Suomi.fi

Suomi.fi-palveluväylän hyödyntäminen

Versio: 1.0

VÄESTÖREKISTERIKESKUS
PL 123 (Lintulahdenkuja 4), 00531 Helsinki
puh. 0295 535 001, faksi 09 876 4369

MUUT TOIMIPISTEET
Ks. www.vrk.fi

www.vrk.fi
kirjaamo@vrk.fi
Y-tunnus: 0245437-2

Väestörekisterikeskus

2.12.2019

Sisällysluettelo

2.12.2019

1 Johdanto

1.1 Dokumentin tarkoitus

Tämän dokumentin tarkoitus on kuvata Suomi.fi-palveluväylän arkkitehtuuri sisältäen Palveluväylän keskeiset hyödyt, periaatteet, rakenteet, ominaisuudet, käyttösuositukset ja velvoitteet. Se kuvaa miten organisaatiot voivat Palveluväylän avulla jakaa tietoturvallisesti tietoja toisilleen, mitä Palveluväyläkokonaisuus sisältää ja miten sitä kannattaa eri tilanteissa hyödyntää. Dokumentti toimii myös kattodokumenttina laajalle joukolle Palveluväylään liittyviä ohjeistuksia ja kuvauksia. Dokumentin avulla lukijalle tarjotaan yleiskuva asioista ja ohjataan tarkempiin kuvauksiin.

1.2 Dokumentin kohderyhmä

Tämä dokumentti on tarkoitettu Palveluväylän hyödyntäjille. Keskeisiä hyödyntäjiä ovat mm. Palveluväylän kautta tarjottavien palveluiden kehittämisestä ja hyödyntämisestä sekä palveluiden integraatioarkkitehtuurista ja infrastruktuurista vastaavat organisaatiot. Dokumentti toimii myös päätöksenteon tukena esim. tiedonvaihdon ratkaisuja päätettäessä.

Viitearkkitehtuurikuvaus on tarkoitettu pääasiassa arkkitehdeille, suunnittelijoille ja kehittäjille. Keskeisiä kohderyhmiä ovat:

- Julkiset tahot, jotka tuottavat tietoa
- Julkiset tahot, jotka hyödyntävät toisten tarjoamaa tietoa
- Yksityiset tahot, jotka hyödyntävät tai tuottavat julkisen hallinnon tietoa
- Tietojärjestelmäintegraattorit, ohjelmistotalot ja tietoliikenteen palveluntarjoajat

1.3 Dokumentin rajaukset ja reunaehdot

Tämä dokumentti keskittyy Suomi.fi-palveluväylän kautta tapahtuvaan tiedonsiirtoon ja palveluiden löydettävyyteen. Dokumentti sisältää yleisiä kuvauksia ja ohjeita väylään liitettävien palveluiden kehittämiseen, julkaisuun, dokumentointiin, ja hyödyntämiseen. Dokumentti ei kuitenkaan kuvaa yksittäisiä väylään liitettäviä tietojärjestelmäpalveluita tai muita väylän hyödyntäjien palveluita.

Tämä dokumentti:

- On osa julkisen hallinnon kokonaisarkkitehtuuria (JHKA)
- Määrittelee kansallisen tiedonvaihdon infrastruktuurin ja sen teknisten ja hallinnollisten palvelujen kokonaisuutta
- Ei sisällä kuvausta Palveluväylän liiketoiminta- ja hallintamallista eikä etenemissuunnitelmaa (roadmap)
- Ei kuvaa Palveluväylän operointiin ja hallinnointiin liittyviä prosesseja
- On osa yhteentoimivuuden kuvauksia ja määrityksiä (www.avoindata.fi)

2.12.2019

2 Periaatetason arkkitehtuurikuvaukset

2.1 Palveluväylän rajaukset ja reunaehdot

Suomi.fi-palveluväylä on ratkaisu julkisen ja yksityisen sektorin tiedonvälitystarpeisiin. Palveluväylä tukee julkisen hallinnon, yritysten ja kolmannen sektorin palveluiden yhdistämistä saumattomaksi ja asiakaslähtöiseksi kokonaisuudeksi hallinnollisista rajoista riippumatta.

Palveluväylä itsessään ei tarjoa loppukäyttäjille näkyviä substanssipalveluita, vaan mahdollistaa näiden tarjoamisen ja kehittämisen. Eri toimijoiden Palveluväylään kytkemät substanssi- ja liiketoimintapalvelut eivät kuulu Palveluväylään. Palveluväylä on tietojärjestelmien välillä oleva komponentti, joten se ei suoraan näy palveluiden loppukäyttäjille, kuten kansalaisille tai viranomaisille.

2.2 Strategiset tavoitteet

Suomi.fi-palveluväylän strategisia tavoitteita ovat:

- Yksinkertaistaa ja helpottaa julkisen hallinnon asiakkaiden - kansalaisten, yritysten ja yhteisöjen - asiointia viranomaisten kanssa turvallisen kanavan välityksellä
- Parantaa tietojen yhteiskäyttöä ja tietojärjestelmien yhteentoimivuutta koko julkisessa hallinnossa
- Mahdollistaa sähköisten palvelujen kustannustehokkuus niiden elinkaaren ajan
- Edistää yritysten mahdollisuuksia hyödyntää julkisen hallinnon tietovarantoja ja palveluja
- Tukea kansantaloutta tehostamalla julkista hallintoa ja luomalla uusia liiketoimintamahdollisuuksia yksityiselle sektorille

Palveluväylän kehitystä ohjaavia vaatimuksia on myös VM:n tavoite keskitetyistä ICT-palveluista. Palveluväylän tavoitteena on tarjota yhtenäinen tiedonvälityksen ratkaisu eri organisaatioiden käyttöön, vaikka sen tekninen toteutus onkin hajautettu.

Julkisessa hallinnossa halutaan edistää avoimen lähdekoodin käyttöä, mikä näkyy mm. JHKA periaatteissa ja hankintaehdoissa (JHS166). Palveluväylän teknistä toteutusta ohjaa tavoite tietojärjestelmien koodin ja rajapintojen avoimuudesta.

2.3 Palveluväylän hyödyt

Suomi.fi-palveluväylä mahdollistaa tietoturvallisen ja vakioidun tavan tietojen siirtoon organisaatioiden välille. Palveluväylän avulla parannetaan palveluiden ja niiden käyttöön liittyvää tietoturvaa, tietosuojaa, läpinäkyvyyttä, laatua ja tiedon luotettavuutta. Palveluväylän yleisiä hyötyjä sen käyttäjille ja palveluntarjoajille on kuvattu Palveluväylän esittelysivulla (https://palveluhallinta.suomi.fi/fi/sivut/palveluvayla/esittely).

Palveluiden tietoturvasta huolehtiminen on laaja kokonaisuus, jossa tietoturvan todellinen taso määräytyy heikoimman osan perusteella. Tietoturvan taso ei riipu pelkästään valituista tuotteista ja teknologioista, vaan myös näiden asetuksista, käyttötavoista, ylläpidosta ja valvonnasta. Toisin kuin muut tietoturvatuotteet, Palveluväylä tarjoaa tiedonsiirron

tietoturvaan laajan kokonaisratkaisun, jossa on huolehdittu yksittäisten osien lisäksi kokonaisuuden yhteentoimivuudesta ja tietoturvasta.

Suomi.fi-palveluväylä eroaa organisaatioiden käyttämistä muista tietoturvatuotteista ja väyläratkaisusta (esim. ESB ja API Gateway tuotteista) seuraavilta osin:

- Suomi.fi-palveluväylä laajentaa tietoturvan hallinnan organisaatiotasolta kansalliselle tasolle mahdollistaen mm. tietoturvapoikkeamiin ja -uhkiin vastaamisen kansallisella tasolla.
- Suomi.fi-palveluväylä muodostaa keskitetysti hallittavan kansallisen tason ekosysteemin. Keskitetty hallinta mahdollistaa löyhemmät kytkökset ekosysteemitoimijoiden välillä. Esim. palveluiden siirto pilveen tai konesalitoimittajan vaihto voidaan suurelta osin tehdä näkymättömäksi muille ekosysteemin toimijoille.
- Suomi.fi-palveluväylä huolehtii tietoturvasta tiedonsiirron molemmissa päissä. Organisaatiot käyttävät yleensä ulkoisille osapuolille tarjottaviin palveluihin sisäisiä tietoturvatuotteita tai väyläratkaisuja (esim. ESB tai API Gateway). Näiden avulla ei voida kuitenkaan varmistua, että tiedonsiirto ja palveluiden käyttö on tietoturvallista. Palvelinpäässä voidaan rajata, että palveluita voidaan käyttää vain tietoturvallisilla teknologioilla. Asiakaspäässä ei kuitenkaan yleensä tehdä samoja rajauksia ja tarkistuksia, eikä asiakkaat ole usein palvelinpään rajauksien tarkoista yksityiskohdista edes tietoisia. Tämä mahdollistaa man-in-the-middle (MITM) hyökkäykset ja viestien salakuuntelemisen, vaikka palvelinpään tietoturva olisikin kunnossa. Suomi.fi-palveluväylää käytettäessä voidaan aina varmistua sekä palvelimen että asiakaspään tietoturvasta, eikä esim. osapuolten tunnistus- ja salausmenetelmiin liittyviä rajauksia ja tarkistuksia tarvitse jättää palveluiden hyödyntäjien vastuulle.
- Suomi.fi-palveluväylässä käytetyt teknologiat on valmiiksi rajattu ja konfiguroitu vastaamaan korkean tietoturvan vaatimuksia. Organisaatiokohtaisissa väyläratkaisuissa (esim. ESB tai API Gateway tuotteet) tietoturvan taso riippuu oleellisesti, kuinka hyvin nämä ratkaisut on konfiguroitu ja kovennettu. Yleensä minkään tietoturvateknologian käyttö ei vielä itsessään takaa korkeaa tietoturvaa, vaan tietoturva määräytyy tarkempien asetusten ja rajausten perusteella (esim. laajasti käytettyä TLS-salausprotokollaa voidaan käyttää täysin tietoturvattomasti). Valitettavan usein vastuu tietoturvallisista asetuksista jää ylläpitäjille ja ohjelmistokehittäjille, vaikka nämä harvemmin ovat tietoturvan erityisasiantuntijoita.
- Suomi.fi-palveluväylä tarjoaa vakioidun *kokonaisvaltaisesti* tietoturvallisen tavan organisaatioiden väliseen tietojenvaihtoon. Vaikka tietoturvalliseen tiedonsiirtoon on olemassa useita standardeja, nämä kattavat yleensä pelkästään yksittäisen osakokonaisuuden. Standardien yhdistämiseen puuttuu vakiintuneet käytännöt ja standardit. REST-palveluiden osalta yksittäisiin osa-alueisiin, kuten pyyntöjen ja vastausten allekirjoituksiin, ei ole yleisiä standardeja. Tämän vuoksi organisaation omia integraatioratkaisuja käytettäessä päädytään yleensä Palveluväylää tietoturvattomampiin ratkaisuihin. Integraatiossa voidaan käyttää tietoturvaltaan laadukkaita yksittäisiä teknologioita, mutta kokonaisuus jää usein puutteelliseksi. Esim. melko usein tyydytään pelkästään linkkitason salaukseen ja osapuolten tunnistamiseen (esim. käyttämällä TLS-protokollaa). Palveluväylässä tietoturva on kerroksellista ja se huomio laajasti eri näkökulmat. Esim. Palveluväylän toteuttama viestien allekirjoitus, pyyntöviestin tiivisteen välittäminen vastausviestissä ja viestien aikaleimaaminen luotetun kolmannen tahon toimesta mahdollistavat yhdessä viestinvälityksen kiistämättömyyden tarkistamisen (ks. luku 2.8). Mikäli viestinvälityksen

kiistämättömyyttä ei ole riittävällä tasolla varmistettu, lokitetuilla viesteillä ei ole juridista todistusarvoa ja osapuolet voivat kieltää toimintansa jälkeenpäin.

2.4 Palveluväylän palvelulupaukset ja käyttösuositukset

Suomi.fi-palveluväylän keskeisimmät ominaisuudet on kuvattu *Palveluväylän palvelulupauksessa [2].* Palvelulupaus sisältää myös käyttösuositukset ja tiedot niistä asioista, joita Palveluväylä ei tällä hetkellä tarjoa.

2.5 Palveluväylän käyttöoikeudet, velvollisuudet ja poikkeusperusteet

KaPA-laki eli laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) määrittelee Julkisen sektorin velvollisuudesta ja oikeudesta käyttää Palveluväylää. Laki myös määrittelee yksityisen sektorin oikeudesta käyttää Palveluväylää tietojen siirtoon. KaPA-lain mukaan seuraavat julkisen hallinnon viranomaiset ovat velvollisia käyttämään Palveluväylää:

- Valtion hallintoviranomaiset, virastot, laitokset ja liikelaitokset
- Kunnalliset viranomaiset niiden hoitaessa laissa niille säädettyjä tehtäviä
- Tuomioistuimet ja muut lainkäyttöelimet

Väestörekisterikeskus on linjannut 11.3.2019 Palveluväylän käyttövelvoitteesta poikkeamisesta (*linjauspäätös VRK/1338/2019 [3]*). Linjauksen mukaan Väestörekisterikeskus katsoo Suomi.fi-palveluväylän käyttövelvoitettujen organisaatioiden voivan poiketa käyttövelvoitteessa seuraavissa tilanteissa:

- Tietojen vastaanottajana on organisaatio, jolla ei ole lain mukaista käyttövelvoitetta
- Eräajo-tyyppiset siirrot, joihin organisaatiolla on jo olemassa ratkaisu
- Liittymät työasemaohjelmistoihin ja mobiililaitteisiin
- ST III tason tiedonsiirto tietyin rajoituksin (ympäristöjen tulee olla Viestintäviranomaisen päätöksellä hyväksytty ST III tasolle)

Mikäli organisaatio katsoo asiointipalvelunsa täyttävän jonkun edellä mainituita poikkeusperusteista, voi se lähtökohtaisesti suoraan VRK:n kirjaamiin perusteisiin nojaten poiketa Suomi.fi-palveluväylän käyttövelvoitteesta. Organisaation tulee kuitenkin ilmoittaa kirjallisesti Väestörekisterikeskukselle, mihin edellä mainittuihin perusteisiin nojaten palvelun käytöstä poiketaan ja millä perusteilla. Väestörekisterikeskus arvio ilmoituksen ja päättää riittääkö ilmoitus vai tuleeko organisaation tehdä virallinen poikkeuslupahakemus. Tarkemmin poikkeusperusteet ja ilmoituksen tietosisältö on kuvattu *linjauspäätöksessä [3]*.

