Kansallinen palveluväylä

Toteutussuunnitelma

Versio 0.6

Päiväys 2.9.2013

Sisällysluettelo

Dokumentin versiohistoria

Versio	Päiväys	Tekijä	Tarkastaja	Hyväksyjä	Muutoshistoria
0.1	20.6.2013	JT			Ensimmäinen versio
0.2	28.6.2013	JT			Lisäyksiä ja tarkennuksia
0.21	1.7.2013	JU			Korjauksia. Lisätty luku 8 Hankkeen riskit
0.3	5.8.2013	JT			Lisäyksiä ja tarkennuksia kehittämiskohteiden kuvauksiin
0.31	6.8.2013	JT, OK, JT			Tarkennuksia
0.4	23.8.2013	JT			Ohjaus-/työryhmien kommenttien mukaiset muutokset
0.5	28.8.2013	MK, JT			Työryhmän työpajan esille tuomat muutokset (aikatauluriskit)
0.6	2.9.2013	JT			Ohjausryhmän kommentit

1 Yleistä

Kansallinen palveluväylä on tiedonvälityskonsepti, jossa eri toimintaympäristöjen palveluiden tarvitsema tieto on saatavilla avoimien rajapintojen yli kaikille tietoa tarvitseville palveluille. 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.

Nykyinen hajautettuihin asiakastietoihin, operatiivisiin järjestelmiin ja tietovarantoihin sekä erillisiin integraatioratkaisuihin perustuva palvelujärjestelmä on rakennettu organisaatiokohtaisiin siiloihin, jossa organisaatiorajojen ylittävien palveluprosessien kehittäminen on vaikeaa. Palveluväylän tavoitteena on nykyistä paremmin mahdollistaa asiakaspalveluiden ja palveluprosessien kehittäminen palveluissa tarvittavan tiedonvaihdon ja yleispalvelut mahdollistavan ratkaisukokonaisuuden avulla.

Tässä dokumentissa kuvataan keskeisimpien kehityskohteiden toteuttamissuunnitelmia sillä tasolla, että niiden pohjalta voidaan käynnistää varsinainen suunnittelutyö. Tämä dokumentti ei pyri olemaan täydellinen suunnitelma. Riskien tarkempi analysointi ja niihin varautuminen jätetään myös tarkemman suunnittelutyön tehtäväksi.

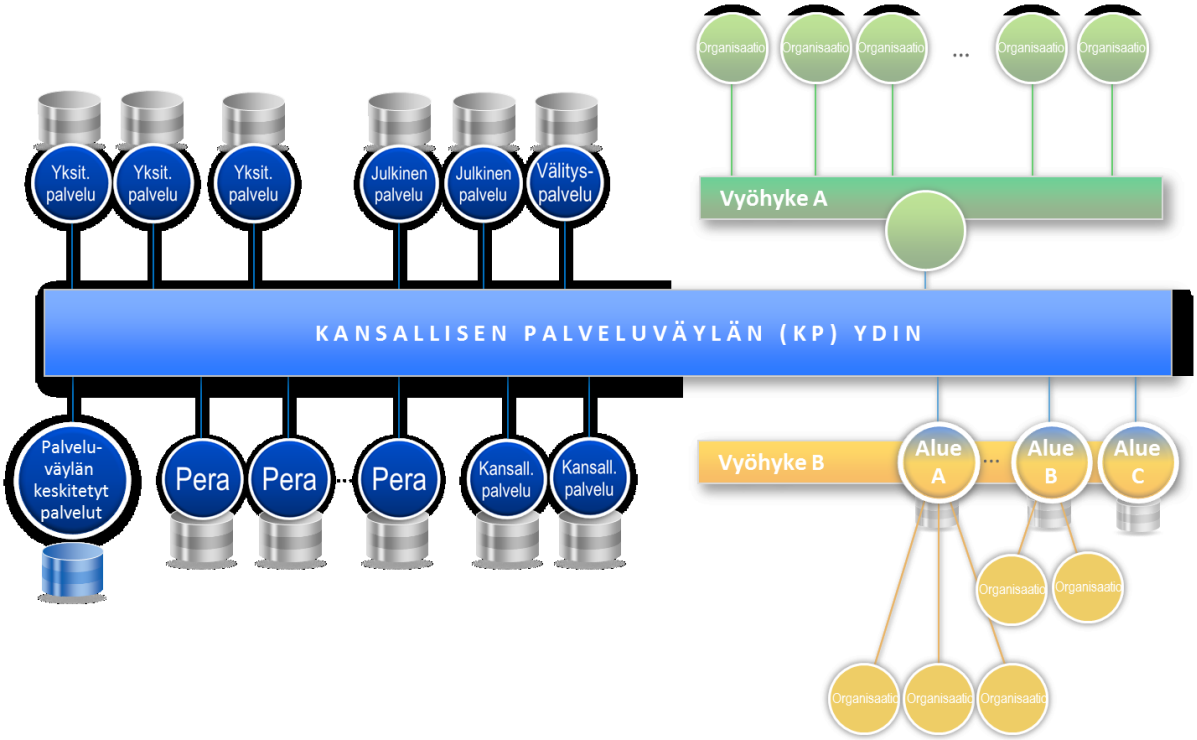
Palveluväylän viitearkkitehtuuri on kuvattu omassa dokumentissaan /1/, jossa on myös useiden kehityskohteiden seikkaperäisemmät esitykset. Osana kehittämispolkua on em. kuvausten tarkentaminen sille tasolle, että tarvittavat toiminnallisuudet voidaan kehittää.

2 Kehittämiskohteiden määrittely ja priorisointi

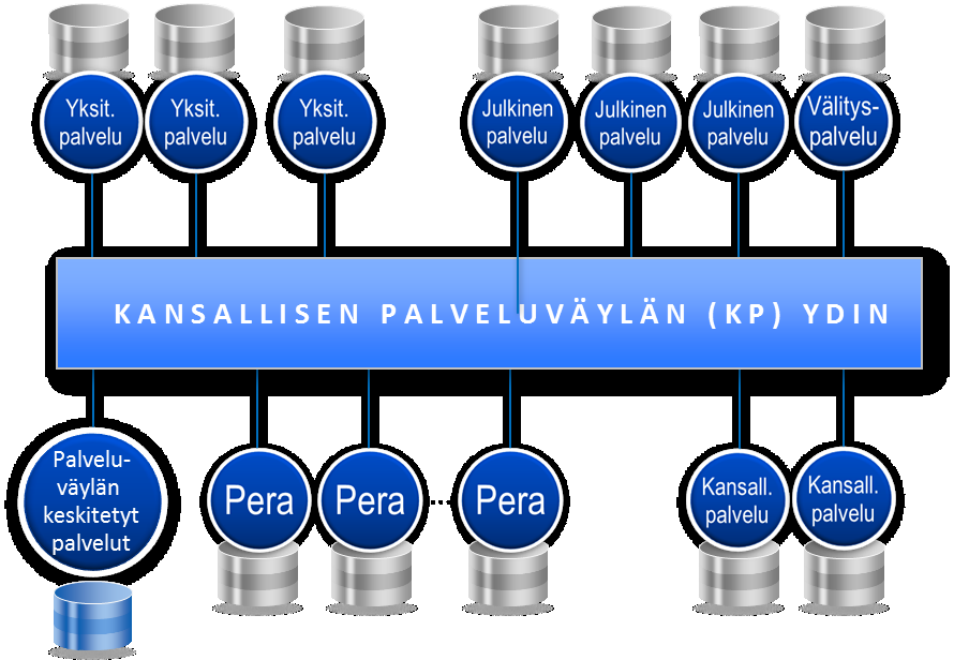
2.1 Taustaa

Kansallinen palveluväylä on kansallisen palveluarkkitehtuurin ytimessä. Merkittävänä yhteentoimivuuden mahdollistajana sen voi nähdä olevan enemmän kuin pelkkä sanomanvälitysratkaisu: se on konkreettinen askel yhtenäisten rajapintojen ja tiedonvaihtoprotokollien käyttöön siirtymisessä. Palveluväylän menestys on riippuvainen siihen liitettävistä tietojärjestelmistä, eli palveluväylän kautta saatavista palveluista, joita voidaan perustellusti pitää tärkeämpinä kuin väylän teknisiä ominaisuuksia. Siksi on huolehdittava, että palveluväylän kautta on mahdollisimman joutuisasti saatavissa kattava kirjo hyödyllisiä palveluita. Kansallisen palveluväylän tunnetuksi tekemiseen on kiinnitettävä huomiota alusta alkaen, jotta sille saataisiin käyttöä ja sen hyödyllisyys sitä myöten lisääntyisi.

