatio	*Organisaatio tai ryhmittymä, joka ohjaa palveluväyläoperaattorin toimintaa ja johtaa kansallisen palveluväylän kehittämistä ja kehittämispolkua strategisella ja taktisella tasolla. Toimii kansallisen palveluväylän omistajan valtuuttamana.*
Valvoja	*Palveluväyläoperaattorin toimintaa ja kansallisen pal-*

	veluväylän toiminnan lainmukaisuutta valvova palveluväylän operatiivisesta toiminnasta ja johtamisesta riippumaton taho.
Palveluväyläoperaattori	*Organisaatio, joka operatiivisesti vastaa kansallisen palveluväylän operatiivisista palveluista vaatimusten mukaisesti. Ylläpitää palveluväylän palvelukuvauksia ja käyttöehtoja, hyväksyy uusien palveluväyläorganisaation liittymisen palveluväylään. Ohjaa operatiivisesti palveluväylän ylläpitäjäorganisaatiota ja järjestää palveluväylän tarvitsemat käyttö-, kapasiteetti- ja ylläpitopalvelut. Koordinoi käytännössä kansallisen palveluväylän kehittämistä. Vastaa palveluväylän tietoturvasta ja järjestää tarvittavat liittyjien ja palvelujen auditoinnit.*
Palveluväylän ylläpitäjätaho	*Palveluväylän tekninen ylläpito-organisaatio.* *Vastaa kansallisen palveluväylän keskitettyjen ratkaisujen ja palvelujen käyttö-, kapasiteetti- ja ylläpitopalveluista. Vastaa keskeisistä palveluväylän operatiivisista ITSM-prosesseista (esim. julkaisunhallinta, häiriönselvitys, konfiguraationhallinta). Vastaa operatiivisesti resurssi- ja komponenttitasoisesta kapasiteetinhallinnasta ja kapasiteettisuunnittelusta.*
Palveluväyläorganisaatio, palvelun omistaja	*Palveluväylään kytketyn liiketoiminta / substanssipalvelun omistaja. Organisaatio, joka on kytkeytynyt palveluväylään. On hyväksynyt palveluväylän käyttöehdot ja ottanut käyttöön liityntäpalvelimen. Pystyy hyödyntämään palveluväylään kytkettyjä palveluja tai itse tarjoaa sinne palveluja. Omistaa palveluväylään tarjoamansa palvelut (Tuottaja) tai palveluväylään kytkettyjen tietovarantoja ja palveluiden hyödyntävät palvelut (Hyödyntäjä).*
Muutoksenhallintaryhmä, CAB	*Palveluväylän yhteisiin palveluihin kohdistuvien muutospyyntöjen käsittelyn vastuuorganisaation (Change Advisory Board, CAB). Puheenjohtajan toimii palveluväyläoperaattorin henkilöstöön kuuluva muutospäällikkö (Change manager). Koostuu myös keskeisten palveluväyläorganisaatioiden, palveluväylän ohjausryhmän ja palveluväylän ylläpitäjän edustajista. Hyväksyy yhteisten palvelujen ja ratkaisujen muutokset.*
Tietoturvaryhmä	*Palveluväylän tietoturvallisuudesta ja tietosuojan varmistamisesta vastaava yhteistyöryhmä.*
Kehittämisryhmä	*Ryhmä, joka käsittelee kansallisen palveluväylän kehittämistarpeet ja suunnittelee uusien toiminnalli-*

	suuksien ja komponenttien versiot.
Kehittäjäorganisaatio	*Organisaatio, joka käytännössä toteuttaa palveluväylän yhteisten teknisten palveluiden ja osakokonaisuuksien kehittämisen. Kehittämisen ohjaus ja hallinta on keskitettyä, mutta varsinainen kehittäminen voidaan tarvittaessa hajauttaa hallitusti useammalle organisaatiolle.* *Kansalliseen palveluväylään kytkettyjen palveluiden kehittämisen järjestämisestä vastaa kyseisen palvelun omistaja – ko. palveluväyläorganisaatio.*
Kumppaniorganisaatio	*Muu kansallisen palveluväylän kehittämiseen liittyvä kumppani tai sidosryhmä. Esimerkiksi jonkun muun valtion kansallisen palveluväylän kehittäjäorganisaatio.*

Keskeisimmät kansallisen palveluväylän toiminnan henkilöroolit ovat:

Henkilörooli	Kuvaus
Loppukäyttäjä, kansalainen	Liiketoiminta- ja substanssipalveluja käyttävä loppuasiakas. Kansallinen palveluväylä on loppukäyttäjälle täysin läpinäkyvä palvelu.
Palveluväyläorganisaation hallinnollinen yhteyshenkilö	Yksittäisen palveluväylään kytkeytyneen palveluväyläorganisaation hallinnollinen yhteyshenkilö vastaa käyttöehtojen noudattamisesta ja mahdollisista maksuista sekä vastaa ko. organisaation palvelujen hyödyntämisen käyttösopimusten solmimisesta.
Palveluväyläorganisaation tekninen yhteyshenkilö	Tekninen yhteyshenkilö toimii palveluväylän kautta palveluja tarjoavan organisaation rajapintana tarjotun palvelun toimivuuteen, suorituskykyyn, virheisiin tai lisätarpeisiin liittyvissä kysymyksissä.
Palveluväylän ohjausorganisaation puheenjohtaja	Palveluväylän omistajan edustaja. Johtaa palveluväylän ohjausorganisaation toimintaa.
Palveluväylän ohjausorganisaation jäsen	Henkilö, jonka palveluväylän omistaja on valinnut palveluväylän ohjausorganisaation jäseneksi. Ohjaa osana palveluväylän ohjausorganisaatiota kansallisen palveluväylän kehittämistä ja toimintaa.
Palveluväylän palvelupäällikkö	Operatiivisen keskitetyn palveluväylätoiminnallisuuden ja jatkuvien palvelujen vastuuhenkilö. Vastaa palveluväylän kokonaispalvelun toimivuudesta sille asetettujen sisältö- ja palvelutasovaatimusten mukaisesti. Sijoittuu palveluväyläoperaattorin henkilöstöön.

Palveluväylän muutospäällikkö	Johtaa muutoksenhallintaryhmän, CABin toimintaa. Sijoittuu palveluväyläoperaattorin henkilöstöön.
Palveluväylän tietoturvapäällikkö	Vastaa kansallisen palveluväylän tietoturvallisuudesta ja riittävästä tietosuojasta. Sijoittuu palveluväyläoperaattorin henkilöstöön.
Palveluväylän julkaisupäällikkö	Hyväksyy uusien versioiden julkaisun ja ns. roll-outin tuotantoympäristöön. Sijoittuu palveluväyläoperaattorin henkilöstöön.
Tukiasiantuntija	Kansallisen palveluväylän tekninen tukihenkilö. Sijoittuu kansallisen palveluväylän service deskiin. Antaa tukea palveluväyläorganisaatioiden teknisille yhteyshenkilöille ja muille nimetyille asiantuntijoille. Tyypillisesti sijoittuu palveluväylän ylläpitäjätahoon.
Ylläpitäjä	Kansallisen palveluväylän tekninen ylläpitäjä. Ylläpitää käytännössä palveluväylää (tietoturvapäivitykset, varmistukset tms.). Tyypillisesti sijoittuu palveluväylän ylläpitäjätahoon.
Päivystäjä	Kansallisen palveluväylän tekninen tukihenkilö. Sijoittuu kansallisen palveluväylän service deskiin. Antaa tukea palveluväyläorganisaatioiden teknisille yhteyshenkilöille ja muille nimetyille asiantuntijoille. Tyypillisesti sijoittuu palveluväylän ylläpitäjätahoon.
Kehittämiskoordinaattori	Henkilö, joka johtaa kansallisen palveluväylän kehittämisryhmää. Vastaa kansallisen palveluväylän kehittämisen koordinoinnista ja yhteentoimivuudesta. Sijoittuu palveluväyläoperaattorin henkilöstöön.
Kehittäjä	Yksittäinen kansallisen palveluväylän yhteisen osan tai palvelujen kehittäjärooli.

Kansallisen palveluväylän rooleja tulee tarkentaa toteutusvaiheessa.

Kansallisen palveluväylän roolit on listattu myös *Liitteeseen 1, KA-taulukot*.

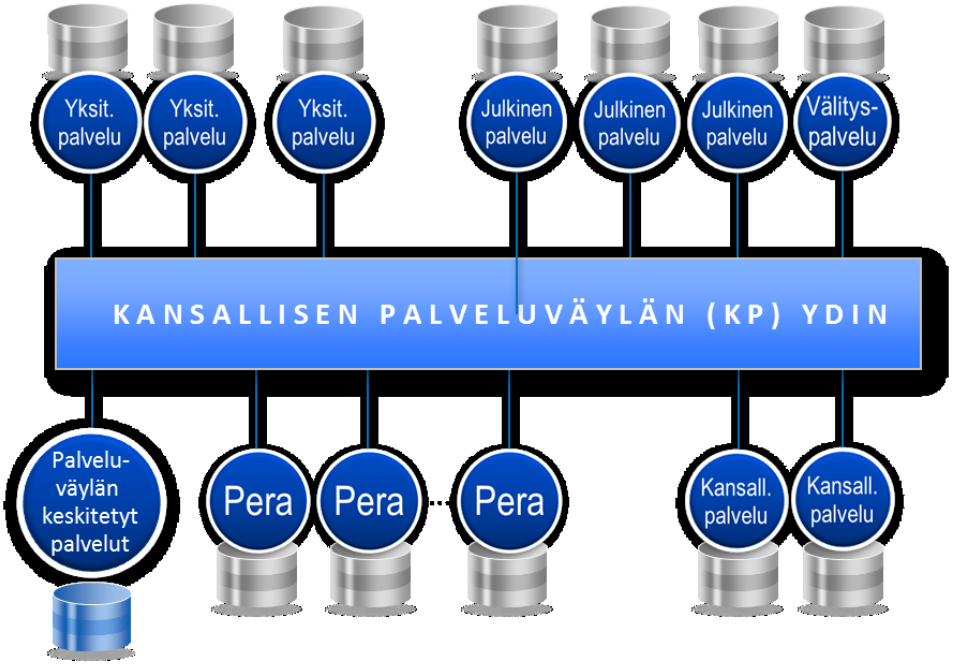
6. Loogisen tason arkkitehtuurilinjaukset

Seuraavaksi kuvattu kansallisen palveluväylän looginen jäsennys on vielä **tuoteriippumaton** kuvaus tavoitetilan loogisesta ratkaisumallista. Looginen ratkaisu voidaan fyysisellä tasolla toteuttaa monilla eri teknologioilla ja tuotteilla.

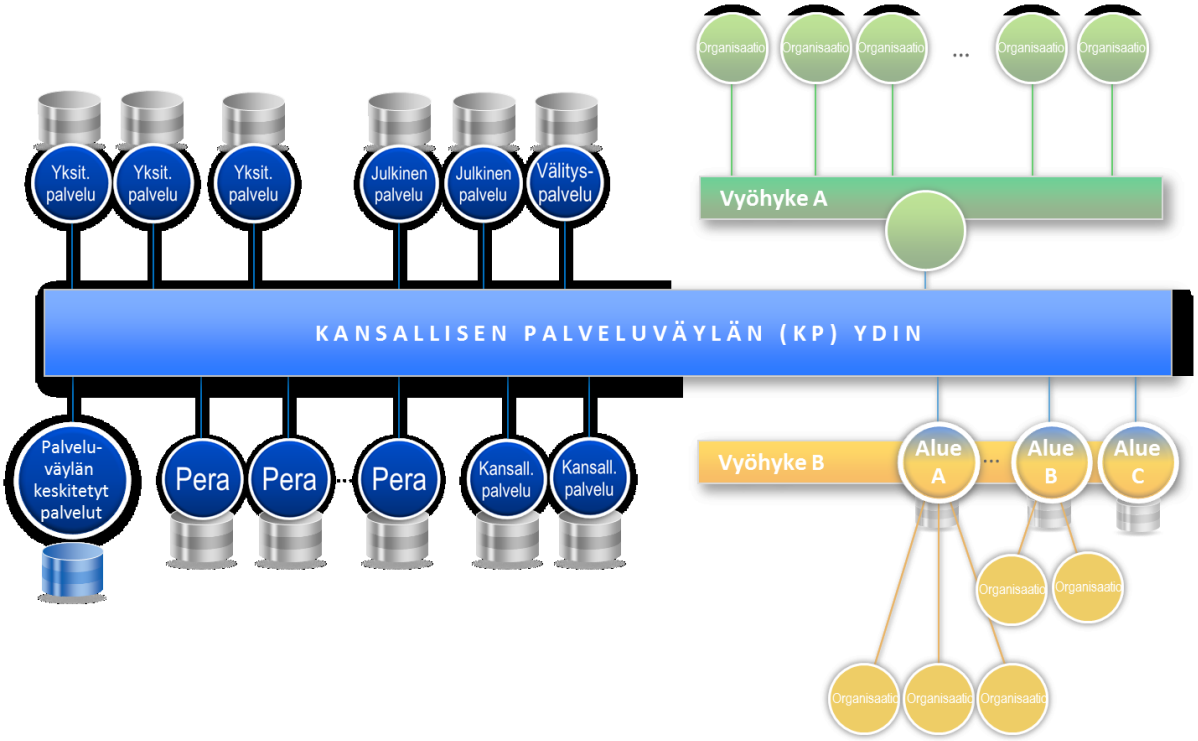
6.1. Valittu ratkaisumalli

Kansallisen palveluväylän viitearkkitehtuurin tavoitetilassa palveluväylä yhdistää palvelujen tuottajat ja hyödyntäjät näiden liityntäpalvelimien kautta kulkevilla viesteillä. Palveluväylän ydin toteutetaan autentikoidun verkoston mal-

lilla, jossa palveluväylä toteutetaan hajautetusti palveluväyläorganisaatioiden liityntäpisteisiin asennettavilla, yhdenmukaisilla liityntäpalvelimilla sekä keskitetysti hallinnoitavilla teknisillä autentikointi- ja palvelut tunnistavilla keskitetyillä palveluilla. Tätä voidaan havainnollistaa alla olevalla kuvalla:



Kansallisen palveluväylän viitearkkitehtuurin määrityksessä on huomioitu olemassa olevat määritykset ja ratkaisut sekä pyritty pitämään niihin kohdistuvien muutostarpeiden määrä mahdollisimman pienenä. Lyhyellä tähtäimellä kansallinen palveluväylä toimii olemassa olevien väyläratkaisujen ja perustietovarantojen yhdistäjänä sekä tarjoaa siihen liittyville tietojärjestelmäpalveluille yhtenäisen tavan välittää tietoja. Valittuun ratkaisuun voidaan **tarvittaessa** kytkeä toimialojen erityistarpeiden mukaisia vyöhykkeitä ja saada ne palveluväylän piiriin:



Mikäli tietyllä toimialalla on erityisvaatimuksia, joita ei voida todennettavasti täyttää kansallisen palveluväylän ytimen yleisratkaisulla, kansallisen palveluväylän ytimeen voidaan kytkeä eri toimialojen tarpeisiin sovitettuja **vyöhykkeitä**, joiden sisällä voidaan tietojenvaihto toteuttaa vyöhykekohtaisilla ratkaisuilla. Vyöhykkeen sisällä liikenne voidaan ohjata dedikoituun verkkoon, jonka SLA voidaan taata. Tavoitteena on, että palveluväylän ytimeen kytkettäviä toimiala- tai toimintoriippuvia vyöhykkeitä on minimimäärä.

Yllä oleva kuva on viitteellinen. Kansallisen palveluväylän arkkitehtuuri ei ota kantaa, mitä vyöhykkeitä palveluväylään tulee rakentaa. Samoin vyöhykkeiden sisäiset liittymäratkaisut ja liittymätopologiat (= mistä pisteistä vyöhyke kytkeytyy kansalliseen palveluväylään) määritetään ko. vyöhykkeen sisällä.

Pitkän aikavälin tavoitteena on, että erilaisia vyöhykkeitä ei tarvittaisi organisaatioiden välisessä tietojen vaihdossa, vaan kaikki ovat suoraan kytkeytyneinä palveluväylään.

6.1.1. Suositellun ratkaisumallin keskeiset hyödyt

Suositellun ratkaisumallin keskeisimmät hyödyt ovat:

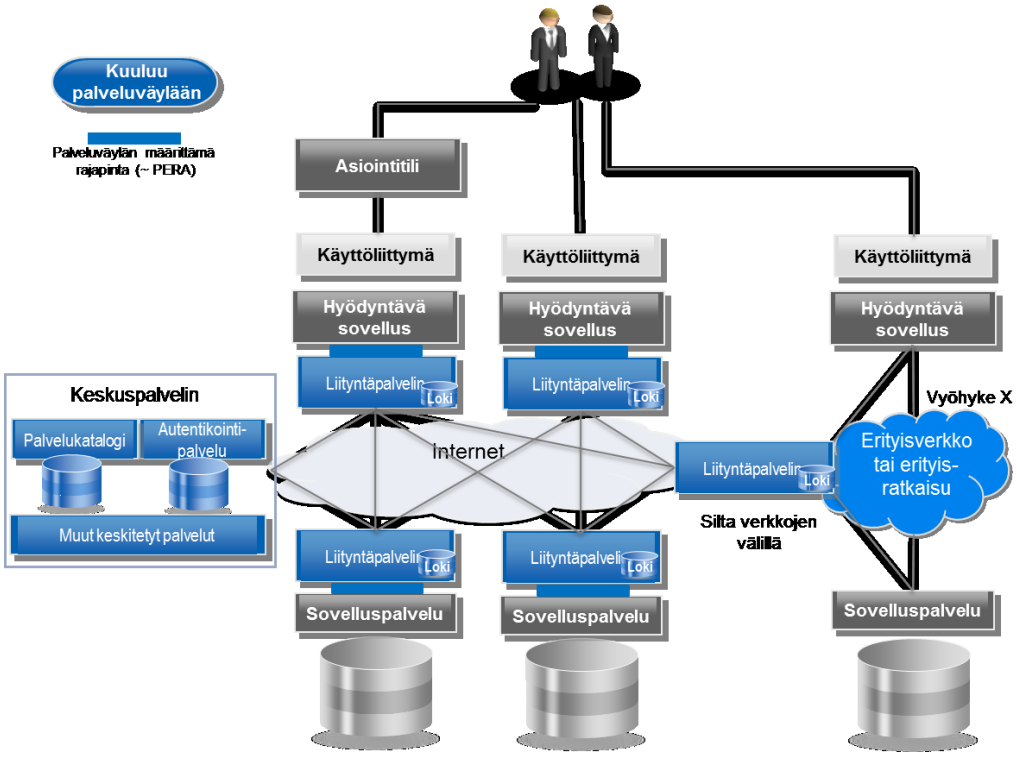
- Systemaattisesti hallittava hajautettu toisiinsa löyhästi kytketty palveluverkosto, jossa viestintä perustuu kahdenväliseen viestintään
- Tuottaa turvallisen päästä-päähän ratkaisumallin, jossa tietoturva voidaan varmistaa usealla eri tasolla
- On helposti laajennettavissa ja muunneltavissa sekä skaalattavissa volyymien kasvaessa
- Luo yhtenäisen käytännön tietojen vaihtoon

- Tukee hyvin monipuolisesti erilaisia tiedonvaihtoteknologioita ja sanomatyyppejä
- Hyödyntää täysimääräisesti olemassa olevan tietojen vaihdon infrastruktuurin sekä ottaa huomioon toimialakohtaiset erityispiirteet

Kansallinen palveluväylä perustuu sanomakeskeiseen palveluarkkitehtuuriin, jossa sanomat välitetään kansallisen palveluväylän välityskanavan läpi. Tämä tukee sekä synkronista että asynkronista viestintää.

6.2. Kansallisen palveluväylän looginen rakenne

Valittu palveluväyläarkkitehtuuri on tietoliikenteellisesti hajautettu ja toiminnallisesti keskitetty. Tietoliikenteellinen hajautus toteutuu väylään liittymisestä palvelinlaitteiden avulla, joita jokaisella väylään liittyvällä organisaatiolla on ainakin yksi. Loogisesti kukin liittyjä muodostaa liityntäpisteen paikallisten palvelujen ja kansallisen palveluväylän palvelujen välille. Liityntäpalvelimet ovat toiminnallisesti osa kansallista palveluväylää, joten palveluväylä näkyy liittyjäorganisaatioille keskitettynä palveluna liityntäpalvelimen kautta.



Liityntäpalvelin tarjoaa palveluväylän ulkopuolelle näkyvät rajapinnat ja se toimii palveluväylän tietoliikenneyhteyksien välittäjänä sekä lokitiedon kerääjänä. Jokaisessa liityntäpalvelimessa on liikennöinnin tunnistamista ja tietoliikenteen salaamista varten organisaatiokohtainen sertifikaatti ja tietous väylän keskitettyjen palveluiden sijainnista. Näiden avulla liityntäpalvelin kykenee luotettavasti ja turvallisesti välittämään rajapinnan kautta saamansa sanomat oikean kohteeseen. Liityntäpalvelinarkkitehtuuri on joustava. Liityntäpalvelin on tyypillisesti organisaatiokohtainen, mutta se voidaan toteuttaa myös alueellisesti tai usean organisaation yhteisellä liityntäpalvelimella. Samoin yhdellä organisaatiolla voi olla useita liityntäpalvelimia.

Viestien välitys tapahtuu kansallisen palveluväylän ytimessä internetin yli kahden liityntäpalvelimen välille muodostetulla salatulla yhteydellä. Yhteydenoton käynnistävä liityntäpalvelin selvittää palveluväylän keskitetyistä palveluista (palvelu- ja nimihakemistot) kohteen liityntäpalvelimen osoitteen ja aloittaa yhteyden muodostamisen, jonka aikana liityntäpalvelimet tunnistavat toisensa sertifikaattien avulla. Mikäli toinen osapuoli ei ole tietojärjestelmän tunnettujen kumppanien listalla, yhteyttä ei muodosteta. Tämä menettely, jossa vain tunnettujen kumppanien yhteydet muodostetaan, vähentää myös palvelunestohyökkäysten mahdollisuuksia ja vaikutuksia.

Liityntäpalvelimet välittävät yhdenmukaisen rakenteen mukaisia viestejä, joita on tarkemmin kuvattu luvussa 6.6. Palveluväylä määrittää viestien kehyksien (kirjekuoret) tietosisällön, mutta ei ota kantaa varsinaiseen sovelluskohtaiseen tietoon (kirjeen sisältö, joka voi olla vaikka sanoman sisällä salattua). Palveluväylä ei täten ota kantaa sanomien sisältöön vaan toimii vain viestien välittäjänä kirjekuoren (header) tietosisällön perusteella. **Kansallinen palveluväylä tarjoaa täten yhden standardin tiedonvälitystekniikan ja sanomamuodon (kirjekuori).**

Kansallisen palveluväylän liityntäpalvelimien sisällöstä, yhdenmukaisuudesta, rajapintakuvauksista sekä keskuspalvelimille määritettävistä keskitetyistä palveluista vastaa yksi keskitetty taho. Tyypillisesti tämä jaetaan vielä omistajarooliin sekä varsinaiseen palveluväyläoperaattorirooliin, joka vastaa palveluväylän operatiivisesta toiminnasta.

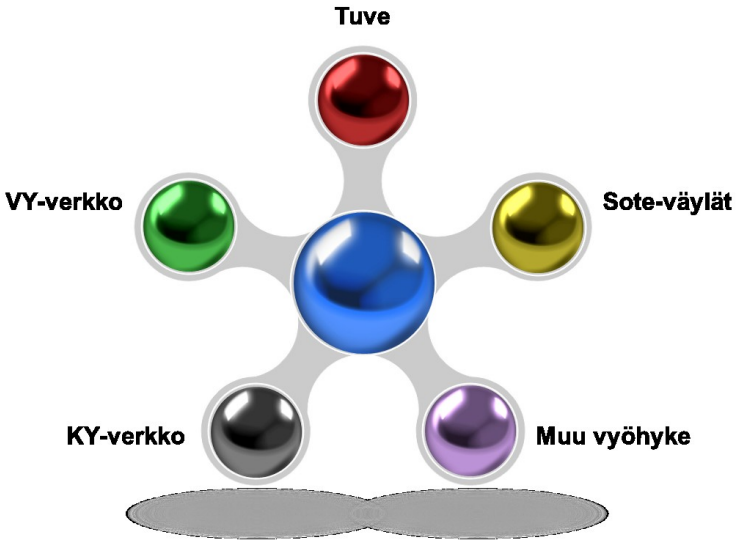
Kansalliseen palveluväylään voidaan liittää kansallisen palveluarkkitehtuurin yleispalveluita, joiden vastuut ja omistajuus voidaan hajauttaa. Vaikka ne näkyvät väylään liittyville tietojärjestelmille kansallisen palveluväylän palveluina, ne eivät ole osa palveluväylän ytimen välttämättömiä teknisiä palveluita. Kansallisen palveluarkkitehtuurin yleispalvelut voivat ratkaista toimialakohtaisia tarpeita (kuten suostumusten hallinta) tai olla teknisesti väylän ulkopuolisesti käytettävissä (kuten loppukäyttäjien tunnistuspalvelut). Ne liittyvät olennaisesti kansalliseen palveluarkkitehtuuriin niiden monikäyttöisyyden vuoksi – palveluväylään liittyneet palveluväyläorganisaatiot luottavat niihin ja ovat hyväksyneet ne palveluja tukeviksi palveluiksi.

Teknisesti itse kansallisen palveluväylän teknisten palvelujen ulkopuolella, mutta oleellisena osana palveluväyläkonseptia, ovat julkishallinnon perustietovarannot, jotka ovat aluksi merkittävimmät palveluväylän kautta tavoitettavat tietolähteet.

Palveluväylään voidaan kytkeä vyöhykkeinä monia erilaisia toimiala- tai organisaatiokohtaisia väyläratkaisuja, joihin kytkeytyneet hyödyntäjät voidaan myöhemmin liittää palveluväylään suoraan. Vyöhykkeitä voidaan lisätä tai vähentää tarpeen mukaan.

Tässä vaiheessa ei oteta tarkasti kantaa, mitkä osaverkot tai toimialat edellyttävät omaa vyöhykettä kytkettynä palveluväylään.

Alle on kuvattu viitearkkitehtuuriprojektissa esiin tulleita vyöhykekandidaatteja:



Esimerkiksi sosiaali- ja terveydenhuollossa on jo toteutettu erilaisia alueellisia viestinvälitysratkaisuja sekä alueellisia liityntäpisteitä, jotka kytkevät alueen potilastietojärjestelmät kansallisiin palveluihin, kuten reseptikeskukseen ja KanTa-palveluihin. Näiden palvelujen tietoturvaan sovelletaan esimerkiksi STM:n laatimia terveydenhuollon välittäjätahon auditointikriteerejä.

Nämä olemassa (tai valmisteilla) olevat ratkaisut sisältävät tyypillisesti palveluita, joihin pääsy on rajoitettua, mutta joista on tarve saada kontrolloidusti yhteys toisiinsa tai esim. perustietovarantoihin. Vyöhykemallilla voidaan vyöhykkeen sisäiselle viestinvälitysratkaisulle mahdollisuus toteuttaa tiedonvälitys tehokkaimmalla mahdollisella tavalla, kuitenkin mahdollistaen myös kansalliseen palveluväylään kytkettyjen palvelujen käyttö. Vyöhykkeen sisäisen tietojen vaihdon infrastruktuurin kehittämisvastuu voidaan näin hajauttaa kyseisen vyöhykkeen vastuutaholle. Vyöhykemallilla vältetään myös olemassa olevien ja toimivaksi osoittautuneiden tiedonvaihtoratkaisujen purkamistarve. Vyöhykkeen sisällä tiedonvälitykseen voidaan kuitenkin tarvittaessa käyttää myös kansallisen palveluväylän teknologiaa, jolloin vyöhykeraja voidaan mahdollisesti tulevaisuudessa poistaa. Tämä voidaan kuitenkin toteuttaa kyseisen vyöhykkeen toiminnalle luontevalla aikataululla.

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

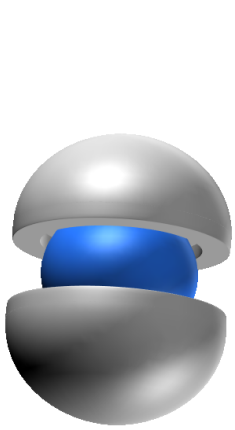
Vyöhykemallia ei saa käyttää väärin perustamalla tarpeettomasti uusi vyöhykkeitä, joissa toimijoiden tietojen integrointi voitaisiin toteuttaa kansallisen palveluväylän ratkaisumallilla. Kaikki uudet eri toimijoiden väliset tiedonvaihtoratkaisut suositellaan toteutettavan kansallisen palveluväylän ytimen toteutusmallilla.

Kansalliseen palveluväylään suositellaan ensimmäiseksi liitettävän perustietovarannot joko suoraan omilla liityntäpalvelimillaan tai nykyisiä rajapintoja hyödyntävien sovittimien avulla, sen jälkeen keskeisimmät palveluarkkitehtuurin yleispalvelut (erityisesti kansalaisen tunnistaminen, valtuutuspalvelu ja

suostumustenhallinta) sekä myöhemmin muita tietovarantoja ja palveluita tarkoituksenmukaisessa, tuottajaorganisaatiolle sopivassa aikataulussa.

6.2.1. Kansallisen palveluväylän kerrosrakenne

Kansallisen palveluväylän arkkitehtuuri perustuu löyhästi toiseensa kytkettyyn kolmeen arkkitehtuurikerrokseen, jossa kansallinen palveluväylä toimii ns. tiedonvaihtokerroksen ratkaisuna.



Sovelluskerros (application layer)

Sovellukseen voidaan määrittää sen tarvitsemat palvelut ja rajapinnat. Rajapinnat tulee olla vähintään muunnettavissa palveluväylän välitettäväksi (rajapintamuunnos, kääriminen palveluväylän siirrettäväksi)

Palveluväylä, tiedonvaihtokerros

Palveluväylään kytkettyjen palvelujen osoitteiden hallinta, reititys oikeaan paikkaan, sanomien salaus, sanomien välitys, lokitus, jäljitys, virheiden käsittely, rajapintojen rakennemääritykset

Tietoliikennekerros (transport layer)

Perusmalli toteutetaan internetin kautta, mutta palveluväylän tiedonvälitysratkaisu tukee myös muita tiedonsiirtotapoja – dedikoidut verkot, MPLS-verkot, muut L1- ja L2 –tason yhteydet

Sovelluskerros

Sovelluskerros irrotetaan selkeästi varsinaisesta palveluväyläkerroksesta. Sovellusten sisäiset sanomat voidaan tuottaa millä ratkaisutavalla vain. Sovelluksen sisäinen sanoma riippuu toimialasta, palvelusta ja tietolähteestä.

Sovellusten sisäiset rajapinnat tulee pystyä käärimään kansallisen palveluväylän mukaiseen kääreeseen (kirjekuori) ja välittämään palveluväylän tiedonvälitysteknologialla, mutta muuten palveluväylä ei ota kantaa sovelluskerroksen sanomasisältöön.