Osa julkishallinnon organisaatioista tarjoaa palveluita, joiden rajapinta ja/tai sisältö on tarkasti määritelty esimerkiksi toimialan standardeissa tai EU:n toimesta. Yleensä nämä palvelut ovat sovitettavissa Palveluväylään joko SOAP- tai REST-palveluina. Jos sovittaminen ei ole mahdollista, voi Palveluväylän käyttövelvoitteesta poikkeaminen olla perusteltua. Kansainvälisistä tai kansallisten kohdealueiden standardoinneista saavutettuja yhteentoimivuuden etuja ei kannata menettää, joten näissä tapauksissa Palveluväylää kannattaa soveltaa vain niiltä osin mitkä ovat standardien noudattamisen rajoissa mahdollista. Näissä poikkeamistapauksissa organisaation tulee tehdä Väestörekisterikeskukselle poikkeuslupahakemus, jollei poikkeaminen perustu edellä kuvattuihin poikkeamisperusteisiin.

Avoimen datan palveluita Palveluväylän käyttövelvoite ei koske. Päätös avoimen datan tarjoamisesta Palveluväylän kautta kannattaa tehdä tapauskohtaisesti (asiaa on käsitelty tarkemmin luvussa 4.3).

2.6 Ohjaavat lait, määräykset ja sidosarkkitehtuurit

Seuraavaan taulukkoon on koottu Suomi.fi-palveluväylää ja sen käyttöä ohjaavat lait, määräykset, sidosarkkitehtuurit ja yhteiset tukipalvelut.

Sidosarkkitehtuurit	Kuvaus, keskeinen sisältö
Lainsäädäntö	
KaPA-laki **Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016)**	Laissa säädetään julkisen hallinnon yhteisistä sähköisen asioinnin tukipalveluista, niitä koskevista vaatimuksista, niiden tuottamiseen liittyvistä tehtävistä sekä tuottamiseen liittyvästä henkilötietojen ja muiden tietojen käsittelystä. Lisäksi laissa säädetään oikeudesta ja velvollisuudesta käyttää yhteisiä sähköisen asioinnin tukipalveluja sekä palvelujen käytön edellytyksistä. Suomi.fi-palveluväylä on yksi em. yhteisistä sähköisen asioinnin tukipalveluista.
Tiedonhallintalaki **Laki julkisen hallinnon tiedonhallinnasta (906/2019)**	Laissa säädetään julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa. Laissa säädetään myös tietojärjestelmien yhteentoimivuuden toteuttamisesta. Laki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteentoimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta.
Digipalvelulaki **Laki digitaalisten palvelujen tarjoamisesta (306/2019)**	Laissa säädetään julkisen sektorin elinten verkkosivujen ja mobiilisovellusten saavutettavuudelle asetetuista minimitason vaatimuksista, saavutettavuuden toteutumisen valvonnasta ja viranomaisten velvoitteista liittyen digitaalisten palvelujen järjestämiseen yleisölle. Saavutettavuudella tarkoitetaan periaatteita ja tekniikoita, joita on noudatettava digitaalisten palvelujen suunnittelussa, kehittämisessä, ylläpidossa ja päivittämisessä, jotta ne olisivat paremmin käyttäjien, erityisesti vammaisten henkilöiden, saavutettavissa.
Hallintolaki (434/2002) ja laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)	Palveluväylän käyttöönottoprosessia ja poikkeusluvan myöntämistä koskeva yleishallinnollinen sääntely. Palveluväylän käyttöönotto on laajasti ymmärrettynä hallintoasia, jossa on noudatettava hyvän hallinnon vaatimuksia. Poikkeusluvan käsittely on julkisen vallan käyttöä, johon tulevat sovellettavaksi hallintomenettelyn vaatimukset (mm. asianosaisen kuuleminen, asian selvittäminen, päätöksen sisältövaatimukset ja perusteleminen, tiedoksianto ja muutoksenhaku).

Palvelinvarmenteisiin liittyvä lainsäädäntö: **EU asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla eIDAS setus, 910/2014)** **Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (tunnistuslaki, 617/2009)** **Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (VTVPL, 661/2009)**	Laissa säädetään osapuolten sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. Laki koskee Palveluväylässä osapuolten tunnistamiseen käytettyjä palvelinvarmenteita. Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista mahdollistaa VRK:n toimimisen varmennepalvelun tarjoajana.
Kansalliset sidosarkkitehtuurit, määräykset ja tukipalvelut	
Yhteentoimivuusalusta **https://yhteentoimiva.suomi.fi/**	Yhteentoimivuusalusta sisältää työkalut ja menetelmät yhteentoimivien tietosisältöjen määrittelyyn. Alusta koostuu tiedonhallinnassa tarvittavista sanastoista, koodistoista ja tietomalleista sekä näiden kuvaamiseen käytettävistä maksuttomista työvälineistä.
VAHTI-ohjeisto **https://www.vahtiohje.fi/**	Valtionhallinnon tietoturvallisuuden ohjeisto. Tietoturvaasetus 681/2010.
Digitaalisten palveluiden asiakaslähtöinen suunnittelu	Dokumentti kuvaa Suomi.fi-palvelukokonaisuuden arkkitehtuurin ja suunnitteluohjeet. Suomi.fi-palvelukokonaisuus sisältää yhteiset alustat ja tukipalvelut sähköisten asiointipalveluiden kehittämiseen ja järjestelmien väliseen tiedonvaihtoon. Suomi.fi-palveluväylä on yksi Suomi.fi-palvelukokonaisuuden palveluista.

2.7 Arkkitehtuuriperiaatteet

Suomi.fi-palveluväylään liitettävien palveluiden kehittämiseen ja ylläpitoon liittyvät keskeiset linjaukset on koottu arkkitehtuuriperiaatteiksi alla olevaan taulukkoon. Lisäksi palvelujen tuottajien ja hyödyntäjien tulee huomioida *Julkisen hallinnon yleiset arkkitehtuuriperiaatteet (JHKA)[1]*.

Nimi	Kuvaus
Suomi.fi-palveluväylä muodostaa hallitun palvelukokonaisuuden, jonka avulla organisaatioiden tietoaineistoja voidaan jakaa ja hyödyntää	Palveluväylä on palvelu, joka sisältää teknisen tiedonvälityksen lisäksi välttämättömät tekniset palvelut sekä ylläpidon ja valvonnan, joiden avulla sitä kautta voidaan jakaa kaikkea kansallista tietoa. Julkisen sektorin velvollisuudesta ja oikeudesta käyttää Palveluväylää säädetään KaPA-laissa.

Suomi.fi-palveluväylä tukee organisaatioiden välisten saumattomien palveluprosessien kehittämistä	Palveluväylää voidaan hyödyntää kytkemään prosesseja saumattomasti toisiinsa. Palveluväylä toimii prosessien edellyttämällä laadulla ja tasolla.
Suomi.fi-palveluväylä tarjoaa yhtenäisen tavan palveluiden julkaisuun, hyödyntämiseen ja löydettävyyteen	Palvelut julkaistaan liityntäkatalogiin, josta palvelukuvausten etsiminen ja niiden sisältöön tutustuminen on mahdollista.
Suomi.fi-palveluväylä on teknisesti hajautettu ja hallinnollisesti keskitetty, hallittu kokonaisuus, jossa vastuu palveluista on väylään kytkeytyvillä palveluntarjoajilla ja kokonaisuuden hallinnasta ja johtamisesta nimetyllä taholla	Palveluväylä tarjoaa vain yhtenäisen tavan tiedonvaihtoon. Vastuu palveluista on palveluntarjoajilla ja integraatiokanavasta sitä tarjoavalla organisaatiolla (esim. VRK).
Kaikki kansalliset organisaatiot voivat hyödyntää Palveluväylään kytkettyjä palveluja tietosuojan ja tietoturvan reunaehtojen puitteissa	Kaikki julkisen hallinnon ja yksityisen ja kolmannen sektorin toimijat voivat julkaista sisältöpalveluja ja hyödyntää muiden palveluja sovittujen käyttöperiaatteiden mukaisesti.
Suomi.fi-palveluväylä on vikasietoinen ja sen palvelutasotavoitteet voidaan sovittaa sitä käyttävien prosessien tarpeisiin	Palveluväylä tukee Liityntäpalvelinten klusterointia mahdollistaen Palveluväylän korkean käytettävyyden ja vikasietoisuuden. Palvelutasotavoitteiden lähtökohtana ovat toiminnan tarpeet. Palvelun vikasietoisuuden toteutus on palvelun tarjoajan vastuulla.
Suomi.fi-palveluväylää voidaan laajentaa ja skaalata kysynnän ja palvelujen kehittyessä	Liityntäpalvelin skaalautuu tehokkaasti tarvittavaan kuormaan Liityntäpalvelinten klusteroinnilla *[4]*. Palveluväylää voidaan myös laajentaa erillisten laajennuskomponenttien avulla (ks. luku 6.2).
Suomi.fi-palveluväylään kytkeytyvät organisaatiot voidaan tunnistaa luotettavasti	Palveluväylään kytketyt tunnistamista edellyttävät toimijat tunnistetaan kiistämättömästi ja luotettavasti luotetun kolmannen osapuolen myöntämien varmenteiden avulla (ks. https://en.wikipedia.org/wiki/Trusted_third_party).
Suomi.fi-palveluväylän kautta välitettävät tiedonsiirrot voidaan jäljittää luotettavasti	Palveluväylä sisältää mekanismin, jonka avulla voidaan kiistattomasti jäljittää sen kautta välitetyn viestin metatiedot sekä varmentaa viestin muuttumattomuus
Suomi.fi-palveluväylä kestää muutosta	Palveluväylä on toteutettu rakenteisesti siten, että siihen voidaan hallitusti tuoda uusia ominaisuuksia ja ratkaisuja vaiheittain - sen arkkitehtuuri on pitkäikäinen. Palveluväylän rakenteet on jäsennetty sellaisiin kokonaisuuksiin, joissa muutokset voidaan kohdistaa rajattuihin osiin.
Suomi.fi-palveluväylä välittää erilaisia viestisisältöjä	Palveluväylän avulla voidaan lähettää erilaisia viestisisältöjä, kuten tekstiä, asiakirjoja ja kuvia.
Suomi.fi-palveluväylän teknologia on toimittajariippumatonta	Palveluväylän tekninen ratkaisu perustuu avoimeen lähdekoodiin ja on toimittajariippumaton. Palveluväylän kehittämiseen ja ylläpitoon on saatavissa usean toimittajan tukea.
Suomi.fi-palveluväylän tulee mahdollistaa eri suojaustason tietojen välittäminen	Palveluväylän kautta voidaan välittää eri suojaustason tietoja sovittimien avulla (ks. esimerkki ST III -tason tietojen välittämisestä Palveluväylän kautta luvusta 5.5.3.).
Suomi.fi-palveluväylään voidaan tuottaa kansalliset liityntäpisteet kansainvälisiin palveluihin	Kerran Palveluväylään tuotetut palvelut ovat käytettävissä palveluväyläfederaation avulla muiden maiden toimijoille. Rajat ylittäviä palveluita on toteutettu esim. Viron kaupparekisterille.

2.8 Tietoturvaperiaatteet

Suomi.fi-palveluväylään liitettävän järjestelmän tietoturvatason tulee vastata järjestelmässä käsiteltyjen tietojen suojausluokitusta. Palveluväylän Liityntäpalvelin ja siihen kytkettyjen tietojärjestelmien hallinta ja tietoturvallisuus ovat liittyvien organisaatioiden vastuulla. Palveluväylän omistaja tai ylläpitäjä eivät vastaa mahdollisista Palveluväylän Liityntäpalvelinten huolimattomasta ylläpidosta tai käytöstä aiheutuvista tietoturvapoikkeamista, tietovuodoista tai käyttöhäiriöistä.

Palveluntarjoajan on määriteltävä palvelun hyödyntäjältä edellytettävä tietoturvataso palvelun käytöstä laadittavassa sopimuksessa tai käyttöehdoissa. Palvelun hyödyntäjän vastuulla on sopimuksessa määritellyn tietoturvatason edellyttämien vaatimusten täyttäminen.

Palveluväylä vastaa organisaatioiden välisestä tunnistamisesta. Palvelun hyödyntäjä vastaa digitaalista palvelua käyttävän loppukäyttäjän tunnistamisesta sekä tarvittaessa identiteetin välittämisestä palveluntarjoajalle.