Kansallisen palveluväylän viitearkkitehtuurin määrityksessä huomioitiin olemassa olevia määrityksiä ja ratkaisuja sekä pyrittiin pitämään niihin kohdistuvien muutoksien määrää mahdollisimman pieninä. Tämä johti ratkaisuun, jossa kansallinen palveluväylä toimii olemassa olevien väyläratkaisujen yhdistäjänä sekä tarjoaa siihen suoraan liittyville tietojärjestelmille yhtenäisen tavan päästä tietoihin käsiksi.



Kuva 2: Palveluväylä yhdistää ensimmäisessä vaiheessa useita kansallisia väyliä



Kuva 1: Tavoitetilassa palveluväylä yhdistää organisaatiot suoraan

Kansallinen palveluväylä mahdollistaa viestien reitittämisen, joten sen avulla voidaan välittää viestejä muihin väyliin ja takaisin edellyttäen, että muilla väylillä on kyvykkyys tarjota palvelujaan ulkopuolisille tietojärjestelmille.

Eri väylissä olevia tietojärjestelmiä voidaan liittää palveluväylään myös suoraan.

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

2.2 Kansallisen palveluväylän kehittämiskohteet lyhyesti

Kansallisen palveluväylän kattama kokonaisuus voidaan jakaa useampaan erilliseen, toisistaan riippumatta toteutettavissa olevaan tehtävään. Väylän toiminnan käynnistämisen kannalta välttämättömät tehtävät on toteutettava korkeammalla prioriteetilla.

Välttämättömiä komponentteja ovat väylään liittymisen teknisten määrittelyjen viimeistely, väylän ydintoiminnallisuuden toteuttaminen sekä väylän ydintoiminnallisuuden operoinnin järjestäminen. Teknisten määrittelyjen tarkentamisessa ja vaihtoehtojen vertailemisessa on hyvä tehdä teknologiakokeiluja, jotta varmistutaan ratkaisun toimivuudesta.

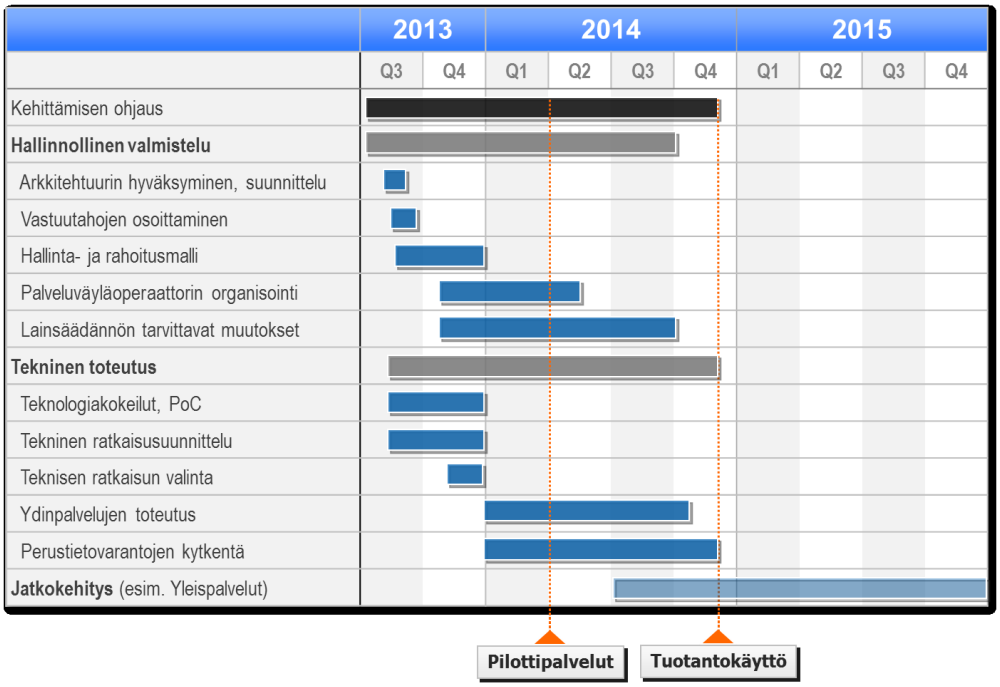
Hallinnollisina kehittämiskohteina ovat palveluväylän toiminnan roolittaminen, käynnistämisen rahoittaminen, liiketoimintamallin määrittäminen, hallintamallin luominen sekä operoinnin järjestäminen.

Käyttöönoton nopeuttamiseksi esim. lopullisen hallintamallin valmistuminen voidaan jättää myöhemmäksi ja käynnistää toiminta väliaikaisin järjestelyin. Myös rahoitusmallin määrittelyä voidaan tehdä käyttöönoton jälkeen, kunhan toiminnan aloittamiselle on olemassa rahoitus ja jatkorahoitukseen on sitouduttu.

2.3 Kehittämiskohteet ja aikataulu

Kansallisen palveluväylän toteuttamisen tehtävät ja karkea aikataulu on esitetty alla olevassa kuvassa.

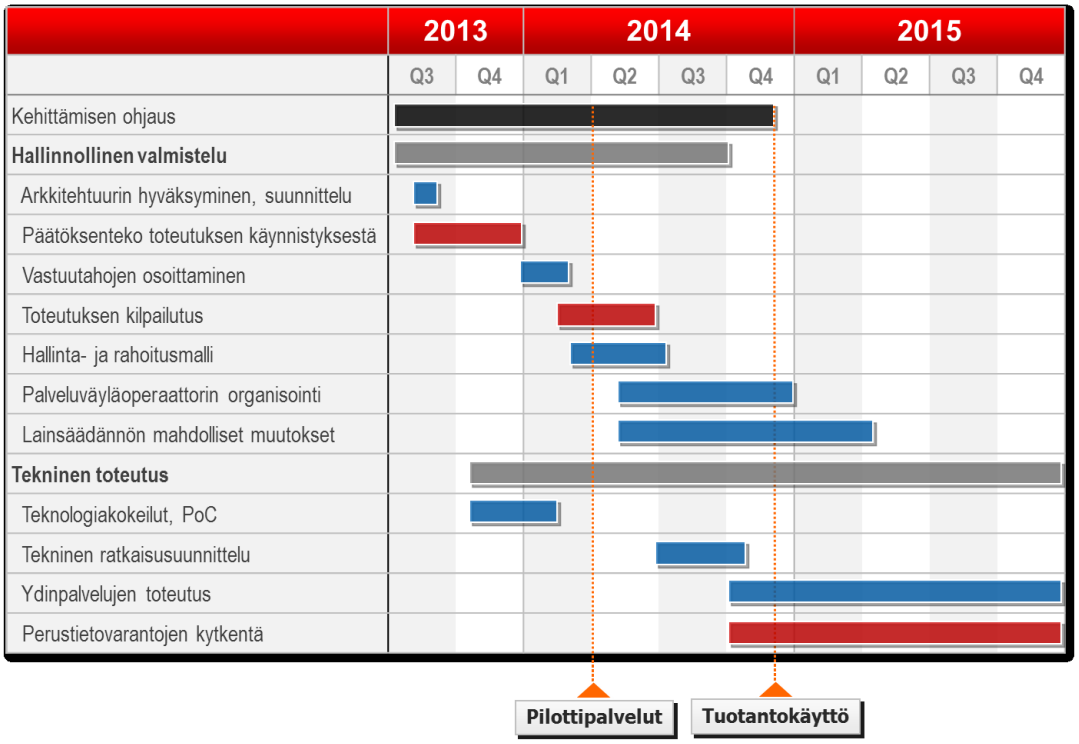
Kuva 3: Kansallisen palveluväylän toteuttamisen tehtävät ja karkea aikataulu



Aikataulussa on ajateltu pilotoinnin alkavan vuoden 2014 ensimmäisen neljänneksen jälkeen jolloin riittävä määrä toiminnallisuuksista pitäisi olla käytettävissä. Varsinainen tuotantokäyttö voisi alkaa vuoden 2014 loppupuolella.

Yllä esitetty aikataulu on optimistinen, olettaen että päätöksenteko sujuu nopeasti ja mahdolliset hankintoihin liittyvät kilpailutukset eivät aiheuta viiveitä.

Alla on esitetty vaihtoehtoinen aikataulu, jossa näitä viiveitä on ennakoitu.