Tiedonvaihtokerros

Kansallinen palveluväylä toimii tässä kerroksessa. Keskeisiä kansallisen palveluväylän palveluita ovat mm.[3]:

- Palveluväylään kytkettyjen liityntäpisteiden ja niissä olevien palvelujen osoitteiden hallinta
- Sanomien välitys palveluväylässä osapuolten välillä
- Palveluväylän palveluiden palvelukatalogin hallinta
- Sanomien reititys oikeisiin osoitteisiin palvelukatalogin ja keskinäisten sopimusten perusteella.
- Osapuolten autentikoinnin / varmentamisen palvelut

[3] Loogiset tietojärjestelmäpalvelut on kuvattu tarkemmin jäljempänä

- Palveluväylän viestien salaus
- Virheiden käsittely ja yksinkertainen uudelleenlähetys
- Viestien ja yhteyksien lokitus ja viestinnän jäljitettävyyden palvelut

Palveluväylä tukee seuraavia tiedonvälitysmalleja:

- **Synkroninen viestinvälitys**
  - Viestinnän käynnistäjä jää odottamaan vastaanottavan pään kuittausta
  - Synkronisessa liikenteessä synkroninen kanava avataan aina päätepisteen palveluun / sovellukseen saakka
- **Asynkroninen viestinvälitys**
  - Viestinnän käynnistäjä ei erikseen odota vastapuolelta teknistä kuittausta.
  - Vastaanottaja voi lähettää tarvittaessa kuittauksena erillisen viestin
- **Pull-tiedonvälitys**
  - Tiedon tai palvelun Hyödyntäjä on aloitteen tekijä ja käynnistää yhteyden ja ”hakee” tiedon Tuottajan palvelusta tai tietolähteestä
- **Push-tiedonvälitys**
  - Tiedon tai palvelun Tuottaja on aloitteen tekijä ja käynnistää yhteyden ja ”lähettää” tiedon Hyödyntäjälle
- **Yhdestä-moneen (one-to-many)**
  - Tuottajasovellus toimittaa sanoman organisaation liityntäpalvelimelle, joka jakaa sen kaikille kyseisen sanoman kohteena olevalle palveluväylään liittyneelle liityntäpisteelle.
  - Tarkoituksena on välittää sama tieto useaan kohteeseen. Tämä toteutetaan asynkronisena viestintänä (ei vastausta) tai vastaanottajilta voidaan vielä edellyttää kuittausta viestin toimittamiseen. Palvelu edellyttää, että kaikki vastaanottajat (Hyödyntäjät) ovat sopineet kyseisestä tiedonvaihdosta etukäteen Tuottajan kanssa keskinäisin sopimuksin. Nämä sopimukset taltioidaan sähköisesti hyödynnettävässä muodossa sopimuskatalogiin
- **Monesta-yhteen (many-to-one)**
  - Useampi palveluväyläorganisaatio toimittaa samaa tietoa yhdelle vastaanottajalle
  - Toteutetaan tyypillisesti normaalilla sopimuskäytännöllä ja erillisillä viesteillä. Palveluväylään voidaan myöhemmissä vaiheissa määrittää myös jalostuneempia integraatiopalveluja, esimer-

kiksi sanomayhdistimiä, jossa liityntäpalvelin kokoaa eri sanomat yhteen sovelluksen ymmärtämäksi yhdistelmäsanomaksi. Tämä ei kuitenkaan kuulu palveluväylän peruspalveluihin.

- *many-to-one toiminnallisuus on perustoimintoja haastavampi toteuttaa, joten sitä ei suositella toteutettavaksi kansallisen palveluväylän ensimmäisessä vaiheessa*

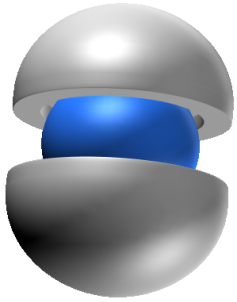
Palveluväylän liityntäpisteen toteuttamista määrittävät seuraavat tekniset periaatteet:

- Klusteroidun liityntäpisteen tapauksessa kaikilla noodeilla (liityntäpalvelimilla) voi olla sama palvelinvarmenne (mikäli klusterilla on yksi ulospäin näkyvä osoite), jotka näin muodostavat yhden loogisen palveluväylälle näkyvän liityntäpisteen.
- Kutakin palveluväylälle näkyvää domain-nimeä varten määritetään oma looginen liityntäpisteensä ja palvelinvarmenteensa (yksi liityntäpiste, yksi palvelinvarmenne)
- Salattu TLS-yhteys muodostetaan palveluväylän hyväksymällä palvelinvarmenteella aina liityntäpisteestä liityntäpisteeseen. Reitillä voi olla tietoliikenneverkon reitityksiä ilman, että TLS-yhteyttä välissä puretaan.

Tietoliikennekerros

Palveluväylä voidaan toteuttaa erilaisten tietoliikenneverkkojen päälle. Kansallisen palveluväylän ydin toteutetaan internetissä tapahtuvan tietoliikenteen päälle, koska tällä halutaan varmistua, että mikä tahansa kansallisen palveluväylän käyttö- ja tietoturvaehdot täyttävä organisaatio voi liittyä kansalliseen palveluväylään ilman liittymistä johonkin tiettyyn dedikoituun tietoliikenneverkkoon. Tietoliikennekerros vastaa itse tietoliikenteen reitittämisestä ja ns. OSI-kerrosmallin L1- ja L2-tason tiedonvälityskerroksen palveluista. Jotkut liityntäpisteet voidaan kytkeä toisiinsa myös dedikoiduilla verkoilla, jos verkot voidaan toteuttaa siten, että samat palvelut ovat käytettävissä kokonaisuudessaan myös internetiin.

Teknisen tietoturvallisuuden kerrosmalli



Sovelluskerros (application layer)

Sovellustason tietoturvaratkaisut, salaukset, tunnistamisvaatimukset

Palveluväylä, tiedonvaihtokerros

Palveuväylä tukee päästä-päähän salausta ja Palveluväyän sanomien allekirjoitusta. Sisältää paikallisten lokien jäljitettävyyden palvelun

Tietoliikennekerros (transport layer)

TLS (https) tason salatut yhteydet, vahva päätepisteiden autentikointi

Kansallisen palveluväylän tekninen tietoturvallisuus noudattaa edellä kuvattua monikerroksista mallia.

Sovelluskerroksessa sanomat voidaan salata, allekirjoittaa ja salata sovellusten edellyttämällä tavalla. Palveluväyläkerros tukee kaikkia tyypillisimpiä sanomasisällön salaus- ja tunnistamisratkaisuja.

Palveluväyläkerros vastaa viestinvälityksessä Hyödyntäjän ja Tuottajan turvallisesta autentikoinnista, viestien turvallisesta välittämisestä osapuolelta toiselle, viestin salaamisesta ja jäljitettävyydestä omien sisäisten palvelujensa avulla.

Osapuolten osoitteita ja palveluja säilytetään keskitetysti hallinnoitavassa palvelukatalogissa ja turvanimipalvelussa. Tänne kootaan palveluväyläorganisaatiot, liityntäpisteiden osoitteet ja liityntäpisteistä tarjottavat palvelut. Tämän lisäksi palveluiden tarkemmat tiedot kootaan palvelukatalogiin ja eri toimijoiden väliset sopimukset palvelujen ja tietolähteiden käytöstä kootaan sopimuskatalogiin.

Palveluväylän liityntäpalvelimien välisissä yhteyksissä käytetään molemminpuolista autentikointia sekä sanomien salausta tarpeen mukaan. Tietoliikennekerroksessa tiedonvälitykseen voidaan käyttää tietoliikennekerroksen salausratkaisuja. Toteutustapana käytetään varmennepohjaista TLS-toteutusta

Kaikki liityntäpalvelimien väliset tiedonsiirtoyhteydet suojataan siten, ettei ulkopuolisilla ole mahdollisuus päästä käsiksi siirrettävään tietoon riippumatta siitä, käytetäänkö internetiä vai dedikoitua tietoliikenneyhteyttä. Sanomaliikenteen kaikkien osapuolten identiteetti tulee varmentaa.

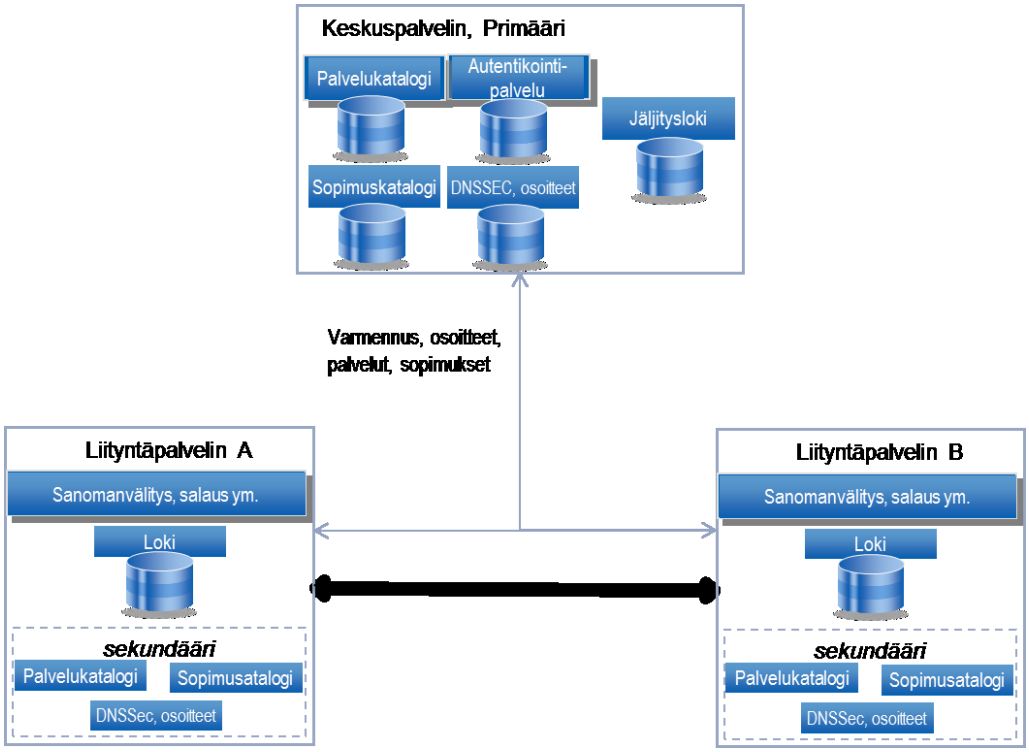
Varmentaminen on pakollista eri palveluväyläorganisaatioiden välisessä tiedonsiirrossa. Tapauksissa joissa yksi palveluväyläorganisaatio välittää tietoa kahden oman loogisen liityntäpisteensä välillä ja näiden liityntäpalvelimet sijaitsevat samassa konesaliympäristössä tai ympäristöissä ei varmennepohjainen tunnistaminen ole pakollista, edellyttäen että konesali- ja käyttöympäristön sisäisestä tietoturvasta on huolehdittu vaatimusten mukaisesti.

6.2.2. Keskuspalvelin vs. liityntäpalvelin

Primääri-sekundäärinoodimalli

Kaikki palveluväylään liittyvät hajautetut liityntäpalvelimet ovat toiminnaltaan samanlaisia. Varsinaiset tiedonsiirrot toteutetaan näiden paikallisten liityntäpalvelimien kahdenvälisinä yhteyksinä.

Palveluväylän keskitetty palveluväyläoperaattori pitää yllä keskuspalvelinta, joka toimii ns. Primäärinoodina. Keskuspalvelimeen (tässä looginen, suositellaan toteutettavan monennetulle alustalle) sijoitetaan palveluväylän tiedonsiirtoa ja palveluiden osoitteiden ja käyttösopimusten hallinnan palvelut. Nämä toimivat palveluväylässä ns. mastertietona, keskuspalvelin **toimii primäärinoodina**.



Palvelukatalogi, turvanimipalvelun osoitetiedot sekä sopimuskatalogi, josta käy ilmi kenellä on oikeus hyödyntää mitäkin tietoa, jaellaan säännöllisesti keskuspalvelimelta tiedon muuttuessa automaattisesti myös paikallisiin liityntäpalvelimiin (**sekundäärinoodi**). Kun paikallinen sovellus haluaa hyödyntää palveluväylään kytkettyä palvelua tai tietovarantoa, kyseisen liityntäpisteen liityntäpalvelin (tässä A) selvittää ensisijaisesti omasta sekundäärinoodiltaan, mistä osoitteesta kyseinen palvelu löytyy, onko sillä oikeus kutsua ko. palvelua ja varmentaa tätä kautta vastapuolen. Vastaavasti B tarkistaa kutsujan tiedot samalla tavalla. Koska myös B:llä on vastaavat tiedot omassa sekundäärinoodissaan, se vastaa kutsuun vain, jos myös sen oman sekundäärinoodin katalogitiedot ovat samat. Sekundäärinoodien yhteydenotossa tarvittaville tie-

doille määritetään vanhenemisaika, jonka jälkeen sekundäärinoodi hakee Keskuspalvelimelta ajantasaiset tiedot.

Tällä primääri-sekundäärinoodiratkaisulla tavoitellaan kansallisen palveluväylän korkeaa, jatkuvaa käytettävyyttä siten, ettei keskuspalvelimen päällä olo ole välttämätöntä kahdenväliselle yhteydenmuodostukselle reaaliaikaisesti. Tämä vähentää keskuspalvelimen kuormitusta ja mahdollistaa sille normaalin ylläpidon edellyttämät säännölliset huoltokatkot ilman, että koko kansallinen palveluväylä on katkon ajan pois käytöstä.

Liityntäpalvelimet voivat käyttää joko keskitettyihin palveluihin kytkettyä varmennepalvelua tai muuta varmentajaa, joka löytyy keskitetyn palvelun luotettujen varmentajien listalta. Nimipalvelu- ja varmenneketjumallia on kuvattu tarkemmin jäljempänä.

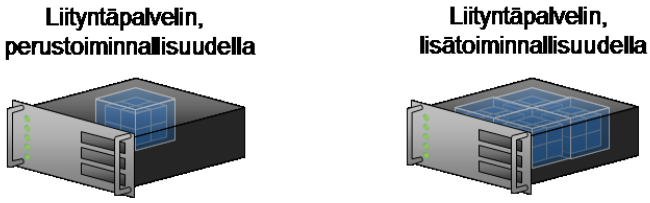
Lokipalvelu

Molemmat paikalliset liityntäpisteet (sekä lähettäjä että vastaanottaja) tallentavat muodostetut yhteydet ja välitetyt sanomat paikalliseen lokiin (viestiloki ja sanomaloki). Tämän avulla esimerkiksi kansalainen voi tarvittaessa jäljittää, mihin hänen tietojaan on välitetty. Sanomalokitietoja ei taltioida keskitettyyn palveluun sellaisenaan suorituskyky- ja tietosuojasyistä. Keskitettyyn palveluun tallennetaan molemmista liityntäpalvelimista ja lokeista vain ns. tiiviste (esim. MD5-tiiviste tai muu luotettava tiiviste), joka on kryptografinen merkkijono, jolla voidaan varmistaa Tuottajan ja Hyödyntäjän liityntäpalvelimilla olevan sanomalokitiedon kiistämättömyys. Tiivisteestä ei pysty päättelemään tai johtamaan käytännössä alkuperäistä viestiä, mutta tiivisteen avulla voidaan varmistaa, että lokitieto on pysynyt muuttumattomana. Tiivisteteknologia tulee voida vaihtaa. Tiivisteen merkitys on vain kiistämättömyys ja sitä tarvitaan vain, jos viestinvälityksen Tuottajan ja Hyödyntäjän viestilokeissa on ristiriita.

Liityntäpalvelimen toiminnalliset moduulit

Liityntäpalvelimet ovat kaikki perusmallissaan samanlaisia. Palveluväyläoperaattori ylläpitää palveluväylän ylläpitäjätahon avustuksella liityntäpalvelimia. Se myös jakelee tai julkaisee haettavaksi liityntäpalvelimien uudet versiot. Liityntäpalvelin toteutetaan ensisijaisesti virtuaalipalvelinpakettina, joka voidaan provisioida/asentaa virtuaalipalvelinalustaan suoraviivaisesti.

Kansallisen palveluväylän suunnittelutyössä on noussut esiin tarjota palveluita erilaisiin käyttötarpeisiin. Tämän johdosta liityntäpalvelimen toiminnallisuus suositellaan toteutettavan moduuleittain, siten että erikseen asennettavilla lisämoduuleilla (sovelluskomponenteilla) voidaan rikastaa ja laajentaa liityntäpalvelimen palveluja:



Perustoiminnallisuuden moduulilla varustettu liityntäpalvelin on peruspalvelin, joka tulee kaikille palveluväyläorganisaatioille. Palveluväyläorganisaatiot voivat kuitenkin tarvittaessa asentaa palveluväylään hallitusti yhdessä sovitut lisämoduulit ja näin laajentaa liityntäpalvelimen ominaisuuksia.

Eri lisämoduuleja ei tässä vaiheessa vielä määritetä tarkasti. Lisämoduulien tarve selviää palveluväylän käytön kehittyessä ja niitä voi tulla lisää koko palveluväylän elinkaaren ajan. Potentiaalisia lisämoduuleja voivat esimerkiksi olla:

- Laajemman toiminnallisuuden integraatiopalvelumoduuli sisältäen esimerkiksi prosessimoottorin ja sanomamuunnostoiminnallisuuden
- Avoimen datan välitysmoduuli
- Tietyn toimialan erityistarpeiden moduuli
- jne.

Kansallisen palveluväylän kehittämisorganisaatio koordinoi liityntäpalvelimien moduulien kehittämistä ja palveluväyläoperaattori testaa ja tarvittaessa auditoi moduulit ennen kuin ne hyväksytään julkaistavaksi liityntäpalvelimiin.

Varsinainen moduulien kehittäminen voidaan kuitenkin tarvittaessa hallitusti hajauttaa.

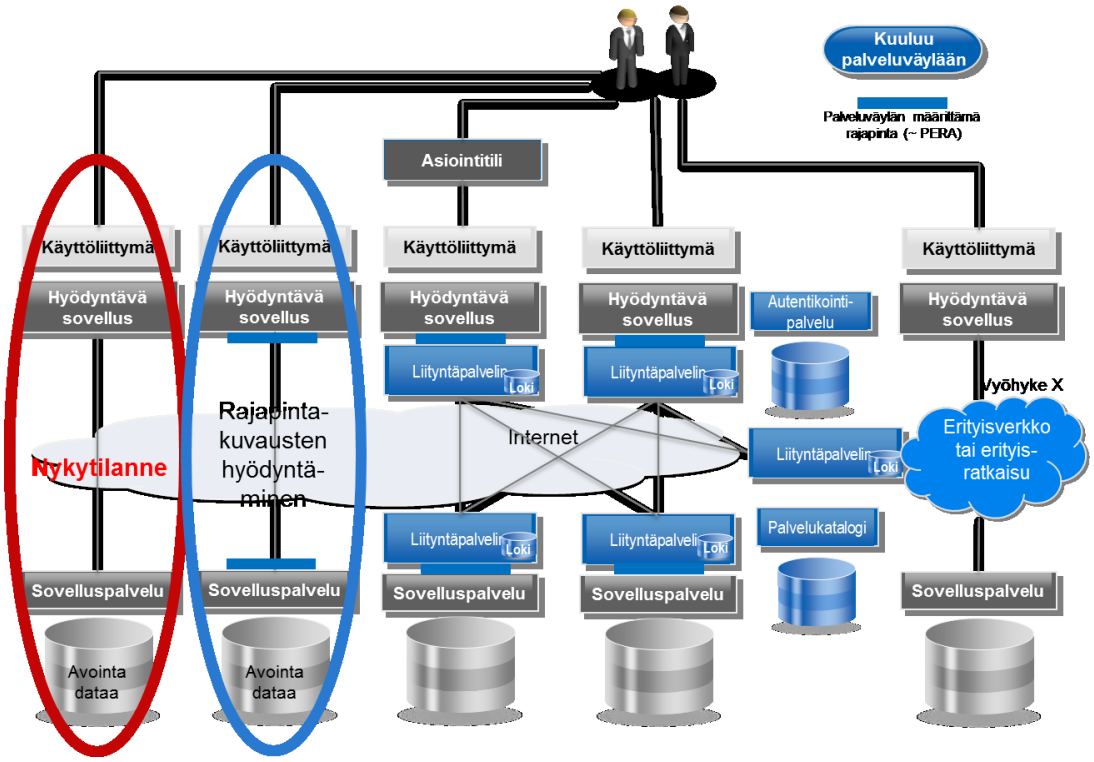
6.2.3. Avoimen datan tuki

Kansallisen palveluväylän myöhemmissä vaiheissa siihen voidaan liittää lisäarvopalveluita, jotka tukevat avoimen datan välittämistä eri osapuolille.

Avoin data sinänsä ei edellytä turvallista osapuolten tunnistamista avoimen tiedon luonteensa johdosta. Avoimen datan palveluiden keskeisimmät haasteet ovat:

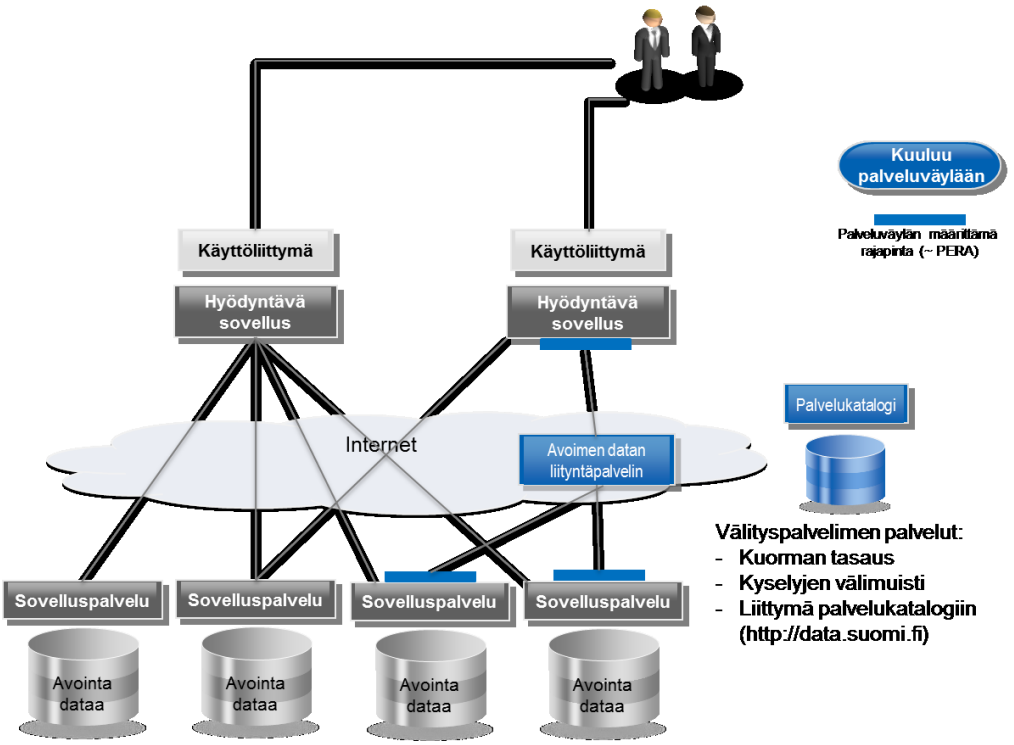
- Avoimen datan palveluiden löytäminen
- Kirjavat rajapinnat ja sanomat
- Potentiaalinen ennakoimaton kuormitus avoimen datan lähteille kysynnän hallinnan puuttumisesta johtuen

Kansallinen palveluväylä voidaan kytkeä avoimen datan tietolähteisiin seuraavasti:



Nykytilanteessa kukin avoimen datan lähde määrittää omat rajapintansa ja kytkentätapansa omista tarpeistaan varsin epäyhtenäisellä tavalla. Kansallinen palveluväylä tuo jo perusmuodossaan kansalliselle tietojenvaihdolle yhtenäisen rajapintamäärityksen, jota voidaan sellaisenaan hyödyntää myös avoimen datan palveluissa. Tämä yksinkertaistaa ja kiihdyttää merkittävästi myös avoimen datan palvelujen hyödyntämistä kansallisen palveluväylän ulkopuolelta.

Myöhemmissä kehitysvaiheissa avoimen datan hyödyntämistä varten voidaan toteuttaa avoimen datan käytön yleispalvelu, joka koostaa avointa dataa yhden palvelun taakse peittäen näin tarpeen mukaan alkuperäisen avoimen datan tietolähteen:



Tässä mallissa avoimen datan käytön välityspalvelu on toteutettu omana palvelukomponenttinaan (moduulina) osaksi liityntäpalvelinta. Tämä avoimen datan liityntäpalvelu sisältää kuorman tasauspalvelun, välimuistipalvelun ja liittymän palvelukatalogiin.

Avoimen datan välityspalvelu vähentää varsinaisen avoimen datan lähteen kuormitusta ja tarpeetonta viestinvälitystä varmistaen näin liiketoimintakriittisten palvelujen ja tiedonvaihdon toimivuuden.

6.2.4. Kansallisen palveluväylän tekninen tietoturva

Palveluväylän välittämä tietoliikenne kulkee julkisessa internetissä, joten palveluväyläratkaisussa on varauduttava avoimen tietoverkon uhkiin. Lisäksi palvelimissa on turvattava kaikki luottamukselliset tiedot niin kauan kuin ne palvelimissa ovat. Palveluväylän rakenteeseen liittyvät määritykset on pidettävä eheinä ja huolehdittava että väylään ei pääse liittymään asiattomia toimijoita.

Palveluväylään kuuluvat laitteet muodostavat nimipalveluissa oman domainin (esim. `palveluvayla.fi`). Palveluväylän nimipalveluissa käytetään turvalaajennoksia (DNS SEC), jossa jokainen nimipalvelun välittämä tieto on allekirjoitettu. Palveluväylässä allekirjoittajana on keskuspalvelin, joka myös on domainin ensisijainen nimipalvelin. Nimipalvelusta saatujen tietojen oikeellisuus voidaan verifioida ja näin olla varmoja, että yhteydenotot tehdään oikeisiin laitteisiin. Nimipalvelua käytetään myös varmenteiden levittämiseen ja muuhun hallinnointiin.

Liityntäpalvelimissa pidetään paikallista nimipalvelua, jonka sisältö päivitetään päänimipalvelimesta tarvittaessa. Täten mahdollinen yhteyskatko keskuspalvelimeen ei haittaa nimipalvelun toimintaa ja estä liityntäpalvelimien välistä viestintää.

Palveluväylän liityntäpalvelimien keskinäiset TLS-salatut tietoliikenneyhteydet tunnistetaan molemmin puolin varmentein. Tunnistuksessa siirretään koko varmenneketju päävarmenteeseen asti, joten ulkopuolisia varmentajia voidaan haluttaessa käyttää. Liityntäpalvelimissa ylläpidetään ajantasaista listaa hyväksytyistä varmentajista. Varmenteita hallitaan nimipalvelun avulla, joten varmenne voidaan tarvittaessa poistaa käytöstä nopeasti ja kyseinen liityntäpalvelin sulkea pois palveluväylästä. Oman varmennepalvelun käyttö on suositeltavampaa, koska tällöin voidaan käyttää lyhytkestoisia varmenteita ilman siitä aiheutuvia lisäkustannuksia.

Kun liityntäpalvelin vastaanottaa palveluviestin salatulla tietoliikenneyhteydellä, palvelukohtaisesta listasta tarkistetaan onko viesti palvelusopimusten mukainen vai evätäänkö viestin käsittely ja vastapuolelle palautetaan virheviesti.

Vaikka liityntäpalvelimet ovat loogisesti osa palveluväylää, sijaitsevat ne organisaatioiden tietoliikenneverkoissa ja ovat organisaation palomuurin takana suojassa.

Liityntäpalvelimiin tarvitsee sallia tietoliikenneyhteydet vain palveluväylään kuuluvista laitteista. Nimipalveluista saadaan koostettua lista sallituista IP-osoitteista, muista osoitteista liityntäpalvelimiin tuleva liikenne voidaan palomuurissa sulkea ja näin estää mm. palvelunestohyökkäykset.

Palveluväylään liittyvät toimijat voidaan hyväksyä myös itseprovisioinnilla. Tällöin liittyjä käynnistää prosessin, jonka lopputuloksena liittyjän tiedot ovat käyttäjäluettelossa, mahdollisesti tarjottu palvelu palvelukatalogissa, liityntäpalvelimelle on varattu IP-osoite ja luotu sertifikaatti (provisioinnissa annetun julkisen avaimen perusteella). Vaihtoehtoisesti toiselta varmennepalvelulta saatu sertifikaatti annetaan provisioinnin aikana. Sekä käyttäjä- että palveluluetteloista ilmenee aluksi, että organisaation tietoja ei ole varmennettu eikä tietojärjestelmien suojaustasoista ole tietoa.

Väylässä tietoa tarjoavat palvelut voidaan luokitella niiden tarjoaman tiedon perusteella (esim.) todentamattomiin, virallisia tietoja tarjoaviin sekä luottamuksellisia tietoja tarjoaviin palveluihin. Kuka tahansa voi tuoda väylään palvelun joka on todentamaton. Luokitusta voi korottaa tähän valtuudet saanut taho. Palvelun luokitus näkyy palveluluettelossa ja hyödyntäjät voivat käyttää tietoa hakiessaan palvelua. Virallista tietoa on esim. julkishallinnon tuottama julkinen tieto. Varmennettuja tietoja tarjoava sovellus edellyttää hyödyntävältä sovellukselta käyttäjän identiteetin tarkistamisen.

Hyödyntävät sovellukset voidaan luokitella (esim.) todentamattomiin ja auditoituihin. Kuka tahansa voi liittää palveluväylään hyödyntäjäsovelluksen todentamattomana. Luokituksen korotuksen voi tehdä siihen valtuutettu taho. Oletusarvoisesti todentamattomat sovellukset voivat hyödyntää niitä palveluja, jotka eivät edellytä kahden välisiä sopimuksia, mutta eivät voi hyödyntää luottamuksellisia tietoja tarjoavia palveluja. Todennetuista hyödyntäjäpalveluista tiedetään, että ne ovat tunnistaneet käyttäjän luotettavasti, joten ne voivat käyttää myös luottamuksellisia tietoja tarjoavia palveluja.

Tietoja tarjoava palvelu voi edellyttää kahdenvälistä sopimusta ennen tietojen vaihtoa, jolloin hyödyntävältä palvelulta voidaan sopimuksellisesti edellyttää enemmän. Näin voidaan edellyttää esim. toivottu tunnistustapa ja varmistua

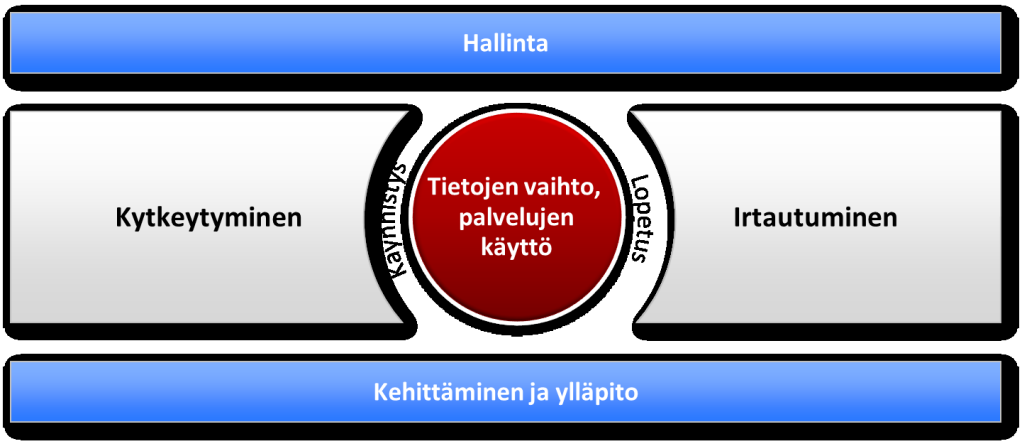
tarvittujen suojaustasojen toteutumisesta. Kahdenväliset sopimukset luetteloidaan keskuspalvelimella, josta ne voidaan tarkistaa.

Liityntäpalvelimien kautta kulkevat sanomat allekirjoitetaan ja tieto kaikista sanomista (niin lähtevistä kuin saapuvistakin) tallennetaan liityntäpalvelimien lokitiedostoihin. Sanomat voivat olla myös salattuja, jolloin niiden sisältöön ei pääse käsiksi edes liityntäpalvelimessa.