Palveluväylä toteuttaa seuraavat tietoturvaperiaatteet:

Periaatteen nimi	Periaatteen kuvaus	Kuvaus toteutumisesta
Palveluväylä todentaa siihen liittyvät toimijat luotettavasti	Palveluväylän kautta kommunikoitaessa voidaan olla varmoja siitä, minkä tahon kanssa kommunikointi tapahtuu.	Palveluväylä todentaa toimijat luotetun tahon myöntämien varmenteiden avulla.
Palveluväylä välittää viestit perille luotettavasti	Kun viesti siirtyy Palveluväylään, voidaan olla varmoja viestin perillemenosta.	Palveluväylä perustuu synkroniseen tiedonsiirtoon. Viestin perillemenosta voidaan varmistua paluuviestin avulla.
Palveluväylä sietää tietoliikenneyhteyksissä esiintyviä katkoja	Palveluväylän toiminta ei halvaannu yksittäisen tietoliikennekomponentin vikaantuessa.	Palveluväylä on hajautettu eikä yksittäisten palvelinten tai tietoliikennekomponenttien vikaantuminen estä tiedonvaihtoa toimivien palvelinten ja tietoliikenneyhteyksien välillä. Palveluväylä tukee myös Liityntäpalvelinten ja näihin liittyvien verkkokomponenttien monistamista *[4]*.
Palveluväylän käytettävyystaso on korkea	Palveluväylän hyödynnettävyyteen voidaan luottaa.	Palveluväylä tukee Liityntäpalvelinten monistamista ja kuormantasausta *[4]*. Liityntäpalvelinten, palveluiden, kuormantasaajien ja tietoliikennekomponenttien monistamisella voidaan käytettävyys skaalata halutulle tasolle.
Palveluväylä ei heikennä siihen liittyvien järjestelmien tietoturvaa	Ratkaisun tarjoamien tiedonsiirtomekanismien tulee noudattaa valtionhallinnon tietoturvavaatimuksia (Valtionhallinnon tietoturvaohjeistukset) riippumatta siitä, onko kyseessä valtionhallinnon	Palveluväylä noudattaa omalta osaltaan valtionhallinnon tietoturvavaatimuksia. Vaatimukset on huomioitu jokaisessa vaiheessa määrittelystä käyttöönottoon. Väylän hyödyntäjien tulee kuitenkin erikseen huomioida

	sisäinen sanomaliikenteenne vai sanomaliikenne ulkoisiin sidosryhmiin. Tietoturva tulee ottaa huomioon jokaisessa vaiheessa määrittelystä käyttöönottoon.	tietoturvavaatimukset omissa toteutuksissaan.
Palveluväylä säilyttää viestien sisällön luottamuksellisuuden lähettäjän ja vastaanottajan välillä	Palveluväylän kautta tapahtuva viestien välitys ei näy ulkopuolisille toimijoille	Palveluväylän kautta tapahtuva tiedonsiirto on aina vahvasti salattua.
Palveluväylä takaa kuljettamiensa viestien muuttumattomuuden	Viestin vastaanottaja voi luottaa vastaanottamansa viestin paikkansapitävyyteen.	Palveluväylän kautta välitetyt sanomat allekirjoitetaan sähköisesti. Sanoman vastaanottava Liityntäpalvelin varmistaa allekirjoituksen avulla sanoman muuttumattomuuden.
Palveluväylä mahdollistaa viestien välityksen kiistämättömyyden tarkistamisen	Jälkeenpäin on mahdollista vahvistaa, että tietty viesti on lähetetty	Palveluväylä mahdollistaa viestien välityksen kiistämättömyyden tarkistamisen. Viestien allekirjoitusten, luotetun kolmannen tahon aikaleimauksen ja paluuviestin sisältämän pyynnön tiivisteen (hash) avulla voidaan jälkikäteen varmistua, että viesti on varmuudella lähetetty ja vastaanottava taho on tämän saanut ja käsitellyt. Palveluväylä tukee kaikkien viestien ja näiden allekirjoitusten lokitusta. Palveluväylän viestiloki aikaleimataan kolmannen osapuolen toimesta, millä varmistetaan viestilokin muuttumattomuus ja varmistetaan, että lokiin kirjatut viestit ovat tietyllä ajanhetkellä olleet varmuudella osapuolten hallussa.

2.12.2019

3 Toiminta-arkkitehtuurin arkkitehtuurikuvaukset

3.1 Konsepti

Suomi.fi-palveluväylä tarjoaa vakioidun tavan tietojen siirtoon organisaatioiden välillä mahdollistaen turvallisten palvelukokonaisuuksien rakentamisen kansalaisille, yrityksille ja viranomaisille. Palveluväylä sisältää myös liityntäkatalogin palveluiden löydettävyyden ja tietojen uudelleenkäytön helpottamiseksi.

Palveluväylä ei ole keskitetty väyläratkaisu vaan hajautettujen palveluiden muodostama kokonaisuus, jossa noudatetaan yhteisesti sovittuja toimintamalleja sopimusten ja viestien vaihdon osalta. Palveluiden hyödyntäminen perustuu aina palvelun tarjoajan ja sen hyödyntäjän väliseen sopimukseen.

Palveluväylän kehittämisestä vastaa Väestörekisterikeskus yhteistyössä Nordic Institute for Interoperability Solutionsin (NIIS) kanssa. Tarkemmin Palveluväylään liittyvät toimijat on kuvattu luvussa 3.3.

3.2 Suomi.fi-palvelut

Suomi.fi-palvelut ovat keskitetysti toteutettuja kansallisia yhteentoimivuuden palveluita. Alla on kuvattu lyhyesti kirjoitushetkellä (2019) olevat Suomi.fi-palvelut:

- **Suomi.fi-palveluväylä** tarjoaa vakioidun tavan siirtää tietoja niin yksityisten kuin julkistenkin organisaatioiden tietojärjestelmien välillä.
- **Suomi.fi-tunnistus** on julkishallinnon yhteinen tunnistuspalvelu, jota asiakasorganisaatiot voivat hyödyntää loppukäyttäjien tunnistamisessa omissa digitaalisissa palveluissaan.
- **Suomi.fi-valtuudet** -palvelun avulla voidaan tarkistaa henkilön tai yrityksen valtuudet asioida sähköisesti toisen henkilön tai edustamansa yrityksen puolesta.
- **Suomi.fi -palvelutietovaranto** on keskitetty tietovaranto, johon organisaatiot tuottavat tiedot tarjoamistaan palveluista ja asiointikanavista. Palvelujen kohderyhmänä voivat olla yksityishenkilöt, yritykset tai viranomaiset.
- **Suomi.fi-verkkopalvelu** tarjoaa asiakasorganisaatiolle mahdollisuuden saattaa omat rekisterinsä loppukäyttäjien ulottuville. Loppukäyttäjä voi nähdä omat tietonsa monista rekistereistä kootusti tunnistautumalla Suomi.fi-palveluun.
- **Suomi.fi-kartat** tarjoaa julkishallinnolle keskitetyn palvelun karttojen ja paikkatietojen hyödyntämiseen.
- **Suomi.fi-maksut** on verkkomaksamisen palvelu, joka mahdollistaa maksujen suorittamisen julkishallinnon organisaatioille turvallisesti niiden omissa digitaalisissa asiointipalveluissa.
- **Suomi.fi-viestit** tarjoaa julkishallinnolle keskitetyn, digitaalisen tavan viestiä kansalaisten ja yritysten kanssa. Palvelun kautta viranomainen voi lähettää viestinsä digitaalisesti riippumatta siitä, haluaako kansalainen/yritys viestinsä digitaalisesti vai perinteisenä paperipostina.

Katso lisätietoja Suomi.fi- palveluista Palveluhallinnan verkkosivulta https://palveluhallinta.suomi.fi.

3.3 Roolit ja toimijat

Väestörekisterikeskus kehittää Suomi.fi-palveluväylää yhteistyössä Nordic Institute for Interoperability Solutionsin (NIIS) kanssa. NIIS vastaa Palveluväylän käyttämän X-Road -teknologian ydinkomponenttien kehittämisestä. Väestörekisterikeskus puolestaan vastaa kehitystyön laadun varmistuksesta, tuotosten kansallisesta jakelusta, keskitettyjen komponenttien palvelutuotannosta ja Palveluväylän asiakkaiden neuvonnasta.

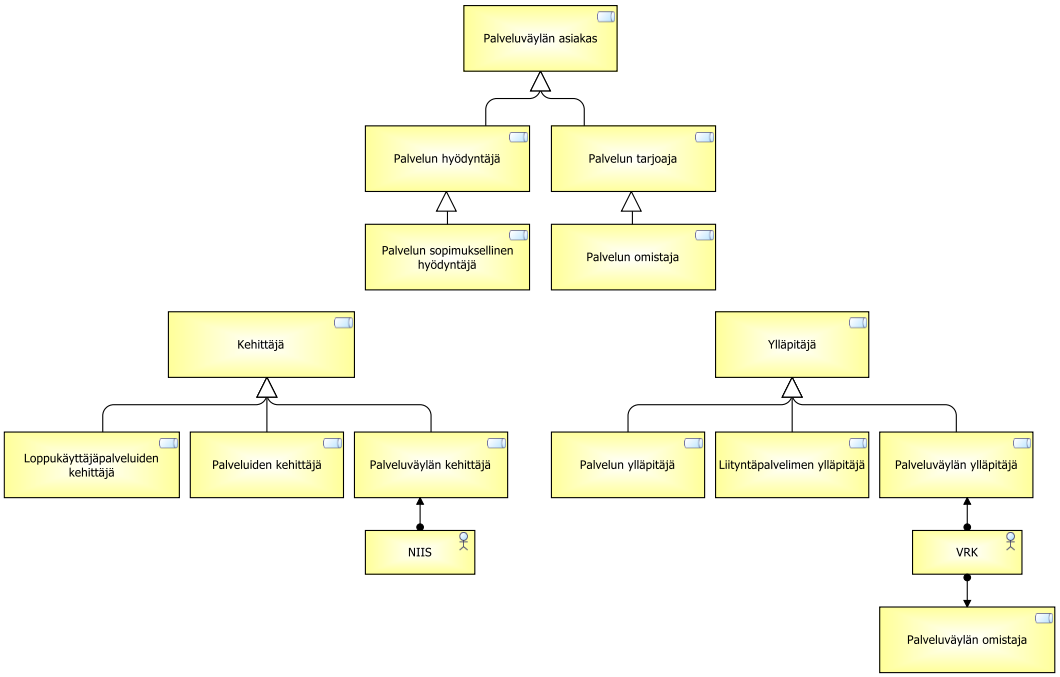
Palveluväylään liittyvät rooli on kuvattu alla olevassa taulukossa.

Rooli	Kuvaus
Palveluväylän asiakas	Palveluväylän asiakas tarkoittaa Palveluväylän palveluun liittyvää organisaatiota. Asiakkaat voivat olla palvelun hyödyntäjiä ja/tai tarjoajia.
Loppukäyttäjä	Loppukäyttäjä on digitaalisten palveluiden käyttäjät, joille Palveluväylän ei pitäisi näyttäytyä muuten kuin palvelunäkymien ja muiden käyttöliittymien kautta tarjottavien palveluiden mahdollistajana. Loppukäyttäjä voi olla esim. viranomaispalvelua käyttävä kansalainen.
Palvelun hyödyntäjä	Palvelun hyödyntäjä on Suomi.fi-palveluväylän kautta liityntöjä (tietovarantoa tai palvelua) hyödyntävä organisaatio. Hyödyntäjiä voivat olla esim. julkishallinnon virastot ja kunnat, jotka hyödyntävät Palveluväylään kytkettyjä yleisiä palveluita. Palvelun hyödyntäjä voi käyttää palvelua itse omistamissaan palveluissaan tai hyödyntäjä voi olla sopimuksellinen hyödyntäjä.
Palvelun sopimuksellinen hyödyntäjä	Palvelun omistaja tekee kahdenkeskisen sopimuksen palvelu sopimuksellisen hyödyntäjän kanssa. Palvelun hyödyntäjä ei välttämättä vastaa itse palvelua hyödyntävästä palvelusta ja tämän kehittämisestä. Esim. Kuntaliitto voi tarjota kunnalle Suomi.fi-palveluväylän palvelua hyödyntävän loppukäyttäjäpalvelun. Loppukäyttäjäpalvelun omistaja ja kehittäjä sekä Suomi.fi-palveluväylän palvelun hyödyntäjä on Kuntaliitto. Palvelun käyttösopimus tehdään kuitenkin kunnan kanssa, joten sopimuksellinen hyödyntäjä on kunta.
Palvelun tarjoaja	Palvelun tarjoaja on Suomi.fi-palveluväylän kautta liityntöjä (tietovarantoa tai palvelua) tarjoava organisaatio. Palvelun voi tarjota suoraan palvelun omistaja tai omistajan puolesta toinen organisaatio (esim. Kuntaliitto), joka vastaa palvelun tuottamisesta, mutta ei ole sopimuksellinen osapuoli palvelun käytössä.
Palvelun omistaja	Palvelun omistaja tekee kahdenkeskisen sopimuksen palvelun sopimuksellisen hyödyntäjän kanssa palvelun käytöstä ja on vastuussa palvelun sopimuksenmukaisesta toiminnasta ja käytettävyydestä. Esimerkkinä VRK tarjoaa palvelun omistajana väestötietojärjestelmän palveluja hyödyntäjien käyttöön.
Palveluväylän omistaja / toimittaja	Palveluväylän omistaja tai toimittaja tarkoittaa Suomi.fi-palveluväylän omistajaa eli Väestörekisterikeskusta.