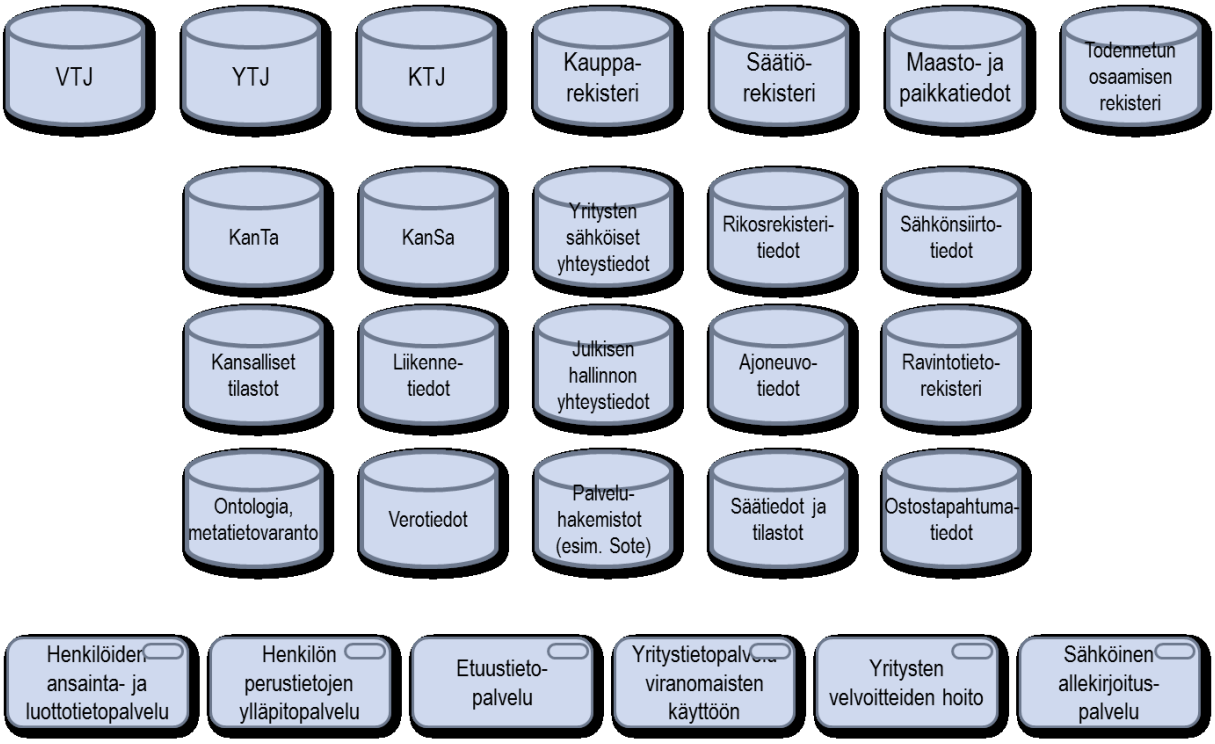


Kuva 4: Kansallisen palveluväylän kehittämisen vaihtoehtoinen aikataulu

Palveluväylän hallinnollisten ja teknisten kehittämiskohteiden lisäksi on huomioitava myös käyttöönoton esteiden poistamisesta. Liiketoimintamallin osalta se tarkoittaa, että ainakaan alkuvaiheessa väylään liittyjiltä ei pitäisi periä korvauksia väylään liittymisestä eikä sen käytöstä. Palveluväylän ydinpalvelujen lisäksi käytettävyyden edellytyksenä voidaan pitää mm. perustietovarantojen kytkemistä palveluväylään sekä kansallisessa palveluarkkitehtuurissa tärkeiksi tunnistettujen kehittämiskohteiden toteuttamisen aloittamista, joita ovat esimerkiksi yleispalveluiksi luokiteltavat tunnistuspalvelut sekä valtuutusten ja suostumusten hallintaan liittyvät palvelut.

Palveluväylän käyttöönoton edistämiseksi on kiinnitettävä huomiota tiedottamiseen, jonka on tavoitettava mahdolliset palveluväylää hyödyntävät tahot.

Viitearkkitehtuuria kehittänyt projektiryhmä näki alla olevassa kuvassa esitetyt palvelut ja tietovarannot erityisen hyödyllisinä palveluväylän substanssipalveluina. Näiden tietovarantojen ja palveluiden kehittämistä palveluväylän kautta saataviksi on syytä harkita osana kansallisen palveluarkkitehtuurin kehittämisohjelmaa.



Kuva 5: Kansallisen palveluväylän kannalta hyödylliset substanssipalvelut.

3 Palveluväylän kehittämisen ohjaus ja tiedottaminen

Toimenpide:

Kansallisen palveluväylän toteuttaminen organisoidaan hankkeeksi, jota ohjaa JulkICT. Toteutushanketta ei tule käynnistää ennen kuin rahoituksesta ja tuotannonaikaisesta ylläpidosta on sovittu. Hanketta ohjaamaan on saatava lisäksi palveluväylän hyödyntäjätahoja, kuten

- palveluväylään liitettävien perustietovarantojen edustus
- perustietovarantoja hyödyntävien julkisen sektorin toimijoiden edustus
- palveluväylään liitettävien vyöhykkeiden edustus (esim. SoTe, VY, KY)
- yksityissektorin edustus

Ohjausryhmän kokoonpano on valittava riittävän laaja-alaisesti, jotta se edesauttaa palveluväylätietouden leviämistä mahdollisimman laajoille joukoille sekä lisää hankkeeseen sitoutumista ydintoimijoiden osalta. Ohjaava ryhmä on kuitenkin hyvä pitää pienenä, jotta se kykenee reagoimaan palveluväylän kehittämistyössä esiin nouseviin asioihin mahdollisimman nopeasti. Ohjausryhmän on kyettävä pitämään toteutus selkeästi vaiheistettuna että hanke pysyy kontrolloitavana.

Palveluväylän tuottamista mahdollisuuksista ja hyödyistä on tiedotettava tehokkaasti substanssitoimijoille. Kehitystyön edetessä on hyvä tuoda näkyviin myös esimerkkisovelluksia ja toiminnallisuuksia. Teknisen kehittämisen lisäksi on hyvä

kehittää uusia toiminnallisia konsepteja joita palveluväylän avulla voidaan tuoda käyttöön.

Palveluväylän kehitystyön etenemisestä on tiedotettava tehokkaasti. Rajapintakuvaukset on tehtävä helposti saataviksi ja esimerkkipalveluiden lähdekoodia on jaettava avoimesti esimerkkeinä väylään liittymisestä. Ohjelmistotoimittajille on järjestettävä seminaareja (tai vastaavia tilaisuuksia), joissa esimerkkejä väylän toiminnallisuudesta käydään läpi ja asiasta kiinnostuneet voivat kokeilla väylän hyödyntämistä käytännössä.

Toimijat:

JulkICT, Toteutushanke

Vastuu:

JulkICT

Aikataulu:

9/2013 – 12/2014

Riskit:

Toteutushanketta ei saada perustettua, palveluväylän kehittäminen viivästyy.

Palveluväylän toteuttamiseen kohdistuu ristiriitaisia vaatimuksia, joiden ratkaisemisesta ei päästä yksimielisyyteen. Käyttöönotto viivästyy.

Palveluväylän toteuttamisen vaiheistaminen ei onnistu ja hankkeessa yritetään tehdä liian montaa asiaa samanaikaisesti. Laatu kärsii.

Palveluväylän toteuttamiseen varattu aika on liian lyhyt ja toteutusta ei saada tehtyä kyseisessä aikataulussa.

Palveluväylän toiminnallisuus soveltuu vain osalle potentiaalisesta käyttäjäjoukosta. Palveluväylän käyttö jää suppeaksi.

Toteutukseen valitaan vääriä teknologioita. Toteutusta joudutaan myöhemmässä vaiheessa muuttamaan.

Vaatimukset ja määrittelyt toteutettavalle järjestelmälle ovat puutteellisia ja toteutus ei täytä oikeita vaatimuksia mitä järjestelmälle tulisi asettaa.

4 Hallinnolliset kehittämiskohteet

4.1 Arkkitehtuurin hyväksyminen

Toimenpide:

Kansallisen palveluväylän arkkitehtuuri viimeistellään viitearkkitehtuurin pohjalta.

Kerätään palautetta, analysoidaan kommentit ja koostetaan yhteisesti hyväksytty arkkitehtuuri toteutettavaksi.

Toimijat:

JulkICT, Kehityshanke, sidosryhmät

Vastuu:

JulkICT

Aikataulu:

9/2013

Riskit:

Arkkitehtuuri on epäselvä tai monimutkainen. Toteutus on vaikeaa.