6.3. Kansallisen palveluväylän tietojenvaihdon keskeiset prosessit

6.3.1. Yleinen prosessijäsennys

Palveluväylä ei toteuta varsinaisia substanssiprosesseja. Kansallisen palveluväylä prosessit voidaan jäsentää lähinnä sen käytön ja siihen liittymisen näkökulmista seuraavasti:



Kansallisen palveluväylän toiminnalliset prosessit ovat monin osin yleisiä ja hallinnollisia. Niiden yksityiskohdat tarkentuvat vasta hallinta- ja liiketoimintamallin tarkentuessa. Tällöin ne tulee kuvata tarkemmin JHS 152 – suosituksen kuvaustason 3 mukaisesti prosessikaavioina.

Seuraavassa on kuvattu sanallisesti kansallisen palveluväylän yleisprosessien keskeiset piirteet.

6.3.2. Kansallisen palveluväylän hallintaprosessit

Palveluväylän hallintaprosessit sisältävät erityisesti palveluväylän muutosten ja kehittämisen hallintaan sekä yleisten käyttöehtojen ja palvelun tuotteistukseen liittyvät pääprosessit:

- Palvelukokonaisuuden tuotteistaminen
- Palveluväylän yhteisten käyttöehtojen ja sopimusmallien hallinta
- Palveluväylän käyttöehtojen noudattamisen valvonta
- Tietojen vaihdon vahvistaminen
- Laskutusprosessi (mikäli palveluväylän käyttö on maksullista)

Palvelukokonaisuuden tuotteistaminen

Palveluoperaattori vastaa kansallisen palveluväylän palvelukokonaisuuden tuotteistamisesta. Tämä sisältää käyttöehtojen ja sopimusmallien laatimisen, palvelutasojen ja palvelusisällön määrittämisen ja dokumentoinnin sekä ylläpito- ja tukiprosessien kuvaamisen osaksi kokonaispalvelua.

Palveluväylän yhteisten käyttöehtojen ja sopimusmallien hallinta

Palveluväyläoperaattori ylläpitää ja hallinnoi kansallisen palveluväylän käyttöehtoja ja sopimusmalleja. Prosessi sisältää muutostarpeiden tunnistamisen, ehtojen muutosehdotusten määrittämisen, muutosten hyväksymisen palveluväylän ohjausorganisaatiossa sekä uusien käyttöehtojen ja sopimusmallien julkaisun.

Prosessi sisältää uusien käyttöehtojen ja sopimusmallien hyväksymisen sekä viestinnän palveluväyläorganisaatioille.

Palveluväylän käyttöehtojen noudattamisen valvonta

Palveluväyläoperaattorin tehtävänä on valvoa, että kansalliseen palveluväylään liittyneet organisaatiot noudattavat palveluväylän käyttöehtoja. Palveluväyläoperaattori valitsee auditoitavat ja tarkastettavat toimijat, operaattori määrittää tarkastettavat tai auditoitavat kohteet, palveluväyläoperaattori tekee tarkastuksen ja laatii raportin tarkastuksesta. Mikäli tarkastuksessa havaitaan poikkeamia, palveluväyläoperaattori määrittää tarvittavat korjaavat toimenpiteet ja valvoo näiden toteutumista. Räikeissä poikkeamissa palveluväyläorganisaatio voidaan poistaa palveluväylästä.

Tietojen vaihdon vahvistaminen

Palveluoperaattori ylläpitää osana kansallisen palveluväylän keskitettyjä palveluja ns. jäljityslokia, johon tallennetaan paikallisten liityntäpalvelimien lokimerkintöjen tiivisteet. Palveluväyläoperaattori käynnistää tarpeen mukaan tietojen vaihdon vahvistamisprosessin. Tässä prosessissa asiakasorganisaatio pyytää vahvistamaan tietyn tai tiettyjen lokimerkintöjen kiistämättömyyden ja muuttumattomuuden, palveluväyläoperaattori vertaa paikallisen lokimerkintöjä omaan tiivisteensä, palveluoperaattori vahvistaa lokimerkintöjen autenttisuuden.

Laskutusprosessi (mikäli palveluväylän käyttö on maksullista)

Mikäli kansallisen palveluväylän käytöstä tehdään maksullista, palveluväyläoperaattori vastaa palveluväylään liittyneiden palveluväyläorganisaatioiden laskutuksesta. Tämä sisältää hinnastojen hallinnan, maksujen määräytymisen hallinnan sekä suoritusten kokoamisen laskuille sekä varsinaisen laskutus- ja reskontratoiminnon.

6.3.3. Kansalliseen palveluväylään kytkeytyminen

Palveluväylään kytkeytyminen kattaa seuraavat pääprosessit:

- Vyöhykkeen kytkeminen palveluväylään

- Organisaation kytkeytyminen palveluväylään
- Tietoa tuottavan palvelun kytkeminen palveluväylään
- Hyödyntävän liityntäpalvelimen kytkeminen palveluväylään

Vyöhykkeen kytkeminen palveluväylään

Vyöhykkeitä palveluväylään tulee kytkeä hyvin hallitusti ja harkitusti. Kansalliseen palveluväylään tulee määrittää vain sellaisia vyöhykkeitä, joiden sisäistä liikennettä ei perustellusti voi toteuttaa kansallisen palveluväylän tekniikalla ja jotka tulee kuitenkin saada palveluväylän piiriin.

Vyöhykkeiden liittämisprosessi räätälöidään jonkin verran aina vyöhykekohtaisesti. Sen peruselementtejä ovat kuitenkin seuraavat askeleet:

- Vyöhyketarpeen tunnistaminen ja vyöhykkeen kytkemisneuvottelujen aloittaminen
- Vyöhykkeen ja palveluväylän ytimen yhteentoimivuuden suunnittelu
    - Vyöhykkeen reunapalvelimen (silta verkkojen välillä) muunnostoimintojen määrittely
    - Vyöhykkeen sisäisen liikenteen reititys palveluväylän ytimeen
    - Palveluväylän ytimen palvelujen reititys vyöhykkeeseen ja sen palveluihin
    - Mahdollisten sanomamuunnosten määrittely
    - Tarvittavien sopimusten määrittely
    - Vyöhykkeen liittämisen perustelujen laatiminen
    - Toteutusaikataulun ja kehittämisen vaiheistuksen suunnittelu
- Vyöhykkeen yhteentoimivuussuunnitelman käsittely kansallisen palveluväylän ohjausorganisaatiossa – vyöhykkeen kytkennän hyväksyminen
- Palveluväylävarmenteen hankinta
- Liityntäpalvelimen pystytys ja käyttöönotto palveluväylän reunalla
- Vyöhykkeen palvelujen testaus
- Vyöhykkeen toimivuuden auditointi, palveluväyläoperaattori järjestää tämän
- Vyöhykkeen palvelujen tuotantokäytön käynnistys

Varsinaisten palveluväylän ytimen palvelujen hyödyntämisen käyttöönotto ja tuottavien palveluiden käyttöönotto toteutetaan normaalisti seuraavassa kuvatun mukaisesti.

Organisaation kytkeytyminen palveluväylään

Palveluväylässä toisensa tunnistaneet osapuolet lähettävät viestejä toisilleen. Väylään liittyminen edellyttää määriteltyjen liittymiskriteerien täyttämisen ja hyväksynnän palveluväyläoperaattorilta. Organisaatio kytkeytyy palveluväylään seuraavasti:

- Organisaatio pyytää kytkeytymislupaa palveluväyläorganisaatiolta (sähköisesti)
- Organisaatio hyväksyy palveluväylän käyttöehdot ja vastaa tietoturvaa ja tietosuojaa koskeviin vaatimuksiin sekä kysymyksiin
- Palveluväyläoperaattori hyväksyy organisaation palveluväyläorganisaatioksi ja lisää uuden organisaation palveluväylän sallittujen organisaatioiden joukkoon sekä määrittää syntyvän liityntäpisteen osoitteen ja nimen turvanimipalveluun.
- Organisaatio hakee liityntäpalvelimelleen varmenteen
- Organisaatio ottaa käyttöön tai provisioi sähköisellä palvelulla itselleen liityntäpalvelimen ja ottaa siinä käyttöön palvelinvarmenteen
- Liityntäpalvelin kytkeytyy palveluväylään ja hakee keskuspalvelimelta oman sekundääripalvelimen tarvitsemat tiedot
- Tarvittavissa liityntäpisteen auditointi

Tulevaisuudessa palveluväylään kytkeytymisen ei välttämättä tarvitse edellyttää lainkaan palveluoperaattorin erillistä hyväksymistä vaan palveluväylään voi liittyä vain käyttöehdot hyväksymällä automaattisesti. Tämä voi kuitenkin heikentää palveluväylän tietoturvaa, joten tähän tulee siirtyä hyvin harkiten. Tässä voidaan hyödyntää edellä kuvattua jakoa luotettuihin ja ei-luotettuihin palveluväyläorganisaatioihin.

Palveluväylän testiympäristöön kytkeytyminen voidaan toteuttaa automaattisesti organisaation hyväksyessä käyttöehdot.

Organisaation kytkeytyminen palveluväylään tarjoaa uudelle palveluväyläorganisaatiolle hyödynnettäväksi vain ne palvelut, joita voi hyödyntää ilman tiedon tuottajan ja uuden organisaation välistä sopimusta.

Tietoa tuottavan palvelun kytkeminen palveluväylään

Uuden tietoa tuottavan palvelun kytkeminen palveluväylään toteutuu seuraavasti (oletus: organisaatio on jo kytkeytynyt palveluväylään ja sillä on toimiva liityntäpalvelin):

- Tuottajaorganisaatio toteuttaa varsinaisen substanssisovelluksen ja palveluväyläsanoman rajapintamuunnoksen palveluväylän sanomarakenteen mukaisesti
- Tuottajaorganisaatio määrittää palvelun tiedot sähköisen palvelun kautta (palvelukatalogissa tarvittavat tiedot)
- Tuottajaorganisaatio määrittelee kyseisen palvelun sopimusehdot yleisen sopimusmallin mukaisesti

- Palveluväyläoperaattori liittää palvelun palvelukatalogiin ja lisää palvelun yleiskuvauksen viestintäaineistoon
- Tuottajaorganisaatio käynnistää palvelun

Hyödyntävän liityntäpalvelimen kytkeminen palveluväylään

Palveluväylässä jo olevaa palvelua hyödyntävä palvelu kytketään palveluväylään seuraavasti (oletus: organisaatio on jo kytkeytynyt palveluväylään ja sillä on toimiva liityntäpalvelin):

- Hyödyntäjäorganisaatio laatii omaan hyödyntäjäsovellukseensa rajapinnan, joka osaa käyttää palveluväylään kytketyn palvelun sanomarakennetta
- Hyödyntäjäorganisaatio tekee sopimuksen hyödynnettävän palvelun tuottajaorganisaation kanssa – tämä toteutetaan sähköisesti ja taltioidaan sähköisesti paikallisiin sekundääripalvelimien sopimuskatalogeihin.
- Molemmat sekundääripalvelimet toimittavat sopimuksen primääripalvelimelle. Jos molemmilta tahoilta tulevat sopimukset ovat samansisältöiset, keskuspalvelin tallentaa sopimuksen keskuspalvelimelle – tämä toimii tämän jälkeen sopimusmasterina
- Hyödyntäjäorganisaatio käynnistää hyödyntävän palvelun

6.3.4. Kansallisen palveluväylän käyttö

Palveluväylän käyttö sisältää seuraavat pääprosessit:

- Palveluväylän toimijoiden välinen tiedonvaihto
- Lokitus ja tiedonvälityksen seuranta

Palveluväylän käyttöprosessit on kuvattu tarkemmin jäljempänä loogisen arkkitehtuurin kuvauksessa.

6.3.5. Kansallisesta palveluväylästä irtautuminen

Palveluväylästä irtautumisen prosesseja ovat:

- Kahdenvälisen käyttösopimuksen irtisanominen
- Yksittäisen palvelun irrottaminen kansallisesta palveluväylästä
- Palveluväyläorganisaation irtautuminen palveluväylästä
- Vyöhykkeen irtautuminen palveluväylästä

Kahdenvälisen käyttösopimuksen irtisanominen

Kaikki sopimusta edellyttävät tiedonvaihtosopimukset tehdään palveluväyläorganisaatioiden kesken kahdenvälisinä. Kumpi tahansa osapuoli voi irtisanoa sopimuksen. Kun sopimus irtisanotaan, sen tiedot poistetaan sopimuskatalogista.

Yksittäisen tuottavan palvelun irrottaminen kansallisesta palveluväylästä

Tietoa tuottava palvelu irrotetaan palveluväylästä seuraavasti:

- Tuottajaorganisaatio ilmoittaa palveluväyläoperaattorille palvelun poistamistarpeesta. Tämä sisältää ajankohdan, jolloin palvelun käyttö päättyy (käyttöehdoissa voidaan asettaa minimi-irtisanomisaika tuottavalle palvelulle)
- Palveluväyläoperaattori ilmoittaa automaattisesti sopimuskatalogista löytyville hyödyntäjille palvelun päättymisestä
- Palveluväyläoperaattori määrittää palvelukatalogiin ko. palvelulle voimassaoloajaksi ko. päättymisajankohdan. Tämä tieto välittyy liityntäpalvelimiin.
- Tuottajaorganisaatio päättää palvelun. Palvelu ei ole käytettävissä
- Palvelu poistuu automaattisesti päättymisaikana palvelukatalogin aktiivisista palveluista.

Vastaavaa toimintoa voidaan käyttää muunneltuna ja yksinkertaistettuna myös tuottavien palvelujen hetkelliseen passivointiin tai päivitykseen esimerkiksi versiopäivityksen yhteydessä.

Palveluväyläorganisaation irtautuminen palveluväylästä

Palveluorganisaatio irtautuu palveluväylästä seuraavasti (oletus: kaikki tietoa tuottavat palvelut on jo irrotettu palveluväylästä edellisen kohdan mukaisesti):

- Palveluväyläorganisaatio ilmoittaa palveluväyläoperaattorille halustaan irtautua palveluväylästä. Samassa yhteydessä ilmoitetaan irtautumisajankohta
- Palveluoperaattori määrittää organisaation voimassaololle päättymisajankohdan
- Organisaatio poistetaan palveluväylän luotetuista tahoista määräaikana. Samalla sen liityntäpisteen varmenne revokoidaan ja liityntäpiste poistetaan turvanimipalvelusta
- Organisaatio purkaa/sammuttaa oman liityntäpalvelimensa

Vyöhykkeen irtautuminen palveluväylästä

Vyöhykkeen irtautumisprosessi palveluväylästä räätälöidään aina tapauskohtaisesti.

6.3.6. Kansallisen palveluväylän kehittäminen ja ylläpito

Kehittäminen voidaan jakaa kahteen osaan:

- Kehittämistarpeiden kokoaminen
- Kehittämisen koordinointi ja kehittäminen

Kehittämistarpeiden kokoaminen

Palveluväyläoperaattori kerää ja kokoaa systemaattisesti palveluväyläorganisaatioiden ja potentiaalisten asiakkaiden kehittämistarpeita kansallisen palveluväylän sisäisille palveluille. Se kokoaa nämä yhteen ja analysoi ne. Kehittämistarpeet käsitellään kehittämisryhmässä, joka täydentää kehittämistarpeita ja priorisoi ne alustavasti. Palveluväylän ohjausorganisaatio valitsee toteutettavat kehittämiskohteet yhdessä palveluväylän omistajan kanssa kansallisen palveluväylän budjetin puitteissa.

Kehittämisen koordinointi ja kehittäminen

Palveluväyläoperaattori sijoittaa hyväksytyt kehittämiskohteet uusiin versioihin ja kehittämiskalenteriin. Palveluväyläoperaattori järjestää kehittämisresurssit ja ohjaa kehittämistä. Kehittäjäksi valittu kehittäjäorganisaatio toteuttaa varsinaisen kehittämisen.

Ylläpito

Ylläpitoprosessit määritetään pääosin ITIL-mallin ja ISO/IEC 20000 – standardin vaatimusten ja hyvien käytäntöjen pohjalta.

Yleisiä keskuspalvelimen ja palvelun ylläpitoprosesseja ovat mm,:

- Tuki- ja ratkaisuprosessit
    - Asiantuntijatuki
    - Ongelmanhallinta
    - Vikatilanneviestintä
- Kontrolliprosessit
    - Muutoksenhallinta
    - Konfiguraationhallinta

Edellisten lisäksi palveluväyläoperaattorin ja mahdollisen sen ohjauksessa toimivan palveluväylän ylläpitäjätahon tulee huolehtia muista ICT-palvelunhallinnan keskeisistä prosesseista kuten

- Jatkuvuuden- ja käytettävyydenhallinnasta
- Tietoturvallisuudenhallinnasta
- Asiakkuudenhallinnasta ja
- Version/julkaisunhallinasta tms.

Näiden yleisten toimintojen lisäksi palveluväyläoperaattori huolehtii kansallisen palveluväylän erityistoimintojen ylläpidosta, kuten:

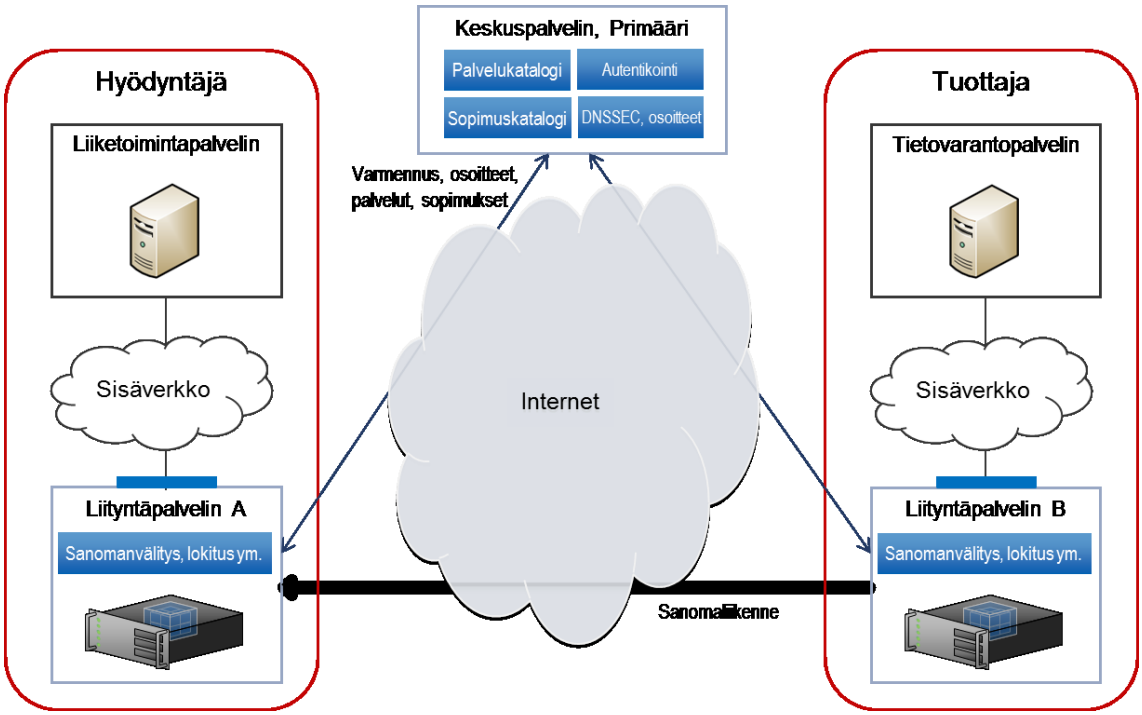
- Nimipalvelun ylläpito
- Sopimuspalvelun ylläpito
- Palvelukatalogin ylläpito

- Käyttöehtojen ylläpito
- Rajapintakuvausten ja skeemojen ylläpito

Palveluväyläoperaattori vastaa myös keskitettyjen palvelujen käyttöpalvelu- ja ylläpitoprosesseista.

6.4. Kansallisen palveluväylän tietojen välittämismalli

Kansallisen palveluväylän tiedonsiirrot toteutetaan aina kahdenvälisinä kahden luotettavasti tunnistetut palveluväylään kytkeytyneen osapuolen välillä. Käytännössä viesti siirtyy osapuolten (Tuottaja ja Hyödyntäjä) liityntäpalvelimien välillä.



Kansallista palveluväylää hyödynnettäessä jokainen yhteys tunnistetaan molemminpuolisesti ennen kuin viestinvälitys aloitetaan.

Tyypillinen sanomanvälitys kahden liityntäpalvelimien kautta kansalliseen palveluväylään kytketyn tietojärjestelmän välillä etenee seuraavasti (tässä esimerkissä Hyödyntäjä on aktiivinen osapuoli ja käynnistää viestinvaihdon):

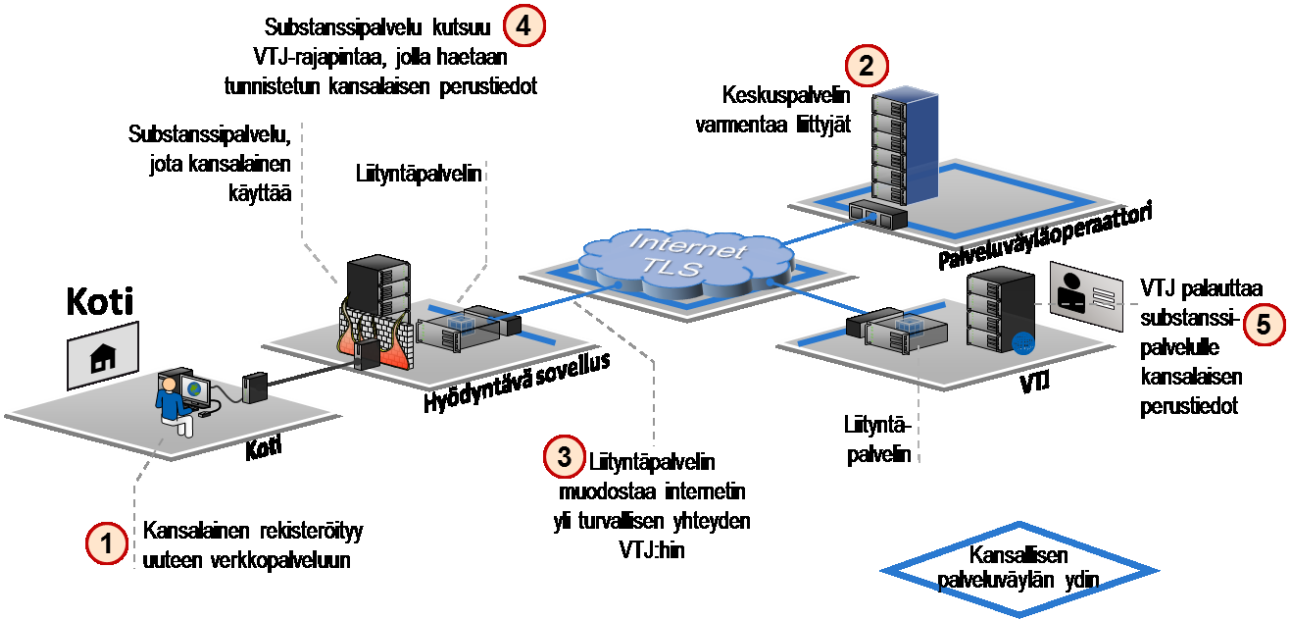
- Hyödyntäjän aktiivinen tietojärjestelmä (liiketoimintapalvelimella) luo palveluväylän sanomamääritysten mukaisen kutsusanoman, jonka kirjekuoressa on tuottavan palvelun tunnistetiedot ja kirjekuoren sisällä kutsuttavan tietovarannon sovelluskohtainen osuus.
- Hyödyntäjän liiketoimintapalvelin lähettää sanoman Hyödyntäjän liityntäpalvelimelle A.
- Liityntäpalvelin A tarkistaa kirjekuoresta kutsuttavan palvelun tiedot ja tarkistaa keskuspalvelimen palvelukatalogista, mistä palveluorganisaatiosta kyseistä palvelua voi saada.

- Liityntäpalvelin A selvittää nimipalveluista Tuottajan liityntäpalvelimen B IP-osoitteen.
- Mikäli sanoma on asynkroninen, liityntäpalvelin kuittaa kutsuviestin vastaanotetuksi Liiketoimintapalvelimelle.
- Hyödyntäjän liityntäpalvelin A ottaa yhteyden kutsuttavan palvelun Tuottajan liityntäpalvelimeen B.
- Liityntäpalvelin B tarkistaa onko liityntäpalvelimella A oikeus olla siihen yhteydessä ja antaa omat tunnistetietonsa.
- Liityntäpalvelin B tarkistaa, että kutsun kohteena olevan Tuottajan liityntäpalvelimen B tunnistetiedot ovat oikeat.
- Jos kummankin pään tunnistetiedot täsmäävät, muodostetaan liityntälaitteiden välille salattu tietoliikenneyhteys.
- Hyödyntäjän liityntäpalvelin A lähettää muodostettua salattua yhteyttä pitkin kutsusanoman Tuottajan liityntäpalvelimelle B.
- Liityntäpalvelin B tarkistaa sopimuskatalogista, onko Hyödyntäjäorganisaation kanssa tehty sopimus kyseisen sanomassa kuvatun palvelun käyttämisestä. Tässä tapauksessa sopimus löytyy.
- Tuottajan liityntäpalvelin B välittää kutsusanoman Tietovarantopalvelimelle, joka kuittaa sanoman vastaanotetuksi. Jos kyseessä on synkroninen sanoma, kuittauksen mukana annetaan vastaus sanomaan.
- Tuottajan tietovarantopalvelin käsittelee kutsun ja muodostaa kutsun parametrien mukaisen vastaussanoman välitettäväksi Hyödyntäjälle.
- Tuottajan tietovarantopalvelin toimittaa sanoman Liityntäpalvelimelle B.
- Tuottajan liityntäpalvelin B välittää vastaussanoman Hyödyntäjän liityntäpalvelimelle B.
- Hyödyntäjän liityntäpalvelin A ottaa vastaan Tuottajan liityntäpalvelimen B lähettämän vastaussanoman.
- Hyödyntäjän liityntäpalvelin A toimittaa vastussanoman varsinaiselle liiketoimintapalvelimessa olevalle liiketoimintasovellukselle käsiteltäväksi. Synkronisessa viestinnässä tästä lähtee vastaus Tuottajan tietovarantopalveluun.

Asynkronisten sanomien vastaukset välitetään kuten muut sanomat, sanoman sisältö indikoi mihin sanomaan se on vastaus.

Kansallisen palveluväylän tarkoitus on toimia loppukäyttäjälle täysin läpinäkyvästi. Loppukäyttäjä näkee kansallisen palveluväylän lähinnä asiointia nopeuttavana ja helpottavana lisäarvona sekä uusina monipuolisina sähköisinä palveluina.

Loppukäyttäjän näkökulmasta kansallinen palveluväylä toimii esimerkiksi seuraavasti:

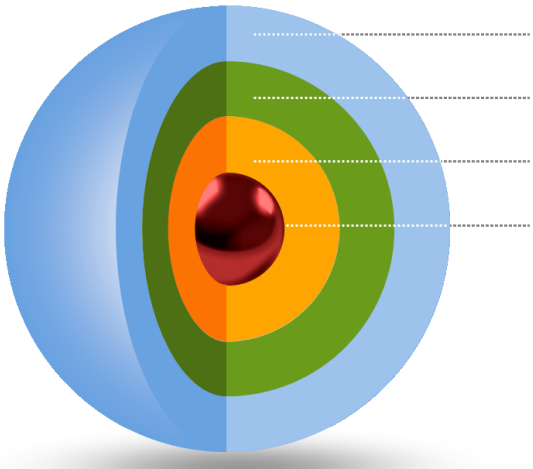


Edellä olevassa esimerkissä hyöty loppukäyttäjälle näkyy siten, ettei hänen tarvitse antaa vahvasti tunnistautuneena lainkaan omia perustietojaan uuteen verkkopalveluun, johon hän rekisteröityy. Substanssipalvelu hakee kansalaisen perustiedot väestötietojärjestelmästä kansallisen palveluväylän kautta täysin automaattisesti. Hyödyntäjän liityntäpalvelin ja VTJ:n liityntäpalvelin molemmat tallentavat tiedon välittämisen omaan lokiinsa. Tämän toiminnallisuuden avulla kansalainen voi myöhemmin tarvittaessa seurata omien tietojensa välittämistä kansallisessa palveluväylässä.

6.5. Kansallisen palveluväylän loogiset tietojärjestelmäpalvelut

6.5.1. Tietojärjestelmäpalvelujen looginen perusjäsennys

Kansallisen palveluväylän tietojärjestelmäpalvelut jäsentyvät edellä kuvatun kerrosmallin mukaisesti:



Eri toimijoiden palveluväylään kytkemät substanssi- ja liiketoimintapalvelut – eivät kuulu palveluväylään

Yleiset lisäarvopalvelut, mahdollistavat lisäarvopalveluita, kiihdyttävät palveluiden kehittämistä

Palveluväylän välttämättömät tekniset palvelut, mahdollistavat väylän käytön

Palvelujen ja tiedon välitysväylä. Ratkaisukokonaisuus, jolla tietolähteet ja palvelut kytketään yhdenmukaisesti toisiinsa

Yhteenveto:

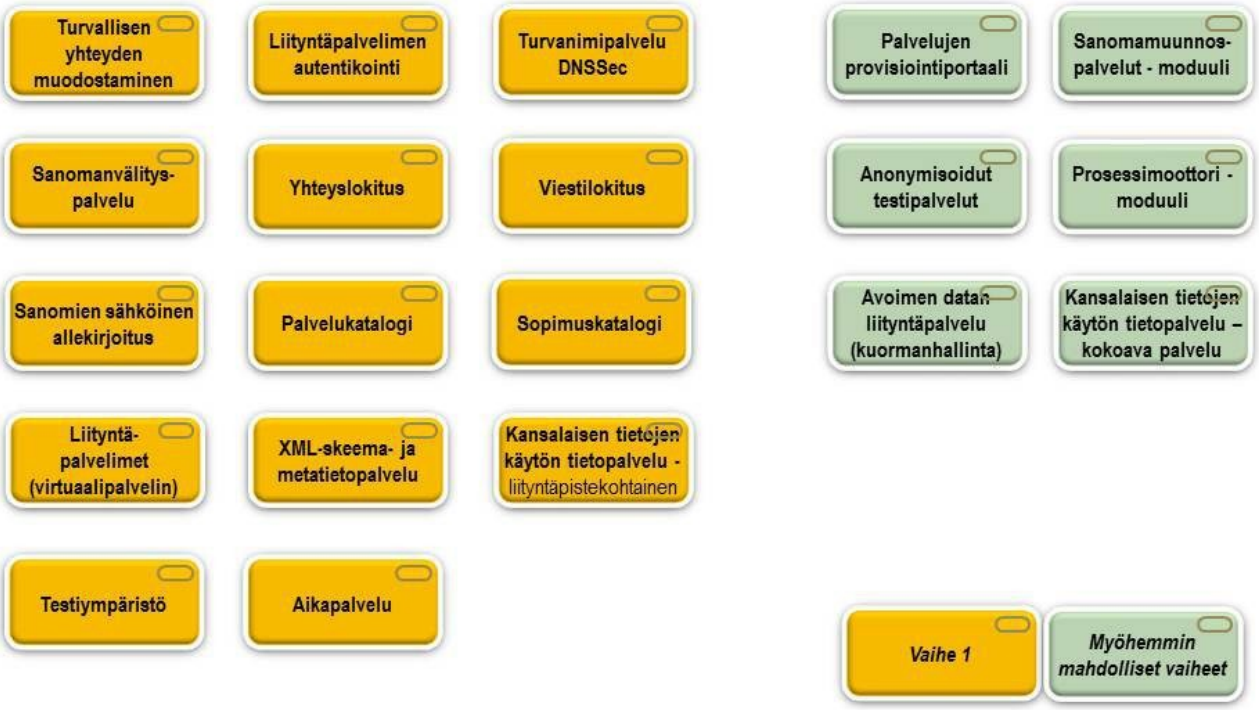
Palveluväylä koostuu kahdesta sisimmästä kerroksesta – tämä mahdollistaa ulommat kerrokset

Seuraavassa on eritelty tarkemmin kansallisen palveluväylän teknisten tietojärjestelmäpalveluiden ja keskeisimpien kansallisen palveluarkkitehtuurin yleispalveluiden sisältö.