Kehittäjä	Kehittäjä voi olla Suomi.fi-palveluväylän kautta tarjottavien palveluiden kehittäjä tai kehittää palveluita, jotka hyödyntävät näitä palveluita.
Palveluiden kehittäjä	Palveluiden kehittäjä rakentaa Suomi.fi-palveluväylän kautta tarjottuja palveluita ja tietovarantoja palvelun hyödyntäjien tarpeisiin.
Loppukäyttäjäpalveluiden kehittäjä	Loppukäyttäjäpalveluiden kehittäjä rakentaa palveluita loppukäyttäjien tarpeisiin hyödyntäen toteutuksissaan Suomi.fi-palveluväylään liitettyjä palveluita ja tietovarantoja.
Palveluväylän kehittäjä	Palveluväylän kehittäjä vastaa Palveluväylän X-road -teknologiaan pohjautuvien ydinkomponenttien kehittämisestä. Palveluväylän kehittäjänä toimii nykyisin Nordic Institute for Interoperability Solutionsin (NIIS).
Ylläpitäjä	Ylläpitäjä vastaa palveluiden, viestinvälityksen ja ajoympäristöjen toimivuudesta, asetuksista ja käytön periaatteista.
Palvelun ylläpitäjä	Palvelun ylläpitäjä vastaa Suomi.fi-palveluväylään liitetyn palvelun ja ajoympäristön toiminnasta ja asetuksista.
Liityntäpalvelimen ylläpitäjä	Liityntäpalvelimen ylläpitäjä vastaa Suomi.fi-palveluväylän Liityntäpalvelimen toiminnasta ja asetuksista. Liityntäpalvelimen ylläpitäjänä voi toimia esim. Valtori.
Palveluväylän ylläpitäjä	Suomi.fi-palveluväylän keskitettyjen asetusten ja palveluiden ylläpidosta vastaava taho. Vastaa mm. keskus- ja konfiguraatio palvelinten ylläpidosta ja Palveluväylän yleisestä toiminnasta ja periaatteista. Nykytilanteessa Palveluväylän toiminnasta vastaa VRK.

Roolien keskinäiset hierarkiasuhteet on esitetty alla olevassa kaaviossa.

2.12.2019

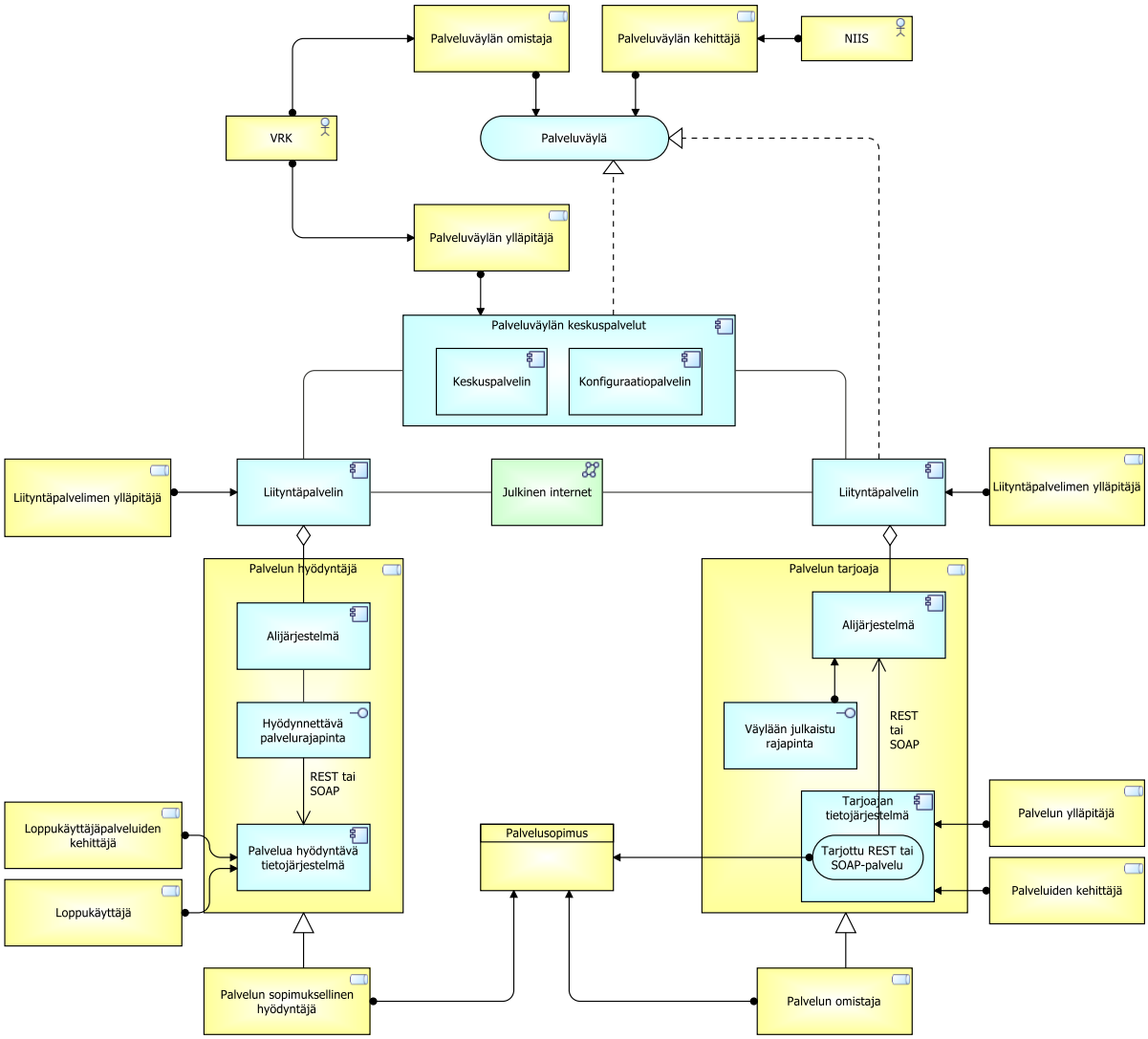


Kuva 1 - Roolihierarkiat

Jokaisella roolilla on oma vastuualueensa Palveluväyläkokonaisuudessa. Palveluväyläkokonaisuudella tarkoitetaan tässä yhteydessä Palveluväylästä ja tähän liitetyistä palveluista ja asiakasjärjestelmistä koostuvaa kokonaisuutta.

Roolien vastuualueet on kuvattu alla olevassa kaaviossa. Kaavio kuvaa miten roolien vastuut jakaantuvat Palveluväyläkokonaisuuden eri osien kesken. Palveluväylän rakenne on kuvattu tarkemmin luvussa 5.2.

2.12.2019



Kuva 2 - Roolien vastuualueet

3.4 Prosessit

Palveluväylä ei toteuta varsinaisia substanssiprosesseja. Palveluväylän hallintaprosessit on kuvattu käyttöönoton prosessikuvauksessa *[31]*. Prosessikuvaus sisältää seuraavat vaiheet:

- Aloitus
- Tekninen suunnittelu
- Toteutus
- Testaaminen ja viimeistely
- Tuotantokäyttö
- Ylläpito

2.12.2019

4 Tietoarkkitehtuurin arkkitehtuurikuvaukset

4.1 Käsitteistö

Palveluväylän käsitteet ja termit on kuvattu *Palveluväylän sanastossa [11]*. Tässä dokumentissa käytetyt termit ja lyhenteet on kuvattu luvussa 7.

4.2 Sopimukset

Suomi.fi-palveluväylän omistajana ja ylläpitäjänä toimii VRK, jolta Palveluväylään liittyjä hakee käyttölupaa käyttöönottoprosessin mukaisesti (ks. *Suomi.fi-palveluväylä - Käyttöönoton prosessi [31]*). Käyttölupa antaa osapuolelle luvan viestiä toisen osapuolen kanssa (tarjoaja-hyödyntäjä). Käyttölupaan liittyy allekirjoitusvarmenne, jolla osapuolten väliset viestit allekirjoitetaan ja jonka perusteella voidaan varmistua käyttöluvan voimassaolosta. Tämän lisäksi palvelun tarjoaja ja hyödyntäjä tekevät tyypillisesti keskenään palvelusopimuksen, jossa voidaan esimerkiksi rajata käyttöoikeus vain tiettyihin palveluntarjoajan tarjoamiin palveluihin.

4.3 Palvelurajapintojen tietomallinnus ja julkaisu liityntäkatalogiin

Palveluväylään julkaistavien palveluiden suunnittelussa on suositeltavaa käyttää Suomi.fi-yhteentoimivuusalustan työkaluja ja kuvausmenetelmää (https://yhteentoimiva.suomi.fi *[15]*). Yhteentoimivuusalusta sisältää työkalut ja menetelmät yhteentoimivien tietosisältöjen määrittelyyn. Alusta koostuu tiedonhallinnassa tarvittavista sanastoista, koodistoista ja tietomalleista sekä näiden kuvaamiseen käytettävistä maksuttomista työvälineistä. Alustalla organisaatio voi helposti käyttää valmiita koodistoja ja tietomalleja omien tietokuvausten pohjana ja jakaa tuotoksiaan muille osapuolille.

Palveluväylään julkaistun palvelurajapinnan käyttämä skeema on suositeltavaa toteuttaa Yhteentoimivuusalustalle kuvatun tietomallin pohjalta. Rajapinnan arvojoukkojen määrittelyssä on suositeltavaa hyödyntää Yhteentoimivuusalustan koodistoja. Tietomallit ja koodistot pohjautuvat yleensä Yhteentoimivuusalustalle kuvattuihin yleisiin ja alakohtaisiin sanastoihin.

Yhteentoimivuusalustan tietomalleja voidaan hyödyntää myös geneeristen palvelurajapintojen tuottamisessa. Palvelu voi tarjota esim. Alustalle kuvattuun tietomalliin pohjautuvan yleisen hakupalvelun, jossa palautettavat tiedot määräytyvät palvelun hyödyntäjän määrittelemien tietomallia noudattavien hakuehtojen mukaisesti. Alustan tietomallista voidaan johtaa esim. GraphQL:n mukaiset skeemat geneerisiä tiedon haku- ja hallintapalveluita varten.

Palvelun tarjoajan vastuulla on julkaista palvelukuvauksensa liityntäkatalogiin, josta palvelun hyödyntäjä saa sen käyttöönsä. Liityntäkatalogissa kuvataan kaikki Suomi.fi-palveluväylän tuotantoympäristöön liittyneet organisaatiot ja organisaatioiden tarjoamat palvelut. Liityntäkatalogi on tehty helpottamaan erityisesti palveluiden löydettävyyttä. Sen kautta pääsee näkemään helposti mitä palveluita Palveluväylän kautta on tarjolla ja ketkä niitä ylläpitävät.

Suomi.fi-palveluväylään liittyneet organisaatiot ja organisaatioiden tarjolla olevat palvelut haetaan liityntäkatalogiin automaattisesti Liityntäpalvelimilta. Käyttöönottavien organisaatioiden yhteyshenkilöiden velvollisuus on organisaationsa yhteystietojen, sekä palveluun liittyvien hallinnollisten tietojen täyttäminen Liityntäkatalogin hallintasivuston kautta.

Liityntäkatalogin lisäksi palvelukuvaukset ovat saatavilla Liityntäpalvelimen tarjoamien metapalveluiden kautta. Metapalveluiden kautta voidaan hakea Palveluväylään liittyneet organisaatiot, näiden tarjoamat palvelut ja palveluiden tekniset rajapintakuvaukset. Liityntäpalvelimen metapalvelut on kuvattu tarkemmin *Suomi.fi-palveluväylä –Metapalvelut [16]* -verkkosivulla.

Avoimen datan palvelut ovat julkisia ja vapaasti erilaisten organisaatioiden hyödynnettävissä. Tämän vuoksi avoimen datan palveluita ei ole yleensä tarpeen julkaista Palveluväylään. Palveluväylään julkaistuihin palveluihin voi kuitenkin liittyä avointa dataa, kuten koodistoja ja arvojoukkoja. Tällaiset koodistot ja arvojoukot voi olla hyödyllistä julkaista Palveluväylään, jolloin palvelun hyödyntäjä saa kaikki tiedot samalla tavalla yhdestä paikasta.

4.4 Lokitiedot

Palveluväylän toimijat vastaavat järjestelmiensä lokisisällöstä pääsääntöisesti itsenäisesti heille lainsäädännön ja muiden säännösten asettamalla tavalla. Palveluväylä ei ota kantaa, miten tietoa tulee järjestelmissä käsitellä ja mitä vaatimuksia käsittelyyn mahdollisesti liittyy. Esim. tietovarantojen ja tietojärjestelmien omistajilla on usein vastuu tuottaa käyttölokia (audit trail) tietojen käsittelystä, esim. kuka on mitäkin tietoa hakenut tai muuttanut. Palveluväylä ei ratkaise tämän kaltaisia järjestelmien sisäisiä lokitustarpeita, vaan sen rooli lokituksessa rajoittuu tiedonsiirtoon järjestelmien välillä.

Palveluväylän lokituksen keskeisimpiä tavoitteita on tarjota riittävä todistusaineisto tiedonsiirron kiistämättömyyden varmistamiseksi. Kiistämättömyyden tavoitteena on, ettei mikään tiedonsiirron osapuoli voi myöhemmin kiistää osallisuuttaan tapahtuneeseen tiedonsiirtoon.

Liityntäpalvelin sisältää seuraavat kolme lokia:

- **Sanomaloki** sisältää Liityntäpalvelimen kautta välitetyt sanomat ja tiedonsiirron kiistämättömyyden varmistamiseen tarvittavat tiedot. Kiistämättömyyttä varten sanomalokiin tallentuu sanoman sisällön lisäksi kaikki otsikkotiedot (metatiedot), sanoman lähettäjän allekirjoitus ja sanoman aikaleimaajan allekirjoitus. Sanomalokin sanomat aikaleimataan luotetun kolmannen osapuolen aikaleimauspalvelun avulla.

  Sanomalokilla on keskeinen rooli tiedonsiirron kiistämättömyyden varmistamisessa. Koska vastaussanoma sisältää otsikkotiedoissa pyyntöviestin tiivisteen, vahvistaa vastapuoli allekirjoituksellaan vastauksen lisäksi myös pyynnön sisällön. Allekirjoituksen avulla voidaan siis kiistämättömästi myöhemmin todistaa, että palvelun hyödyntäjä on sanoman lähettänyt ja sen on palvelu muuttumattomana vastaanottanut ja lähettänyt siihen sanomalokiin kirjatun vastauksen. Aikaleimaamisen avulla voidaan varmistaa sanomalokiin kirjattujen sanomien muuttumattomuus ja että sanoma on tietyllä ajanhetkellä ollut varmuudella osapuolten hallussa.