Arkkitehtuuria ei saada hyväksyttyä. Hanke viivästyy.

Ristiriitaiset vaatimukset monimutkaistavat ja hidastavat toteutusta.

Valittavat arkkitehtuuriratkaisut eivät täytä järjestelmään kohdistuvia toiminnallisia ja ei-toiminnallisia vaatimuksia.

Valittavat tekniset ratkaisut eivät ole pitkäikäisiä. Toteutusta joudutaan muuttamaan myöhemmässä vaiheessa.

Ydintoiminnallisuuksista ja toteuttamisen vaiheistamista ei päästä yhteisymmärrykseen. Ensimmäinen toteutusvaihe kestää tarpeettoman pitkään, hanke viivästyy.

4.2 Vastuutahojen osoittaminen

Toimenpide:

Palveluväylän kehittämisen ja toteuttamisen rooleihin nimetään organisaatiot ja henkilöt. Keskeisimmät roolit ja tehtävät on kuvattu /1/[1] luvussa 5.3. ja liitteessä 1.

Palveluväylän keskeisin toimija on sen omistaja, joka vastaa palveluväylän toiminnasta ja tarkoituksenmukaisuudesta kansallisiin yhteentoimivuuden infrastruktuurivaatimuksiin nähden.

Toimijat:

JulkICT, sidosryhmät

Vastuu:

[1] Dokumentin referenssidokumentteihin viitataan merkinnöllä /*n*/, jossa *n* on luvussa 9 listattu referenssi.

JulkICT

Aikataulu:

9/2013

Riskit:

Vastuullisia tahoja ei saada nimettyä. Hanke viivästyy.

Vastuullisella taholla ei ole vaadittua kompetenssia sille allokoituun tehtävään. Kehittäminen, toteuttaminen ja käyttöönotto viivästyvät.

Vastuutahoksi nimetään instanssi, jolla ei ole taloudellisia edellytyksiä toimia tehtävässä.

Vastuutahoksi tulee organisaatio, jota ei ole vielä olemassa. Vastuutahon puuttuessa tälle kuuluvat toiminnot viivästyvät, sitä myöden palveluväylän kehittäminen ja/tai käyttöönotto viivästyy.

4.3 Hallinta-, palvelutuotanto- ja liiketoimintamallit

Toimenpide:

Kansallisen palveluväylän hallinta-, palvelutuotanto- ja liiketoimintamallit täsmennetään ja hyväksytään. Kehityshanke vastaa palveluväylän hallinnasta ja toiminnan kustannuksista kunnes vastuuorganisaatiot on saatu nimitettyä, rahoituksen yksityiskohdista sovittua ja hallintamalli viimeisteltyä.

Palveluväylän toteutushanketta ei tule käynnistää ennen kuin rahoituksesta ja tuotannonaikaisesta ylläpidosta on sovittu. Myös väylän hyödyntämisen edellytyksistä ja liittyvien organisaatioiden velvollisuuksista on saatava perusperiaatteet sovittua ennen kuin palveluväylään voidaan ottaa toimijoita mukaan.

Hallintamallin toimijat ja toimijoiden keskeisimmät tehtävät on kuvattu /1/ luku 5.3. ja liite1. Rahoitus-, hallinta- ja liiketoimintamalleja on lisäksi analysoitu erikseen /3/.

Toimijat:

JulkICT, Toteutushanke, Sidosryhmät

Vastuu:

JulkICT

Aikataulu:

9/2013 – 12/2013

Riskit:

Palveluväylän rahoituksesta ei saada päätöstä, käyttöönotto viivästyy.

Palveluväylän rahoitus-/liiketoimintamalli ei houkuttele toimijoita palveluväylän käyttäjiksi, palveluväylän käyttö jää vähäiseksi.

Palveluväylän käyttöehtoja ei saada kirjattua, palveluväylän käyttöönotto viivästyy.

Palveluväylän käyttöehdot rajoittavat toimintaa liiaksi ja palveluväylää ei haluta käyttää, väylän käyttö jää vähäiseksi.

Palveluväylän käyttöehdot ovat liian löysät tai epäselvät ja siksi väylään ei saada keskeisiä palveluja. Väylän käyttö jää vähäiseksi.

Hallintamallista ei päästä yksimielisyyteen, sitä ei saada kuvattua tai muusta syystä vahvistettua. Hanke joutuu vastaamaan palveluväylän hallinnoinnista ja pitkäjänteinen kehitystyö kärsii.

Hallintamallista tulee monimutkainen tai jäykkä, palveluväylä ei kehity tarpeiden mukaisesti.

Palveluväylän rooleihin liittyviä tehtäviä ei ole määritelty selkeästi.

Palveluväylän omistajuus ei ole selkeästi määritelty. Omistajan ohjauksella tapahtuvat toiminnot, kuten palveluväylän kehitys ja operointi kilpailutetaan ja ohjataan puutteellisesti tai ristiriitaisesti. Palveluväylän kehitys, toteutus ja operointi tehdään tehottomasti ja huonolaatuisesti.

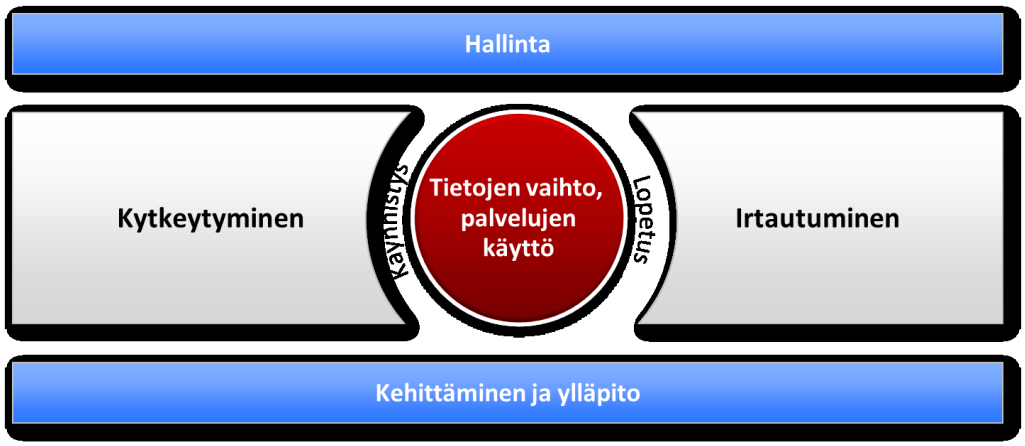
4.4 Palveluväyläoperaattorin organisointi

Toimenpide:

Palveluväyläoperaattori vastaa kansallisen palveluväylän käytännöistä, kuten käytettävyydestä, operoinnista ja palveluväylän käyttäjäksi liittymiseen tarvittavista asioista.

Palveluväyläoperaattoriksi valittu organisaatio käynnistää palveluväylän hallinnolliset ja toiminnalliset prosessit sekä tekee käyttöönoton palveluväylän ydinpalveluille.

Palveluväyläoperaattorin prosessit voidaan luokitella seuraavasti:



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

Palveluväyläoperaattori on tuotantoympäristön, eli palveluväylän ydin- ja teknologiapalveluiden (kuten hallinta-, valvonta- ja varmistuspalvelut, /1/ luku 6.7) lisäksi vastuussa myös testiympäristöistä (kts 5.4.13), jossa liittymiselle ei ole merkittäviä kriteerejä ja jossa voidaan käyttää testipalveluja (kts myös luku 5.2).

Kuvattavien prosessien sisällöt on hahmoteltu tarkemmin Kansallisen palveluväylän viitearkkitehtuurin (/1/) luvussa 6.3.

Toimijat:

JulkICT, Toteutushanke, Palveluväyläoperaattori

Vastuu:

Palveluväyläoperaattori

Aikataulu:

10/2013 - 5/2014

Riskit:

Operaattori ei nauti kaikkien palveluväylän potentiaalisten käyttäjäorganisaatioiden luottamusta, palveluväylää hyödynnetään suunniteltua vähemmän.

Operaattoriksi valitulla taholla ei ole riittäviä resursseja operaattorina toimimiseen, käyttöönotto viivästyy.

4.5 Lainsäädännöllisten muutosten valmistelu

Toimenpide:

Palveluväylän hyödyntämiselle ei ole välittömiä lainsäädännöllisiä esteitä. Koosteisten, eri hallinnonalojen yli käyvien palvelujen luominen todennäköisesti kohtaa sellaisia, joten palveluväylää hyödyntävien uusien käyttötapausten avulla on syytä aloittaa lainsäädäntötarkastelut hyvissä ajoin.