Tässä viitearkkitehtuurissa ei määritetä tarkasti, mitä substanssi- ja liiketoimintapalveluja (yllä olevassa kuvassa oleva uloin sininen kerros) kansalliseen palveluväylään tulee kytkeä.

6.5.2. Kansallisen palveluväylän tekniset tietojärjestelmäpalvelut

Edellä olevien rajausten, tavoitteiden ja reunaehtojen sekä arkkitehtuuriperiaatteiden pohjalta edellä kuvattua yleistä viestinvälityksen tietojärjestelmäpalvelulistaa voidaan rajata ja täsmentää. Kansallisen palveluväylän kaikkein keskeisimmät tekniset tietojärjestelmäpalvelut (vaihe 1) ja mahdollisesti myöhemmin kehitettävät palvelut ovat seuraavat:



Yllä olevassa kuvassa on keltaisella (kuvassa vasemmalla) kuvattu ne kansallisen palveluväylän välttämättömät tekniset sisäiset tietojärjestelmäpalvelut, jotka tulee toteuttaa jo ensimmäisessä kehitysvaiheessa. Kuvassa oikealla on vihreällä värillä puolestaan kuvattu merkittävää lisäarvoa tuovia kansallisen palveluväylän teknisiä tietojärjestelmäpalveluja, joita ei aivan välttämättä tarvita kehittämisen ensimmäisessä vaiheessa, mutta jotka on hyvä toteuttaa mahdollisimman nopeasti jatkokehityksessä.

Yllä kuvatut tietojärjestelmäpalvelut ovat loogisia ja ne voidaan koota tarvittaessa toteutusvaiheessa yhteen tai useampaan fyysiseen palvelutoteutukseen.

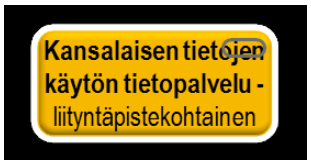
Esimerkiksi turvanimipalvelu, palvelukatalogi ja sopimuskatalogi voidaan mahdollisesti osittain tai kokonaan toteutustasolla yhdistää.

Ensimmäisen vaiheen tietojärjestelmäpalvelut

Seuraavassa on kuvattu tiiviisti yksittäisten kansallisten palveluväylän tietojärjestelmäpalvelu sisältö:

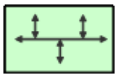
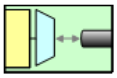
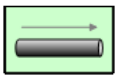
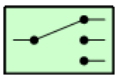
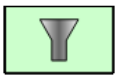
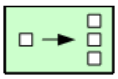
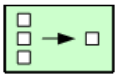
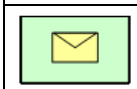
	Kyseessä on tekninen palvelu, jolla muodostetaan salattu yhteys liityntäpisteisiin asennettujen liityntäpalvelimien välille. Yhteys muodostetaan aina kahdenvälisenä yhteytenä Hyödyntäjän ja Tuottajan välille. Yhteys toteutetaan palveluväylän ytimessä internetin yli, mutta voidaan erillisessä Vyöhykkeessä toteuttaa myös dedikoidun tietoliikenneverkon läpi.
	Autentikointipalvelu, jolla liityntäpalvelimet (tai liityntäpiste) kiistämättömästi autentikoidaan. Käytännössä varmennepalvelu, joka varmentaa tiedonvälityksen molemmat osapuolet. Molemmat osapuolet tarkistavat toisen osapuolen varmenteen ja yhteys muodostetaan vain molempien osapuolten hyväksyessä varmenteet. Kansallinen palveluväylä sisältää oman sertifikaattipalvelun CA sekä kuvauksen, mihin muihin sertifikaattipalvelun tuottajiin se luottaa. Tällä varmistetaan se, että sertifikaattipalvelut voidaan hajauttaa tarvittaessa. Autentikointipalvelu (CA, varmennepalvelu) vähentää uhkaa ns. man-in-the-middle tietoturvahyökkäyksille.
	Virtuaalinen palvelinpaketti, jonka palveluväylään kytkeytyvä organisaatio voi asentaa virtualisoidulle palvelinalustalle tai fyysiseen palvelimeen ja näin kytkeytyä kansalliseen palveluväylään. Kyseessä on palveluväyläoperaattorin tuotteistama helposti asennettava kokonaispalvelu, joka sisältää kaikki tässä kuvatut loogiset tietojärjestelmäpalvelut paketoituna kokonaisuutena.
	Turvanimipalvelu (DNSSec, Domain Name System Security Extensions) on kansallisen palveluväylän sisäinen nimipalvelu. Palveluväylän palvelut kootaan yhteen sisäiseen domainiin, joiden nimiä hallitaan korotetun turvallisuuden nimipalvelulla. Turvanimipalvelu antaa palveluväylään kytketyn palvelun IP-osoitteen varmennettuna palvelua hyödyntävälle osapuolelle.

	Varsinainen sanomien välittämisen ja ohjaamisen sovellus, joka toimittaa sanomat lähettäjältä vastaanottajalle. Lähettää ja välittää kansalliseen palveluväylään määritettyjä sanomia. Sanomanvälityspalvelun keskeiset sisäiset viestinvälityksen palvelut on vielä eritelty tarkemmin jäljempänä.
	Yhteyslokitus on lokipalvelu, joka taltioi eri tiedonvaihdon osapuolten muodostamat yhteydet. Toteutetaan siten, että yhteydenmuodostus lokitetaan sekä tuottaja- että hyödyntäjäpäähän paikallisiin yhteyslokeihin. Tämän lisäksi yhteydenmuodostus lokitetaan md5-tiivisteenä tai vastaavana kansallisesti keskitettyyn yhteyslokiin (tästä voidaan käyttää myös nimitystä yhteydenottojen jäljitysloki), jotta yhteydenmuodostuksen kiistämättömyys voidaan varmistaa. Yhteyslokin lokitietojen säilytysaika on parametroitavissa.
	Viestilokitus (sanomalokitus) on lokipalvelu, joka taltioi eri tiedonvaihdon osapuolten siirtämät sanomat. Toteutetaan siten, että palvelujen välillä välitetyt sanomat lokitetaan sekä tuottaja- että hyödyntäjäpäähän paikallisiin viestilokeihin (sanomalokeihin). Tämän lisäksi välitetyistä sanomista tallennetaan tiivisteenä (MD5 tai muu luotettava tiiviste) lokimerkinnät keskitettyjen palvelujen sanomalokitiivisteeseen (tästä voidaan käyttää myös nimitystä sanomien jäljitysloki), jotta välitettyjen sanomien kiistämättömyys voidaan varmistaa. Varsinaisia välitettyjä sanomia ei taltioida kansalliseen keskitettyyn lokiin. Viestilokin lokitietojen säilytysaika on parametroitavissa.
	Palvelu, jonka avulla palveluväylän kautta välitetyt sanomat voidaan sähköisesti allekirjoittaa. Sähköisellä allekirjoituksella voidaan varmistua siitä, ettei sanomat muutu "matkan varrella".
	Ns. UDDI-katalogi, joka kuvaa, mitä SOA-palveluja tai muita palveluja palveluväylässä on käytettävissä ja hyödynnettävissä. Sisältää esim. palvelujen rajapintakuvaukset sekä vastuuorganisaation ja palvelun SLA-lupauksen.

	Katalogi, joka sisältää palveluväyläorganisaatioiden ja palveluväyläoperaattorin väliset sopimukset sekä palveluväyläorganisaatioiden kahdenväliset sopimukset. Kahdenvälisillä sopimuksilla hyödyntäjä- ja tuottajaosapuoli sopivat, mihin tarkoitukseen hyödyntäjä saa palvelua käyttää ja mitä tarjolla olevia palveluja ja rajapintoja hyödyntäjällä on oikeus käyttää. Sopimuskatalogi toteutetaan sähköisesti luettavaan muotoon, jotta tuottajat voivat tämän avulla hallita automaattisesti tiedon jakelua ja esimerkiksi näin varmistaa palveluväylään kytkettyjen tietojen lainmukaisen tietosuojan. Sopimuskatalogi on tarkoitus jakaa myös osaksi liityntäpalvelinta, jotta liityntäpisteiden välinen viestinvälitys ei edellytä reaaliaikaista yhteyttä kansallisen palveluväylän keskitettyihin palveluihin.
	Keskitetty palvelu, joka sisältää yleisimmät kansallisessa palveluväylässä käytettävät XML-skeemat sekä metatietopalvelun käytetyistä luokituksista, tunnisteista tms. Käytetään lähinnä kehittämisen tukena, ei operatiiviseen viestinvälitykseen.
	Kansalaisen tietojen käytön tietopalvelu on perusmuodossaan palveluväyläorganisaatiokohtainen kuhunkin liityntäpisteeseen sijoitettu tietojärjestelmäpalvelu, jonka avulla voidaan kustakin liityntäpisteestä selvittää, mitä tietoja tietystä yksilöitävästä käyttäjästä on välitetty ja käsitelty. Tietopalvelu kokoaa tietonsa palveluväyläorganisaation liityntäpisteen viestilokista.
	Palvelu tarjoaa loogisen testiympäristön kansalliseen palveluväylään. Palvelua käytetään kansalliseen palveluväylään kytkettävien palvelujen kehittämisen tukena ja kehittämisalustana.
	Aikapalvelu synkronoi kansallisen palveluväylän liityntäpalvelimien sekä keskuspalvelimien kellot. Palvelun avulla voidaan kansallisen palveluväylän kautta tehtyihin transaktioihin liittää luotettava aikaleima. Tämä varmistaa prosessien ja viestien järjestyksen (kausaliteetin) ja luotettavan lokituksen. Tämän avulla voidaan luotettavasti jäljittää viestien ja sanomien käsittelyn sekä lokitietojen ajanhetki. Palvelussa suositellaan käytettäväksi Mitta-

	tekniikan keskuksen NTP-aikapalvelua tai vastaavaa luotettavaa aikapalvelua.

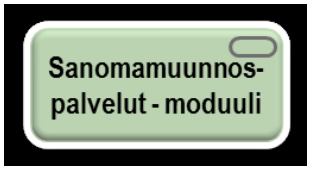
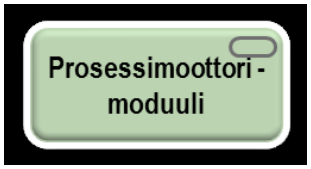
Edellä kuvatun **sanomanvälityspalvelun** sisäiset viestinvälityksen palvelut voidaan jäsentää valtion integraatioarkkitehtuurissa määritettyjen tietojärjestelmäpalvelujen pohjalta vielä tarkemmin seuraaviin osapalveluihin:

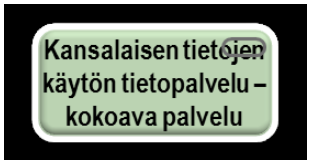
	**Sanomaväylä (message bus)** *Kansallisen palveluväylän keskeisin osa. Sanomaväylä tarjoaa palveluväylään kytketyille palveluille mahdollisuuden palvelujen väliseen sanomanvälitykseen.*
	**Kanava-adapteri (channel adapter)** *Kanava-adapterin avulla palvelu voi lähettää ja vastaanottaa sanomia sanomanvälitysjärjestelmästä.*
	**Sanomakanava (message channel)** *Sanomakanava kytkee sovellukset toisiinsa. Tuottava palvelu kirjoittaa tietoa kanavaan ja hyödyntävä palvelu lukee sitä kanavasta.*
	**Sanomareititin (message router)** *Sanomareititin ohjaa sanomat oikealle vastaanottajalle/ottajille sanoman header-tietojen tai kutsuttavan palvelun tietojen perusteella.*
	**Sanomasuodatin (message filter)** *Sanomasuodatin poistaa ei-toivotut sanomat määriteltyjen kriteerien perusteella. Sopimuskatalogi toimii loogisesti sanomasuodattimena ja estää tiedonjaon olemassa olevien sopimusten vastaisesti.*
	**Jakaja (splitter)** *Jakaja jakaa yhdistelmäsanoman erillisiksi yhtä asiaa koskeviksi sanomiksi. Mahdollistaa ns. one-to-many -sanomaliikenteen kansallisessa palveluväylässä.*
	**Yhdistäjä (aggregator)** *Yhdistäjä kerää (ja säilyttää) yksittäiset sanomat kunnes kaikki yhtä kokonaisuutta koskevat sanomat on vastaanotettu. Yhdistäjä kokoaa nämä sanomat yhdeksi sanomaksi ja julkaisee sen.* Mahdollistaa ns. many-to-one –sanomaliikenteen kansallisessa palveluväylässä.
	**Kääre (envelope, wrapper)** *Kääre sisältää sovellustietoa sanomavälitysjärjestelmän hyväksymässä muodossa.*

Myöhempien vaiheiden tietojärjestelmäpalvelut

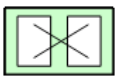
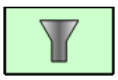
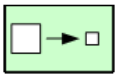
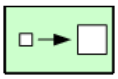
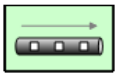
Edellä on tunnistettu ensivaiheen välttämättömien tai erittäin kriittisten kansallisen palveluväylän palvelujen lisäksi myös joukko muita palveluväylän tekni-

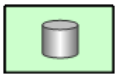
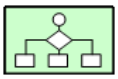
siä palveluja, jotka ovat varsin hyödyllisiä kansallisen palveluväylän käytön edistämiselle, mutta joita voidaan tarvittaessa siirtää myöhempiin kehitysvaiheisiin. Näitä ovat:

	Edellä kuvatun palveluväylän perustoiminnallisuuteen kuuluvan sanomavälityksen tietojärjestelmäpalvelun laajennus, joka sisältää sanomamuunnosten käsittelyn erityispalvelut, kuten sanomarikastimen, sanomasuodattimen tms.. Lisäpalvelut toteutetaan liityntäpalvelimeen asennettavalla palvelumoduulilla. Ks. tarkempi erittely näistä osapalveluista jäljempänä.
	Edellä kuvatun palveluväylän perustoiminnallisuuteen kuuluvan sanomavälityksen tietojärjestelmäpalvelun laajennus, joka sisältää laajemman sääntökoneen ja prosessimoottorin. Tämän tietojärjestelmäpalvelun avulla liityntäpalvelimeen voidaan luoda monimutkaisempia sanomanvälitys- ja palvelujen kutsusääntöjä. Prosessimoottori toteutetaan liityntäpalvelimeen asennettavalla palvelumoduulilla. Ks. tarkempi kuvaus jäljempänä.
	Testipalvelu, joka tarjoaa palveluväylään kytkettyjen tietolähteiden ja palvelujen anonymisoitua dataa testikäyttöön. Anonymisoidusta datasta sovitaan palveluväylän tietolähteiden omistajien kanssa.
	Lisäarvopalvelu, jonka avulla avoimen datan tietolähteitä voidaan koota yhteen yhden palvelun taakse. Palvelu sisältää rajoitetusti cache-ominaisuuksia, joilla voidaan vähentää vähentävät varsinaisten avoimen datan lähteiden kuormitusta.
	Palveluväyläorganisaatioille tarkoitettu lisäarvopalvelu, jonka avulla voidaan automaattisesti itsepalveluliittymän avulla provisioida uusi palvelu palveluväylään tai erityisesti uusi liityntäpalvelin palveluväylään. Tämä madaltaa erityisesti palveluväylään jo kytkettyjen palvelujen hyödyntämistä. Yksittäinen organisaatio voi tämän lisäarvopalvelun avulla puoliautomaattisesti kytkeytyä palveluväylään, hy-

	väksyä sen käyttöehdot ja käyttää suoraan niitä palveluväylään kytkettyjä palveluja, jotka eivät edellytä kahdenvälistä sopimusta tuottavan palvelun omistajan kanssa.
	Vrt. kansallisen palveluväylän perustoiminnallisuuteen kuuluva liityntäpistekohtainen kansalaisen tietojen käytön tietopalvelu. Tämä keskitetty palvelu kokoaa yhteen kaikista liityntäpistekohtaisista viestilokeista tiettyä käyttäjää koskevan tiedonvaihdon ja palauttaa tämän palveluna loppukäyttäjälle tai tietoa käsittelevälle tietojärjestelmäpalvelulle. Ominaisuus on tarkoitettu erityisesti kansalaisen käyttöön, jotta hän voi seurata omien tietojensa käyttöä kokonaisuutena. Palvelu hyödyntää hajautettuja liityntäpistekohtaisia kansalaisen tietojen käytön tietopalveluja.

Myöhemmissä vaiheissa sanomanvälitystoiminnallisuutta voidaan laajentaa vielä seuraaviin osapalveluihin. Tämä suositellaan toteutettavan erillisellä liityntäpalvelimeen asennetavalla integraatiopalvelumoduulilla:

	**Sanomamuunnin (message translator)** *Sanomamuunnin muuntaa sanoman yhdestä muodosta toiseen. Sanomamuunnin muuntaa sanomia rakenteellisesti ja sisällöllisesti.*
	**Laajennettu sanomasuodatin (message filter)** *Perustoiminnallisuutta laajentava sanomasuodatintoiminnallisuus.*
	**Sisältösuodatin (content filter)** *Sisältösuodatin poistaa vastaanottajan kannalta merkityksetöntä tietoa sanomasta.*
	**Sanomarikastin (content enricher)** *Sanomarikastin lisää sanomaan puuttuvia tietoja, joita se hakee ennalta määritetystä tietovarannosta.*
	**Tietotyyppikanava (datatype channel)** Tietotyyppikanava on erikoissanomakanava joka voi välittää vain jotain tiettyä sanomamuotoa.
	**Valvontaväylä (control bus)** *Valvontaväylää käytetään sanomanvälityksen valvontaa ja hallintaan. Valvontaväylä käyttää samoja sanomanvälitysmekanismeja kuin sovellustiedot. Tarvittavat tiedot sanomanvälitykseen osallistuvien komponenttien hallitsemiseksi välitetään erillistä kanavaa käyttäen.*

	**Sanomansäilytys (message store)** *Sanomasäilytys on väliaikaistietovaranto, jossa säilytetään tietoa sanomista / sanomatiedot.*
	**Prosessityökalut (process manager**) *Prosessityökaluilla määritellään ja hallitaan integraatio- ja tiedonvälitysprosesseja.*

Laajennettujen integraatiopalvelujen tavoitteena on tuoda kansalliseen palveluväylään liittyneille palveluväyläorganisaatioille kustannustehokas ja kattava integraatioratkaisukokonaisuus, jonka avulla niiden on helpompi toteuttaa liiketoiminta- ja substanssiprosesseja paremmin tukevia tietojärjestelmäpalveluja.

Kansallisen palveluväylän omistaja vastaa kaikista edellä mainituista palveluväylän teknisistä palveluista.

Palveluväylän teknisten tietojärjestelmäpalveluiden sijoittuminen loogisesti kansallisen palveluväylän eri osiin (erityisesti keskitettyjen ja hajautettujen palvelujen sijoittuminen) on kuvattu tarkemmin jäljempänä loogisen arkkitehtuurin osiossa.

Tietojärjestelmäpalvelut on listattu *Liitteeseen 1, KA-taulukot*.

6.5.3. Kansalliseen palveluväylään kytkettävät keskeisimmät kansallisen palveluarkkitehtuurin yleispalvelut

Palveluarkkitehtuurin yleispalvelut eivät ole välttämättömiä kansallisen palveluväylän toiminnalle eivätkä tästä syystä kuulu palveluväylän teknisiin ydinpalveluihin. Yleispalvelut ovat kuitenkin yleisesti muiden palvelujen kanssa yhdessä käytettäviä mahdollistavia sähköisiä palveluita, jotka merkittävästi edistävät varsinaisten sähköisten substanssi- ja liiketoimintapalvelujen kehit-

tämistä. Palveluarkkitehtuurin yleispalvelut eivät tyypillisesti ole sellaisenaan loppukäyttäjälle hyödyllisiä, vaan niitä käytetään läpinäkyvästi muiden palveluiden osana tai tukena. Viitearkkitehtuurivaiheessa seuraavien palveluarkkitehtuurin yleispalveluiden on tunnistettu olevan kaikkein keskeisimpiä kansallisen palveluväylän muita substanssipalveluja tukevia yleispalveluja:

Kansalaisen tunnistaminen

Tällä tarkoitetaan yksittäisen kansalaisen luotettavaa tunnistamispalvelua. Tällä hetkellä tyypillisin kansalaisen tunnistamisratkaisu on Vetuma ja siihen kuuluvat vahvan tunnistamisen välineet. Tämän haasteena on se, että esimerkiksi Vetumaan kuuluva pankkitunnuksilla tapahtuva tunnistaminen on maksullinen ja kaupallinen palvelu, jonka laajentaminen kaikkiin palveluihin on osin hankalaa.

Valtiovarainministeriö, liikenne- ja viestintäministeriö sekä Sitra ovat kuitenkin valmistelleet kansallisen sähköisen tunnistusratkaisun uudistamista (valmistelun yhteydessä on kuultu pankkeja ja mobiilioperaattoreita sekä muita sidosryhmiä). Uuden tunnistusratkaisun suunnittelu- ja toteutusperiaatteita ovat:

- Kustannustehokkuus,
- kansainvälinen yhteensopivuus,
- avoimuus,
- kehittyvä ratkaisu,
- luotettavuus,
- helppokäyttöisyys sekä

- uuden tunnistusratkaisun tulee olla nykyisiä ratkaisuja edullisempi sekä sähköisten palvelujen tarjoajille että niiden käyttäjille.

Uuden tunnistusratkaisun avulla voidaan entistä paremmin edistää sähköisen asioinnin laajenemista ja monipuolistumista sekä kokonaan uusien sähköisen liiketoiminnan mahdollisuuksien syntymistä.

Ehdotuksena on, että kansallisessa sähköisessä tunnistusratkaisussa valtio tuottaa kaikille kansalaisille varmenteet, julkisen varmennehakemiston sekä niihin liittyvät peruspalvelut (ns. kansallinen varmenneinfra). Uuden kansalaisen tunnistamisratkaisun tavoitellaan olevan helposti käyttöönotettavissa, riittävän turvallinen ja se tukee eri tunnistusvälineiden käyttöä.

Varmenteeseen perustuva, vapaasti valittavissa oleva tunnistusväline tarjoaa kansalaisille pääsyn kaikkiin sähköisiin palveluihin. Sähköisten palvelujen tarjoajille riittää puolestaan vain yhden tunnistuspalvelun käyttöönottaminen kaikkien potentiaalisten asiakkaiden tunnistamiseksi.

Nykyisille tunnistuspalvelujen tuottajille, kuten pankeille tarjoutuu mahdollisuuksia siirtyä uusiin luotettaviin tunnistusratkaisuihin kustannustehokkaasti. Mobiilioperaattoreille avautuu mahdollisuus saada käyttäjä- ja käyttömäärät nopeaan kasvuun, joka myös edistää lisäpalveluliiketoimintaa.

Kansalaisen tunnistamispalvelu on keskeisin kansallisen palveluväylän käyttöä kiihdyttävistä palveluarkkitehtuurin yleispalveluista. Se suositellaan toteutettavan samanaikaisesti kansallisen palveluväylän ensimmäisen vaiheen toteutuksen kanssa.

Ammattilaisen tunnistaminen

Ammattilaisen tunnistamispalvelun avulla voidaan tunnistaa eri ammattikuntien edustajia. Erityisen hyödyllinen tämä on luvanvaraisen toiminnan ja ammattioikeuksia edellyttävien palvelujen kehittämisen tukena. Nykyisin keskeisin ammattilaisen tunnistamiseen liittyvä palvelu koskee terveydenhuollon ammattilaisen tunnistamista.

Ammattilaisen tunnistamispalvelu voidaan tulevaisuudessa toteuttaa todennäköisesti samalla teknisellä perusmallilla kuin kansalaisenkin tunnistaminen. Tällöin on keskeistä erottaa ammattilaisen pääsynhallintakokonaisuudessa henkilön tunnistamisen palvelu hänen käyttöoikeuksiensa määrittävästä palvelusta. Tyypillisesti tunnistamispalvelu vain luotettavasti vahvistaa, kuka henkilö väittää olevansa. Ammattilaisen tunnistamisessa tämän jälkeen selvitetään tämän tunnistetun henkilön oikeudet tuottaa haluttuja palveluja esimerkiksi ammattioikeusrekisterin avulla (vrt. Valviran Terhikki-rekisteri, johon on tallennettu terveydenhuollon ammattilaisten ammattioikeus- ja ammatillisen pätevyyden tiedot).

Organisaation tunnistaminen

Organisaation tunnistamisen tarkoituksena on tunnistaa organisaation ja erityisesti yrityksen edustaja ja määrittää tämän rooli kyseisessä yrityksessä.

Lähtötilanteessa palvelu on toteutettu ns. Katso-palveluna. Katso-tunnistus on Verohallinnon tarjoama, yrityksiä varten luotu tapa tunnistautua viranomaisten sähköisiin palveluihin. Katso-palvelussa organisaation edustaja voi perustaa Katso-tunnisteen sekä hallinnoida organisaation tietoja, alitunnisteita ja valtuuksia.

Katso-palvelu on tarkoitus korvata ns. RoVa-palvelulla. Rooli- ja valtuutuspalvelu RoVa on yritysten ja yhteisöjen sähköisessä asioinnissa tarvittavien rooli- ja valtuutustietojen hallintaan tarkoitettu palvelu.

Julkishallinnon sähköiset asiointipalvelut hyödyntävät yhteiskäyttöistä ja keskitettyä rooli- ja valtuuspalvelua sähköisten asiointitapahtumien oikeudellisuuden todentamisessa. RoVa-palvelun tavoitteena on antaa varmuus siitä, että asiointipalvelua käyttävällä henkilöllä on valtuus asioida edustamansa yrityksen tai tahon puolesta.

RoVa-palvelun ensisijaisena tarkoituksena on tarjota julkishallinnon sähköisille asiointipalveluille ajantasainen, tarkka ja kattava tieto yrityksen tai muun tahon edustajana asioivan henkilön rooleista palveluissa. RoVa-palvelu on tarkoitettu koko julkishallinnon käyttöön. Palvelua voivat hyödyntää mm. viranomaiset ja kunnat, mutta myös yritykset ja muut yhteisöt.

Asiointitilit

Asiointitilillä tarkoitetaan kansalaiselle tai yritykselle suunnattua sähköisen asioinnin tiliratkaisua, joka kokoaa yhteen viranomais- ja/tai yksityisen sektorin asioinnin perustietoja. Tyypillisesti asiointitilin kautta loppukäyttäjä voi käynnistää sähköiset asiointipalvelut, viestiä halitusti palveluntarjoajan kanssa ja saada tiedon asioinnin etenemisestä. Jotkut asiointitilit taltioivat myös asiakkaan asiointiin liittyvät päätökset ja liiteaineiston.

Keskeisimpiä asiointitilejä lähtötilanteessa ovat Valtiokonttorin hallinnoima kansalaisen asiointitili sekä työ- ja elinkeinoministeriön yrityksen palvelukokonaisuudessa SADe-hankkeessa kehitettävä yrityksen asiointitili.

Yrityksen asiointitili on viranomaisen ja yrityksen välinen vuorovaikutteinen sähköistä asiointia tukeva palvelu. Yrityksen asiointitili mahdollistaa yritykselle ja viranomaiselle keskitetyn, tietoturvallisen ja luotettavan, ns. yhden luukun periaatteella toimivan tavan asiointien hoitamiseen. Asiointitilin kautta kansalainen löytää asiointeja koskevat dokumentit sekä asian käsittelyyn liittyvät tiedot ja viestit. Tilille toimitetaan joko suoraan tai linkkeinä asian käsittelyyn liittyvät päätökset, täydennyspyynnöt ja dokumentit kokonaan sähköisessä muodossa.

Yrityksen asiointitilin kriittisen menestystekijän muodostavat siihen liitetyt sähköistetyt viranomaispalvelut. Tavoitteena on, että yrityksen asiointipalvelut

voidaan kytkeä suoraan yrityksen asiointitiliin kattavasti yrityksen toimialasta ja koosta riippumatta.

Maksamisen palvelut

Maksamisen yleispalvelu on tarkoitettu sujuvaan ja helppoon verkkomaksamiseen. Lähtötilanteessa julkisen hallinnon maksuja voidaan maksaa Vetuma-palvelun maksuratkaisulla, jossa maksamisen välineiksi soveltuu verkkopankki tai luottokortti. Tämän lisäksi on käytössä yksityisiä verkkomaksamisen palveluita, jotka kattavat myös muita verkkomaksamisen välineitä (esim. PayPal). Maksamisen yleispalvelu kokoaa yhteen osaksi palveluväylää tehokkaat sähköisen maksamisen välineet.

Maksamisen välineet voidaan kytkeä tarvittaessa kaikkiin kansallisiin palveluväylään kytkettyihin palveluihin.

Suostumusten ja tahdonilmaisujen hallinta

Suostumusten hallinta ja valtuutusten ja tietopyyntöjen hallinta muodostavat ns. tiedonluovutusten hallinnan palvelukokonaisuuden. Tiedonluovutusvaltuuksien hallinnalla hallitaan tietojen välittämistä ja luovuttamista toimijalta toiselle

Suostumuksella tarkoitetaan asiakkaan – kansalaisen tai yrityksen – antamaa suostumusta viranomaiselle tai muulle palveluntuottajalle, jolla asiakas sallii käyttää itseään koskevaa tietoa tai esim. suostuu asioinnissa käyttämään sähköisiä välineitä perinteisten keinojen sijaan (esim. päätöksiä ei tällöin tarvitse toimittaa paperilla). Suostumus voi koskea myös suostumusta toimenpiteeseen tai tehtävään. Jos kansalainen ei ole antanut suostumusta tietojen luovutukseen viranomaiselle, niin viranomaisen tulee kunnioittaa tätä asiakkaan tahtoa, ellei laki anna viranomaiselle muuten oikeutta käyttää ko. tietoa.

Muita tahdonilmaisuja voivat olla esimerkiksi elinluovutustestamentti tai elvytyskielto tms.

Kansalaisella on oikeus myös tietyissä tapauksissa määrittää kielto kyseisen tiedon luovuttamiseen. Teknisesti kielto on ”negatiivinen suostumus” ja voidaan erottaa suostumuksista yhdellä lisäattribuutilla.

Suostumusten hallinnan keskeisiä ominaisuuksia ovat:

- Asiakkaan suostumuksen / valtuutuksen antaminen, suostumuksen tai valtuutuksen luominen
- Suostumusten kokoaminen asiointitilille tai suostumustilille
- Suostumusten liittäminen niitä koskeviin palveluihin ja tietoihin
- Suostumuksen peruuttaminen

- Paperilla tehtyjen suostumusten tallentaminen manuaalisesti suostumuskantaan (huom. tämä saattaa arkistointinäkökulmasta edellyttää kuitenkin myös paperiasiakirjan arkistoimista)

Suostumukset jaetaan kahteen luokkaan:

- Tiedonluovutusta koskevat suostumukset
- Toimenpidesuostumukset

Suostumustenhallintaan kuuluu myös käyttäjän antama suostumus sähköisen asiointikanavan käyttöön viranomaistasolla (tämä on toimenpidesuostumus). Sähköiset palvelut voivat tarkistaa suostumuksenhallintapalvelusta, onko asiakas antanut suostumuksensa asiointitilin ja sähköisen asioinnin käyttöön kyseisen viranomaisen palveluja koskien. Tarkistaminen tapahtuu käyttäen suostumuksenhallintaan toteutettua käyttöliittymää tai sähköistä palvelua.