  Sanomalokin sisältö riippuu Liityntäpalvelimen asetuksista. Asetuksissa voidaan määritellä mm. lokitetaanko sanomalokiin pelkät otsikot (metatiedot) vai myös sanomien sisällöt (ks. lisätietoja sanomalokin asetuksista *System Parameters User Guide [13]* ohjeesta). *RFC3161-standardiin [*14*]* pohjautuvan sanomalokin aikaleimauksen toteutustapa on kuvattu tarkemmin arkkitehtuurimäärittelyssä *X-Road Security Architecture [*5*]*.

- **Käyttöloki** (audit trail) on Palveluväylän hallintakäyttöliittymän kautta tehtyjen tilamuutosten ja asetusten muutosloki. Liityntäpalvelimen käyttöloki kohdistuu liityntäpalvelimen tila- ja asetustietoihin, eikä sitä tule sekoittaa palveluiden ja asiakasjärjestelmien käyttölokeihin. Ks. lisätietoja käyttölokista *Security Server User Guide [12]* -ohjeesta.
- **Järjestelmäloki** on Liityntäpalvelimen tekninen tapahtumaloki, joka sisältää liityntäpalvelimen eri komponenttien kirjaamat tekniset tapahtumat, kuten virhetilanteet. Ks. lisätietoja järjestelmälokista *Security Server User Guide [12]* -ohjeesta.

5 Tietojärjestelmäarkkitehtuurin kuvaukset

5.1 Palveluväylän tietojärjestelmäpalvelut

Alla oleva kaavio esittää Palveluväylään liittyvät palvelut ja tietokokonaisuudet. Sovelluskomponenteittain kuvatut Palvelut käsittävät sekä Palveluväylän tarjoamat että Palveluväylän käyttämät luotettujen kolmannen osapuolten tarjoamat palvelut.

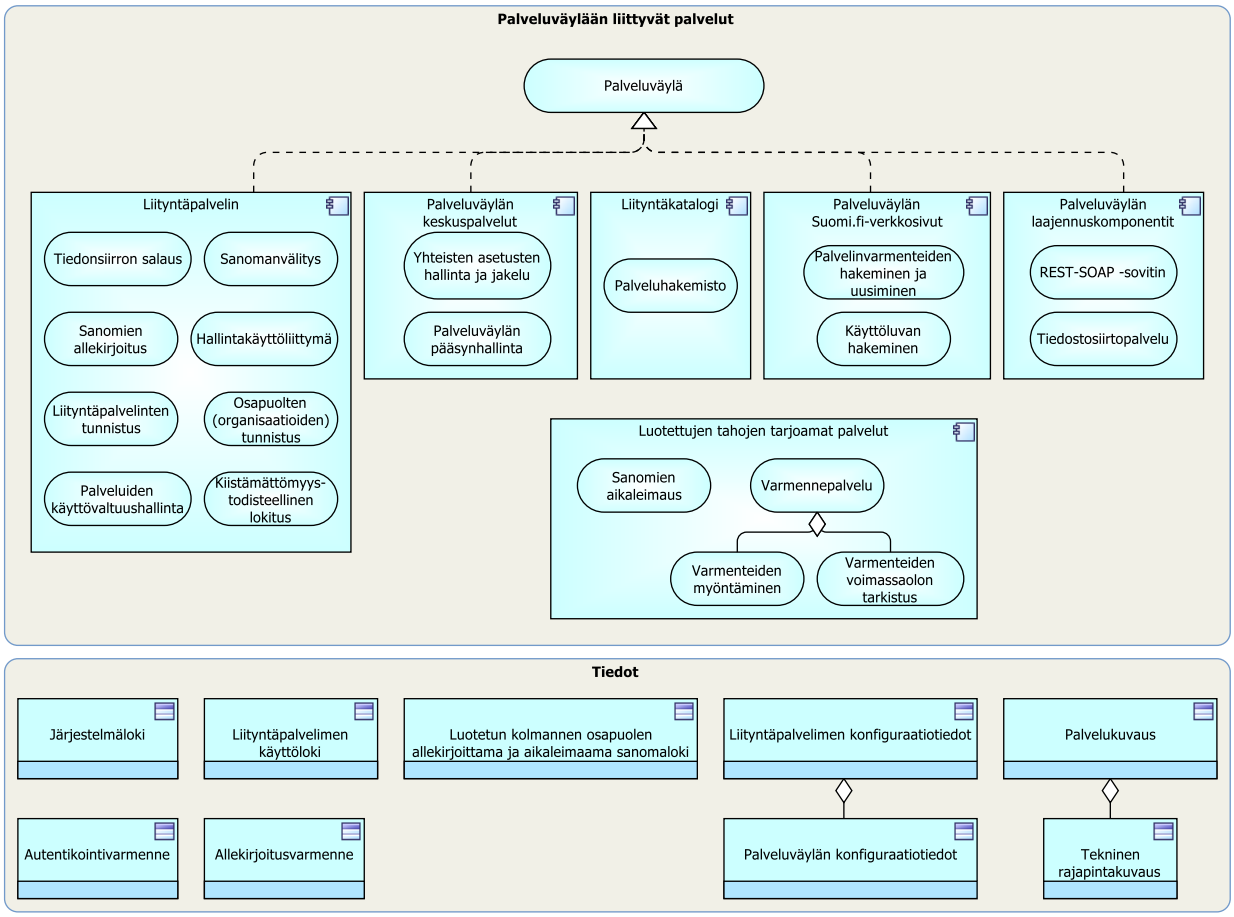
Liityntäpalvelin toteuttaa valvonnan, hallinnan ja viestinnän kiistämättömyyden kannalta oleelliset lokit. Lokien sisällöt on kuvattu luvussa 4.4.

Palveluväylässä viestintään käytetään autentikointi- ja allekirjoitusvarmenteita. Autentikointivarmenne on Liityntäpalvelinkohtainen varmenne, jolla liityntäpalvelimet tunnistavat toisensa ja jota käytetään Liityntäpalvelinten välisten yhteyksien salaamiseen. Allekirjoitusvarmenne on organisaatiokohtainen varmenne, jota käytetään palvelun omistajan ja sopimuksellisen hyödyntäjän tunnistamiseen ja Palveluväylän kautta lähetettyjen sanomien allekirjoittamiseen.

Liityntäpalvelimen konfiguraatiotiedot käsittävät sekä paikallisesti Liityntäpalvelimella hallittavat asetukset että keskitetysti Keskuspalvelimella hallittavat kaikille Liityntäpalvelimille yhteiset Palveluväylän konfiguraatiotiedot (ks. luku 5.6).

Palveluväylään julkaistut palvelut kuvataan Liityntäkatalogissa, jota on käsitelty tarkemmin luvussa 4.3.

Palveluväylään on tarjolla erilaisia laajennuskomponentteja. Kaavioon näistä laajennuksista on poimittu REST-SOAP -sovitin ja tiedostosiirtopalvelu. Laajennuskomponentit on kuvattu luvussa 6.2.



Kuva 3 – Palveluväylän palvelut ja tietokokonaisuudet

5.2 Järjestelmäarkkitehtuurin yleiskuva

Alla oleva arkkitehtuurikuva esittää Suomi.fi-palveluväylän rakennetta. Palvelun tarjoaja sekä hyödyntäjä integroituvat Liityntäpalvelinten kautta toisiinsa. Tarjottavan palvelun rajapinta julkaistaan Liityntäkatalogiin ja Liityntäpalvelimen alijärjestelmään. Sama Liityntäpalvelin voi palvella useita eri organisaatioita ja näiden alijärjestelmiä. On suositeltavaa, että organisaatiolla on yksi alijärjestelmä sen jokaista asiakasjärjestelmää kohden. Palvelun käyttöoikeuksien määrittely tapahtuu aina alijärjestelmäkohtaisesti, joten näin menetellen oikeudet palveluun voidaan määritellä asiakasjärjestelmäkohtaisesti.

Palvelun hyödyntäjät voivat hakea palveluita Liityntäkatalogista. Liityntäkatalogi sisältää palvelun yleisten tietojen lisäksi palvelun tarkan teknisen rajapintakuvauksen, jota palvelun hyödyntäjä tarvitsee palvelun käyttöön.

Organisaatiot ja liityntäpalvelimet tunnistetaan luotetun kolmannen tahon myöntämien varmenteiden avulla. Varmenteiden voimassaolo varmistetaan varmenteen myöntäjän tarjoaman OCSP-palvelun avulla. Liityntäpalvelin aikaleimaa palvelimen lähettämät ja vastaanottamat viestit niiden muuttumattomuuden varmistamiseksi luotetun kolmannen osapuolen tarjoaman aikaleimapalvelun avulla. Sallitut varmenteiden myöntäjät ja aikaleimapalvelun tarjoajat on määritelty Palveluväylän konfiguraatiotiedoissa. Palveluväylän konfiguraatiotiedot sisältävät näiden lisäksi tiedot kaikista Palveluväylään liitetyistä Liityntäpalvelimista, niitä käyttävistä organisaatioista ja Liityntäpalvelinten keskitetysti hallittavista asetuksista.

2.12.2019

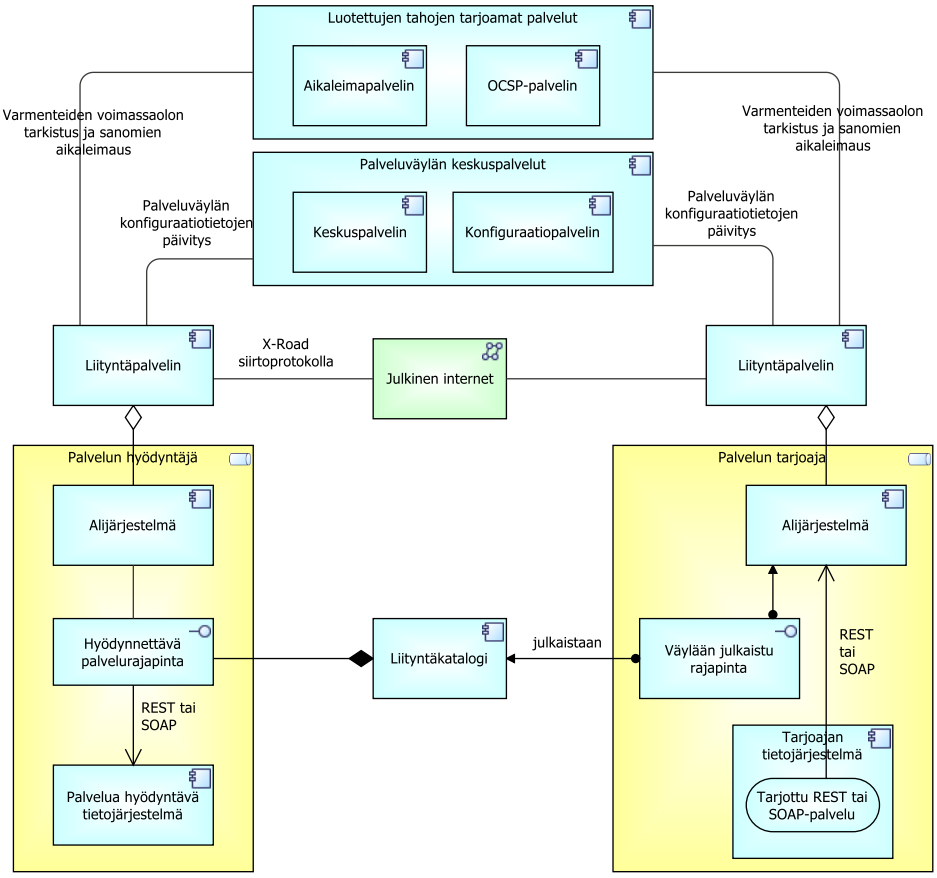
Konfiguraatiotiedot tallennetaan säännöllisesti päivittyvinä paikallisina kopioina jokaiselle liityntäpalvelimelle joko suoraan keskuspalvelimelta tai tämän välimuistina (tiedonsiirron puskurina) toimivalta konfiguraatiopalvelimelta. Paikallisen kopion ansiosta Liityntäpalvelinten ei tarvitse olla yhteydessä keskuspalveluihin sanomien lähetyksen yhteydessä.

Palveluväylään julkaistu palvelu voi olla joko REST- tai SOAP-palvelu. Molempien osalta palveluiden rajapinnat viestisisältöjen skeemoineen tulee kuvata huolellisesti. Palveluiden toteutustavalla (REST vai SOAP) ei ole yleensä merkittävää eroa työmääriin. Alun perin muuta kuin Palveluväylää varten toteutetun REST-palvelun julkaiseminen Palveluväylään on kuitenkin yleensä helpompaa kuin muuhun käyttöön toteutetun SOAP-palvelun. Asiaa on käsitelty tarkemmin luvussa 5.5.4.

Palveluväylä huolehtii tietojen välittämisestä, mutta se ei ota tarkemmin kantaa pyyntö- ja vastausviestien sisältöön. Se ei sisällön osalta esimerkiksi edellytä tai tarkista tarkkojen REST-periaatteiden noudattamista. Esimerkiksi tiedonhakupalvelu voi pohjautua HTTP-protokollan GET-pyynnön sijaan POST-pyyntöön. Tämä mahdollistaa perinteisten REST-palveluiden lisäksi modernimmat ja monikäyttöisemmät palvelutoteutukset. Palvelurajapinta voi pohjautua esimerkiksi GraphQL-kieleen.