Lainsäädännön avulla voidaan edistää palveluväylän käyttöä, esim. velvoittamalla julkisen hallinnon toimijoita palveluväylän hyödyntäjiksi ja/tai palvelun tarjoajiksi.

Hankkeessa on selvitelty lainsäädäntöä /2/.

Toimijat:

JulkICT, Toteutushanke, sidosryhmät

Vastuu:

JulkICT

Aikataulu:

10/2013 – 10/2014

Riskit:

Lainsäädännön esteet tulevat esiin vasta palveluja käynnistettäessä. Toteutettujen palvelujen käyttöönotto estyy tai viivästyy.

Lainsäädäntö jarruttaa koosteiden palveluiden luomista, palveluväylästä saatava lisäarvo (nykyiseen verrattuna) jää pieneksi.

5 Tekniset kehittämiskohteet

Palveluväylän teknisiä kehittämiskohteita ovat mm:

- Määrittelydokumentaatio, etenkin rajapintojen kuvaukset
- Liityntäpalvelinohjelmiston/ohjelmistojen kehittäminen ja tuotteistaminen helposti asennettavaksi ohjelmistopaketiksi
- Ydinpalvelujen määrittely, kehitystyö, dokumentointi ja käyttöönotto
    - Tarvittavien (mahdollisesti virtuaalisten) palvelimien hankinta, käyttöönotto ja konfigurointi
    - Palveluväylän oman varmennepalvelun pystytys
    - Palveluväylän DNS-domainin rekisteröinti ja turvanimipalvelujen käynnistys
    - Palveluhakemiston sisällön määritys ja hakemistopalvelun käynnistys
    - Sopimushakemiston sisällön määritys ja hakemistopalvelun käynnistys
- Itseprovisiointipalvelun kehittäminen
- Palveluväylään liittymisen dokumentaatio

5.1 Teknologiakokeilut

Toimenpide:

Viitearkkitehtuurin mukaisia ratkaisuja on olemassa (ainakin) Ruotsissa ja Virossa. Sitra järjestää jo teknisiä kokeiluja Viron X-Roadin käytöstä, ja niistä saadaan kokemuksia analysoitavaksi. Arkkitehtuurin vaatimien muutoksien vaikutukset (esim. REST-rajapinnat, erilaiset sanomasisällöt) toiminnallisuuteen ja suorituskykyyn on hyvä mitata ja todentaa niiden merkitys verrattuna olemassa oleviin implementaatioihin.

Ydin- ja teknologiapalvelujen (toiminnallisuudet kuvattu luvuissa 6.5 ja 6.7, /1/) toteuttamiseen on olemassa valmiita ratkaisuja, niiden ominaisuuksia ja soveltuvuutta kansallisen palveluväylän tarpeisiin kokeillaan. Näitä ovat mm.:

- liityntäpalvelinohjelmistot (Viron X-Road, Ruotsin SHS,…)

- aikapalvelu (tutkitaan vaihtoehtoja, verrataan oman palvelun hyötyjä vs. ulkopuolisen palvelun käyttöä, esim. Mittatekniikan keskuksen NTP-palvelu)
- nimipalvelu (DNS SEC)
- palvelukatalogin toteutusvaihtoehdot
- sopimuskatalogin toteutusvaihtoehdot
- varmennepalvelun toteuttamisen vaihtoehdot, tiheästi vaihtuvat varmenteet lisäävät väylän turvallisuutta

Useimpiin toiminnallisuuksiin on saatavissa avoimen lähdekoodin ratkaisuja, joiden soveltuvuus on syytä tutkia. Kokeiluissa on keskityttävä ratkaisujen tietoturvaan, luotettavuuteen, skaalautuvuuteen, suorituskykyyn, konfiguroitavuuteen ja hallintaan.

Toimijat:

JulkICT, Palveluväyläoperaattori, sidosryhmät

Vastuu:

JulkICT

Aikataulu:

9/2013 – 12/2013

Riskit:

Teknologiakokeiluissa ei saada oleellisia asioita irti. Tehdään vääriä valintoja.

Teknologiakokeilujen tekijät verifioivat eri asioita kuin pitäisi, koska vaatimukset ja testitapaukset puuttuvat. Kokeilujen tuloksista ei ole hyötyä.

Osaa kokeiltavista tuotteista ei osata konfiguroida siten, että niiden kyvykkyydestä saataisiin totuudenmukainen kuva. Tehdään vääriä valintoja.

Tehdään toimittajariippuvaisia valintoja, joista ei ole myöhemmässä vaiheessa mahdollista irtaantua.

Palveluväyläoperaattoria ei ole valittu ja operaattori ei osallistu valintojen tekoon. Kokeiluista saatavia oppeja ei hyödynnetä palveluväylän toiminnassa.

5.2 Tekninen ratkaisusuunnittelu

Toimenpide:

Kuvataan Kansallisen palveluväylän komponenttien toiminnallisuudet (mm. /1/ luvut 6.4, 6.5 ja 6.7) ja rajapinnat.

Palveluväylän tekniset rajapintakuvaukset (/1/ luku 6.6 ja liite 4) pohjautuvat löyhästi Julkishallinnon perustietovarantojen rajapinnat (PERA) -työryhmän kuvaamiin sekä Viron X-Road:n rajapintoihin käsittäen tiedonsiirtoprotokollan sekä palveluiden välillä

välitettävät kutsu- ja vastaussanomat, jotka sisältävät yleiset metatiedot ja palvelukohtaisen sisältöosan.

Rajapinnan täsmentämisen lisäksi tehdään esimerkkitoteutukset tuottaja- ja hyödyntäjäpalveluiksi, jotka myös asetetaan palveluväylän testausympäristöön käytettäviksi. Näiden esimerkkitoteutusten lähdekoodi annetaan yleiseen käyttöön helpottamaan palveluväylään liittyvien organisaatioiden työtä.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä, sidosryhmät

Vastuu:

JulkICT

Aikataulu:

9/2013 – 12/2013

Riskit:

Komponenttien toiminnallisuudet kuvataan puutteellisesti. Kokonaisuuden toiminnallisuus ei ole optimaalinen.

Komponenttien vikasietoisuuden ratkaisut määritellään epäselvästi. Komponenttien toteutukset eivät ole käytännössä riittävän vikasietoisia.

Rajapintakuvauksista puuttuu jotain oleellista tai ne ovat moniselitteisiä ja se aiheuttaa palveluväylään yhteentoimimattomuutta ja muutostarpeita.

Rajapintojen toteuttaminen on monimutkaista. Hanke viivästyy.

Toteutus suunnitellaan sellaiseksi, että sen muuttaminen myöhemmässä vaiheessa on vaikeaa ja kallista.

5.3 Teknisen ratkaisun valinta

Toimenpide:

Valitaan teknologiakokeilujen ja teknisten määrittelyjen perusteella palveluväylän toteutuksessa käytettävät valmiit komponentit sekä päätetään kehitettävistä toiminnallisuuksista ja kehitystyön vastuista.

Toimijat:

JulkICT, sidosryhmät, Palveluväyläoperaattori

Vastuu:

JulkICT

Aikataulu:

11/2013 – 12/2013

Riskit:

Valmiit komponentit eivät toteuta luvussa 5.2 määriteltyjä ominaisuuksia riittävän hyvin. Käyttöönotto viivästyy.

Järjestelmän ominaisuuksia ei ole riittävän selkeästi asetettu, valintaa ei voida tehdä.

Palveluväyläoperaattoria ei ole valittu tähän mennessä, jolloin muut valitsevat operaattorin puolesta toteutuksen komponentit ja operaattori ei ole valintoihin sitoutunut. Vaihtoehtoisesti odotetaan palveluväyläoperaattorin osallistumista valinnan tekoon ja aikataulu venyy.

5.4 Palveluväylän ydinpalvelujen ja toiminnallisuuksien toteutus

Toteutetaan arkkitehtuurin ja rajapintamääritysten mukaiset ydinpalvelut, jotka on kuvattu luvussa 6 (/1/). Näistä keskeisin on liityntäpalvelinohjelmisto (tarkempi toiminnallinen kuvaus /1/ luku 6.4) sekä teknologiakokeilujen perusteella valitut soveliaat valmiit (tai kehitettävät) ohjelmistot (mahdollisesti palveluna) seuraaviin palveluihin (toiminnallisuudet on tarkemmin kuvattu luvussa 6.4, 6.5 ja 6.7 /1/):

- aikapalvelu
- nimipalvelu (DNS SEC)
- palvelukatalogi
- sopimuskatalogi
- varmennepalvelu

Lisäksi palveluväylään liittymisen toimenpiteet on selkeästi dokumentoitava. Liittymistä helpottavan itseprovisioinnin toiminta on määriteltävä ja toteutettava.