Sähköisiä palveluita käytettäessä on varmistettava, että kyseiseen asiointiin voidaan käyttää sähköistä kanavaa ja että viranomaisella on oikeus päästä käsiksi kyseisen tietoon. Jos suostumusta ei ole tai käyttäjä on peruuttanut suostumuksen, niin sähköinen palvelu ei siirrä asiakasta koskevaa tietoa vaan palauttaa virheilmoituksen pyytävälle järjestelmälle. Asiakas voi koska tahansa perua suostumuksensa ja tämä tulee ottaa huomioon sähköisiä palveluita kehitettäessä.

Aivan kaikkiin palveluihin ja tietoihin ei välttämättä tarvita lainkaan suostumusta. Tätä varten palveluun voidaan määritellä säännöstö, jossa kuvataan: tarvitaanko tähän tiedon luovuttamiseen suostumus, keneltä tarvitaan suostumus ja kuinka monen ko. roolin edustajan suostumus tarvitaan. Esimerkiksi tarvitaanko alaikäisen oppijan molemmilta huoltajilta suostumus tai valtuutus vai riittääkö vain toisen huoltajan suostumus.

Valtuutusten ja puolesta-asioinnin hallinta

Valtuutuksilla tarkoitetaan mahdollisuutta valtuuttaa toinen taho toimimaan puolestaan viranomaisasioinnissa. Monissa tapauksissa huoltajilla on lain perusteella jo valtuutus toimia huollettavan puolesta tietyissä asioissa. Valtuutusten hallinta kattaa myös nämä ns. automaattivaltuutukset. Sähköisten valtuutusten avulla varmistetaan, että tietyllä toimijalla on palvelun kohteen antama oikeus toimia edustamansa yhteisön tai henkilön edustajana (puolesta-asioijana).

Kun valtuutuksia käytetään, sähköiset palvelut suorittavat asiointiin liittyvät valtuutusten tarkastukset tarpeen mukaan. Jos viranomainen tai yritys on todennut henkilön oikeuden toimia toisen edustajana ja edustaja on antanut suostumuksen viranomaiselle, niin viranomainen voi lähettää asiaan liittyvät viestit suoraan edustajan asiointitilille tai asioinnin yhteystietoihin. Asiointitilin yhteydessä suositellaan käytettävän ns. roolipohjaista toteutustapaa, jossa henkilöt käyttävät vain omaa asiointitiliään, jonne saapuvat myös heidän mahdollisten edustettaviensa viestit. Näin valtuutukset voidaan kohdistaa palveluihin ja tietyn rajoitetun kohteen asioihin, ei kaikkeen valtuuttajaa koskevaan tietoon.

Työ- ja elinkeinoministeriön kehittämisvastuulla oleva Rooli- ja valtuutuspalvelu (Rova) toimii jatkossa organisaatioiden puolesta-asioinnin palveluna.

Keskeiset valtuutusten hallintaan liittyvät toiminnallisuudet ovat:

- Asiakkaan valtuutuksen antaminen, valtuutuksen luominen
- Valtuutuksen liittäminen valtuutetun ja valtuuttajan valtuutusprofiiliin
- Valtuutusten hyväksyminen (valtuutettu voi hyväksyä tai hylätä hänelle annetun valtuutuksen)
- Valtuutusten liittäminen niitä koskeviin palveluihin
- Valtuutuksen peruuttaminen
- Paperilla tehtyjen valtuutusten tallentaminen manuaalisesti valtuutuskantaan (huom. tämä saattaa arkistointinäkökulmasta edellyttää kuitenkin myös paperiasiakirjan arkistoimista)

Tietopyyntöjen hallinta

Tilanteessa, jossa lainsäädäntö sallii tiedon luovutuksen tai jopa edellyttää tiedon julkisuutta, viranomaisen tulee hallita näitä tietoja koskevia tietopyyntöjä. Tietopyyntöjen jättämisen ja käsittelyn perusominaisuuksia ovat:

- Tietopyynnön luominen
  - Pyynnön tekijän tiedot, tiedot tahosta, jolle tietopyyntö lähetetään, tietopyynnön kohde (asiakas, kansalainen), luovutettavan tiedon kuvaus, tiedon käyttötarkoitus, aikaleima, tila: avoin
  - Tietopyyntö tallentuu tietopyyntöjen tietovarantoon ja linkittyy kyseisen asiakkaan viestinvälityslokiin, kun tieto välitetään tuottajalta hyödyntäjälle – kaikilla kansalaisilla on lakiin perustuva oikeus saada tietää, mihin häntä koskevaa tietoa on käytetty ja mihin sitä on luovutettu
- Tietopyynnön vastaanotto ja käsittely
  - Tietopyyntö ohjautuu siinä kuvatulle viranomaistaholle ja kyseinen taho käsittelee tietopyynnön.
  - Tietopyyntö voidaan hyväksyä tai hylätä.
  - Hyväksytty tietopyyntö antaa tiedon pyytäjälle oikeuden päästä kyseiseen tietoon tai palveluun käsiksi
- Tietopyyntöjonon hallinta
  - Tietylle taholle lähetettyihin avoimiin tietopyyntöihin tulee olla selkeä näkymä.

Huom. kaikkiin tiedonluovutusvaltuutuksiin tulee määrittää sekä kansalaisen, valtuutetun, tiedon luovuttajan ja hyödyntäjän hakutoiminnot kyseisiin tiedonluovutuksiin ja niiden valtuutuksiin.

Kansallisen palveluarkkitehtuurin yleispalveluiden omistajuus voi vaihdella. Tässä vaiheessa ei oteta kantaa, minkä tahon tulisi toimia minkäkin yleispalvelun omistajana. Yleispalvelut eivät välttämättä ole kansallisen palveluväylän omistajan omistuksessa tai ohjauksessa.

6.6. Kansallisen palveluväylän tietoarkkitehtuuri

6.6.1. Sanoma- ja rajapintasisältö

Kansallisen palveluväylän sanomarakenteeksi suositellaan PERA- ja X-Road-tyyppisen sanomarakenteen yhdistelmää muutamin lisäpiirtein. Kansallisen palveluväylän tulee aktiivisesti edetä kohti REST-tyyppistä toteutusta. Tämä suositellaan toteutettavan yhteistyössä valittavan pohjaratkaisun (rajapintamääritys, jonka pohjalta kansallinen palveluväyläratkaisu kehitetään) vastuukehittäjän kanssa jotta kehittämisen synergiaetu voidaan jatkossakin säilyttää.

Seuraavassa on kuvattuna kansallisen palveluväylän suositeltu sanomarakenne. Viestit voidaan välittää joko SOAP- tai REST-mallilla ja tiedot esittää joko XML- tai JSON-muodossa.

Sanomien mahdollinen salaaminen ja allekirjoittaminen on sovellustason asia, koska välityspalvelimien välinen TLS-yhteys takaa sanoman välittämisen luottamuksellisuuden ja eheyden.

Kansallisen palveluväylän sanoman otsikkokentät olisivat seuraavat:

Kuvaus	**Tarkennuksia**
Sanoman otsikko (<Header>)	
Pakolliset tiedot	
kutsuva organisaatio	sama kuin kutsuvan organisaation varmenteella
palveleva organisaatio	sama kuin palvelevan organisaation varmenteella
kutsuttava palvelu	sanoman kohdistaminen oikealle palvelulle – tämä on REST-implementaatiossa osa URL:ia.
viestin yksilöivä tunnus	globaalisti yksikäsitteinen tunnus sanoman jäljitykseen
aikaleima	kutsun alkuperäinen muodostamishetki (ISO 8601 / UTC). Käytetään mm. vanhentuneiden sanomien tunnistamiseen ja poistamiseen
Valinnaiset tiedot	
alkuperäinen kutsuva organisaatio	viestiketjun aloittaja, jos eri kuin kutsuva – alkuperäisen organisaation varmenteelta
kutsun käynnistäneen henkilön tunniste vies-	muoto OID, CCX tai CC:R:X[4] (CC on maakoodi, R organisaatio X tunnus) esim:

[4] Loppukäyttäjätunnukselle olisi hyvä löytää yleispätevämpi muoto, joka ottaisi huomioon myös muiden maiden kansalaiset. Yleisistä virallisista kansallisista tunnisteista (Suomessa HETU) tämä saadaan lisäämällä kansallisen tunnisteen eteen maakoodi. Maassa voi olla useita virallisesta tunnisteesta poikkeavia tunnuksia. Tällaisia ovat erillisen rekisteröinnin vaativat järjestelmät ja esim. virkamiehen tunnistamisen menetelmät, joissa käytetty yksilöivä tunniste ei ole HETU. Lisäksi opetushallinnon puolella käyttäjän identiteetin ilmaistaan OID:n avulla.

tiketjun aloittavassa organisaatiossa	1.2.246.562.24.10000000009 tai FI311299-0123. Tietojärjestelmän oma käyttäjätunnus on muotoa FI:OmaOrg:UserId
kutsun käynnistäneen henkilön tunnistamis-tapa	Esim. VIRTU, MOBILE[operator], BANK[name], PASSWORD, ID-CARD. Käytetty tunnistustapa voi vaikuttaa annettavaan palveluun.
kutsun käynnistävän henkilön asema	kutsun käynnistäneen henkilön asema / rooli organisaatiossa, voidaan hyödyntää käyttövaltuuden tarkistamisessa
valtuutusperuste	mihin valtuutukseen kysely perustuu, voidaan hyödyntää käyttövaltuuden tarkistamisessa
asynkroninen kutsu	oletusarvona synkroninen kutsu, sanomanvälitystavan valinta. Vastaussanomalle voidaan asettaa osoite, mikäli se halutaan välityspalvelimen konfiguraatiosta poikkeavaan osoitteeseen
voimassaolo	kutsussa: kuinka ajantasaista tietoa haetaan; vastauksessa: kuinka kauan tiedon oletetaan olevan validi. Mahdollistaa kyselyjen vähentämisen välimuistien avulla

6.6.2. Kansallisen palveluväylän loogiset tietovarannot

Kansallisen palveluväylän sisäiset loogiset tietovarannot ovat edellisten tietojärjestelmäpalveluiden ja viestinvälitystarpeiden mukaan seuraavat:

Näistä keskuspalvelimeen sijoitettavia keskitettyjä tietovarantoja (master) ovat:

- Palvelukatalogi (primääri)
- Sopimuskatalogi (primääri)
- DNSSec turvanimet ja osoitteet (primääri)
- Kansallisen palveluväylän varmennepalvelun varmenteet
- Skeemat ja metatiedot
- Viesti- ja yhteyslokintiivisteet (sekundääri, kiistämättömyyttä varten)

Hajautetusti yksittäisten palveluväylään kytkettyjen organisaatioiden liityntäpalvelimeen sisällytettyjä tietovarantoja puolestaan ovat:

- Viesti- ja yhteysloki (primääri, sekä lähettäjällä että vastaanottajalla)
- Palvelukatalogi (sekundääri)
- Sopimuskatalogi (sekundääri)
- DNSSec turvanimet ja osoitteet (sekundääri)

Palvelukatalogi

Palvelukatalogi sisältää tiedot palveluväylään kytketyistä palveluista ja niiden liityntäpisteistä. Ratkaisumallina käytetään laajennettua UDDI-palvelukatalogimallia, jossa palveluista taltioidaan teknisesti luettavaan muotoon ainakin:

- Palveluväyläorganisaatio, joka tarjoaa ko. palvelun
- Liityntäpiste, josta ko. palvelu löytyy
- Palvelun nimi
- Kuvaus
- Palvelutyyppi
- SLA
- Sanomasisältö
- Virheilmoitukset
- Edellytykset (pre-condition)
- Jälkitila (post-condition)

Palveluiden tietoihin voidaan liittää myös muita lisätietoja ja attribuutteja, kuten esimerkiksi edellyttääkö palvelu kahdenkeskistä sopimusta vai onko palvelu vapaasti kaikkien palveluväylään kytkeytyvien organisaatioiden hyödynnettävissä.

Palveluun voidaan kuvata myös tekstimuodossa sen käyttöehdot.

Keskitetyn palvelun palvelukatalogi monistetaan automaattisesti kaikkiin paikallisiin liityntäpalvelimiin.

Sopimuskatalogi

Sopimuskatalogi sisältää tiedot eri palveluväyläorganisaatioiden välisistä palvelujen ja tietojen käytön sopimuksista. Sopimukset laaditaan yhteisesti määritettyjen sopimusmallien pohjalta aina kahdenvälisinä sopimuksina tietojen Hyödyntäjän ja Tuottajan välillä. Tieto sopimuksesta tallennetaan keskitettyyn sopimuskatalogiin.

Sopimuskatalogiin tallennetaan ainakin:

- Sopijapuolet (hyödyntäjä ja tuottaja)

- Päivämäärä
- Sopimuksen kesto (vapaaehtoinen), voi olla voimassa myös toistaiseksi
- Palvelut, joihin hyödyntäjällä on käyttöoikeus
- Palvelujen käyttöön liittyvät mahdolliset maksut ja veloitukset
- Ehdot, jotka hyödyntäjän tulee täyttää tuottajan palveluita hyödynnettäessä.

Keskitetyn palvelun sopimuskatalogi monistetaan automaattisesti kaikkiin paikallisiin liityntäpalvelimiin. Vaihtoehtoisesti voidaan monistaa vain ne sopimukset, joissa ko. liityntäpisteen/liityntäpalvelimen omistaja on sopimusosapuoli.

Viesti- ja yhteysloki

Viesti- ja yhteysloki tallennetaan viestinvälitysten osapuolten liityntäpalvelimiin. Sekä lähettävä että vastaanottava osapuoli tallentaa lokitiedon paikalliseen lokiin.

Lokeihin tallennetaan sekä yhteyksien muodostaminen ja kesto että varsinaiset sanomat. Lokiin merkitään viestin aikaleima ja sanomat. Sanoma itsessään sisältää tiedon osapuolista ja muista metatiedoista.

Lokin säilytysaika voidaan parametroida. Palveluväyläoperaattori määrittää säilytysajan oletusarvon.

Keskitettyyn palveluun ei tallenneta varsinaisia viestejä vaan ainoastaan kryptografiset tiivisteet kyseisistä sanomista. Näin voidaan varmistaa lokitietojen muuttumattomuus ja kiistämättömyys.

Varmenteet

Kansallisen palveluväylän suositellaan käyttävän omaa tai yhtä luotettua varmennepalvelua, josta liityntäpisteiden varmenteet jaellaan ja joka varmentaa osapuolet.

Keskitettyihin palveluihin suositellaan mallia, jossa palveluväylään voidaan merkitä, mihin muihin varmennepalveluihin kansallinen palveluväylä luottaa. Näin paikalliset palveluväyläorganisaatiot voivat tarpeen mukaan käyttää myös muita varmennepalveluita.

Skeemat ja metatiedot

Tietovaranto pitää kirjaa sanomaskeemoista ja metatiedoista. Tätä tietovarantoa käytetään lähinnä kansalliseen palveluväylään kytkettävien palvelujen kehittämisen tukena.

DNSSec turvanimet

Tämä looginen tietovaranto kytkeytyy tiiviisti palvelukatalogiin. Se pitää kirjaa turvallisesti, mistä IP-osoitteesta mikäkin liityntäpiste ja sen palvelut löytyvät.

6.7. Teknologiapalvelut

6.7.1. Käyttö- ja kapasiteettipalvelut

Palveluoperaattori vastaa keskuspalvelimien käyttö- ja kapasiteettipalveluista. Tässä palvelinten käyttö- ja kapasiteettipalveluilla tarkoitetaan palvelukokonaisuutta, joka koostuu seuraavista osapalveluista:

- Konesalipalvelut
- Palvelinlaitteiden ja tallennusjärjestelmien kapasiteettipalvelut
- Palvelinten, sovellusten ja tukijärjestelmien hallintapalvelut sisältäen normaalit kunnossapitotoimenpiteet ja tietoturva- ja versiopäivitykset
- Valvontapalvelut sisältäen infrastruktuurin, alustojen ja palvelinten käyttöjärjestelmä- sekä sovellustason valvonnan
- Varmistuspalvelut
- Tietokantapalvelut

Käyttö- ja kapasiteettipalvelujen sisältö ei poikkea merkittävästi yleisistä korkean käytettävyyden alustan ammattimaisista palveluista.

Keskuspalvelimen monentaminen ja kuormantasaus

Keskus- ja liityntäpalvelimen teknologia tulee suunnitella ja toteuttaa skaalautuvasti ja muokattavasti siten, että palveluiden suorituskykyä voidaan joustavasti kehittää palveluvolyymin ja palveluväylään kytkettyjen organisaatioiden ja palvelujen karttuessa.

Edustakerros, sovelluskerros ja tietovarantokerros on suorituskyvyn muokattavuuden takia hyvä erottaa toisistaan. Palvelinalustan teknisen roolituksen tulee soveltaen noudattaa seuraavaa kerrosmallia:

Palvelinjärjestelmät sijoitetaan yllä kuvattuihin teknologiakerroksiin. Teknologiakerrokset varmistavat ns. **vertikaalisen skaalautuvuuden**, jonka avulla eri teknologiakerrosten pullonkauloja voidaan parantaa ko. kerroksen palvelinkapasiteetin ja suorituskyvyn nostolla. Palvelinkerrosten tulee olla mahdollisimman riippumattomia.

Kansallisen palveluväylän liityntäpalvelimeen ei liity kovin merkittävää *esityskerrosta*, koska liityntäpalvelin toimii lähinnä viestinvälittäjänä eikä loppukäyttäjälle näkyvänä kokonaisuutena. Sama koskee pääpiirteittäin myös kes-

kuspalvelinta, mutta sen kohdalla tulee kuitenkin huolehtia kansallisen palveluväylän operointikäyttöliittymäkerroksen riittävästä suorituskyvystä.

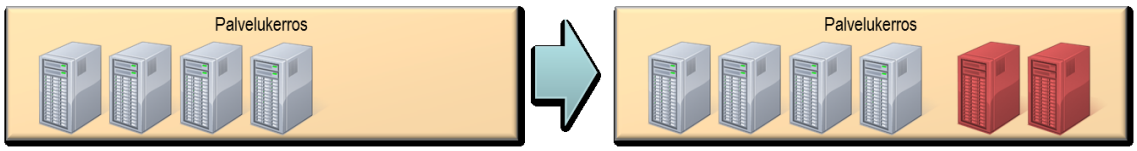
Palvelukerrokseen sijoitetaan teknologiamallissa varsinaiset liityntä- ja keskuspalvelimen palvelut: sanomavälitys, nimipalvelut, palvelukatalogi, varmennuspalvelut jne..

Tietovarantokerros sisältää tarvittavat tietokantapalvelimet tai tietokannat (ks. loogiset tietovarannot jäljempänä).

Ratkaisumallilla voidaan tarvittaessa parantaa myös tietoturvaa. Tämä tehdään jakamalla liikenne kerroksien mukaan segmentteihin Virtual Routing and Forwarding (VRF) ratkaisulla ja käyttämällä palomuuria kerroksien välisessä liikenteessä. Näin liikenne kerroksien välillä voidaan rajata.

Horisontaalinen skaalautuvuus

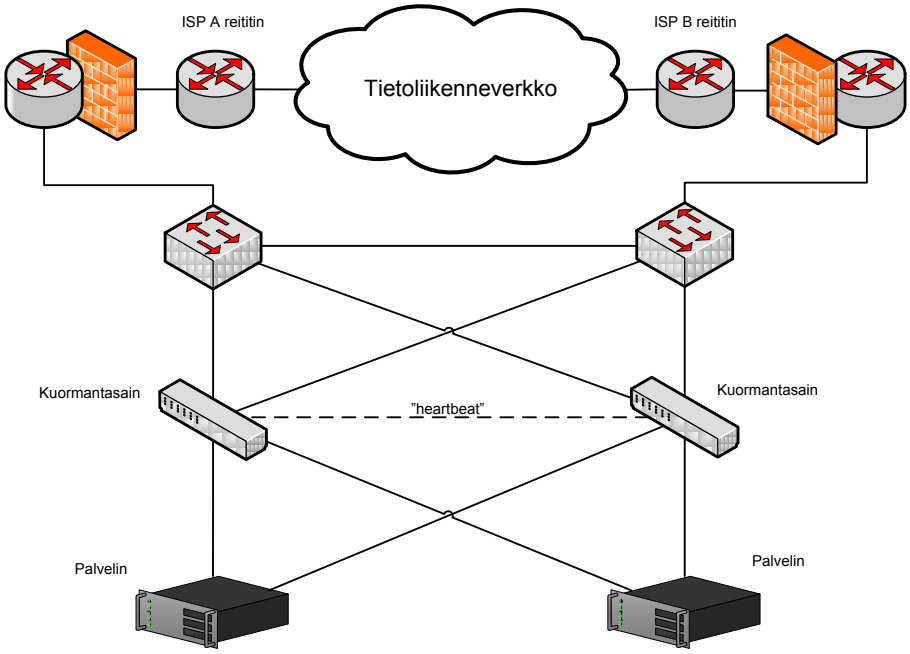
Yhden teknologisen palvelinkerroksen sisällä on hyvä käyttää teknologiaa, joka mahdollistaa **horisontaalisen skaalautuvuuden**. Horisontaalisessa skaalautuvuudessa palvelinkapasiteettia voidaan palvelukerroksen sisällä lisätä tai vähentää kuorman mukaan ilman käyttökatkoa.



Monennettu kerroksellinen palveluarkkitehtuuri mahdollistaa myös korkean käytettävyyden alustojen toteuttamisen esimerkiksi FailOver-klusteriteknologialla.

Skaalautuva ympäristö voidaan toteuttaa palvelinvirtualisoinnilla tai skaalautuvalla sovellus- ja tietokantateknologialla.

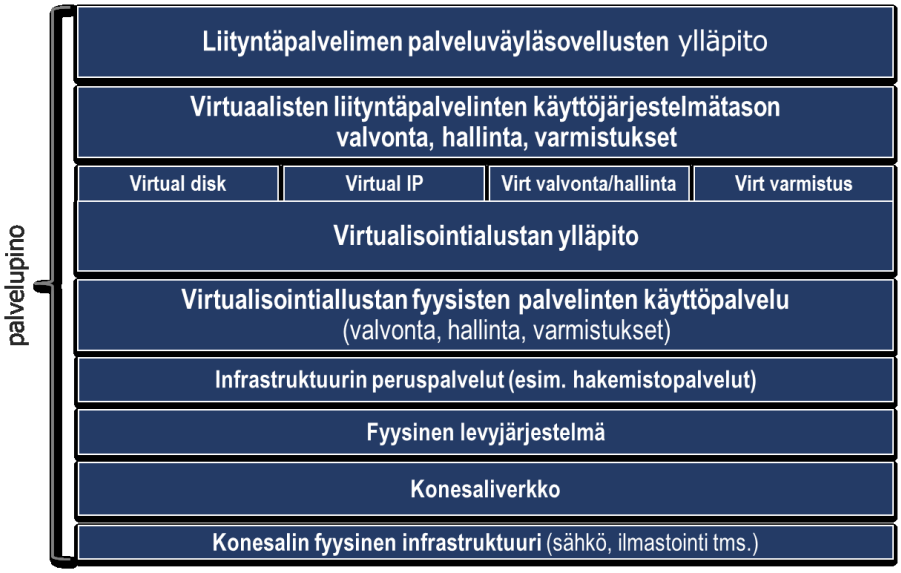
Keskuspalvelin ja keskeisimmät liityntäpalvelimet suositellaan monennettavan asetettujen palvelutasotavoitteiden saavuttamiseksi. Monennetun (klusteroidun) palvelinympäristön ja tietoliikenneverkon kytkimen väliin voidaan kriittisissä kohteissa kytkeä yksi tai monennettu kuormantasain.



Liityntäpalvelimen toteuttaminen virtuaalipalvelimena

Liityntäpalvelin koostuu tuotteistetusta paketista palveluväylän yhteen sovitettuja sovelluskomponentteja sekä tietokantoja, jotka kootaan helposti asennettavaksi kokonaisuudeksi yhteen. Liityntäpalvelin koostetaan sekä asennettavaksi paketiksi että valmiiksi provisioitavaksi virtuaalipalvelimeksi.

Mikäli liityntäpalvelin tai keskuspalvelin toteutetaan virtuaalipalvelintekniikalla on huolehdittava koko palvelupinon valvonnasta sekä virtualisoidussa palvelimessa, virtualisointialustassa että näiden taustalla olevassa fyysisessä infrastruktuurissa:



6.7.2. Tietoliikennepalvelut

Kansallisen palveluväylän ydin toteutetaan siten, että liityntäpisteiden välinen liikenne välitetään salatusti internet-verkossa. Internet-verkkoon ei saa yhtä

kattavia palvelutasotavoitteita kuin ns. dedikoituihin tai suljettuihin verkkoihin (esim. käytettävyys, läpäisykyky, viive ja viiveen vaihtelu, pakettivirhesuhde jne.). Tämä johtaa siihen, ettei palveluväylään kytkettyyn palveluunkaan voida määrittää kovin yksityiskohtaisia SLA-tavoitteita. Palveluväylään kytketyn palvelun suorituskyky hyödyntäjiin päin riippuu sekä tuottavan organisaation internet-yhteyden kapasiteetista ja laadusta että hyödyntävän organisaation internet-yhteyden kapasiteetista ja laadusta. Pienillä volyymeillä tämä ei ole haaste, mutta sanomakoon ja sanomanvälitysvolyymin lisääntyessä riittävään kapasiteettiin tulee kiinnittää huomiota sekä tuottavassa että hyödyntävässä päässä.

Palveluväylään liittyvän organisaation tulee itse mitoittaa ja hankkia palvelun käytön kannalta riittävän korkeakapasiteettinen ja korkealaatuinen internet-liittymä. Kriittisissä palveluissa internet-liittymät suositellaan kahdennettavan siten, että ne hankintaan toisistaan riippumattomilta operaattoreilta.

Palveluväylän vyöhykkeissä voidaan käyttää myös dedikoituja verkkoja, joille voidaan taata yhteinen, tarkemmin määritelty palvelutaso ja turvallisuus.

6.7.3. Valvonta- ja hallinta-arkkitehtuuri

Valvonnan ja hallinnan yleiset periaatteet

Kansallisen palveluväylän valvonta- ja hallinta jakautuu kahteen osaan:

- Keskitettyjen palvelujen valvontaan ja hallintaan
- Liityntäpisteiden ja palveluväylään kytkettyjen palvelujen hajautettuun valvontaan ja hallintaan

Molempiin osakokonaisuuksiin voidaan hyödyntää soveltaen samaa valvonta- ja hallinta-arkkitehtuuria, sovittaen tarpeet palveluväylään kytketyn palvelun SLA-tavoitteisiin.

Seuraavaan on koottu erityisesti kansallisen palveluväylän keskitettyjen palvelujen valvonta- ja hallinta-arkkitehtuurin perusteet.

Kaikki kriittiset ja tärkeät palveluväylän keskitettyjen palvelujen osat ja teknologiat (keskuspalvelinkokonaisuus) tulee olla kytkettynä jatkuvaan, automaattihälytyksiin perustuviin valvontajärjestelmiin. Tästä vastaa palveluväylän ylläpitäjätaho.

Kansallisen palveluväylän keskuspalvelimet ja tietovarannot tulee sijoittaa siten, että palveluväylän tietoturvavaatimukset täyttyvät. Koska palveluväylän ytimen tiedot eivät ole turvallisuusluokiteltuja, voidaan palvelimiin soveltaa Vahti 1/2002 suositusta siltä osin kuin se kattaa käytettävyyden ja luotettavuuden vaatimukset.

Palveluvaylän ydinpalvelut ja tietovarannot sisältävätpalvelimet tulee sijoittaa sellaisiin laitetiloihin, jotka mahdollistavat alempana esitetyt palvelutasot. Palveluväylän ydinpalveluiden tulee olla kahdennettuina erillisissä, riittävän kaukana toisistaan sijaitsevissa laitetiloissa, jotka ovat tarkoituksenmukaisesti suojattuja.

Järjestelmien valvontaa ja hallintaa saavat toteuttaa vain nimetyt ja palveluväyläoperaattorin hyväksymät henkilöt. Ylläpitäjätahon tulee varmistaa, ettei muilla sen työntekijöillä ole pääsyä asiakkaan tietoihin tai järjestelmään.

Palveluväylän ylläpitäjätahon asiantuntijoilta vaaditaan henkilökohtainen salassapitositoumus. Näiden asiantuntijoiden tulee myös suostua perusmuotoiseen turvallisuusselvitykseen.

Tarkemmat valvonnan ja hallinnan turvallisuusvaatimukset kuvataan tietoturvapolitiikassa ja -ohjeistuksessa.

Keskitettyjen palvelujen palvelutasotavoitteet

Laatumääreitä koskeva terminologia

Kansallisen palveluväylän keskitettyjen palvelujen (ja soveltaen myös liityntäpisteen palvelujen, palvelun kohteena olevien substanssiprosessien tarpeiden mukaisesti) palvelutasot koostuvat soveltuvista laatumääreistä sekä näiden palveluun valituista tasoista. Laatumääreellä tarkoitetaan palvelun laatua koskevaa, vielä luokittelematonta tekijää ja sen yksikköä. Laatumäärettä käytetään laadun mittaamiseen. Esim. palveluaika (yksikkö = aikaväli tunteina ja minuutteina), käytettävyys (yksikkö = käytettävyysprosentti), toimitusaika (yksikkö = kesto). Palvelutasolla taas tarkoitetaan tietyn laatumääreen luokiteltua laadullista tasoa, joka on asiakkaan valittavissa kyseiseen palveluun. Esim. palveluajan palvelutasoluokkia voivat olla mm. ”arkisin klo 8-16” ja ”24/7 kaikkina vuoden päivinä”.

Seuraavaan on koottu kansallisessa palveluväylässä käytettävien laatumääreiden keskeiset määritelmät:

Laatumääre	**Kuvaus**
Palveluaika	Service Hours. Sovittu aikaväli, jolloin asiakkaalle tai palvelun kohteelle tuotetaan palvelukuvauksen mukaista palvelua. Esimerkiksi arkisin klo 8-16.
Käytettävyys	Availability. Käytettävyydellä tarkoitetaan kohteena olevan laitteen, palvelun päälläoloa ja kykyä tuottaa sitä palvelua, jota kohteelta edellytetään, sovitun toiminnon suoritus vaadittuna aikana. Käytettävyys lasketaan vähentämällä käyttökatkojen aika ideaalikäytettävyydestä palveluaikana. Tässä käytettävyys vastaa ITIL-termiä availability, jolla suosituksen laatimishetkellä on ITSMF-Finlandin termistössä kaksi rinnakkaista suomennosta: käytettävyys ja saatavuus. Käytettävyydellä ei tässä siis tarkoiteta helppokäyttöisyyttä (usability).
Maksimikatko	Pisin yksittäinen yhtämittainen palvelukatko, joka sallitaan palvelun palvelutasotavoitteiden puitteissa

	palveluaikana sovitulla tarkasteluvälillä. Esim. 2 tuntia yhden kalenterikuukauden aikana. Huom. tämä yksittäisen katkon enimmäispituus on määritelty tässä suosituksessa aina pienemmäksi kuin kaikkien palvelukatkojen kumulatiivinen kesto.
Reagointiaika	Response Time. Aika, jonka kuluessa tapahtuman tai häiriön havaitsemisesta tulee häiriön korjaaminen tai tapahtuman käsittely aloittaa. Reagointiaika riippuu yleensä häiriön kriittisyysluokasta. Häiriö voidaan havaita joko asiakkaan häiriöilmoituksesta (tapahtuma) tai toimittajan itsenäisen valvontahälytyksen tai muun havainnon (event management) pohjalta
Ratkaisuaika	Aika häiriön tai ongelman havaitsemisesta, jonka aikana toimittajan tulee saada poistettua häiriö tai ongelma tai muuten normalisoida palvelu.
Ratkaisukyky	Koskee keskitettyjen palvelujen asiantuntijoille tarkoitettu teknistä tukea: Ratkaisukyvyllä tarkoitetaan ylläpitäjätahon palvelupisteen (Service desk, help desk) tai muun asiakkaan palvelupyynnön vastaanottavan tahon kykyä ratkaista ko. palvelupyyntö siirtämättä / ohjaamatta palvelupyyntöä eteenpäin muille tukitasoille / palvelujonoille.
Tavoiteaika	Koskee keskitettyjen palvelujen asiantuntijoille tarkoitettu teknistä tukea: Tavoitettavuudella tarkoitetaan keskitettyjen palvelujen ylläpitäjätahon palvelupisteen (Service desk, help desk) kykyä vastata sovitussa ajassa sinne tuleviin palvelupyyntöihin. Tyypillisesti tavoitettavuus koskee puhelinpalvelua ja sähköistä yhteydenottovälinettä ja tavoiteaika määritetään keskimääräisenä tavoitettavuutena.