X-Road-instanssit, kuten Suomi.fi-palveluväylä ja Viron X-Road-asennus, tukevat federointia. X-Road-instanssien federointi mahdollistaa viestinvälityksen instanssien välillä. Federointi määritellään Keskuspalvelimilla. Esim. Suomen Palveluväylän Keskuspalvelimelle on määritelty federointituki Viron X-Road-instanssiin rajat ylittävää viestinvälitystä varten. Jotta Liityntäpalvelin voisi käyttää Keskuspalvelimen tukemia muita X-Road-instansseja, tulee nämä instanssit vielä erikseen määritellä Liityntäpalvelimen asetuksissa. Pääsyä muihin X-Road-instansseihin hallitaan siis sekä keskitetysti että paikallisesti Liityntäpalvelimen asetuksissa.

Lisätietoja teknisestä ratkaisusta ja arkkitehtuurista, ks. *X-Road Security Architecture. Nordic Institute for Interoperability Solutions (NIIS) [5]*. Tiedonsiirtoprotokolla palvelunhyödyntäjän tai -tuottajan tietojärjestelmästä Liityntäpalvelimelle on kuvattu REST-palveluille *X-Road: Message Protocol for REST [8]* -määrittelyssä ja SOAP-palveluille *X-Road: Message Protocol [7]* -määrittelyssä. Liityntäpalvelimien välinen tiedonsiirtoprotokolla on kuvattu *X-Road: Message Transport Protocol [6]* määrittelyssä.



Kuva 4 – Arkkitehtuurin yleiskuva

5.3 Palveluväylän palvelut

Palveluväylän palvelut on kuvattu *Liityntäkatalogissa [25]*. Kirjoitushetkellä (Marraskuu 2019) Suomen Palveluväylään on liittynyt 134 organisaatiota, joilla on Palveluväylään määriteltynä 314 alijärjestelmää. Liityntäkatalogin lisäksi palveluita voi hakea Liityntäpalvelimen metapalveluiden avulla (ks. luku 4.3).

Ajantasaiset Palveluväylän käyttäjätilastot ovat saatavissa X-Roadin statistiikkapalvelusta (*X-Road Simple Statistics API [24]*).

5.4 Palveluiden suunnittelun periaatteita

Alla on listattu yleisiä periaatteita ja ohjeita palveluiden suunnitteluun:

- **Palveluiden autonomisuus:** Palvelun tulisi pääsääntöisesti toteuttaa yksittäisen, rajatun toiminnallisuuden, jolla ei ole riippuvuuksia muihin Palveluväylän palveluihin. Laajemman liiketoimintalogiikan toteuttaminen on palvelun hyödyntäjän vastuulla.
- **Transaktionaaliset palvelut:** Palveluväylä ei tarjoa tukea transaktioiden hallintaan, vaan se on palvelun tarjoajan ja hyödyntäjän vastuulla. Palvelun suunnittelussa tulisi huomioida transaktioiden hallinnan kannalta oleelliset kompensaatiomallit, joita palvelun hyödyntäjät voivat käyttää laatiessaan transaktionaalisuutta edellyttäviä palveluketjuja.
- **Koostetut palvelut:** Palvelu voi yhdistää useita, toisiinsa liittyviä tietovarantoja yhden atomisen palvelurajapinnan taakse. Tyypillisiä esimerkkejä koostetulle palvelulle on, kun eri

hallinnon tasoilla ylläpidetään rinnakkaisia rekistereitä. Tällöin ei voida olettaa palvelun hyödyntäjän tuntevan eri rekistereitä ylläpitäviä tahoja tai ylläpitologiikkaa koostaakseen palvelun itse. Koostetun palvelun tuottaminen edellyttää hallintamallista sopimista rekisterinpitäjätahojen kesken. Suositeltavaa on, että koostepalvelusta vastaa jokin keskitetty julkinen taho.

- **Palveluiden versionhallinta:** Palveluväylä tukee palveluiden eri versioiden samanaikaista tarjoamista. Liitettävien palveluiden versionhallinta ja palvelukutsujen välittäminen oikeaan versioon on palvelun tarjoajan vastuulla.

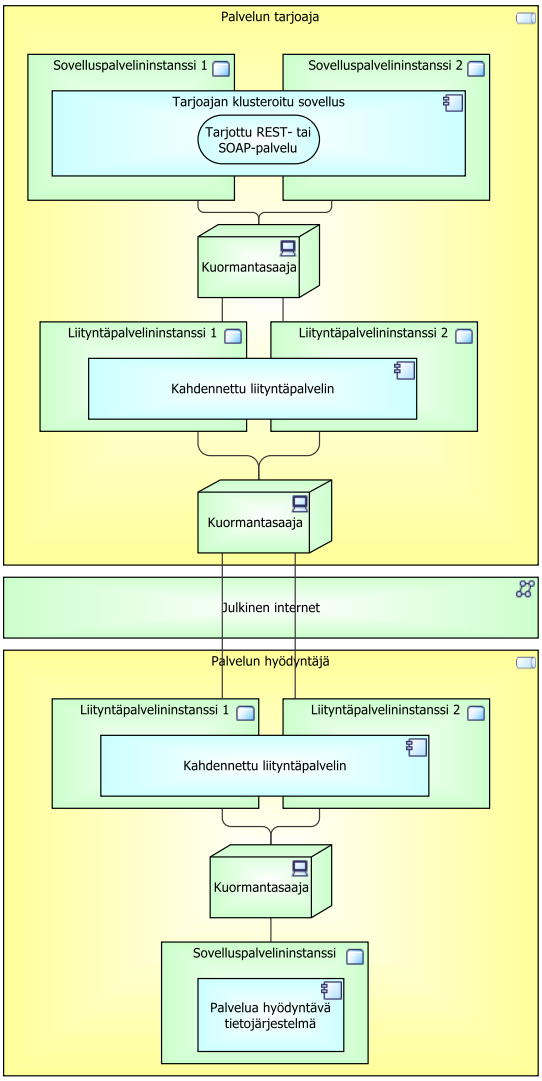
5.5 Palveluväylän käyttösuositukset

Seuraavissa aliluvuissa on kuvattu Palveluväylän käyttösuositukset liittyen suorituskyvyn ja luotettavuuden parantamiseen, palomuurien käyttöön, turvaluokitellun tiedon välittämiseen, monikanavajulkaisuun ja sovitinpalveluiden käyttöön.

5.5.1 Palveluväylän palveluiden suorituskyvyn ja luotettavuuden parantaminen

Palveluväylän ja tähän liitettyjen palveluiden suorituskykyä ja saatavuutta (availability) voidaan parantaa palveluiden ja palvelinten monistamisella (klusteroinnilla). Liityntäpalvelin- ja palveluinstanssit on mahdollista kahdentaa alla olevan kaavion mukaisesti (instansseja voidaan monistaa tarvittu määrä eli myös kahta enemmän). Kuorman tasaaminen kahdennettujen Liityntäpalvelininstanssien ja palveluinstanssien välillä hoidetaan ulkoisella kuormantasaajalla.

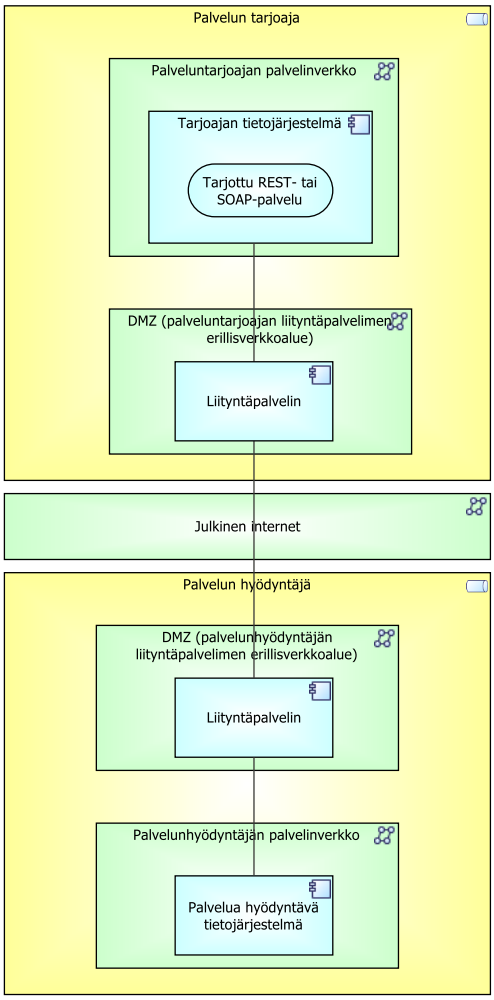
Kuormantasaajan käyttö ja instanssien monistaminen mahdollistavat palvelun käyttäjämäärän kasvattamisen ja vasteaikojen parantamisen. Lisäksi kuormantasaajan avulla järjestelmä toimii aikaisempaa paremmin myös mahdollisissa vikatilanteissa. Kuormantasaaja poistaa vikaantuneen liityntäpalvelimen (tai palveluinstanssin) käytöstä (liikennettä ei enää ohjata sille) ja liikenne ohjautuu muille, toiminnassa oleville liityntäpalvelimille (tai palveluinstanseille). Kuormantasaajan käyttö on kuvattu tarkemmin *Suomi.fi-palveluväylä – Ulkoisen kuormantasaajaan käyttäminen palveluväylässä [4]* -ohjeessa.



Kuva 5 – Liityntäpalvelinten ja palveluiden kahdennus

5.5.2 Palomuurisuositukset

Alla olevassa kaaviossa on kuvattu palomuurien avulla toteutettavat verkkojen eristämissuositukset. Liityntäpalvelin on suositeltavaa sijoittaa kaavion mukaisesti omalle DMZ-vyöhykkeelle eli erottaa sekä julkisesta Internetistä että muusta palvelinverkosta. Liityntäpalvelimelta ei tulisi olla pääsyä Liityntäpalvelimelle julkaistun palvelun käyttämiin palveluihin. On myös suositeltavaa, ettei Palveluväylään julkaistuun palveluun anneta pääsyä muuta kuin Liityntäpalvelimen DMZ-vyöhykkeeltä, jollei palvelua ole julkaistu muihin kanaviin.



Kuva 6 – Palvelinverkkojen eristämissuositukset

5.5.3 Turvaluokitellun tiedon välittäminen Palveluväylässä

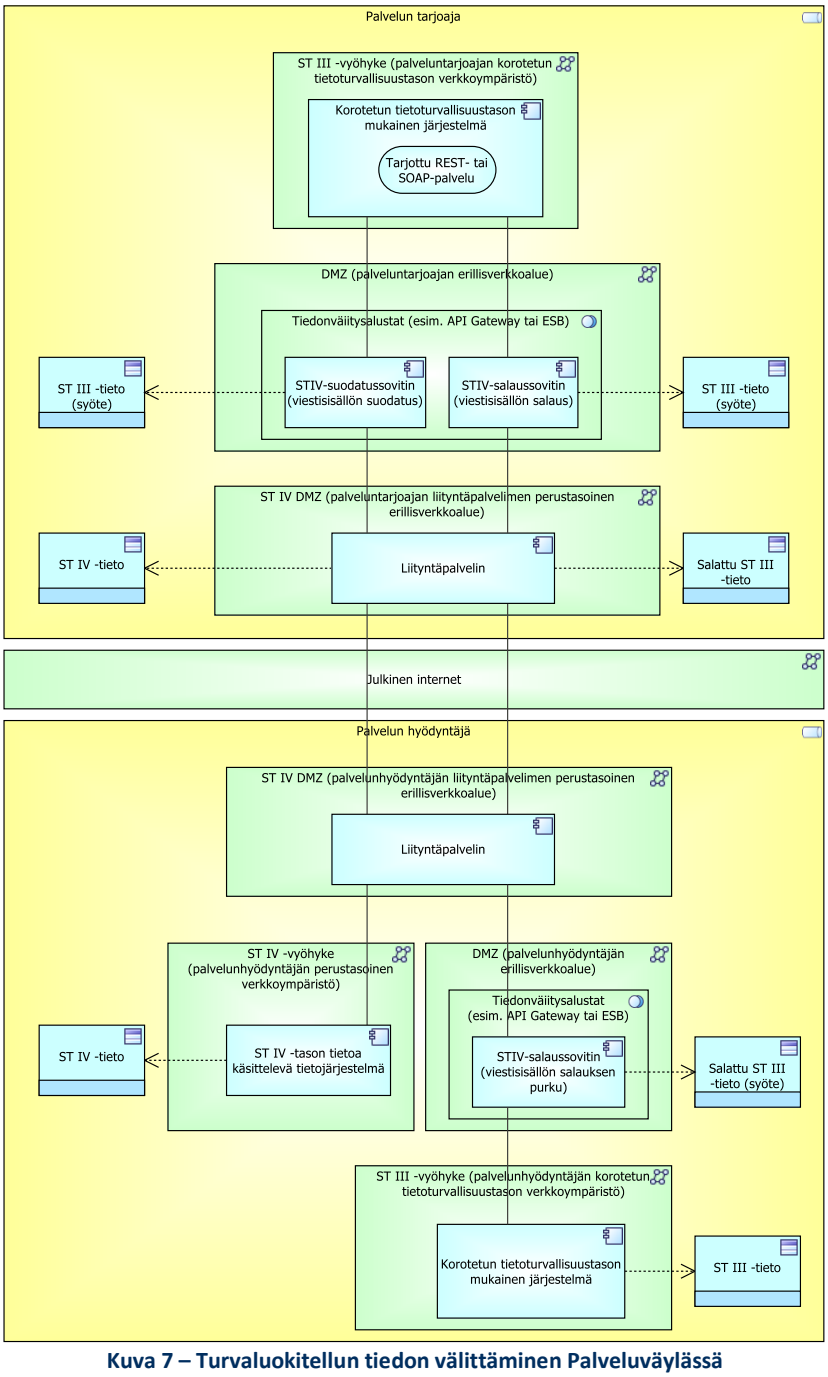
Alla olevassa kaaviossa on kuvattu, miten turvaluokiteltua tietoa voidaan välittää Palveluväylän kautta.