Palveluväyläoperaattori vastaa osaltaan tuotantoympäristön teknologiapalveluista (kts. luku 4.4), joita ovat mm:

- hallintapalvelut
- valvontapalvelut
- varmistuspalvelut

Konfiguraatiot ja käyttötavat ohjeistetaan ja dokumentoidaan palveluväyläoperaattorin henkilökunnalle. Palveluväylän on kyettävä toipumaan mahdollisista häiriöistä. Vaikka väylän arkkitehtuuri onkin vikasietoinen ja kestää replikointien avulla ydinpalvelujen poissaolon, on esim. ydinpalvelimien täydellisestä tuhoutumisesta toipumisen prosessit dokumentoitava ja toimiviksi testattava.

Palveluväylän käyttöönottaminen edellyttää ydinpalveluista vain nimipalvelun olemassaoloa. Aikapalvelua voidaan ainakin aluksi, mahdollisesti koko ajan, käyttää palveluväylän ulkopuolelta. Palveluväylää voi käyttää aluksi ilman palvelu- ja sopimuskatalogeja ja varmenteet voidaan hankkia ulkopuolisilta tahoilta, vaikkakin oman CA:n pystytys ja käyttö on suositeltavaa.

5.4.1 Turvallisen yhteyden muodostaminen

Liityntäpalvelimen TLS-yhteyksien muodostamisessa yhteyden salaaminen.

Toiminnallisuus on osa liityntäpalvelinohjelmistoa, kts 5.4.3.

5.4.2 Liityntäpalvelimien autentikointi

Liityntäpalvelimen TLS-yhteyksien muodostamisessa tapahtuva palvelinvarmenteihin perustuva molemminpuolinen tunnistaminen TLS-protokollan mukaan.

Normaalin TLS-toiminnallisuuden lisäksi implementaatioon on integroitava CRL[2]-toiminnallisuus. Tämä voidaan tehdä joko hyödyntämällä turvanimipalveluita tai erillisiä CRL-protokollia, joilla tieto evätyistä varmenteista välittyy valitulle TLS-implementaatiolle (esim. paikallisella levyllä olevan CRL-tiedoston ylläpito).

Toiminnallisuus edellyttää varmennepalvelun olemassaolon (kts 5.4.14) ja liityntäpalvelimelta kyvyn päivittää oma varmenteensa.

Toiminnallisuus on osa liityntäpalvelinohjelmistoa, kts 5.4.3. ja vaatii varmenteiden automaattisen luomisen ja CRL:n käsittelyn osalta toteutusta myös keskuspalvelimeen.

5.4.3 Liityntäpalvelinohjelmisto

Liityntäpalvelinohjelmisto toteuttaa seuraavat palveluväylän tekniset tietojärjestelmäpalvelut:

- Turvallisen yhteyden muodostaminen
- Liityntäpalvelimien autentikointi
- Turvanimipalvelu (sekundäärinen palvelin), kts 5.4.4
- Sanomanvälityspalvelu, kts 5.4.5
- Yhteyslokitus
- Viestilokitus
- Sanomien sähköinen allekirjoitus
- Palvelukatalogi (sekundäärinen palvelin), kts 5.4.9
- Sopimuskatalogi (sekundäärinen palvelin), kts 5.4.10
- Itseprovisiointi, kts 6.1.1

Lisäksi liityntäpalvelimessa on hyvä toteuttaa esim. paikallinen palomuuri, joka sallii internetin kautta yhteydet vain palveluväylään liitetyistä laitteista (automaattisesti päivittyvä konfiguraatio on tehtävissä helposti nimipalveluja hyödyntäen).

Liityntäpalvelin on riippuvainen palveluväylän keskuspalveluista.

Toimenpide:

Kehitetään ja tuotteistetaan liityntäpalvelinohjelmisto (tarkempi toiminnallinen kuvaus luvussa 6.4, /1/). Osa liityntäpalvelimen toiminnallisuudesta on muiden kehitysprojektien

[2] Certificate Revocation List, käytöstä poistettujen varmenteiden lista

tuotosten integrointia osaksi liityntäpalvelimen ohjelmapakettia (lähinnä sekundääripalvelimet).

Tuotteistus sisältää käyttöönoton seikkaperäisen dokumentaation sekä pitkälti konfiguroidun, asennettavan ohjelmistopaketin tuottaminen aitoon ajoympäristöön sekä virtuaalikoneympäristöön (ohjelmiston tulisi olla valmiiksi asennettavissa yleisesti käytetyillä virtuaalikoneilla, kuten VirtualBox, VMWare Player, VMWare ESXi, Microsoft Hyper V, MED-V jne). Ohjelmisto kysyy käynnistyessään siltä puuttuvat tiedot, generoi omat salausavaimensa, ottaa yhteyden palveluväylän keskuspalvelimeen, provisioi itsensä palveluväylän komponentiksi (saa ohessa mm. palveluväylän sisäisessä viestinnässä tarvittavan varmenteen, jonka ottaa käyttöön) ja käynnistää paikallisten sekundääripalvelimien tietojen synkronoinnin. Itseprovisiointipalvelua on kuvattu tarkemmin luvussa 6.1.1.

Välttämättömät tiedot: /1/ Liite 4.1.

Liityntäpalvelinohjelmisto voi perustua esim. Viron X-Road Security Server toteutukseen, johon lisätään mahdollisesti erillisenä komponenttina palveluväylän rajapinnan toteutus sekä tässä luvussa erikseen esitetyt toiminnallisuudet.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

JulkICT, jatkossa Palveluväylän ohjausryhmä

Aikataulu:

1/2014 – 10/2014

Riskit:

Liityntäpalvelun kehittäminen ei perustu valmiisiin ratkaisuihin, työmäärä kasvaa suureksi ja aikataulu venyy.

Tekniset määritykset osoittautuvat hankaliksi toteuttaa, aikataulu venyy.

Perustaksi otettu valmis ratkaisu ei taivu tarvittaviin muutoksiin helposti, aikataulu venyy.

5.4.4 Turvanimipalvelun (DNS SEC) käyttöönotto

Toimenpide:

Kehitetään/valitaan ja sovitetaan palveluväylän nimipalvelinohjelmisto, jonka avulla jaellaan palveluväylään liitettyjen keskuspalvelujen ja liityntäpalvelimien osoitetietoja sekä varmenteita.

Nimipalvelin toteuttaa hajautetun mallin, jossa primääripalvelin on keskuspalvelimella ja sekundääripalvelimet liityntäpalvelimissa.

Turvanimipalvelimilla olevat tiedot ovat keskuspalvelimen allekirjoittamia, joten keskuspalvelimen varmenteen on oltava mukana liityntäpalvelimien asennuspaketeissa.

Nimipalvelussa on listattuna palveluväylään liittyneiden laitteiden IP-osoitteet. Palomuureissa voidaan sulkea muista osoitteista tulevat yhteydenotot ja näin estää palvelunestohyökkäykset ja muut asiattomat yhteydenotot. Nimipalvelun oheen on syytä luoda ohjelma, joka tuottaa ajanmukaisen konfiguraation yleisimmin käytössä oleville palomuurisovelluksille (vähintään välityspalvelimen sisäiselle palomuurille, jonka päivitys voidaan automatisoida internetistä tulevien yhteydenottojen osalta – toteutetaan osana liityntäpalvelinohjelmistoa, kts. 5.4.3).

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2014 – 10/2014

Riskit:

Turvanimipalvelimen käyttö on monimutkaista ja hankalaa.

5.4.5 Sanomanvälityspalvelu

Liityntäpalvelimen päätoiminnallisuus on välittää sanomia. Toiminnallisuuden kuvaus: /1/ Liite 4.1.

Sanomanvälityksen toiminnallisuus kuvataan tarkemmin lopullisessa arkkitehtuurityössä (kts 4.1) ja teknisessä ratkaisusuunnittelussa (kts 5.2).

Toiminnallisuus on osa liityntäpalvelinohjelmistoa, kts 5.4.3.

5.4.6 Yhteyslokitus

Liityntäpalvelin taltioi lokeihinsa tiedot kaikista yhteyksien avaamisista ja päättymisistä riippumatta siitä onko se yhteyden käynnistäjä vai vastaanottaja. Tiedot taltioidaan paikallisiin lokeihin.

Toiminnallisuus on osa liityntäpalvelinohjelmistoa, kts 5.4.3.