Keskitettyjen palvelujen laatumääreet ja palvelutasot

On hyvä huomata, että ns. päästä-päähän –palvelujen kokonaispalvelutaso riippuu kansallisen palveluväylän palvelutason lisäksi myös Tuottajan ja Hyödyntäjän sovellusten ja palvelujen palvelutasosta, tietoliikenneverkon palvelutasosta sekä loppukäyttäjän ICT-infrastruktuurin ja päätelaitteiden palvelutasosta[5].

Kansallisen palveluväylän keskitettyjen palvelujen palvelutasoon sovelletaan seuraavia laatumääreet:

[5] Palvelutasojen määräytymistä on kuvattu mm. JHS 174 suosituksessa.

- Palvelinten ja sovelluksen laatu
    - Käytettävyys, maksimikatkot, reagointiaika, ratkaisuaika, palveluaika,
- Asiantuntijatuen palvelutaso
    - Palveluaika, tavoitettavuus, ratkaisukyky

Näiden lisäksi paikallisiin liityntäpalvelimiin voidaan soveltaa seuraavia laatumääreitä soveltaen:

- Liityntäpalvelimen suorituskyky ja virhesuhde
    - Välitettyjen sanomien kulkuaika liityntäpalvelun läpi (mediaani ja maksimi)
    - Välitettyjen sanomien määrä (maksimimäärä, jolla suorituskyky voidaan saavuttaa)
    - Välitettyjen sanomien virheettömyys (sanomavirhesuhde)

Palveluväylä on hajautetun arkkitehtuurinsa myötä riippumaton keskuspalvelujen jatkuvasta saavutettavuudesta, joten palvelutasolle voidaan asettaa pienempiä vaatimuksia Keskitettyjen palvelujen palvelutasotavoitteisiin sovelletaan JHS-174 –määrityksissä kuvattua palvelinten käyttöpalveluiden palvelutasoluokitusta ja määrittää sen palvelutasotavoitteet seuraavasti:

Osakokonaisuus	Palvelutasotavoite, SLT
Palveluväylän keskitettyjen palvelujen konesalin tietoliikennepalvelut	Palvelutaso **III, Laajennettu** • Palveluaika: P3 arkisin 7-21; la, su 9-18 • Käytettävyys: K3=99,5% • Vasteaika: V2=Reagointiaika 2 h, ratkaisuaika 1 tp
Palvelinten käyttöpalvelut	Palvelutaso **C, Laajennettu** • Palveluaika: P3= arkisin 7-21, la,su 9-18 • Käytettävyys: K2=99% • Vasteaika: V2=Reagointiaika 2 h, ratkaisuaika 1 tp
Keskitettyjen palvelujen sovelluspalvelut	Palvelutaso **C, Laajennettu** • Palveluaika: P3= arkisin 7-21, la,su 9-18 • Käytettävyys: K2=99% • Vasteaika: V2=Reagointiaika 2 h,

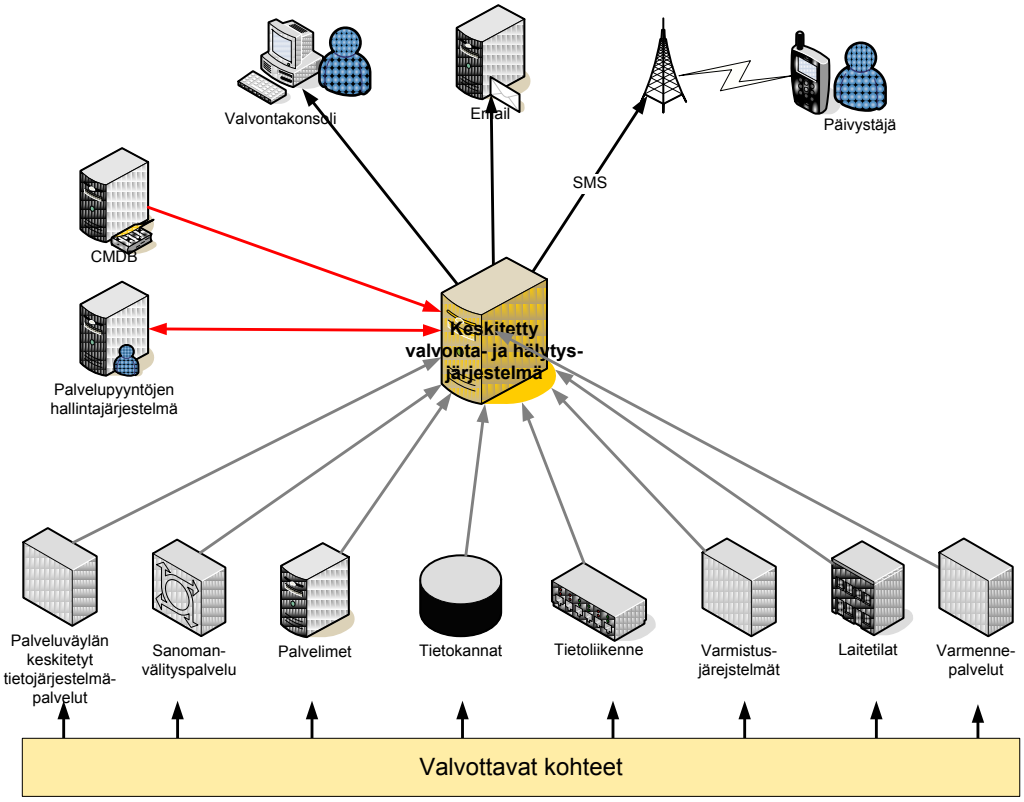
	ratkaisuaika 1 tp
Keskitettyjen palvelujen tukipalvelut	Palvelutaso **4, Laaja tuki** • Palveluaika: P3= arkisin 7-21, la,su 9-18 • Tavoitettavuus: T2=80% yhteydenotoista vastataan 1 min kuluessa • Ratkaisukyky: R2= 1. yhteydenottopiste ratkaisee 70% häiriöilmoituksista

Valvonnan teknologia-arkkitehtuuri

Valvontaratkaisu tulee pyrkiä keskittämään siten, että valvontatiedon avulla voidaan keskitetysti arvioida esim. häiriöiden laajuus ja hälyttää sovitut asiantuntijat apuun.

Tässä kuvattu valvonta-arkkitehtuuri koskee erityisesti kansallisen palveluväylän keskuspalvelinta, mutta sitä voidaan hyödyntää soveltaen myös paikallisten liityntäpalvelimien ja sovelluspalvelimien infrastruktuurin valvonnassa palvelun kriittisyys- ja palvelutasovaatimuksiin sovittaen.

Valvonta toteutetaan tavoitetilassa keskitetyllä ratkaisulla seuraavasti.



Pääperiaate valvonnassa on se, että keskitetty valvontajärjestelmä toimii häiri-

öiden ja hälytysten valvontamonitorina ja ottaa vastaan teknologia- ja kohdekohtaisten valvonta-agenttien tai valvontaratkaisujen tuottamat hälytykset, arvioi niiden vakavuuden ja kansallisen palveluväylän keskitettyjen palvelujen SLA-määritysten perusteella ja hälyttää oikean tahon selvittämään vikaa. Tarkempi selvitys ja säännöllinen trendiseuranta tehdään pääsääntöisesti teknologiakohtaisilla työkaluilla.

Valvottavat kohteet

Keskeisimmät valvottavat kohteet voidaan jakaa seuraaviin pääluokkiin:

- Laitetilojen-infrastruktuuri / taloautomaatio
- Palvelimet ja levy/varmistusjärjestelmät
- Tietoliikenne
- Infrastruktuuri-järjestelmät
- Sovellukset
- Tietoturva / palvelunestohyökkäykset / sähköiset murtautumisyritykset

Valvontakohteiden valvontarajat on kuvattu tarkemmin *Liitteessä 1, KA-taulukot*.

Laitetilat

Laitetiloista valvotaan sähkönsyöttöä, lämpötilaa sekä ilmankosteutta. Keskeiset laitetilat varustetaan varavoimalaittein sekä normaalista ilmanvaihdosta erotetuin jäähdytysjärjestelmin. Ilmankosteudesta valvotaan staattisen sähkön muodostumisen takia myös alarajaa.

Laitetilojen suunnittelussa hyödynnetään joko valtionhallinnon Vahti-ohjeita tai Viestintäviraston laitetilasuosituksia.

Tietoliikenne

Tietoliikenteen keskeiset valvottavat kohteet ovat käytettävyys, liikennöintivolyymi ja viive.

Kriittisistä verkon osista arvioidaan myös viiveen vaihtelua, pakettivirhesuhdetta sekä läpäisykykyä.

Mittaustavoissa sovelletaan JHS 174-suosituksessa kuvattuja mittausmenetelmiä.

Palvelimet

Oletusarvoisesti valvotaan palvelimien resursseja (muistinkäyttö, jonotusajat, levytilat, prosessorien käyttö) sekä palvelujen ja prosessien päällä oloa.

Tietokannat

Tietokannoissa valvotaan rajoitetusti mm. kantojen koon muutoksia, taulualueiden kokoja.

Sovellustason valvonta ja hallinta

Sovellusvalvonnassa hyödynnetään sovellusten omia valvontatyökaluja tai soveltuvin osin olemassa olevia teknologia-alustan hallinnan työkaluja.

Saatavuus, huolto- ja tukivaatimukset

Hankittavan teknologian varaosien ja huollon saatavuus pitää varmistaa koko ko. teknologian elinkaaren ajaksi. Tukipalvelut tulee saada suomen kielellä.

7. Liitteet

Liite 1, KA-taulukot

Liite 2, Lähtötilannearvio

Liite 3, Tekniset määritykset

Liite 4, Ratkaisumallin skenaarioarvio

Liite 1, KA-taulukot

Kokonaisarkkitehtuuritaulukot on koottu omaan excel-taulukkoon.

Liite 2, Tiedonvälitysratkaisujen nykytila

Kansallinen tiedonvälityksen lähtötilanne yleisesti

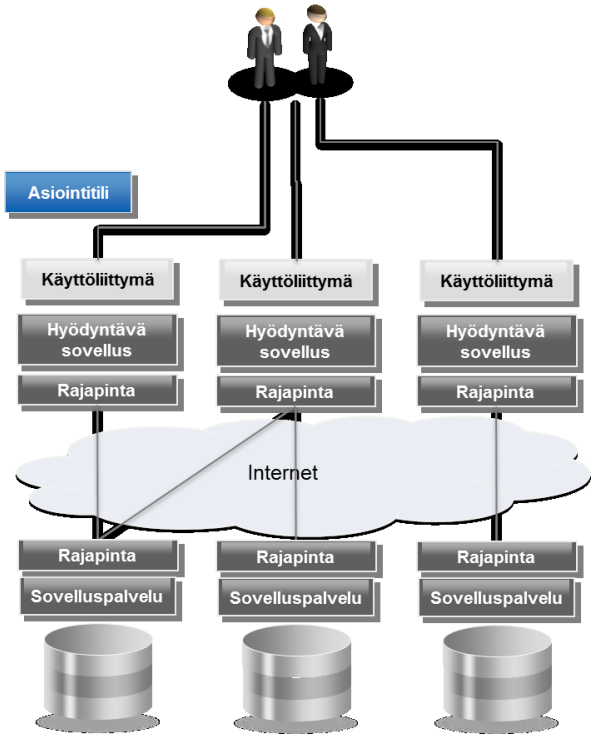
Suomessa organisaatioiden välinen tiedonvälitys on ollut ratkaisukeskeistä ja toimialasidonnaista. Ratkaisuilla on pääasiassa haettu pikaisia kustannussääs-töjä ja ne ovat perustuneet kulloinkin vallitseviin teknologiaratkaisuihin.

Suomessa on erillisiä ratkaisuja maksuliikennetietojen välitykselle organisaa-tioiden ja pankkien välillä. Laskutietoja välittävät pankkien lisäksi erikoistu-neet EDI-operaattorit. Yritysten verkkolaskuosoitteistoa ylläpitää Tieke ry omilla verkkosivuillaan.

Viranomaisten tietovarantoja on avattu yksitellen ja kunkin varannon hyödyn-tämisen rajapinta on kehitetty yksilöllisesti. Julkishallinnon perustietovarantо-jen rajapinnat (PERA) –työryhmä on määritellyt suositeltavat rajapinnat, mutta suositusten mukaisten rajapintojen kehittäminen ja käyttöönotto on kesken, koska rajapinnat uusitaan pääosin vasta kun tietojärjestelmät tulevat elinkaa-rensa päähän. Valtaosa viranomaisten välisistä tiedonsiirroista on eräsiirtoja, jolloin tietojen ajantasaisuus kärsii ja tiedoista syntyy useita kopioita.

Yritysten viranomaisraportointiin on Tyvi-palvelu, jolla on useita operaattorei-ta jotka toimivat yrityksille keskitettyinä raportointipisteinä. Kansalaiset asioi-vat jokaisen viranomaisen kanssa erikseen, pääasiassa viranomaisen tarjoamaa käyttöliittymää hyväksikäyttäen. Kunnat ja valtio rakentavat erillisiä asiointiti-lejä sähköistä asiointia keskittämään.

Kansalainen tunnistetaan yleisesti verkkopankkitunnuksin, virkamies virkakor-tilla tai Virtu:lla.



Voidaankin perustellusti todeta, että sinänsä toimiva kansallinen tiedonvälitys on hajautunut. Yhteisten komponenttien puuttuessa uusien sähköisten palveluiden ja prosessien luominen on monimutkaista ja työlästä, koska se edellyttää useiden erilaisten teknologioiden yhdistämistä.

Tarkastellut lähtötilanteen ratkaisut

Kansallisen palveluväylän tavoitteena on mahdollistaa entistä paremmin asiakaspalveluiden ja palveluprosessien kehittäminen palveluissa tarvittavan tiedonvaihdon mahdollistavan ratkaisukokonaisuuden avulla.

Nykyinen hajautettuihin asiakastietoihin, operatiivisiin järjestelmiin ja tietovarantoihin sekä erillisiin, sinänsä toimiviin integraatioratkaisuihin perustuva palvelujärjestelmä on rakennettu organisaatiokohtaisiin siiloihin, joka on johtanut rakenteeseen, jossa uusien organisaatiorajojen ylittävien palveluprosessien kehittäminen on vaikeaa.

Nykytilasta valittiin tarkasteltaviksi otanta julkishallinnon perustietovarannoista (Kaupparekisteri, YTJ, VTJ sekä KTJ Kiinteistörekisteri), olemassa olevia (julkisen hallinnon) integraatioratkaisuja ja palveluväyliä (VIA, Alli, KANTA, OPH ja Helsingin kaupunki) sekä julkishallinnon käyttämiä palveluväyliä (Belgia, Ruotsi ja Viro). Lisäksi tutkittiin, voitaisiinko Julkishallinnon perustietovarantojen rajapinnat (PERA) –työryhmän tuloksia hyödyntää hankkeessa, ja millä reunaehdoilla.

Tarkasteltujen perustietovarantojen rajapinnat ovat teknologioiltaan hyvin lähellä PERA-vaatimuksia ja ne ovat kohtuullisen pienellä työllä muutettavissa PERA-yhteensopiviksi. Lisäksi KTJ Kiinteistörekisterin uusi rajapinta on jo valmiiksi PERA-linjauksien mukainen. Jokaisella tutkitulla perustietovarannolla on mahdollisuus palvella nykyistä suurempiakin kyselymääriä.

Julkishallinnon integraatioratkaisut ovat rajoitetulle käyttäjäkunnalle tarkoitettuja, joskin KANTA-palveluihin on määritelty hyödyntäjän rajapinta myös internetin kautta (pienet apteekit). Osa ratkaisuista pohjasi kaupalliseen tuotteeseen, OPH:n ratkaisu on rakennettu avoimen lähdekoodin tuotteilla. Helsingin kaupungilla on palveluväylän käyttöönotto vasta aluillaan, joten heidän kokemuksensa väylän käyttöönoton vaiheistuksesta olivat hyödyllisiä.

Tarkasteltuja julkishallinnon palveluväyliä oli toteutettu kahdella erilaisella tavalla: Belgiassa väylä oli keskitetty, kaupalliseen tuotteeseen perustuva ESB-ratkaisu. Ruotsissa ja Virossa väylä laajeni siihen liittyvän organisaation sisäverkkoon asti; väylään liityttiin erityisen turvareitittimen avulla joiden keskinäinen, internetin yli suojatuilla yhteyksillä kommunikoiva verkko muodosti väylän.

Belgian Federal Service Bus (FSB)[6] on tarkoitettu viranomaisten tietovarantojen hyödyntämiseksi, joten käyttö rajoittuu julkishallinnon rekisterien käyttöön. Vain julkishallinnon viranomaiset tai näiden puolesta toimivat yritykset voivat tarjota palveluja väylässä. Kuukausittain väylässä on kulkenut n. 1,2milj viestiä (maksimi vuodelta 2011, kesäkuu), eli n. 400.000 päivässä (tä-

[6] http://www.fedict.belgium.be

mä pitää sisällään tunnistamiseen käytetyt viestit, joita on n. puolet). Palvelua hallinnoi The Belgian Federal ICT Service (FEDICT). Operoinnissa on 72 henkilön organisaatio n. 10M€ vuosikustannuksilla (2011). Kehittämisprojekteihin käytetyt kustannukset olivat vajaat 15M€ vuonna 2011.

Ruotsin Spridnings- och Hämtningssystem SHS (englanniksi Government eLink (GeL)) kehitystyö alkoi 1997 ja käyttöönotto 2001. Se tarjoaa infrastruktuurin julkisten toimijoiden väliseen tiedonvälitykseen, myös yritykset voivat hyödyntää väylää. Väylää käyttää n. 130 (pääasiassa valtionhallinnon) organisaatiota, palveluita on n. 500 ja päivittäisiä sanomia 1,3 miljoonaa (2011). Väylän määrittelyjä koordinoi Försäkringskassan ja väylään liittymisen voi ostaa palveluna kahdelta yksityiseltä toimijalta. Toimintoja operoivat kaupalliset toimijat jotka perivät kulut asiakkailta.

Viron X-Roadin ensimmäinen versio otettiin käyttöön 2001. Se on SHS:n tavoin julkisen internet-verkon päälle rakennettu tietoliikenteellisesti hajautettu ja hallinnallisesti keskitetty palveluverkko, jossa kahden verkkoon liittyneen organisaation välillä kuljetetaan allekirjoitettuja standardimuotoisia sanomia suojatuin ja molemmin puolin tunnistetuin suorin yhteyksin. Väylään saa liittyä niin julkisia kuin yksityisiäkin organisaatioita, kunhan sitoutuvat väylän sääntöihin. Palveluväylän palvelujen hyödyntäminen vaatii kahdenväliset sopimukset hyödyntäjän ja tietopalvelun välillä. X-Road on toteutettu avoimen lähdekoodin tuotteilla. Vuonna 2011 väylässä kulki n. 240 miljoonaa viestiä, eli n. 650.000 viestiä päivässä. Väylää hyödyntää n. 800 organisaatiota, joista tiedon tarjoajia on n. 150. Väylän toiminnallisuudesta vastaa 5 hengen organisaatio, jonka vuosittainen kustannus on n. 1M€,

Sanoma- ja rajapintasisältöjen tarkastelu

Rajapintojen ja tietosisällön osalta tarkastelu on kohdistunut perustietovarantojen (PERA) rajapintamäärityksiin sekä hajautetun verkoston integraatioratkaisujen sanomasisältöihin (erityisesti Ruotsin SHS ja Viron X-Road). Tarkempi analyysi on tehty X-Roadista, mutta sanomarakenne on vastaavanlainen myös muissa ratkaisuissa. Kansallisten perustietovarantojen rajapintamääritykset eivät ole yhteensopivia esimerkiksi X-Roadin rajapintakuvausten kanssa ilman sovituskerroksia.

Tarkastelu kohdistuu sekä sanomaliikenteen välitystapaan, että sanomien tietosisältöihin. Välitystapoja on kaksi perustyyppiä, SOAP ja REST, joita myös vertaillaan keskenään alempana.

X-Road

SOAP-mallissa siirretään XML-muotoista rakenteista tietoa HTTP-protokollan välityksellä. X-Road pohjautuu SOAP:iin ja XML-sanomien sisällöt on määritelty X-Road –dokumentaatiossa. Jos X-Road –arkkitehtuuriin halutaan liittää palvelu, joka ei tue suoraan SOAP:ia ja/tai määriteltyjä sanomia, se tulee liittää adapterikomponentin välityksellä. Adapterin tehtävä on muuntaa sanomat X-Road –määritysten mukaisiksi.

X-Roadin pyynnöt ja vasteet ovat muotoa:

Pyyntö

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
            <SOAP-ENV:Header>
                        Header components
            </SOAP-ENV:Header>
            <SOAP-ENV:Body>
                        <m:service xmlns:m=”URI”>
                        <request>
                        Request components
                        </request>
                        </m:service>
            </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Vaste

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
            <SOAP-ENV:Header>
                        Header components
            </SOAP-ENV:Header>
            <SOAP-ENV:Body>
                        <m:serviceResponse xmlns:m=”URI”>
                        <request>
                        Request components
                        </request>
                        <response>
                        Response components
                        </response>
                        </m:serviceResponse>
            </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Pääosa viestien tunnistekenttiä ja muuta teknistä tietoa ovat otsikkokentissä (<SOAP-ENV:Header/>). Alla on kuvattuna X-Roadin otsikkokentät selityksineen. Siinä sanomissa kentät ovat muotoa **<xrd: otsikko/>**.

Pakolliset:

consumer	string Name of the service requester institution
producer	string Name of the service provider
service	string Name of the service to be invoked
userId	string ID code of the person invoking the service This code could be in one of the two forms: CCX or CC:R:X where · CC - two-letter country code in capital letters, e.g. EE for Estonia · R - ID of the registry · X - registry value or code The first form is used in countries where exists unique and universal person identification code. For example: EE12345678901 or UK:XYZ:123456789
id	string Unique identifier
issue	string Name of file or document related to the service invocation

Valinnaiset:

unit	string Registration code of the institution or its unit on whose behalf the service is used
position	string Organizational position or role of the person invoking the service
userName	string Name of the person invoking the service
async	boolean Specifies asynchronous service. If the value is "true", then the security server performs the service call asynchronously.

authenticator string Authentication method, one of the following: · ID-CARD – use a certificate of identity · CERT – use another certificate · EXTERNAL – authenticate through a third-party service · PASSWORD – authenticate with a password Details of the authenticator (e.g. the identification of a bank for external authentication) can be given in brackets after the authentication method.

paid string The amount of money (in the smallest monetary unit, e.g cents) paid for invoking the service

currency string three-letter currency code in capital letters

Sekä X-Road että PERA jakavat virheet ns. protokollavirheisiin ja sovellusvirheisiin. Protokollavirheet ovat tiedonsiirron teknisiä virheitä, eli normaaleita HTTP-virhekoodeja. Sovellusvirheiden tarkoitus on antaa kutsuvalle järjestelmälle tarkempaa tietoa siitä, miksi pyyntöön ei voitu toimittaa vastausta.

X-roadin virhesanomat ovat joko muotoa:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
            <SOAP-ENV:Header>
                  components of header
            </SOAP-ENV:Header>
                  <SOAP-ENV:Body>
                        <SOAP-ENV:Fault>
                        <faultCode>fault code</faultCode>
                        <faultActor>fault actor</faultActor>
                        <faultString>fault string</faultString>
                        <detail>fault details</detail>
                        </SOAP-ENV:Fault>
                  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

tai:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
            <SOAP-ENV:Header>
                  contents of header
            </SOAP-ENV:Header>
                        <SOAP-ENV:Body>
                  <m:serviceResponse xmlns:m="URI">
                        <request>
                              contents of the request component
                        </request>
                        <response>
                              <faultCode>fault code</faultCode>
                              <faultString>fault string</faultString>
                        </response>
                  </serviceResponse>
            </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Sanomissa olevan `<faultCode/>` –kentän mahdolliset arvot ja niitä vastaavat tekstikuvaukset on määritelty tarkemmin X-Road-dokumentaatiossa.

PERA

PERA-määritykset on tehty käytettäväksi joko SOAP-mallin mukaisesti X-Roadin tavoin, tai vaihtoehtoisesti REST-mallin mukaisesti. Alla on kuvattu REST-mallin mukainen toteutus.

REST:ssä otsikkotiedot voidaan liittää suoraan kutsuvaan HTTP-viestiin sen sijaan, että ne välitettäisiin aina XML-muodossa, kuten SOAP:ssa. Jos tarvitaan tarkempaa sanomasisältöä, se voidaan välittää esimerkiksi XML-muodossa, mutta ei ole siihen rajattu. Erityisesti JSON-formaatti on paljon käytetty XML:n sijaan.

Esimerkki kutsusanomasta:

```
https://tuotanto.esimerkki.fi/palveluX/v2/metodi
```

Vasteessa palautetaan pyydetty sisältö esimerkiksi XML- tai JSON-muodossa.

PERA:n otsikkokentät jakautuvat kahteen kategoriaan, Kutsuketjuun ja Palvelukutsuun. Nämä on kuvattu seuraavassa. Pakolliset kentät on merkitty *-merkillä.

*Kuljetuskehys
*Kutsuketju
    *KutsuketjuTunnus (UUID/GUID string)
    AlkamisAika (time)
    *Aloittaja
        *PalveluTunnus
        JärjestelmäTunnus
        *OrganisaatioTunnus
        AliorganisaatioTunnus
        *KäyttäjäTunnus (string)
*Palvelukutsu
    *KuljetuskehysVersio
    *PalvelukutsuTunnus
    *AlkamisAika
    *Lahettaja
        PalveluTunnus
        JärjestelmäTunnus
        *OrganisaatioTunnus
        AliorganisaatioTunnus
        KäyttäjäTunnus
        SalasanaTeksti
    *Vastaanottaja
        JärjestelmäTunnus
        OrganisaatioTunnus
        AliorganisaatioTunnus
Uudelleenlähetys

PERAn REST-mallissa virheet palautetaan HTTP-viesteinä POST-metodia käyttäen muodossa:

```
POST HTTP://<URL root>/<aineiston tyyppi>/<aineiston tunnus>/virhe
```

jossa virhe on muotoa

```
<virhe>
    <virhekoodi>404.1</virhekoodi>
    <selite>
        Aineistoa ei löydy määritetystä URI-osoitteesta.
        Aineistolle ilmoituksessa välitetty URI on:
        SFTP://esimerkki.fi/perusaineisto/org2/2011-11
    </selite>
</virhe>
```

PERAn virhekoodit, kuten yllä oleva 404.1, pohjautuvat HTTP-virhekoodeihin niitä tarkentaen.

Vertailu

Sanomien välitystavalle on kaksi vaihtoehtoa, SOAP ja REST. Näistä kahdesta REST on modernimpi, joustavampi ja kevyempi. SOAP:ssa kaikki tietosisältö on XML-rakenteessa joko viestin header- tai body-osassa, joten viestit täytyy aina avata ja lukea, jotta viestin tarkoitus saadaan selville. Tämä lisää tiedonkäsittelykuormaa ja saattaa tuottaa ongelmia erilaisissa kauttakulkupalvelimissa, kuten edustajat (proxy) ja NAT-muunnokset. REST käyttää HTTP:n normaaleja metodeita (POST, PUT, GET, DELETE) ja esittää sanoman reitittämiseen liittyvät tiedot HTTP-otsakkeissa.

Sanomasisällöt poikkeavat toisistaan siinä määrin, että suora vastaavuus ei ole toteutettavissa. Poimintoja sanomien erilaisuuksista ovat mm.:

- X-Roadissa on maksamiseen liittyviä kenttiä, joita PERA:ssa ei ole. Koska palveluväylän on tarkoitus olla kansallinen eli myös muun kuin julkisen hallinnon käyttöön, nämä ovat hyödyllisiä sisältöjä.
- X-Roadissa ei ole aikaleima-kenttää, joten palveluviestin ajankohdat eivät ole niin helposti selvitettävissä.
- PERAssa on useita organisaatioon liittyviä osittain pakollisia kenttiä, jotka eivät hyvin sovellu ei-julkishallinnon käyttöön.

Tietoturvallisuuden osalta kummassakin tapauksessa voidaan käyttää siirtoprotokollana HTTPS:ää, eli TLS-suojattua yhteyttä.

Yllä olevan perusteella todetaan, että REST on näistä kahdesta suositeltavampi sanomanvälitysmalli. Muunnos SOAP- ja REST-sanomien välillä on varsin suoraviivainen, jos sanomasisällöt ovat vastaavat. Mahdollinen SOAP-REST -muunnos tulisi tehdä mahdollisimman lähellä tietoa tuottavaa palvelua.

Sanomasisältöjen suhteen kummassakin vertailtavassa mallissa oli puutteita, joten päädyttiin tekemään niistä hieman kehitetty malli, joka on kuvattuna muualla tässä dokumentaatiossa. Tämä aiheuttaa muutostarpeita niihin toteutuksiin, jotka ovat nykyisten PERA-määritysten mukaisesti. Muutokset ovat kuitenkin melko pieniä, eikä niiden pitäisi aiheuttaa merkittäviä kustannuksia.

Lainsäädäntötarkastelu

Palveluväylää ja sen hyödyntämistä ohjaa joukko lakeja, joista keskeisimmät on listattu tarkemmin *Liitteessä 1, KA taulukot*. Nämä voidaan ryhmitellä seuraavasti:

- Tiedonhallintaa koskeva yleislainsäädäntö
- Sähköisiä palveluja koskeva yleislainsäädäntö
- Sektorikohtaisia tietojärjestelmäratkaisuja ohjaavat lait

Palveluväylän rakentamisen ja toimintamallin suunnittelussa tulee lisäksi ottaa huomioon mm. hankinta- ja kilpailulainsäädäntö.

Palveluväylä on tiedonvälitysratkaisu, joka korvaa nykyisiä ratkaisuja. Tähän tiedonvälitystoimintaan ei liity palveluväylästä johtuvia erityisvaatimuksia. On kuitenkin huomattava, että tietyssä erityislainsäädännössä otetaan melko tar-

kasti kantaa kyseisten substanssitietojen lokitietojen käsittelyyn. Tyypillisesti integraatioratkaisut taltioivat sanomanvälityksen lokitietoja, joten tämä tulee ottaa huomioon kansallisen palveluväylän suunnittelussa. Esimerkiksi Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159 kuvataan: ” Kansaneläkelaitos ei saa antaa valtakunnallisten tietojärjestelmäpalvelujen järjestämiseen liittyvien potilasrekistereiden tai niihin liittyvien lokirekistereiden käsittelyä tai säilyttämistä toimeksiantotehtävänä ulkopuolisille.” Kyseisen lainsäädännön reunaehto tulee ottaa huomioon loogista arkkitehtuuria kehitettäessä.