Kaaviossa vasemmalla puolella on kuvattu, miten ST III -tason tietoa käsittelevästä tietojärjestelmästä siirretään ST IV -tasoista tietoa Palveluväylän kautta ST IV -tasoista tietoa käsittelevään tietojärjestelmään. Liityntäpalvelimelta ei saa olla suoraa pääsyä ST III -tason tietoa käsittelevään korotetun tietoturvallisuustason tietojärjestelmään, vaan tiedon tulee kulkea erillisverkkoalueella toimivan suodatussovittimen kautta. Suodatussovittimella varmistetaan, että ST III -tason tietoa ei päädy Liityntäpalvelimelle eli se toimii tietoturvayhdyskäytävänä korotetun tietoturvallisuustason tietojärjestelmän ja perustasoisen tietojärjestelmän välillä. Ks. lisätietoja sisältöä alkiotasolla suodattavista hyväksyttävistä yhdyskäytäväratkaisuista Kyberturvallisuusviraston ohjeesta *[26]*.

Kaaviossa oikealla puolella on kuvattu, miten Palveluväylän kautta voidaan välittää ST III -tasoista tietoa erillisellä salaussovittimella salattuna. ST III -tason tietoa käsittelevä salaussovitin tulee olla omassa vyöhykkeessään, eikä ST III -tason tietoa käsittelevään sovitinpalveluun (ja tämän verkkoalueeseen) saa olla suoraa pääsyä Liityntäpalvelimelta. Tiedonsiirron

kummankaan pään Liityntäpalvelimella (ja tämän verkkoalueelta) ei ole näin koskaan pääsyä salaamattomaan ST III -tason tietoon.

Kaaviossa suodatus- ja salaussovitin on rakennettu tiedonvälitysalustatuotteen (esim. API Gateway) päälle. Sovitin voi olla rakennettu myös täysin itsenäisenä sovelluksena. Molemmissa tapauksissa on tärkeää, että toteutus täyttää Kybertuvallisuuskeskuksen vaatimukset ja VAHTI-suositukset (mm. yhdyskäytäväratkaisujen yleiset suunnitteluperiaatteet *[26]*, ohje salauskäytännöistä *[27]* ja kryptografiset vahvuusvaatimukset *[28]*) sekä toteutus auditoidaan kolmannen osapuolen toimesta.



Kuva 7 – Turvaluokitellun tiedon välittäminen Palveluväylässä

5.5.4 Monikanavajulkaisu ja sovitinpalvelut

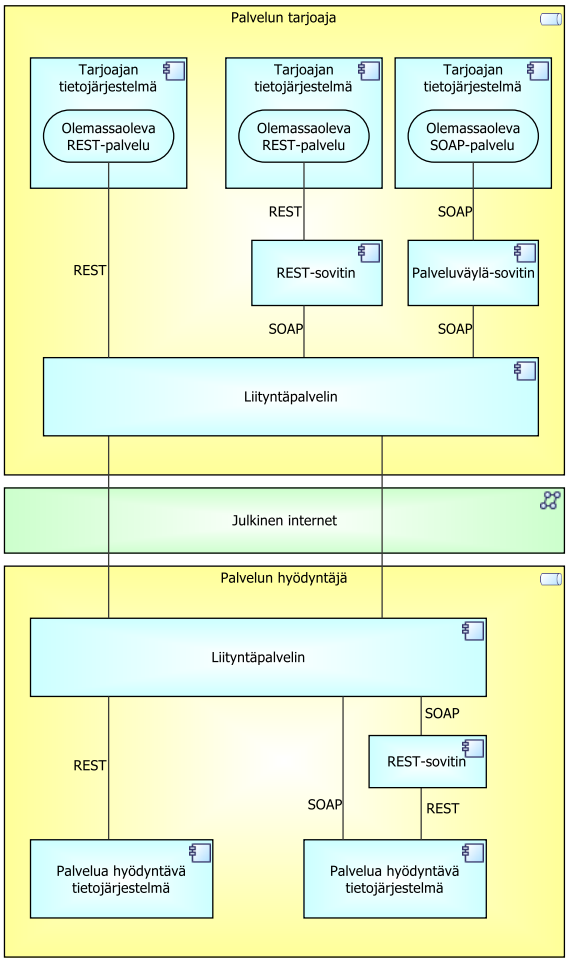
Alla on kuvattu miten alun perin muuhun kanavaan kuin Palveluväylään julkaistut REST- ja SOAP-palvelut voidaan julkaista Palveluväylään muuttamatta itse palvelua. Palveluväylä voi korvata entisen julkaisukanavan tai se voi toimia toisena rinnakkaisena julkaisukanavana samalle palvelulle (monikanavajulkaisu).

REST-palvelu, jota ei ole alun perin toteutettu julkaistavaksi Palveluväylään, on huomattavasti helpompi julkaista Palveluväylään kuin vastaava SOAP-palvelu. Olemassaolevat REST-palvelut voidaan yleensä julkaista sellaisenaan Palveluväylään muuttamatta palvelutoteutusta tai tarvitsematta lisätä erillistä Palveluväylä-sovitinta (kaaviossa vasemmanpuoleinen käyttötapaus) *[9]*.

Jos REST-palvelu halutaan julkaista Palveluväylään SOAP-palveluna, voidaan tähän käyttää REST-sovitinta (kaaviossa keskimmäinen käyttötapaus). REST-sovitinpalvelu (tarkemmin REST-SOAP -sovitin) on X-Roadin liityntäpalvelimen ja liitettävän järjestelmän väliin sijoittuva komponentti, joka sovittaa liitettävän järjestelmän tarjoamat palvelut X-Road-tiedonsiirtoprotokollan mukaiseen muotoon (ks. yleiskuvaus laajennuskomponenteista luvusta 6.2). Ennen Palveluväylän REST-tukea tämä oli ainoa tapa julkaista REST-palveluita Palveluväylään. Nykyisin Palveluväylä tukee suoraan REST-palveluita ja niiden monimuotoista sisältöä (toisin kuin SOAP, REST ei rajaa rajapinnoissa käytettyä tiedon esitysmuotoa, vaan palvelut voivat palauttaa suoraan esim. binäärimuotoista dataa kuten kuvia *[9])*.

REST-sovitinta voidaan käyttää myös asiakaspäässä. Asiakaspäässä REST-sovitin mahdollistaa Palveluväylään julkaistun SOAP-palvelun kutsumisen asiakaspäässä REST-palveluna. Toisin kuin SOAP-palvelua, Palveluväylään julkaistua REST-palvelua voidaan kutsua vain REST-palveluna (ts. Palveluväylästä ei löydy tälle valmista sovitinta).

SOAP-palvelu, jota ei ole alun perin suunniteltu julkaistavaksi Palveluväylään, tarvitsee erillisen Palveluväylä-sovittimen palveluväyläjulkaisua varten, jollei palvelutoteutusta haluta muuttaa (kaaviossa oikeanpuoleinen käyttötapaus). Tämä johtuu siitä, että palvelun tulee rajapintakuvauksessaan tukea palveluväyläkohtaisia SOAP-otsikoita (headers) ja palvelun tulee palauttaa nämä otsikot takaisin vastausviestissään. REST-palveluiden osalta vastaavaa tarvetta ei ole, koska Liityntäpalvelin lisää palvelun puolesta tarvittavat otsikot vastaukseen (otsikot lisätään REST-palveluissa SOAP-otsikoiden sijaan HTTP-protokollan mukaisiin otsikkotietoihin). On tärkeä huomata, että tarve kaaviossa kuvatulle Palveluväylä-sovittimelle koskee vain tilannetta, jossa Palveluväylälle julkaistavaan palveluun ei haluta tehdä muutoksia. SOAP-palvelu voi myös suoraan itse tukea Palveluväylän tarvitsemia otsikoita, jolloin erilliselle sovittimelle ei ole tarvetta.



Kuva 8 – Palveluväylän sovitinpalvelut

5.6 Valvonta- ja hallinta-arkkitehtuuri

Liityntäpalvelimet tukevat sekä paikallista että keskitettyä valvontaa ja hallintaa. Osaa Liityntäpalvelinten asetuksista hallitaan keskitetysti kansalliselta Keskuspalvelimelta käsin (ks. luku 5.2). Paikallisesti Liityntäpalvelimen asetuksia hallitaan Liityntäpalvelimen hallintakäyttöliittymän ja konfiguraatiotiedostojen avulla. Hallintakäyttöliittymän kautta tehdyt muutostoimenpiteet kirjautuvat käyttölokiin. Liityntäpalvelimen hallinta on kuvattu dokumentissa *Security Server User Guide [12]*. Konfiguraatiotiedostojen avulla hallittavat Liityntäpalvelimen järjestelmäasetukset on kuvattu dokumentissa *X-Road: System Parameters User Guide [13]*.

Liityntäpalvelimen valvonta jakautuu kahteen osaan: ajoympäristön ja operatiiviseen valvontaan. Ajoympäristön valvonta käsittää esim. käyttöjärjestelmän, muistin, levytilan ja CPU-kuorman. Operatiivinen valvonta kerää tietoja tiedonsiirroista Liityntäpalvelinten välillä. Näitä tietoja ovat esim. pyyntö- ja vastausviestien aikaleimat, koot, prosessointiajat sekä asiakasjärjestelmän ja palvelun tunnisteet. Ajoympäristön valvonta on kuvattu tarkemmin dokumentissa *X-Road: Environmental Monitoring Architecture [29]* ja operatiivinen valvonta dokumentissa *X-Road: Operational Monitoring Daemon Architecture [30]*.

Liityntäpalvelin tukee sekä ajoympäristön valvonnan että operatiivinen valvonnan osalta keskitettyä valvontaa. Keskitettyä valvontaa voidaan tehdä kansallisen tason lisäksi myös

paikallisella tasolla. Esim. Liityntäpalvelimen ylläpitäjä voi keskitetyn valvonnan kautta valvoa samalla työkalulla kaikkia ylläpitämiään Liityntäpalvelimia ja näihin liitettyjä palveluita (edellyttäen, että palveluissa on tälle tuki). Liityntäpalvelin tarjoaa valvontatietojen välittämiseen ulkoisiin valvontajärjestelmiin SOAP- ja JMX-rajapinnan.

Käyttöoikeudet valvontatietoihin on rajattu Liityntäpalvelimen omistajalle ja Keskuspalvelimelle määritellylle kansallisen valvonnan alijärjestelmälle. Liityntäpalvelimen asetuksissa voidaan tarvittaessa rajata kansallisen valvonnan saamia valvontatietoja.

Edellä kuvattujen valvontamekanismien lisäksi Liityntäpalvelin tarjoaa järjestelmä-, käyttö- ja sanomalokin järjestelmän toiminnan, muutosten ja Liityntäpalvelinten välisen tiedonsiirron valvontaan (ks. lisätietoja lokitiedoista luvusta 4.4).

6 Teknologia-arkkitehtuurin kuvaukset

6.1 Palveluväylän tekninen yleiskuvaus

Palveluväylä on tarkoitettu synkroniseen point-to-point viestintään organisaatioiden välillä eikä se korvaa organisaatioiden sisäisesti käyttämiä integraatioratkaisuja. Palveluväylä perustuu avoimen lähdekoodin teknologioihin ja avoimiin standardeihin. Tällä valinnalla on haettu kustannustehokkuutta, uudelleenkäytettävyyttä ja toimittajariippumattomuutta.

Palveluväylän arkkitehtuuri on kuvattu ylätasolla *X-Road Security Architecture [5]* -dokumentissa. Liityntäpalvelimen ja Keskuspalvelimen osalta tarkemmat tekniset yksityiskohdat ja arkkitehtuuri on kuvattu dokumenteissa *X-Road: Security Server Architecture [22]* ja *X-Road: Central Server Architecture [23]*.

6.2 Palveluväylän laajennuskomponentit

Laajennuskomponentit ovat X-Road -yhteisön kehittämiä Palveluväylän käyttöä ja valvontaa helpottavia uudelleenkäytettäviä piensovelluksia. Palveluväylän laajennuskomponentit on kuvattu X-Road Components *[10]* -verkkosivulla.

Esimerkkeinä laajennuskomponenteista ovat REST-SOAP -sovitin ja tiedostosiirtopalvelu. REST-SOAP -sovitinpalvelu on kuvattu luvussa 5.5.4. Tiedostosiirtopalvelu on tarkoitettu Palveluväylän kautta tehtävään tiedostojen siirtoon asiakasjärjestelmän ja palvelimen välillä. Tiedostopalvelua voi käyttää esim. ajastettuihin eräajosiirtoihin tai käyttäjän kertaluonteisesti komentoriviltä käynnistämiin siirtoihin. Tiedostosiirtopalvelun asiakasohjelman avulla tiedostoja voi listata ja siirtää FTP-tyyppisten LIST, GET- ja PUT-komentojen avulla, eli listata ja hakea tiedostoja palvelimelta tai lähettää niitä sinne. Tiedostosiirtopalvelu on perinteisiä tiedoston siirtotapoja (esim. SFTP ja SCP) tietoturvallisempi (käytännössä hyödyt ovat samat kuin luvussa 2.3 listatut Palveluväylän hyödyt muihin tietoturvatuotteisiin ja väyläratkaisuihin verrattuna).