5.4.7 Viestilokitus

Liityntäpalvelin taltioi lokeihinsa tiedot kaikista välittämistään sanomista. Tiedot taltioidaan paikallisiin lokeihin.

Viestilokituksen toteutustapa täsmentyy lopullisessa arkkitehtuurityössä (kts 4.1) ja teknisessä ratkaisusuunnittelussa (kts 5.2). Lisäksi tarkemmin määriteltävä kansalaisen tietojen käytön tietopalvelut (kts 5.4.12 ja keskitetty versio 6.1.6) voivat vaikuttaa toteutukseen.

Toiminnallisuus on osa liityntäpalvelinohjelmistoa, kts 5.4.3.

5.4.8 Sanomien sähköinen allekirjoitus

Liityntäpalvelin voi allekirjoittaa välittämänsä sanoman, mikäli sen katsotaan tuottavan palveluväylän hyödyntäjille lisäarvoa. Allekirjoitus perustuu liityntäpalvelimien varmenteisiin.

Toiminnallisuus on osa liityntäpalvelinohjelmistoa, kts 5.4.3.

5.4.9 Palvelukatalogin kehittäminen ja käyttöönotto

Toimenpide:

Kehitetään/valitaan ja sovitetaan tarkempien määritysten (kts. 5.2) mukainen, hajautetulla mallilla toimiva palvelukatalogi.

Primääripalvelin asennetaan palveluväyläoperaattorin keskuspalvelimille.

Sekundääriversiot toimivat liityntäpalvelimissa.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2014 – 10/2014

Riskit:

Soveltuvaa palvelukatalogia ei ole valmiina ja se on kehitettävä itse. Aikataulu venyy,

5.4.10 Sopimuskatalogin kehittäminen ja käyttöönotto

Toimenpide:

Kehitetään/valitaan ja sovitetaan tarkempien määritysten (5.2) mukainen, hajautetulla mallilla toimiva sopimuskatalogi.

Primääripalvelin asennetaan palveluväyläoperaattorin keskuspalvelimille.

Sekundääriversiot toimivat liityntäpalvelimissa.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2014 – 10/2014

Riskit:

Soveltuvaa sopimuskatalogia ei ole valmiina ja se on kehitettävä itse. Aikataulu venyy.

5.4.11 XML-skeema- ja metatietopalvelun kehitys ja käyttöönotto

Toimenpide:

Kehitetään/valitaan ja sovitetaan tarkempien määritysten (5.2) mukainen, keskitetty XML-skeema ja metatietopalvelu.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2014 – 10/2014

Riskit:

5.4.12 Kansalaisen tietojen käytön tietopalvelu

Toimenpide:

Kehitetään/valitaan ja sovitetaan tarkempien määritysten (5.2) mukainen kansalaisen tietojen käytön tietopalvelu.

Palveluväylän ydin on tietoinen vain sanomien otsikoista, ei sanoman rungosta, joten palveluväylä ei voi toteuttaa toiminnallisuutta, mikäli ko. tietoja ei ole otsikoissa. Kyselypalvelun yleisosat voidaan kehittää keskitetysti ja substanssipalvelu (tai siitä tietoinen osa) integroituu siihen.

Ennen palvelun kehittämistä on syytä selvittää mahdollisten juridisten reunaehtojen vaikutus eri ratkaisumalleihin ja valita toteutukselle sopiva arkkitehtuuri (lokitetaan paikallisesti kaikki tarpeelliset tiedot standardissa muodossa jolloin välityspalvelin voi vastata kyselyihin tai välitetään kysely substanssipalvelulle joka vastaa).

Toimijat:

JulkICT, Tekninen kehittäjä, Liittyvä organisaatio

Vastuu:

Liittyvä organisaatio

Aikataulu:

1/2014 – 10/2014

Riskit:

Liittyvä organisaatio ei toteuta tarvittavaa toiminnallisuutta palveluunsa, jollei siihen ole velvoitetta.

5.4.13 Testiympäristöjen luonti eri tarkoituksiin

Toimenpide:

Luodaan ympäristöt, joissa palveluväylään liittymistä, käyttöä ja tietojen tarjoamista voi kokeilla ja testata.

Testiympäristöjen kautta tietoja hyödyntävistä ohjelmista luodaan valmiita esimerkkisovelluksia, joiden lähdekoodi on saatavilla useammalla ohjelmointikielellä. Myös tiedon tarjoajasovelluksen lähdekoodi on saatavilla (mahdollisesti jonkun perustietovarannon liittämisessä käytetty ohjelmakoodi).

Testiympäristöön voidaan liittää myös oikeita tietovarantoja joko suoraan tai tietovarannon kopiota käyttäen.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2014 – 10/2014

Riskit:

Testiympäristöstä tulee liian raskas. Testiympäristöön on hankala kytkeytyä.

Testiympäristöön liittymisen dokumentaatio ei ole riittävän selkeää.

Testiympäristön hyödyntämisen esimerkkiohjelmat eivät kata riittävästi hyödyntäjien tarpeita.

Testiympäristön käytön virheilmoitukset eivät ole riittävän selkeitä ja oikeisiin korjaustoimenpiteisiin opastavia.

Testiympäristössä välitetään luottamuksellista, oikeaa tuotantodataa.

5.4.14 Aikapalvelu

Toimenpide:

Otetaan käyttöön palveluväylää tarkoituksenmukaisimmin palveleva aikapalvelu teknologiakokeilujen (kts 5.1) ja sopimusteknisten asioiden selvitysten mukaisesti.

Oletusarvoisesti otetaan käyttöön Mittatekniikan keskuksen tai muun julkisen toimijan NTP-palvelu.

Toimijat:

JulkICT, Palveluväyläoperaattori

Vastuu:

JulkICT

Aikataulu:

1/2014 – 3/2014

Riskit:

Aikapalvelun käytöstä ei sovita tuottajan kanssa, palvelu on pois käytöstä huomaamatta.

Aikapalvelun hyödyntämistä ei konfiguroida vikasietoiseksi.

5.4.15 Varmennepalvelun käyttöönotto

Toimenpide:

Kehitetään/valitaan ja sovitetaan varmennepalvelu palveluväylän käyttöön. Varmennepalvelulla luodaan väylään liittyvien liityntä- ja keskuspalvelimien varmenteet. Varmennepalvelu kytketään turvanimipalveluun, jonka avulla varmenteita voidaan levittää, mikäli se on tarkoituksenmukaista.

Varmennepalveluun rakennetaan koneellinen rajapinta varmenteiden automaattiseen luontiin, välittämiseen ja käyttöönottoon. Varmenteiden voimassaoloaikoja pidetään tarkoituksenmukaisen lyhyinä ja varmennepalvelu luo automaattisesti uusia varmenteita ennen edellisten varmenteiden vanhenemista. Uudet varmenteet aktivoidaan automaattisesti välityspalvelimissa esim. nimipalvelujen kautta saatuina (osa välityspalvelinohjelmiston kehitystyötä, 5.4.3).

Toimijat:

JulkICT, Palveluväyläoperaattori

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2014 – 10/2014

Riskit:

Sopivaa ohjelmistoa ei ole saatavilla ja sovittaminen / kehittäminen vie aikaa. Aikataulu venyy.

5.5 Perustietovarantojen kytkeminen palveluväylään

Toimenpide:

Perustietovarannot ovat oleellinen ryhmä tiedon tuottajaorganisaatioita palveluväylässä.

Keskitetysti kehitettävillä sovitinratkaisuilla saadaan synergiaetua kun verrataan sitä tietojärjestelmäkohtaisesti toteutettaviin integraatioihin. Siksi on suositeltavaa liittää avoimilla rajapinnoilla varustetut perustietovarannot keskitetysti palveluväyläorganisaation toimesta. Tällöin tietovarannon tuominen palveluväylään ei kuormita tietovarannon hallinnoijaa ja perustietovarannot voidaan tuoda palveluväylän kautta hyödynnettäviksi nopeastikin.

Keskeisimpiä kytkettäviä tietolähteitä ovat seuraavat kansalliset perustietovarannot:

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

Toimijat:

JulkICT, Tekninen kehittäjä

Vastuu:

JulkICT

Aikataulu:

1/2014 – 10/2014

Riskit:

Hallinnolliset syyt hidastavat perustietovarannon liittämistä palveluväylään.

6 Jatkokehitys

6.1 Tietojärjestelmäpalvelut

6.1.1 Sanomamuunnospalvelut

Toimenpide:

Kehitetään sanomavälityksen tietojärjestelmäpalvelun laajennus, joka sisältää sanomamuunnosten käsittelyn erityispalvelut, kuten sanomarikastimen, sanomasuodattimen tms..