Suunnittelussa tulee ottaa huomioon mm. tietoturvallisuusasetus (681/2010), jonka perusteella on määriteltävä, minkä suojaustasojen tietoa palveluväylän kautta voidaan välittää. Vähimmäistarve lienee tasot IV ja III.

Palveluväylän ydinkomponenttien (nimipalvelut, varmentaja, tapahtumaloki ja palveluhakemisto) osalta on otettava huomioon sähköistä viestintää koskeva lainsäädäntö ja viranomaismääräykset.

Kukin palveluväylään liitetty järjestelmä hallitsee omia tietojaan sekä vastaa siitä, että muiden tarvitsemat tiedot ovat saatavissa välitysalustan kautta ottaen huomioon tietojen käyttöön liittyvät mahdolliset rajoitukset. Palvelujen kannalta palveluväylään liittyminen ei aiheuta tarvetta muuttaa niitä koskevia säädöksiä. Palveluväylän ja yhteisten rajapintamääritysten käyttö voi tuoda esille tarpeita yhtenäistää myöhemmin eri tietovarantoja ja palveluja koskevaa lainsäädäntöä.

Palveluväylän yhteyteen kehitettävillä yhteisillä teknisillä tukipalveluilla, kuten valtuutuspalvelut ja suostumusten hallintapalvelut, voidaan myöhemmin helpottaa sektorikohtaisissa tietojärjestelmiä koskevissa laeissa olevien monimutkaisten vaatimusten toteuttamista.

Palveluväylän käyttö voidaan tehdä julkisella sektorilla pakolliseksi määrittelemällä se julkisen hallinnon tietohallinnon ohjauksesta annetun lain 634/2011 11§:n mukaiseksi yhteiseksi palveluksi, jonka käytöstä voidaan määrätä valtioneuvoston asetuksella.

Palveluväylä on avoin sekä julkisen että yksityisen sektorin palveluille. Liitettäville palveluille ja niiden tuottamiselle on asetettava tietoturvallisuutta koskevat perusvaatimukset, jotka ovat palveluista riippuvia, eikä palveluväylä saa niitä huonontaa. Tietoturvallisuuden arvioinnin kriteeristönä voi käyttää esim. VAHTI-ohjeita. Vaadittava tietoturvallisuustaso on suhteutettava palvelun luonteeseen ja eri palvelutyypeillä (yhteiset tukipalvelut, tietovarantopalvelut, yhteisöpalvelut ja kansalaispalvelut) voi olla eri vaatimustasoja. Yksityisten palvelujen suhteen palveluväylän tulisi olla avoin kilpailulle eli kaikkien palvelutarjoajien tulisi voida liittyä väylään samoilla ehdoilla.

Palveluväylän teknisen perusratkaisun osalta on käytettävissä kaupallisia ja avoimen koodin ohjelmistoihin perustuvia ratkaisuja. Kaupallisen ratkaisun hankinta edellyttää normaalia hankintamenettelyä. Avoimen koodin ratkaisujen osalta palveluväylästä vastaava julkinen taho voi asentaa ne tietotekniseen ympäristöönsä. Hankintayksikkö ei maksa ohjelmistoista mitään. Tässä tapauksessa kyse ei oikeustapausten mukaan ole julkisesta hankinnasta. Avointen ohjelmistojen valinnan ja asennuksen jälkeen palveluväylästä vastaava taho

hankkisi normaaleilla hankintamenettelyillä tarvitsemansa kehittämis-, tuki- ja tuotantopalvelut.

Palveluissa tarvittavan liityntäpalvelinohjelmiston toteuttamistavaksi kannattaa harkita avoimen lähdekoodin ohjelmistoa. Avoimen lähdekoodin mukaisen ratkaisun käyttöönotto palveluväylään kytkeytyvissä organisaatioissa olisi tällöin lisensioinnin ja hankinnan näkökulmasta varsin mutkatonta.

Yhteenveto lähtötilanteesta

Tarkasteltujen perustietovarantojen rajapinnat ovat teknologioiltaan hyvin lähellä niin PERA- kuin X-Road määrityksiä ja ne ovat kohtuullisen pienellä työllä muutettavissa PERA- tai X-Road tyhteensopiviksi - tai ehdotetun palveluväyläarkkitehtuurin mukaisiksi - joko suoraan tai erillisen sovittimen avulla. Jokaisella tarkastellulla perustietovarannolla on mahdollisuus palvella nykyistä suurempia kyselymääriä.

Väyläratkaisut ovat pääasiassa toimialaspesifejä ja niissä oli omia tietoturvarajauksia.

Tarkastellut kansalliset palveluväylät ovat pääasiassa tarkoitettu julkishallinnon käyttöön, joskin Virossa väylässä on paljon yksityisiä toimijoita. Palvelutuotannon järjestäminen on tehty kovin erilaisilla tavoilla (Belgiassa julkishallinnon organisaatio työllistää 72 henkilöä, Virossa 5 ja Ruotsissa toiminnasta vastaavat yksityiset toimijat).

Kansallisen palveluväylän liiketoimintamalli on saatava sellaiseksi, että se ei estä siihen liittymistä. VIA:n liiketoimintamalli on osoittanut miten merkityksellinen osa menestystä se on.

Nykyinen lainsäädäntö mahdollistaa palveluväylän välittömän käyttöönoton. Nykyinen lainsäädäntö antaa myös mahdollisuuden pakottaa julkisen sektorin toimijat väylän käyttäjiksi valtioneuvoston asetuksella.

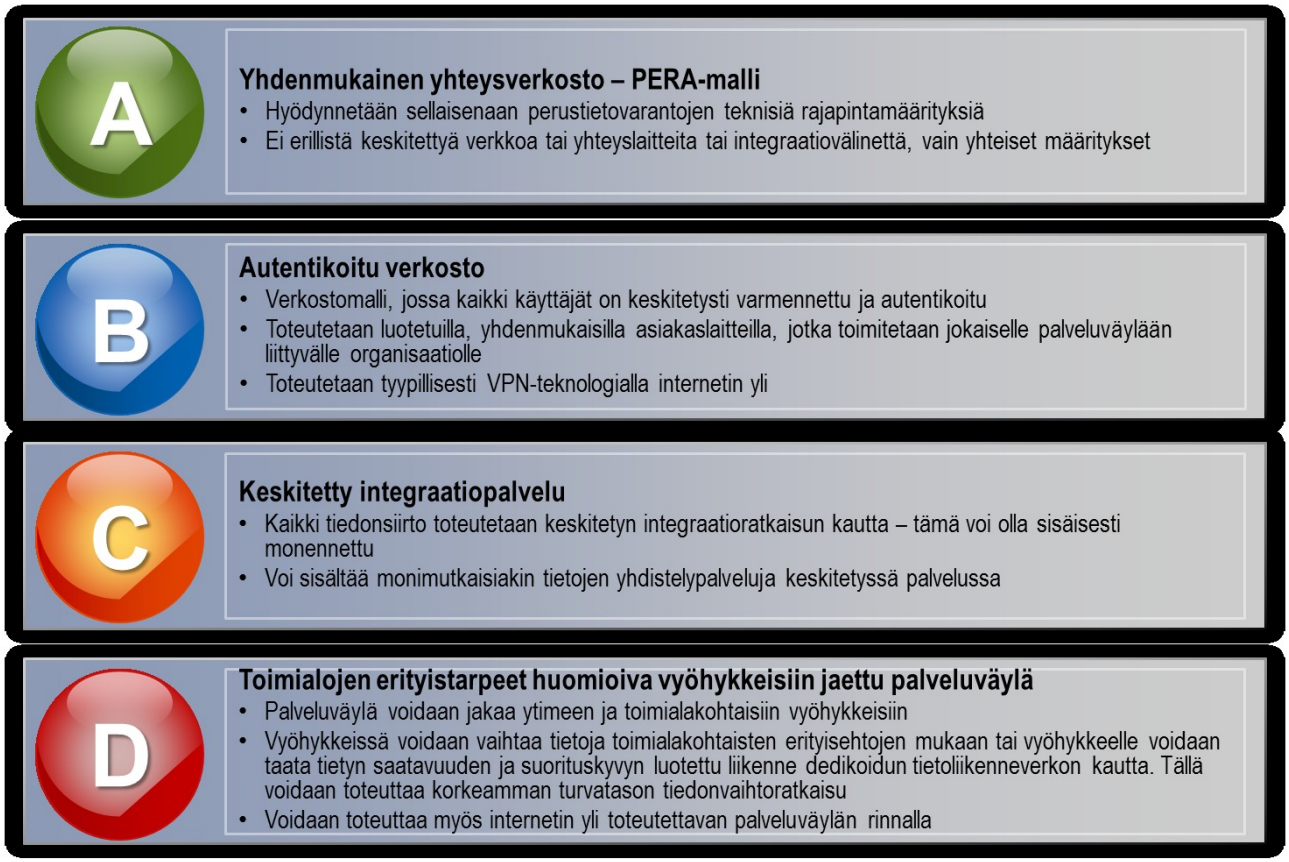
Tarkasteltuja kohteita on kuvattu tarkemmin *Liitteessä 2.2, Lähtötilanteen integraatioratkaisujen arviot*.

Liite 3, Ratkaisumallin skenaarioarvio

Kansallisen palveluväylän looginen perusrakenne voidaan määrittää useilla eri tavoilla. Nykytilatarkastelusta voidaan jo havaita, että eri maissa ja eri tarkoituksiin on määritelty ja toteutettu eri ratkaisumalleja.

Kansallisen palveluväylän päärakenteen määrittämiseen on käytetty skenaariotarkastelua, jossa on tarkasteltu usean eri mallin toimivuutta edellä kuvattujen tavoitteiden, rajausten ja reunaehtojen ja tavoitteiden pohjalta.

Tarkastelussa keskityttiin neljään pääskenaarioon, joita tarkasteltiin erikseen ja erilaisina yhdistelminä. Viitearkkitehtuuria laatinut työryhmä tunnisti seuraavat kansallisen palveluväylän loogiset pääratkaisumallit (skenaariot) periaate- ja käsitetason viitearkkitehtuurin pohjalta:



Näistä skenaario A kuvaa lähinnä nykymallia, jossa rajapinnat yhtenäistetään perustietovarantoihin laaditun rajapintamääritysten pohjalta. Skenaario B kuvaa hajautettua palveluväylää (vrt. Viron ja Ruotsin malli), skenaario C kuvaa keskitettyä palveluväylää (vrt. VIA ja Belgian ratkaisu) ja skenaariossa D kiinnitetään huomiota vielä eri toimialojen erityistarpeisiin (esim. SLA- tai varautumisvaatimukset) ja olemassa oleviin ratkaisuihin (esim. Sote-sektorin tiedon välityksen vaatimukset ja ratkaisut).

Projektiryhmä laati yleisen tietojärjestelmäpalvelukartan ja edellä kuvattujen periaate- ja käsitetason kuvausten pohjalta skenaarioanalyysin, joka perustuu erilaisiin ratkaisumallien skenaarioihin.

Skenaariot arvioitiin seuraavien arviointinäkökulmien pohjalta:

- Hyödyt palveluväylään liittyvien toimijoiden kannalta
- Nopeus kytkeä palveluita palveluväylään ja tätä kautta tuottaa loppukäyttäjien lisäarvopalveluita
- Kustannustehokkuus – sekä kehittäminen ja jatkuva ylläpito
- Olemassa olevien ratkaisujen hyödyntäminen
- Yhteentoimivuus kaikkien toimialojen ja erityisvaatimusten näkökulmasta
- Uudelleenkäytettävyys
- Hallittavuus ja muunneltavuus
- Skaalautuvuus ja suorituskyky
- Turvallisuus
- Kehittämisaikataulu
- Riskit
- Muut reunaehdot

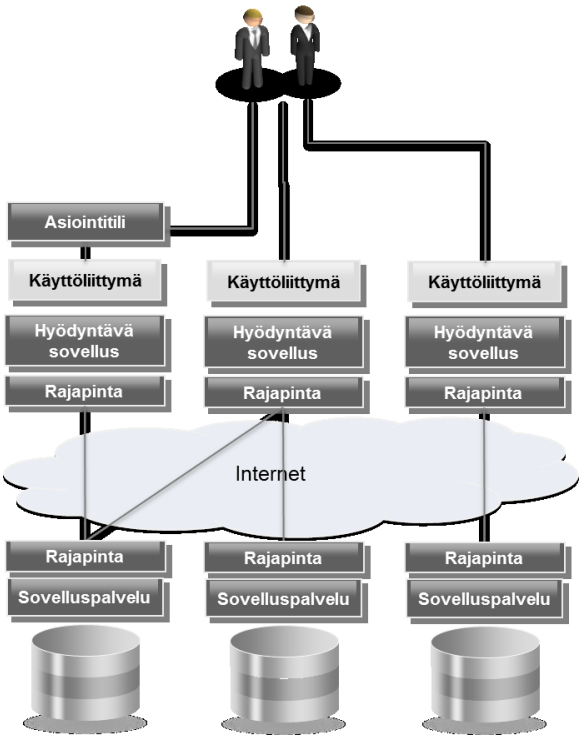
Seuraavaan on koottu arviot edellä tunnistetuista pääskenaarioista.

Skenaariot arvioitiin ns. SWOT-mallilla kuvaamalla ko. skenaariosta, sen:

- S = Strength, vahvuudet
- W = Weakness, heikkoudet
- O = Opportunity, mahdollisuudet
- T = Threats, uhkat

0: Lähtötilanne (ns. 0-skenaario)

Lähtötilanteessa ei ole olemassa kansallista, yhtenäistä kaikille toimialoille ja sekä julkiseen hallintoon että yksityiselle sektorille tarkoitettua tietojen vaihdon infrastruktuuria.

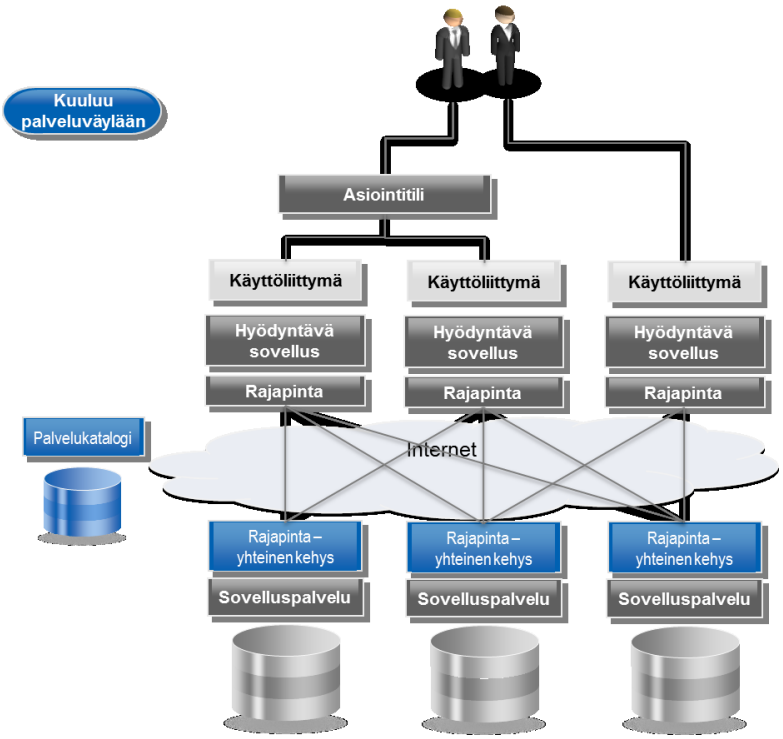


Kukin toimija sopii erikseen tietolähdekohtaisilla käyttöehdoilla kytkeytymisestä kyseiseen tietolähteeseen. Rajapinnat on määritetty tapauskohtaisesti eikä niitä ole yhtenäistetty. Liityttäessä johonkin toiseen palveluun tai tietolähteeseen, määritetään taas tapauskohtaisesti uusi rajapinta ja tarvittaessa kytkeydytään jopa erilliseen tietoliikenneverkkoon, jotta tietolähteeseen päästään kytkeydyttyä.

Kansallisten palvelujen hyödyntäminen on vaivalloista ja hidasta sekä epäjohdonmukaista. Joillakin toimialoilla on erillisiä, kyseisen toimialan erityispiirteisiin sovitettuja tiedonvaihtoratkaisuja, mutta toimialojen välinen tiedonsiirto ja palvelujen hyödyntäminen on tapauskohtaista ja usein hankalaa.

A: Yhdenmukainen yhteysverkosto – ns. PERA-malli

Yhdenmukaisella yhteysverkostolla tarkoitetaan nykymallin laajennusta, jossa eri tietolähteiden rajapintamääritykset yhtenäistetään.

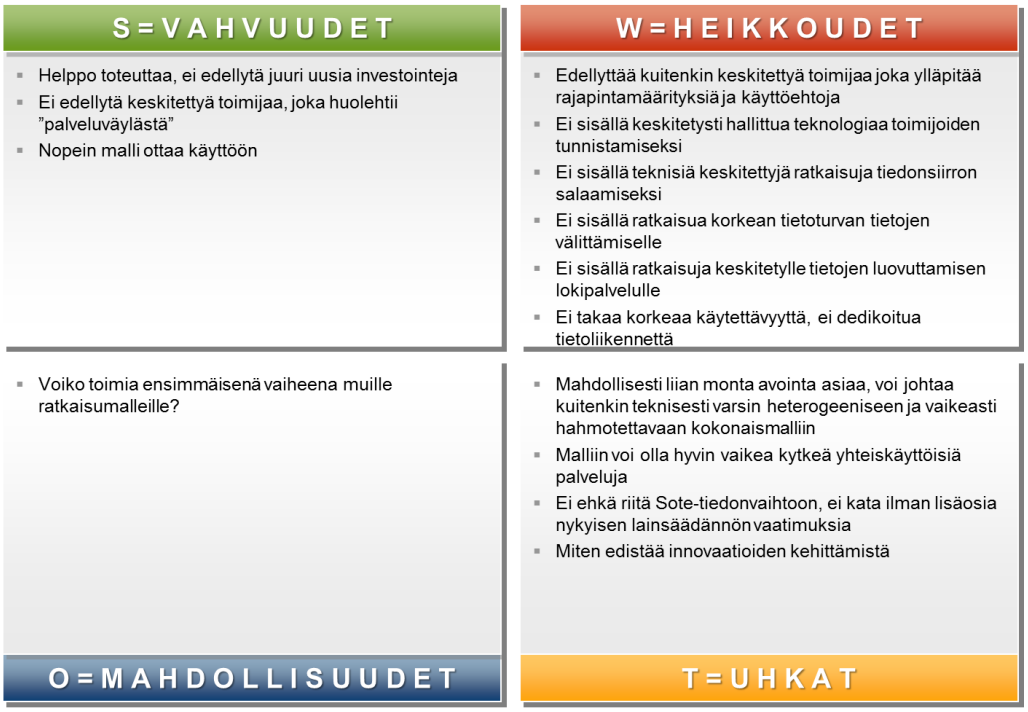


Luotettu yhteistyöverkosto on lähellä nykytilaa eikä sen käyttöönotto edellytä erillistä palveluväyläoperaattoria tai keskitettyä omistajaa. Ratkaisussa jokainen löyhään väylään liittyvä organisaatio toteuttaa yhteisen rajapintamäärityksen (esim. perustietovarantojen PERA-rajapintamääritysten pohjalta). Tämä mahdollistaa mm. viestien reitityksen väylään liittyneiden organisaatioiden kesken. Ratkaisussa ei ole lainkaan keskitettyjä komponentteja, ja organisaatioiden väliset yhteydet on muodostettava ja hallinnoitava kahdenvälisinä.

Mallissa ei oteta kantaa miten yhteydet muodostetaan, se on toimijoiden välinen asia, joskin luottamuksellinen viestintä edellyttää salattuja yhteyksiä tai sanomia. Oletettavasti viestintään käytettäisiin suojattuja yhteyksiä internetin yli tai toimijoiden ollessa jo samassa tietoliikenneverkossa kyseistä verkkoa.

Skenaarion SWOT-analyysi

Tämän skenaarion SWOT-arvio on seuraava:

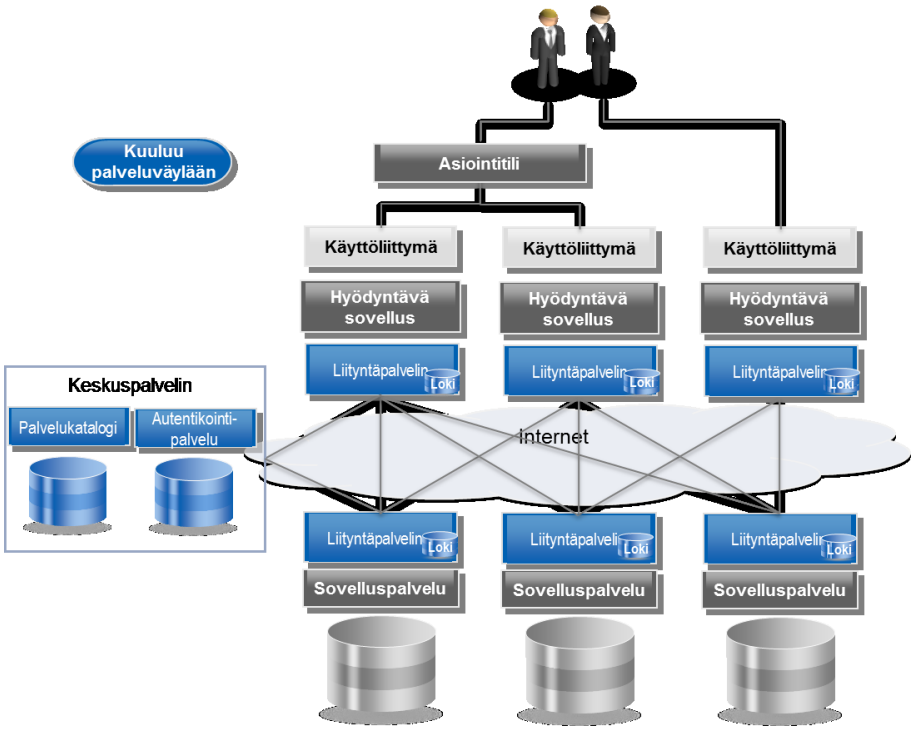


Skenaarioarvion yhteenveto:

Tämä skenaario on helppo toteuttaa eikä edellytä merkittäviä lisäinvestointeja eikä monimutkaista organisaatiota. Malli on kuitenkin hyvin samankaltainen kuin epäoptimaaliseksi todettu lähtötilanne. Ratkaisumalli ei tuo riittävästi uusia toimintoja ja malleja yhdenmukaiseen tietojen yhdistämiseen eikä madalla tarpeeksi kynnystä kytkeä eri palveluita kansalliseen ekosysteemiin. Malli ei riittävästi kiihdytä loppukäyttäjäpalvelujen tuottamista eikä ratkaise palvelujen kiistämättömyyttä ja kansalaisen tietojen jäljitettävyyttä yhtenäisellä tavalla.

B: Autentikoitu verkosto

Autentikoitu verkosto perustuu hajautettuun tietojenvaihtoinfrastruktuuriin, jossa tiedonvaihdon palvelimet on yhtenäistetty, mutta sijoitettu hajautetusti palveluväylään kytkeytyneisiin organisaatioihin.



Autentikoidussa verkostossa on keskitetty toimija, joka huolehtii väylään liittyvien organisaatioiden tunnistamisesta ja varmentamisesta ja määrittää palveluväylän käytön yleiset käyttöehdot. Viestinnän yhdenmukaistamiseksi ja yhteisten palvelujen käytön helpottamiseksi yhteydet toteutetaan yhdenmukaisilla organisaatioittain käyttöönotettavilla liityntäpalvelimilla, jotka edellyttävät liittyvän organisaation palveluilta määrittelyjen mukaista kommunikaatiota (määritys voi olla käytännössä vastaavanlainen kuin luotetun yhteysverkon rajapinnan määritys). Liityntäpalvelimet piilottavat palveluväyläorganisaatioilta väylän arkkitehtuurin, joka käytännössä rakentuu liityntäpalvelimien välisistä salatuista yhteyksistä internetin yli. Liityntäpalvelimet huolehtivat keskitettyjen palveluiden (kuten palveluhakemisto, autentikointipalvelin) hyödyntämisestä, sanomien reitittämisestä ja mahdollisista sanomien jakamisesta ja kokoamisista.

Skenaarion SWOT-analyysi

Tämän skenaarion SWOT-arvio on seuraava:

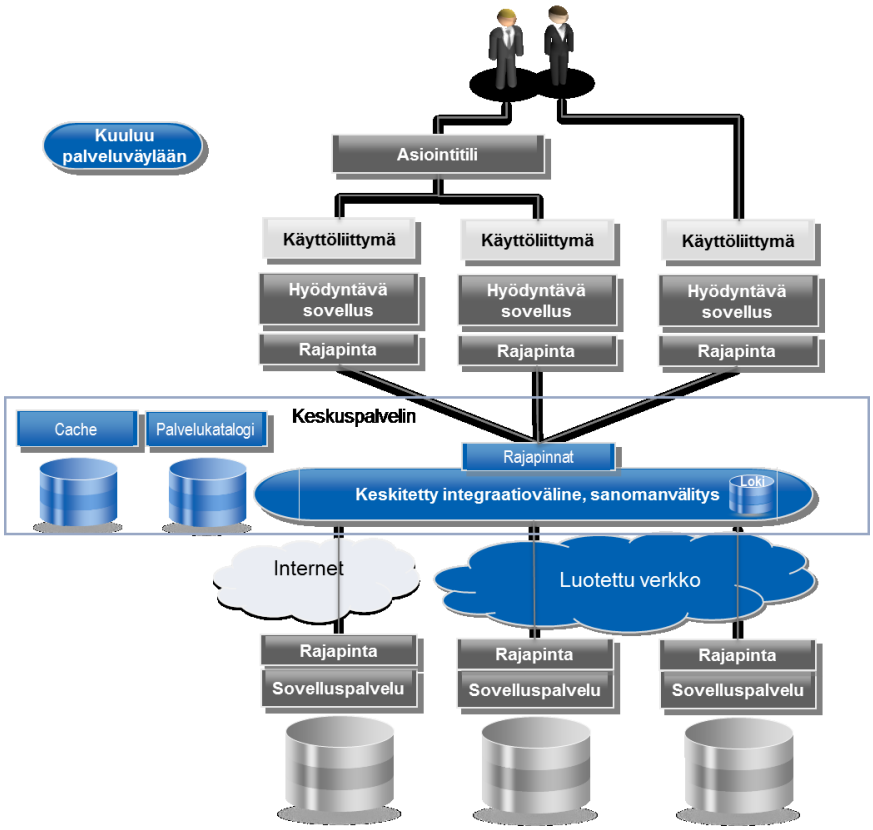
Skenaarioarvion yhteenveto:

Skenaarion keskeinen vahvuus on sen redundanssi ja hyvä jatkuvuus erityistilanteissa, koska se perustuu hajautettuun malliin. Ratkaisu muodostaa yhtenäisen tavan kytkeytyä ja liittyä palveluväylään sekä tuo mukanaan tavan hallita turvallisesti ja jäljitettävästi kansalaisten tietojen välittämistä. Yhtenäiset rajapintamallit ja yhtenäinen teknologia nopeuttavat uusien palvelujen tuomista kansalliseen palveluväylään.

Skenaarion haasteena on erityisesti sen toteuttaminen internetin yli. Tämä ei täytä kaikkien erityistoimialojen tarpeita ja vaatimuksia eikä internetin yli tapahtuvalle viestinnälle voi määrittää luotettavaa SLA-määritystä. Malli ei myöskään täysimääräisesti hyödynnä jo olemassa olevia tiedonvälityksen toteutuksia vaan edellyttäisi merkittävää nykyratkaisujen purkamista.

C: Keskitetty integraatiopalvelu

Keskitetty integraatioratkaisu perustuu malliin, jossa kansallisesti toteutetaan yksi integraatioväline, joka yhdistää kaikki kansalliseen palveluväylään palveluja tuottavat ja näitä hyödyntävät organisaatiot.



Keskitetyssä integraatiopalvelussa väylässä on keskitetty integraatioratkaisu, jonka kautta kaikki viestintä kulkee eri osapuolille. Se tarjoaa täten selkeän kontrollipisteen kaikelle kommunikaatiolle. Kaikki väylän hallinnointi on keskitettyä. Keskitettyyn integraatioratkaisuun on helppo tuottaa sanomien käsittelyyn liittyviä keskitettyjä palveluita ja se voi toimia tarvittaessa läpinäkyvänä välivarastona (cache) eri tietolähteille.

Keskitetyn väylän rajapintamääritys voi olla samanlainen kuin luotetun yhteysverkon rajapinnan määritys.

Skenaarion SWOT-analyysi

Tämän skenaarion SWOT-arvio on seuraava:

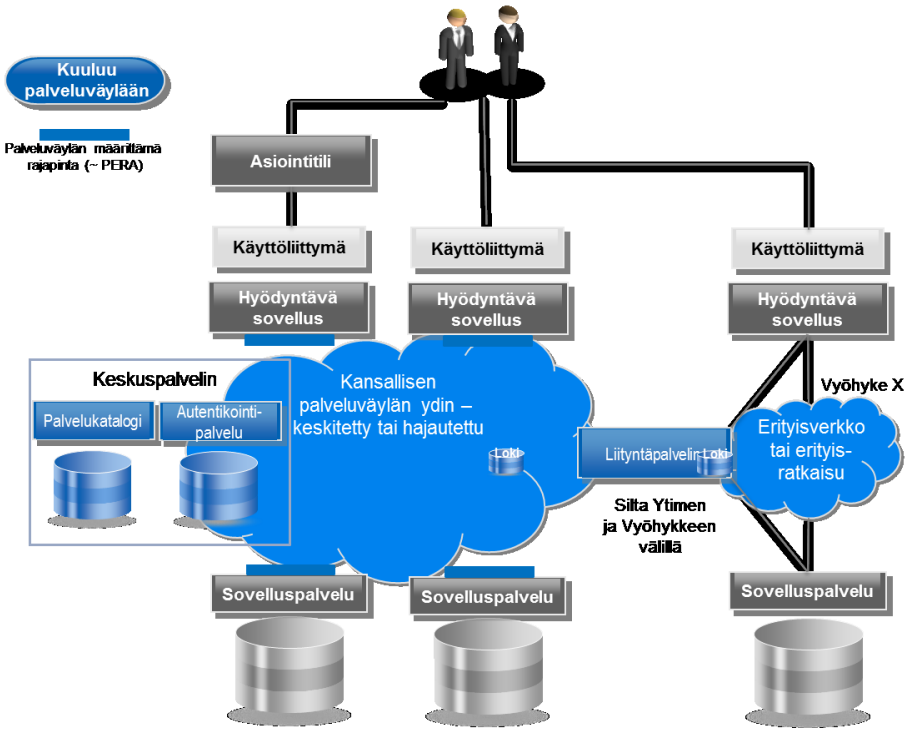
Skenaarioarvion yhteenveto:

Tämän skenaarion keskeinen vahvuus on siinä, että keskitetyssä ratkaisussa voidaan tietojen välittämisen toimivuutta valvoa kattavasti ja keskitetty tietojen yhdistäminen ja muuntaminen voidaan toteuttaa keskitettyinä muuntopalveluina. Ratkaisumalli sopii myös erityisen hyvin viestien välivarastointiin ja vähentää täten tarpeen mukaan lähdejärjestelmien kuormitusta. Malli voidaan suhteellisen helposti myös kytkeä eri tietoliikennetason verkkoihin.

Mallin haasteet tulevat voimakkaasta keskittämisestä. Viestien lokitus ja välivarastointi on haastavaa nykyisen tietosuojalainsäädännön näkökulmasta ja yksi keskitetty piste muodostaa potentiaalisen pullonkaulan sekä jatkuvuuden että suorituskyvyn näkökulmasta. Keskitetty ratkaisu tulee mitoittaa huippukuormia varten, joten se saattaa olla ”hiljaisina aikoina” vajaakäytöllä. Ratkaisu ei tässä muodossaan vielä sisällä toimijoiden luotettavaa tunnistamista täysimääräisesti.