6.3 Koulutus ja testaus

Palveluväylään tutustumiseen ja oppimiseen on tarjolla laajasti ohjeistuksia (mm. X-Road Knowledge Base), koodiesimerkkejä, koulutusta (mm. X-Road Academy) ja tukipalveluita (mm. Slack-kanava kehittäjien väliseen keskusteluun). Nämä X-Road yhteisön palvelut löytyvät osoitteesta: https://x-road.global/resources *[20]*. Palveluväylän ja tähän liitettyjen palveluiden kokeilemiseen on myös tarjolla julkinen valmiiksi konfiguroitu ympäristö testipalveluineen (*X-Road Playground [21]*).

Palveluväylää hyödyntävien järjestelmien kehittämistä ja testausta varten Liityntäpalvelimesta ja Keskuspalvelimesta on saatavilla Docker-imaget (*X-Road Security Server Docker image [17]* ja *X-Road Central Server Docker image [18]*). Liityntäpalvelimesta on saatavissa myös valmiiksi konfiguroitu ja täysin itsenäinen Docker-image (*Standalone Security Server Docker image [19]*), joka on valmis käytettäväksi muutamassa minuutissa ilman normaalia liityntäpalvelimen asennus-, määritys- ja rekisteröintiprosessia (tämä ei voi olla kuitenkaan yhteydessä muihin Liityntäpalvelimiin).

7 Termit ja lyhenteet

Termi	Selitys
Alijärjestelmä	Alijärjestelmä on asiakasjärjestelmän tai loogisen asiakasjärjestelmäkokonaisuuden yksilöivä tunnus Palveluväylässä, ja sitä käytetään palveluiden kutsumisessa sekä Palveluväylään liitettyjen palveluiden käyttöoikeuksien määrittelyssä. Alijärjestelmä voi olla asiakasjärjestelmäkohtainen tai vaihtoehtoisesti myös useat yhden loogisen kokonaisuuden muodostavat asiakasjärjestelmät voivat hyödyntää samaa alijärjestelmää palveluiden kutsumiseen. Palveluväylän käyttöoikeuksien määrittely tapahtuu alijärjestelmätasolla, jonka vuoksi lähtökohtaisesti tulisi aina käyttää asiakasjärjestelmäkohtaisia alijärjestelmiä.
Avoin data	Avoin data on julkista koneluettavaa tietoa, joka on maksutta erilaisten organisaatioiden hyödynnettävissä. Tiedon hyödyntäminen voi tapauskohtaisesti vaatia käyttäjän/hyödyntäjän tunnistuksen ja/tai käyttöehtojen hyväksymisen. Käyttöehtojen tulee kuitenkin sallia tiedon uudelleenkäyttö.
ESB	Enterprise Service Bus. ESB suomennetaan usein palveluväyläksi. Tässä dokumentissa palveluväylällä tarkoitetaan aina ESB:n sijaan Suomi.fi-palveluväylää. ESB on keskitettyyn tiedonvälitykseen ja palveluiden orkestrointiin perustuva arkkitehtuuri tai tähän perustuvaa toteutusratkaisu. ESB-ratkaisut ovat käytännössä aina organisaatiokohtaisia, eikä niiden tarjoamat tietoturva- ja muut ominaisuudet ylitä organisaatiorajoja, kuten Suomi.fi-palveluväylä. Toisin kuin ESB, Suomi.fi-palveluväylä perustuu hajautettuun malliin eikä siinä ole ESB:n kaltaista yksittäistä keskitettyä tiedonvälityspistettä, jonka kautta kaikki tiedot kulkevat.
Federointi	Federointi (en. federation) on X-Road version 6 mukanaan tuoma uusi ominaisuus, joka mahdollistaa tiedonvaihdon eri X-Road-asennusten kesken. Viron ja Suomen X-Road-asennukset voidaan federoinnin avulla integroida toisiinsa, jolloin niihin liitetyt suomalaiset ja virolaiset järjestelmät pystyvät keskustelemaan keskenään X-Roadin välityksellä.
GraphQL	GraphQL on palvelurajapinnoissa käytetty tiedon kysely -ja muokkauskieli. GraphQL sisältää lisäksi kielen rajapinnan skeeman määrittelyyn. Palvelun hyödyntäjä voi skeemaan pohjautuen muodostaa haluamansa kyselyt ja päättää mitä skeeman mukaisia tietoja hakee ja millä hakuehdoilla.
Keskuspalvelin	Keskuspalvelin (en. Central Server) on X-Road-ratkaisun keskuskomponentti, joka pitää sisällään tiedot kaikista palveluväylään liitetyistä Liityntäpalvelimista sekä niitä käyttävistä organisaatioista. Nämä tiedot tallennetaan säännöllisesti päivittyvinä paikallisina kopioina jokaiselle Liityntäpalvelimelle, jonka ansiosta Liityntäpalvelinten ei tarvitse olla yhteydessä Keskuspalvelimeen sanomien lähetyksen yhteydessä. Uusien Liityntäpalvelinten ja organisaatioiden lisääminen edellyttää aina Keskuspalvelimen kautta tapahtuvaa palveluväylän ylläpitäjän suorittamaa hyväksymistä. Suomi.fi-palveluväylän ylläpitäjänä toimii VRK.

Liityntäkatalogi	Liityntäkatalogi on Palveluväylään liitettyjen palveluiden eli liityntöjen sekä niiden tietojen hyödyntämisen keskitetty esilletuontipaikka. Liityntäkatalogi on ihmisluettava portaali, jossa esitetään Palveluväylään liitetyt palvelut rajapintakuvauksineen sekä palveluiden tekniset lisätiedot, tietosisällöt, vasteajat ja omistajan yhteystiedot. Liityntäkatalogin liityntöjen tiedot päivittyvät Liityntäpalvelimilta automaattisesti joka yö. Metadatan tuottamisesta vastaavat liityntöjen omistajaorganisaatiot.
Liityntäpalvelin	Liityntäpalvelin (en. Security Server) on X-Road-ratkaisun keskeinen komponentti, jonka kautta tietolähteiden ja tietojärjestelmien liittäminen Palveluväylään tapahtuu. Jokaisella Palveluväylään liitetyllä järjestelmällä on oltava käytössään Liityntäpalvelin, jonka kautta kaikki Palveluväylään lähetettävät tai sieltä vastaanotettavat sanomat kulkevat. Liityntäpalvelin vastaa mm. palvelukutsujen välittämisestä järjestelmien välillä, palvelukutsujen varmennekättelystä, tietoliikenteen ja sanomien salauksesta, lokituksesta ja käyttöoikeuksien hallinnasta. Liityntäpalvelin voi olla organisaatiokohtainen tai monen organisaation kesken yhteinen.
Palveluväylä, Suomi.fi-palveluväylä	Suomi.fi-palveluväylä on Suomessa käytetty X-Road-ratkaisuun perustuva standardi tapa siirtää tietoa tietovarantojen ja niitä hyödyntävien tietojärjestelmien välillä.
REST	REST (en. Representational State Transfer) on HTTP-protokollaan perustuva arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen. REST ei rajaa rajapinnoissa käytettyä teknologiaa tai tiedon esitysmuotoa. Yleisin REST-sovelluksissa käytetty tiedonesitysmuoto on tällä hetkellä JavaScript Object Notation (JSON).
SOAP	SOAP (en = Simple Object Access Protocol) on XML-kieleen pohjautuva tietoliikenneprotokolla. Palveluväylän kautta tarjottavat palvelutoteutukset voivat perustua joko SOAP-protokollan mukaiseen tiedonsiirtoon tai tiedon esitysmuodosta riippumattomaan REST-arkkitehtuurimalliin. SOAP toimii useiden eri protokollien yli, mutta Palveluväylässä sitä käytetään vain HTTP-protokollan yli.
X-Road	X-Road on Virossa alun perin kehitetty ja käytössä oleva ohjelmisto, joka toimii osana Suomi.fi-palveluväylän teknistä ydintä. X-Road tarjoaa standardoidun ja tietoturvallisen tavan siirtää tietoa tietovarantojen ja niitä hyödyntävien tietojärjestelmien välillä. X-Roadin kehittäjänä toimii nykyisin Nordic Institute for Interoperability Solutionsin (NIIS).

8 Viittaukset

1 JHKA, Julkisen hallinnon arkkitehtuuriperiaatteet. Valtiovarainministeriö. 26.4.2017 v. 1.91. Julkisen hallinnon kokonaisarkkitehtuuri.
https://wiki.julkict.fi/julkict/juhta/juhta-tyoryhmat-2016/jhka-tyoryhma/jhka-2.0/jhka-2-0-8-periaatteet/
2 Palveluväylän palvelulupaus. Väestörekisterikeskus.
https://esuomi.fi/palveluntarjoajille/palvelulupaukset/#tab-id-4
3 Väestörekisterikeskuksen linjaus liittyen Suomi.fi-palveluväylän käyttövelvoitteesta poikkeamiseen. VRK/1338/2019. 11.3.2019.
https://esuomi.fi/?mdocs-file=22664
4 Ulkoisen kuormantasaajaan käyttäminen palveluväylässä. Väestörekisterikeskus.
https://esuomi.fi/palveluntarjoajille/palveluvayla/tekninen-aineisto/hyva-tietaa/ulkoisen-kuormantasaajan-kayttaminen-palveluvaylassa/
5 X-Road Security Architecture. Technical Specification, v. 0.3. 29.6.2019. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road/blob/develop/doc/Architecture/arc-sec_x_road_security_architecture.md
6 X-Road: Message Transport Protocol. Technical Specification, v. 2.4. 04.03.2019. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road/blob/develop/doc/Protocols/pr-messtransp_x-road_message_transport_protocol.md
7 X-Road: Message Protocol v4.0. Technical Specification, v. 4.0.21. 06.03.2018. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road/blob/develop/doc/Protocols/pr-mess_x-road_message_protocol.md
8 X-Road: Message Protocol for REST. Technical Specification, v. 1.0.0. 25.04.2019. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road/blob/develop/doc/Protocols/pr-rest_x-road_message_protocol_for_rest.md
9 Blog: Two Steps from X-Road REST Support. 27.03.2019. Petteri Kivimäki.
https://www.niis.org/blog/2019/3/25/two-steps-from-the-x-road-rest-support
10 X-Road Components. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road-code-samples/blob/master/COMPONENTS.md
11 Palveluväylän sanasto. Väestörekisterikeskus.
https://esuomi.fi/palveluntarjoajille/palveluvayla/sanasto/
12 Security Server User Guide, v. 2.31. 4.11.2019. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-ss_x-road_6_security_server_user_guide.md
13 X-Road: System Parameters User Guide, v. 2.47. 2.7.2019. Nordic Institute for Interoperability Solutions (NIIS).
https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-syspar_x-road_v6_system_parameters.md#21-changing-the-system-parameter-values-in-configuration-files
14 RFC3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). 2001. IETF.
https://tools.ietf.org/html/rfc3161
15 Suomi.fi-yhteentoimivuusalusta ja -menetelmä. Väestörekisterikeskus.
https://yhteentoimiva.suomi.fi/
16 Suomi.fi-palveluväylä – Metapalvelut. Väestörekisterikeskus.
https://esuomi.fi/palveluntarjoajille/palveluvayla/tekninen-aineisto/rajapintakuvaukset/metapalvelut/
17 X-Road Security Server Docker image. Nordic Institute for Interoperability Solutions (NIIS).
https://hub.docker.com/r/niis/xroad-security-server
18 X-Road Central Server Docker image. Nordic Institute for Interoperability Solutions (NIIS).
https://hub.docker.com/r/niis/xroad-central-server/
19 Standalone Security Server Docker image. Nordic Institute for Interoperability Solutions (NIIS).
https://hub.docker.com/r/niis/xroad-security-server-standalone
20 X-Road Resources. Nordic Institute for Interoperability Solutions (NIIS).
https://x-road.global/resources

2.12.2019

21 X-Road Playground. Nordic Institute for Interoperability Solutions (NIIS). https://x-road.global/xroad-playground

22 X-Road: Security Server Architecture. Technical Specification, v.1.8. 25.10.2019. Nordic Institute for Interoperability Solutions (NIIS). https://github.com/nordic-institute/X-Road/blob/develop/doc/Architecture/arc-ss_x-road_security_server_architecture.md

23 X-Road: Central Server Architecture. Technical Specification, v.2.4. 2.3.2018. Nordic Institute for Interoperability Solutions (NIIS). https://github.com/nordic-institute/X-Road/blob/develop/doc/Architecture/arc-cs_x-road_central_server_architecture.md

24 X-Road Simple Statistics API. Nordic Institute for Interoperability Solutions (NIIS). https://app.swaggerhub.com/apis-docs/NIIS/x-road-statistics/

25 Suomi.fi-palveluväylän Liityntäkatalogi. Väestörekisterikeskus. https://liityntakatalogi.suomi.fi/

26 Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. 20.12.2018. Kyberturvallisuuskeskus. https://legacy.viestintavirasto.fi/attachments/Yhdyskaytavaratkaisuohje.pdf

27 VAHTI 2/2015 Ohje salauskäytännöistä. Julkisen hallinnon ICT, Valtiovarainministeriö. https://www.vahtiohje.fi/web/guest/2/2015-ohje-salauskaytannoista

28 Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen -kansalliset suojaustasot. 28.11.2018. Kyberturvallisuuskeskus. https://legacy.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf

29 X-Road: Environmental Monitoring Architecture. Nordic Institute for Interoperability Solutions (NIIS). https://github.com/nordic-institute/X-Road/blob/develop/doc/EnvironmentalMonitoring/Monitoring-architecture.md

30 X-Road: Operational Monitoring Daemon Architecture. Nordic Institute for Interoperability Solutions (NIIS). https://github.com/nordic-institute/X-Road/blob/develop/doc/OperationalMonitoring/Architecture/arc-opmond_x-road_operational_monitoring_daemon_architecture_Y-1096-1.md

31 Suomi.fi-palveluväylä - Käyttöönoton prosessi. Väestörekisterikeskus. https://palveluhallinta.suomi.fi/fi/sivut/palveluvayla/kayttoonotto/prosessi