D: Toimialojen erityistarpeet huomioiva vyöhykkeisiin jaettu palveluväylä

Tämä skenaario perustuu malliin, jossa eri toimialojen erityistarpeet voivat muodostaa itsenäisiä aliverkkoja – Vyöhykkeitä – kansalliseen palveluväylään.



Toimialatarpeet huomioiva vyöhykkeisiin jaettu palveluväylä eristää toimialakohtaisen tai muusta syystä erityistarpeisiin perustuvan vyöhykkeen palveluväylästä. Palveluväylään kytkettävän vyöhykkeen sisällä voidaan tietojen vaihto toteuttaa joko palveluväylän ratkaisumallia soveltaen tai kokonaan vyöhykkeen sisäisellä ratkaisulla. Vyöhykkeen ja palveluväylän internetin kautta toteutetun ytimen väliin määritetään liityntäpalvelin – silta, joka välittää läpinäkyvästi viestit vyöhykkeen sisältä palveluväylän palveluille ja päinvastoin. Vyöhykemallilla voidaan esimerkiksi toteuttaa korkean tietoturvallisuuden ja suorituskyvyn SLA-taattu tietoliikenneverkko. Sen avulla voidaan myös tarvittaessa toteuttaa korkean turvaluokituksen omaavan tiedon välittäminen. Muuten väylä voi olla arkkitehtuuriltaan jokin edellä mainituista vaihtoehdoista.

Yllä mainittuja ratkaisuja voidaan yhdistellä sen mukaan, mitkä ovat väylään liittyvien organisaatioiden tarpeet ja reunaehdot. Esimerkiksi toimialakohtainen SLA-taattu palveluväylä ja siihen liittyneet organisaatiot voidaan liittää autentikoidun verkoston tarjoamiin palveluihin yhteisen liityntäpisteen kautta.

Skenaarion SWOT-analyysi

Tämän skenaarion SWOT-arvio on seuraava:

Skenaarioarvion yhteenveto:

Tässä mallissa yhdistyy monia edellä kuvattujen skenaarion parhaita puolia. Ratkaisu luo yhtenäisen inrastruktuurin kansalliseen tietojen välittämiseen. Tämä sisältää sekä turvallisen palveluiden ja tietolähteiden autentikoinnin, salatut yhteydet, yhtenäiset rajapinnat sekä helpon kytkeytymisen palveluväylään. Tämän lisäksi ratkaisumalli kuitenkin hyödyntää täysimääräisesti jo olemassa olevan kehityksen ilman, että nykyisiä ratkaisuja tarvitsee purkaa. Palveluväylän ydin ja vyöhykkeet voidaan myös toteuttaa ja kehittää eri aikaan ja eri vastuutahojen toimesta, mikä helpottaa kansallisen palveluväylän kehittämispolun määrittämistä ja investointien rahoittamista.

Toimialojen erityispiirteet huomioon ottava skenaario on kuitenkin muita tässä kuvattuja skenaarioita monimutkaisempi. Sen hallintaan tulee yksi ulottuvuus lisää vyöhykeperiaatteen takia. Palveluväylän ytimen ja vyöhykkeiden välisen tiedonvälityksen yksityiskohdissa on myös muita skenaarioita enemmän ratkaistavia seikkoja (esimerkiksi miten tuottajaorganisaatio sopii vyöhykkeen sisällä olevan hyödyntäjän kanssa tietojen käytöstä).

Liite 4, Tekniset kuvaukset

Tietojen välittämismalli

Tietojen välittäminen Palveluväylässä voidaan jakaa seuraaviin osiin:

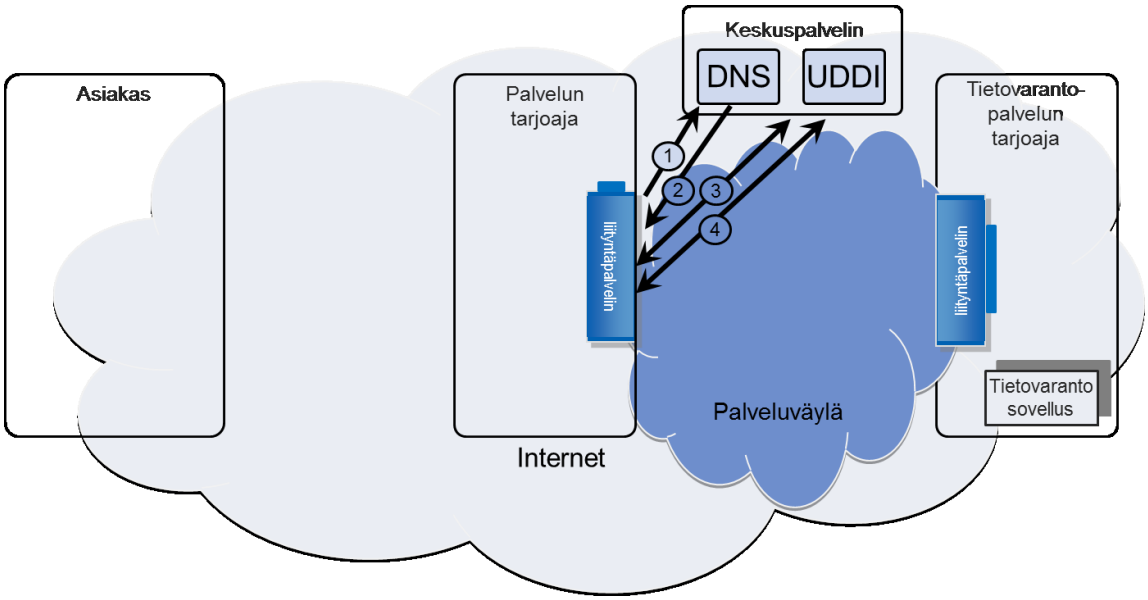
- Perustiedot
- Yhteyden muodostaminen
- Sanomien välittäminen

Perustiedot ovat pysyväisluontoisia tietoja, jotka asennetaan liityntäpalvelimeen käyttöönoton yhteydessä ja jotka päivittyvät harvoin. Oikeat perustiedot ovat edellytys yhteyksien muodostamiselle. Näitä tietoja ovat mm:

- liityntäpalvelimen julkinen IP-osoite ja domain-nimi
- liityntäpalvelimen oma varmenne, siihen liittyvät julkinen ja salainen avain mahdollistamaan suojattujen yhteyksien muodostaminen
- keskuspalvelimen nimi, varmenne sekä julkinen avain mahdollistamaan yhteydet keskuspalvelimelle sekä varmistamaan nimipalveluista saatavien tietojen allekirjoituksen oikeellisuus
- avustavien palvelimien nimet, kuten hakemistopalvelu, aikapalvelu, lokipalvelu jne.
- palveluväylän nimipalvelimien IP-osoitteet (vähintään kaksi) mahdollistamaan muiden toimijoiden osoitteiden selvittäminen
- yhteyksien muodostuksessa hyväksyttyjen päävarmentajien varmenteet vastapuolien identiteetin todentamiseen
- asynkronisen sanoman maksimi-ikä

Yhteyden muodostaminen tehdään liityntäpalvelimessa olevien perustietojen avulla. Välitettäväksi saadussa viestissä on joko kohdepalvelun tunnus tai yleinen palvelutyyppi johon halutaan yhteys. Alla olevassa kuvauksessa jätetään huomiotta mahdollinen väylän ydinpalvelun sijainti paikallisesti, koska tietojen säilyttäminen paikallisesti on osa palveluväylän suorituskyvyn ja toimintavarmuuden kasvattamista, johon liittyy myös muutosten välittäminen paikallisiin kopioihin. HTTP-yhteydet luodaan uudelleenkäytettävinä, jolloin yhteyksiä ei tarvitse välttämättä muodostaa jokaisen kyselyn kohdalla.

Hyödyntäjäsovelluksen liityntäpalvelin kysyy perustietoihin määritellystä nimipalvelusta, mikä on perustiedoista saatavan nimen (esim. `ud-di.palveluvayla.fi`) perusteella hakemistopalvelun IP-osoite (1). Nimipalveluista voidaan samalla tarkistaa, ettei vastapuolen varmennetta ole evätty. Saadun vastauksen (2) allekirjoitus tarkistetaan perustiedoissa olevaa keskuspalvelun julkista avainta vastaavaksi. Liityntäpalvelin muodostaa suojatun ja salatun yhteyden hakemistopalveluun (3), kuten luvussa 0 kuvataan.



Liityntäpalvelin kysyy ja saa hakemistopalvelusta vastauksena tavoiteltavan tuottajapalvelun liityntäpalvelimen nimen (4). Mikäli haku on tehty palvelutyypin perusteella, liityntäpalvelin valitsee omilla kriteereillään parhaiten sopivan tuottajapalvelun (esim. onko palvelun käyttö sopimuksellisesti mahdollista jne.).

Erityistapaus palvelutyypistä on tilauspalvelu, johon liityntäpisteet voivat rekisteröityä ja näin liittyä yhdeltä monelle lähetettävän viestinnän hyödyntäjiksi. Käyttökohteena on esim. muutostiedon välittäminen, jolloin kaikki ko. muutoksesta kiinnostuneet tahot saavat ajantasaisesti muuttuneen tiedon ilman että ne aktiivisesti pollaisivat tietolähdettä ja aiheuttaisivat tarpeetonta kuormaa kyselyillään. Liityntäpalvelin hakee hakemistosta listan liityntäpalvelimista, joihin sanoma on välitettävä.

Liityntäpalvelimen nimen perusteella haetaan nimipalveluista vastaava IP-osoite samoin kuin haettiin hakemistopalvelujen osoite. Myös yhteyden muodostaminen liityntäpalvelimeen tehdään vastaavalla tavalla.

Sanomien välittäminen tapahtuu viestissä olevien tietojen perusteella (viestikehykset on tarkemmin kuvattu kappaleessa 6.6). Välitettävä sanoma voi olla synkronisesti tai asynkronisesti välitettävä ja kohdistua yhteen tai useampaan kansalliseen palveluväylään kytkettyyn palveluun. Välitetyistä viesteistä kirjataan kehyksen tiedot aikaleimattuina lokeihin ja määrämittaiseksi kasvaneista lokitiedoista lasketaan tarkistussumma, joka lähetetään keskuspalvelimelle.

Hyödyntäjän liityntäpalvelin kuittaa asynkronisen viestin vastaanotetuksi kun käytettävä palvelu on hakemiston avulla löydetty ja tiedetään kutsutun palvelun olevan olemassa. Viesti tallennetaan pysyvässä muistissa olevaan jonoon, josta se ei häviä esim. virtakatkossa. Sanoma välitetään jonosta tuottajan liityntäpalvelimelle, mikäli se ei aikaleimansa mukaan ole vanhempi kuin perustiedoista ilmenevä palveluväylälle asetettu sanoman suurin sallittu ikä. Tässä tapauksessa sanoma hävitetään ja asia kirjataan lokeihin.

Tuottajan liityntäpalvelin kuittaa asynkronisen sanoman vastaanotetuksi kun se on vastaanottanut sen hyödyntäjän liityntäpalvelimelta ja taltioinut sen tilapäisesti niin että sanoma ei mahdollisessa virtakatkossa pääse katoamaan.

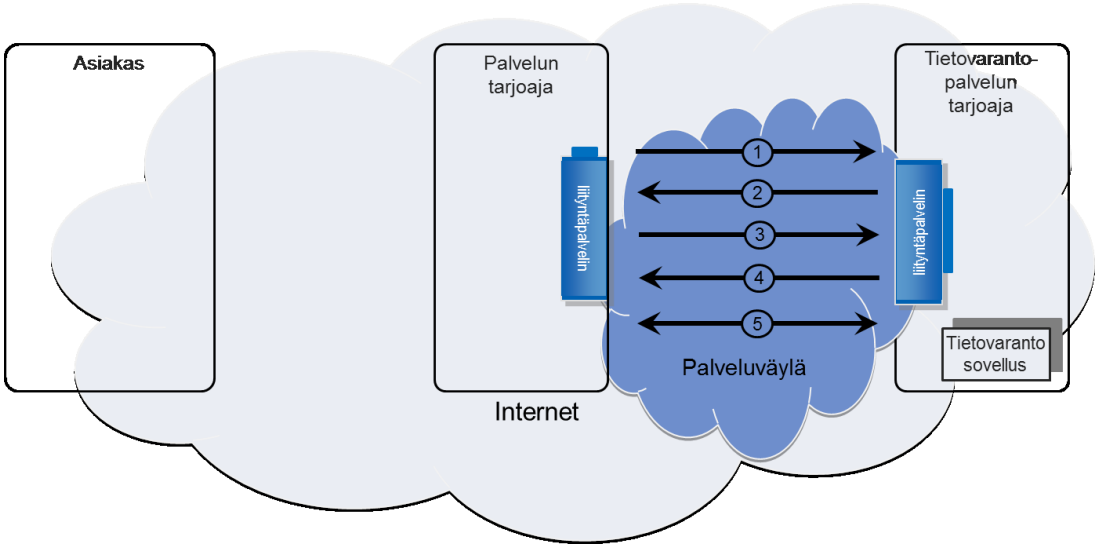
Ennen sanoman edelleen välittämistä tuottajan liityntäpalvelin tarkistaa, että sanoma ei ole vanhentunut, jossa tapauksessa sanoma hävitetään, asia kirjataan lokeihin ja viestin alun perin lähettäneelle liityntäpalvelimelle lähetetään virhesanoma. Mikäli viesti ei ole liian vanha, yritetään se välittää tuottajasovellukselle.

Asynkronisesta viestistä ei lähetetä kuittaussanomaa alkuperäiselle sovellukselle, asynkronisten sanomien mahdolliset kuittaamiset on rakennettava sovellustasolle – tämä on analoginen UDP-protokollan viestinvälityksen kanssa.

Synkroninen viestintä poikkeaa asynkronisesta viestinnästä siinä, että yhteydet ovat auki koko ketjun ja tuottajasovelluksen vastaus välitetään tiedonvälitysketjua pitkin takaisin hyödyntäjäsovellukselle. Myös vastauksen tiedot taltioidaan aikaleimattuina lokeihin.

Palvelimien tunnistaminen

Kuten aiemmin on kuvattu, hyödyntävän palvelun liityntäpalvelin selvittää kohdelaitteen IP-osoitteen nimipalvelujen avulla ja tarkistaa että saatu osoite on keskuspalvelimen allekirjoittama. Kohdelaite voi olla toinen liityntäpalvelin tai esim. jokin keskuspalveluista.



Varsinainen yhteydenmuodostus tehdään TLS-protokollaa hyödyntäen, jolloin laitteiden välillä tapahtuu molemminpuolinen tunnistaminen hieman yksinkertaistaen seuraavasti:

1. Lähdeorganisaation (useimmiten Hyödyntäjä) liityntäpalvelin muodostaa TCP-yhteyden kohdeorganisaation (Tuottaja) liityntäpalvelimeen.
2. Kohdeorganisaation liityntäpalvelin vastaa palauttamalla varmenteensa sekä kaikki varmenneketjun varmenteet aina varmennepalvelun päävarmenteeseen asti. Lisäksi kohdeorganisaation liityntäpalvelin pyytää lähdeorganisaation liityntäpalvelimelta varmenteen.
3. Lähdeorganisaation liityntäpalvelin tarkistaa saamansa varmenteet, päävarmenteen on löydyttävä paikallisista perustiedoista eikä mikään varmenteista saa löytyä varmenteiden kumoamislistasta. Jos lähdeor-

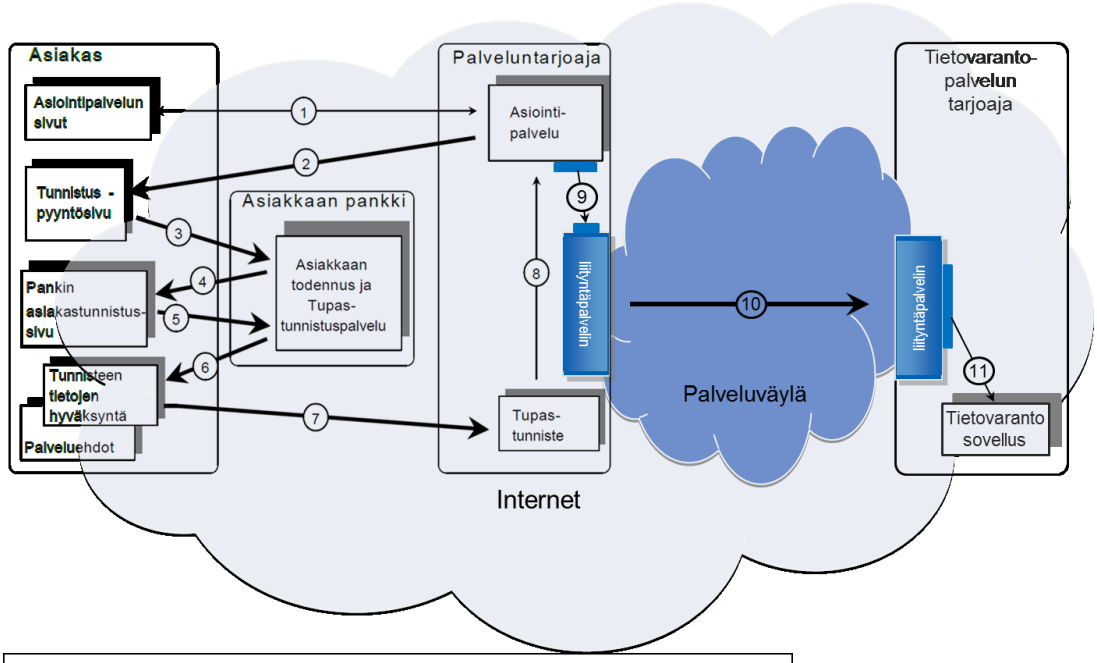
ganisaation liityntäpalvelin hyväksyy kohdeorganisaation liityntäpalvelimen varmenteen, se lähettää oman varmenteensa (ja koko varmenneketjun).

4. Kohdeorganisaation liityntäpalvelin tarkistaa lähdeorganisaation liityntäpalvelimen varmenteen kelvollisuuden vastaavasti kuin lähdeorganisaation liityntäpalvelin ja käynnistää yhteyden salaamiseen tarvittavien tietojen vaihdon hyödyntäen liityntäpalvelimen varmenteessa ollutta julkista avainta sekä omaa salaista avaintaan.
5. Liityntäpalvelimet neuvottelevat yhteyden salauksessa käytettävät salausavaimet ja sanomien turvallinen välitys voi alkaa.

Kansalaisen tunnistaminen

Palveluväylän ekosysteemissä palveluväylän avulla palveluja tarjoava hyödyntäjäsovellus tunnistaa käyttäjänsä. Vaikka loppukäyttäjän tunnistaminen ei ole osa palveluväylän toiminnallisuutta, kuvataan tässä yksi tapa tunnustaa kansalainen loppukäyttäjänä, koska ekosysteemissä on todennäköisesti yhteisesti hyväksyttävä mitä tunnistustapoja hyödyntäjäpalvelujen on käytettävä.

Oheisessa kuvassa esitetään viestinvälitys kun kansalainen kirjautuu TUPAS-tunnistuksen avulla hyödyntäjäpalveluun verkkoselaimellaan.



Askeleet 1-8 lähde: Pankkien TUPAS-tunnistuspalvelu palveluntarjoajille, Versio 2.3c 28.3.2011

Tunnistusviestien välitys on seuraava:

1. Tunnistautuva asiakas on yhteydessä palveluntarjoajan asiointipalveluun.
2. Asiointipalvelu (palveluväylään kytketty sovellus) lähettää asiakkaalle tunnistuspyynnön, joka sisältää tapahtumaan liittyvät yksilöintitiedot.
3. Asiakas painaa toimintopainiketta, joka johtaa verkkoselaimen ottamaan yhteyden valitun pankin tunnistuspalveluun.

4. Pankin tunnistuspalvelu esittää asiakkaalle tunnistuspyynnön.
5. Asiakas tunnistautuu pankkinsa verkkopalvelun tunnisteilla.
6. Onnistuneen tunnistuksen jälkeen pankki muodostaa vastaussanoman, ”Tupastunnisteen”, joka näytetään asiakkaalle.
7. Asiakas tarkastaa tunnisteen tiedot ja hyväksyy tunnisteen välittämisen palveluväylään kytketylle hyödyntäjäsovellukselle. Hyväksyntä siirtää Tupas-tunnisteen asiointipalvelulle.
8. Palveluväylään kytketty asiointipalvelu (hyödyntäjäsovellus) varmistaa vastaanottamansa Tupas-tunnisteen eheyden ja ainutkertaisuuden ja toteaa asiakkaan tunnistetuksi pankin tunnistuspalvelusta saadun tunnisteen avulla.
9. Asiointipalvelu, eli palveluväylään kytketty hyödyntäjäsovellus, lähettää palvelupyynnön palveluväylän liityntäpalvelimelle ja merkitsee sanomassa käyttäjäksi tunnistetun asiakkaan sekä tunnistustavaksi Vetuman.
10. Palveluväylän liityntäpalvelimet tunnistavat toisensa ja välittävät sanoman suojattua yhteyttä pitkin
11. Sanoma välitetään palveluväylään kautta tuottajasovellukselle

Esimerkki palveluväylän sanomasta

REST-mallilla toteutettuna palvelukutsu ja vaste näyttäisivät seuraavalta. Esimerkissä kaikki kyselyn tiedot ovat suoraan HTTP-otsikossa itse määriteltyinä kenttinä (Yrd-alkuiset) sen sijaan, että ne olisivat XML- tai JSON-muodossa, kuten vastauksessa. Esimerkissä otsikkotietoina ovat kaikki kyselykerrasta toiseen muuttuvat tiedot, joten varsinaisen kyselyn vastaus voidaan tarvittaessa taltioida välimuistiin vastaavia kyselyjä varten. Siltä varalta että (mahdollisessa) välimuistissa olisi jo saman kyselyn vastaukset, tässä kyselyssä on rajattu hyväksyttävä vastauksen taltiointiaika 30 päivään.

```
GET /kansalaisrekisteri/030900-1230?q=names HTTP/1.1
Host: www.palveluvayla.fi
Yrd-Originator: www.kansalaisportaali.fi
Yrd-Id: kansalaisportaali.fi-3eb7fbed9396fda70ca1215d3f3fe1
Yrd-Timestamp: 2013-04-31T13:14:15Z
Yrd-UserId: FI311299-0123
Yrd-Position: Researcher
Yrd-Authenticator: MOBILE; DNA
Cache-control: private, maxage=2592000 s-maxage=2592000
Accept: application/json; application/xml
```

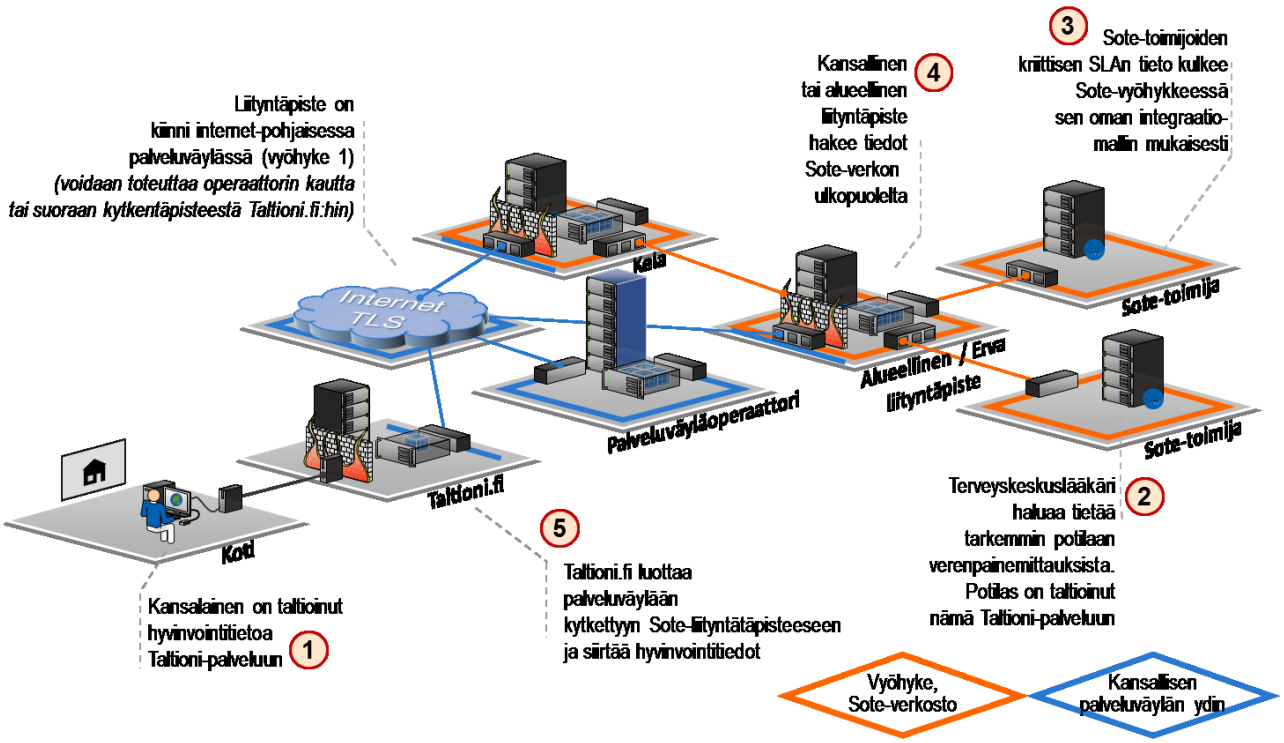
Alla esimerkkivastaus JSON-muodossa. Tässä JSON-vastauksen rakenteeseen on viittaus Content-Type otsikossa:

```
HTTP/1.1 200 OK
Date: Wed, 28 Oct 2013 13:14:15 GMT
Last-Modified: Wed, 12 Oct 2009 17:50:00 GMT
Content-Length: 178
Content-Type: text/json;
              profile=http://www.vrk.yrd.fi/json/yroad.jsd
Server: www.palveluvayla.fi
Yrd-Id: kansalaisportaali.fi-3eb7fbed9396fda70ca1215d3f3fe1
Yrd-Timestamp: 2013-04-31T13:14:16Z
```

```
{
  "PersonInformation" : {
    "Id" : "030900-0123",
    "Names" : {
      "Surname" : "Kekkonen",
      "FirstName" : "Urho",
      "OtherNames" : "Kaleva"
    }
  }
}
```

Tiedonsiirto vyöhykkeen ja palveluväylän välillä

Tiedonsiirto määriteltyjen, palveluväylään kytkettyjen vyöhykkeiden ja palveluväylän ytimen välillä toteutetaan aina vyöhykkeen reunalle, vyöhykkeen ja palveluväylän ytimen väliin asennetun vyöhykkeen liityntäpisteen kautta. Tämä vyöhykkeen liityntäpiste näkyy kansallisen palveluväylän ytimeen päin aivan tavallisena liityntäpisteenä, mutta vyöhykkeeseen päin se puolestaan näkyy ko. vyöhykkeen tietojen vaihtoon määriteltynä kytkentäpisteenä. Tietojen vaihto vyöhykkeen ja kansallisen palveluväylän välillä voidaan toteuttaa esimerkiksi seuraavasti:

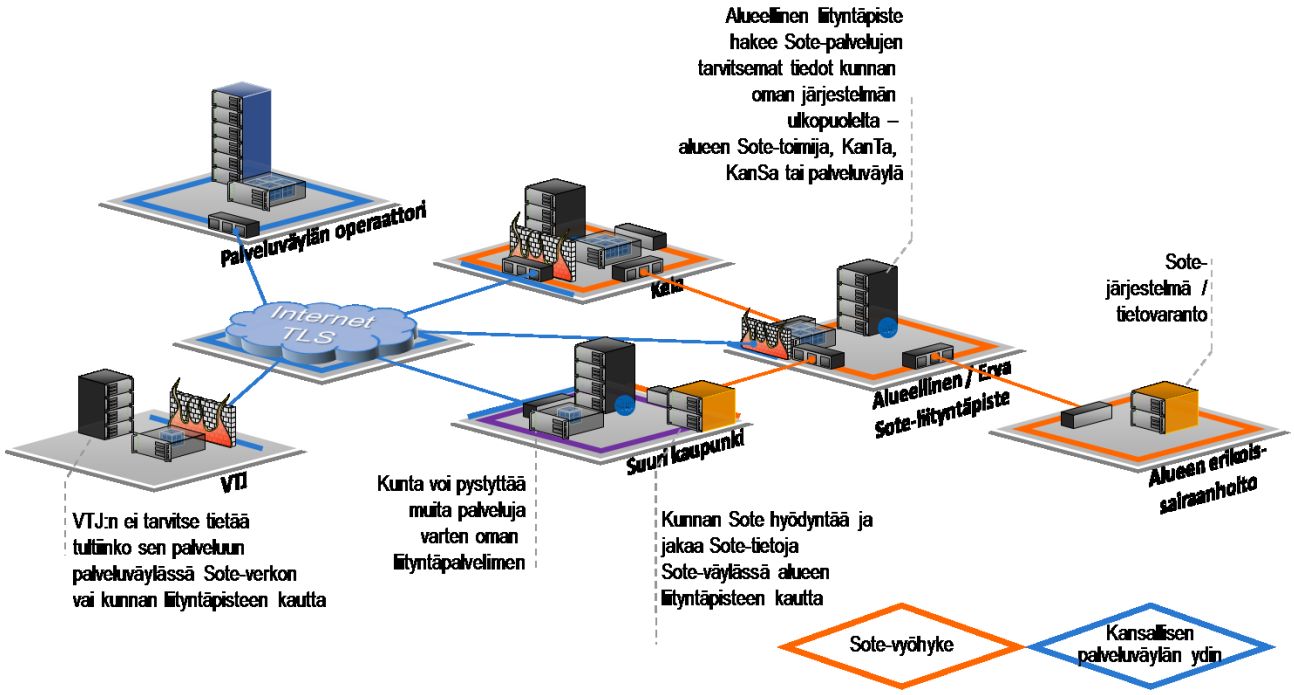


Yllä olevassa kaaviossa vyöhykkeen sisällä oleva terveyskeskuslääkäri saa vaivattomasti kansallisen palveluväylän kautta asiakkaan itse tuottamat hyvinvointitiedot esimerkiksi diagnoosin tai hoitosuunnitelman laatimisen tueksi. Vyöhykkeen ja palveluväylän ytimen välillä oleva liityntäpiste muuntaa sanomat ja viestit täysin läpinäkyvästi muodosta toiseen.

Kansallisen palveluväylän sanomamäärityksen on vyöhykemallia varten määritetty erillinen kenttä, jossa voidaan erottaa sanoman palveluväylään näkyvä välittäjätaho varsinaisesta kutsuja/päätepisteorganisaatiosta.

Vyöhykkeen tai yksittäisen organisaation liityntäpisteiden määrää kansallisen palveluväylän ytimeen ei ole rajoitettu. Vyöhykkeeseen voidaan toteuttaa tarvittaessa useita liityntäpisteitä kansallisen palveluväylän ytimeen. Vastaavasti yksittäisellä organisaatiolla voi olla useita liityntäpisteitä sekä vyöhykkeisiin tai kansallisen palveluväylän ytimeen. Tämä voi olla tarpeen erityisesti monialaorganisaatiolla, jotka joutuvat toimintansa reunaehtojen takia noudattamaan eri toiminnoissaan useiden eri toimialojen määräyksiä.

Seuraavassa on kuvattu esimerkiksi suuren kaupungin mahdollista kytkeytymistä kansalliseen palveluväylään.



Tarpeettomien liityntäpisteiden toteuttamista tulee kuitenkin välttää.