Lisäpalvelut voidaan toteuttaa liityntäpalvelimeen asennettavalla palvelumoduulilla tai erillisellä palvelulla, tarkennetusta arkkitehtuurista riippuen.

Toimijat:

Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

8/2014 – 12/2014

Riskit:

XXXX

6.1.2 Prosessimoottori

Toimenpide:

Kehitetään sanomavälityksen tietojärjestelmäpalvelun laajennus, joka sisältää laajemman sääntökoneen ja prosessimoottorin.

Tämän tietojärjestelmäpalvelun avulla liityntäpalvelimeen voidaan luoda monimutkaisempia sanomanvälitys- ja palvelujen kutsusääntöjä.

Laajennukset voidaan toteuttaa liityntäpalvelimeen asennettavalla palvelumoduulilla tai erillisellä palvelulla, tarkennetusta arkkitehtuurista riippuen.

Toimijat:

Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

8/2014 – 12/2014

Riskit:

XXXX

6.1.3 Anonymisoidut testipalvelut

Toimenpide:

Kehitetään testipalvelu, joka tarjoaa palveluväylään kytkettyjen tietolähteiden ja palvelujen anonymisoitua dataa testikäyttöön.

Tiedon tuottaja vastaa lähdetiedon anonymisoinnin periaatteiden määrityksistä ja testauksesta sekä anonymisoidun tiedon toimittamisesta ko. palveluun. Kaikkea palveluväylään kytkettävää tietoa ei edellytetä anonymisoitavaksi ja käytettäväksi ko. palvelun kautta.

Anonymisoidusta datasta sovitaan palveluväylän tietolähteiden omistajien kanssa.

Toimijat:

Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

8/2014 – 12/2014

Riskit:

XXXX

6.1.4 Avoimen datan liityntäpalvelu

Toimenpide:

Kehitetään lisäarvopalvelu, jonka avulla avoimen datan tietolähteitä voidaan koota yhteen yhden palvelun taakse.

Palvelu sisältää rajoitetusti cache-ominaisuuksia, joilla voidaan vähentää varsinaisten avoimen datan lähteiden kuormitusta.

Toimijat:

Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

1/2015 – 6/2015

Riskit:

Palvelulle ei ole tarvetta.

Palvelun kehittäminen erilaisille avoimen datan rajapinnoille sisältää rajoitetusti synergiaa.

Palvelun hyödyntäminen hidastaa avoimen datan saamista käyttöön.

6.1.5 Itseprovisiointipalvelun tekninen määrittäminen ja toteuttaminen

Toimenpide:

Kehitetään/valitaan ja sovitetaan palveluväylän itseprovisiointipalvelu, jonka avulla organisaatio voi liittyä palveluväylään ilman että liittyminen työllistää palveluväyläoperaattoria. Osa itseprovisioinnista on välityspalvelinohjelmistoa (kts 5.4.3), osa keskuspalvelimella olevaa toiminnallisuutta.

Itseprovisiointi on oleellinen osa välityspalvelinohjelmiston käyttöönottoa. Välityspalvelimen ohjelmistopaketti sisältää tarpeelliset tiedot, jotta toiminto voi käynnistyä. Näitä ovat mm:

- Keskuspalvelimen DNS-nimi ja IP-osoite
- Testipalvelimen DNS-nimi ja IP-osoite
- Keskuspalvelimen julkinen avain
- Testipalvelimen julkinen avain

Kun välityspalvelinohjelmisto käynnistetään ensimmäisen kerran (tai jokin pakollisista määritystiedoista puuttuu) käyttäjältä kysytään välityspalvelimen IP-osoite sekä halutaanko liittyä tuotanto- vai testiympäristöön. Sen jälkeen:

- Käyttäjää pyydetään hyväksymään palveluväylän käyttöehdot
- Välityspalvelin generoi itselleen julkisen ja salaisen avaimen (jos näitä ei vielä ole olemassa, testaus- ja tuotantoympäristöissä käytetään eri avainta).
- Käyttäjältä kysytään organisaation perustietoja, kuten
  - liittymän tyyppi (palveluväylän hyödyntäjä ja/tai tuottaja)
  - tarjotun palvelun attribuutteja palvelukatalogia varten
- Julkinen avain ja käyttäjän antaman tiedot organisaatiosta välitetään keskuspalvelimelle salatulla yhteydellä (vain keskuspalvelin tunnistetaan, koska välityspalvelimella ei tässä vaiheessa ole varmennetta)
- Keskuspalvelin tarkistaa välityspalvelimen IP-osoitteen perusteella sen DNS-nimen ja käyttää sitä palveluväylän sisäisen DNS-nimen muodostamisessa (`sovellus.firma.fi` muotoon `sovellus.firma.palveluvayla.fi`).
- Keskuspalvelin generoi välityspalvelimen varmenteen (palveluväylän DNS-nimi ja välityspalvelimen julkinen avain)
- Lisätään välityspalvelimen IP-osoite, DNS-nimi ja varmenne nimipalveluun, palvelusta annetut tiedot palvelukatalogiin ja organisaatiosta annetut tiedot sopimuskatalogiin
- Keskuspalvelin antaa välityspalvelimelle palveluväylän perustietoja, mm:
  - palveluväylän nimipalvelimien IP-osoitteet
  - aikapalvelimien osoitteet

- Välityspalvelin konfiguroi ja käynnistää omat peruspalvelunsa, mm:
  - aikapalvelu
  - nimipalvelut
- Välityspalvelin saa nimipalveluista uuden varmenteen, jonka se ottaa käyttöön (välityspalvelimen normaali toiminnallisuus, uusi varmenne otetaan aina käyttöön kun sellainen on saatavilla).

Itseprovisioinnin jälkeen uusi hyödyntäjä / palvelu on liitetty palveluväylään ja sen kautta voidaan hyödyntää palveluja jotka eivät vaadi kahdenvälisiä sopimuksia.

Toimijat:

JulkICT, Palveluväyläoperaattori, Tekninen kehittäjä

Vastuu:

Palveluväyläoperaattori

Aikataulu:

8/2014 – 12/2014

Riskit:

Itseprovisiointimahdollisuuden puute on riski palveluväylän käytön leviämiselle.

6.1.6 Kansalaisen tietojen käytön tietopalvelu – kokoava palvelu

Toimenpide:

Kehitetään/valitaan ja sovitetaan tarkempien määritysten (5.2) mukainen kansalaisen tietojen käytön tietopalvelu.

Palveluväylän ydin ei ole tietoinen sanomien kirjekuorien sisällöstä, joten palveluväylä ei voi toteuttaa toiminnallisuutta, vaan siihen tarvitaan erillinen substanssipalvelu. Kyselypalvelun yleisosat voidaan kehittää keskitetysti ja substanssipalvelu integroituu siihen.

Ennen palvelun kehittämistä on syytä selvittää mahdollisten juridisten reunaehtojen vaikutus eri ratkaisumalleihin ja valita toteutukselle sopiva arkkitehtuuri.

Suorituskykymielessä tehokkain ratkaisu olisi kerätä käyttötiedot keskitettyyn palvelimeen, jonne tietoa tarjoava sovellus ne välittäisi samalla kun se vastaa palvelupyyntöön. Vaihtoehtoisesti jokainen kansalaisen tietoja tarjoava palvelu voi tarjota kyselyrajapinnan, joita keskitetty koostepalvelu hyödyntää ja tarjoaa yhdistelmänä kansalaiselle.

Toimijat:

JulkICT, Tekninen kehittäjä, Liittyvä organisaatio

Vastuu:

Liittyvä organisaatio

Aikataulu:

8/2014 – 12/2014

Riskit:

Liittyvä organisaatio ei toteuta tarvittavaa toiminnallisuutta palveluunsa, jollei siihen ole velvoitetta.

Juridiset syyt estävät palvelun tehokkaan toteuttamisen.

6.2 Yleispalvelut

Kansallisen palveluväylän viitearkkitehtuuria suunniteltaessa esille nousi kansallisen palveluarkkitehtuurin yleisiä palveluita, joita ei voida laskea kuuluviksi palveluväylän tekniseen ytimeen. Palveluita on käsitelty tarkemmin /1/ luku 6.5.3, ja ne ovat:

- Kansalaisen tunnistaminen
- Ammattilaisen tunnistaminen
- Organisaation tunnistaminen
- Asiointitilit
- Maksamisen palvelut
- Suostumusten ja tahdonilmaisujen hallinta
- Valtuutusten ja puolesta-asioinnin hallinta
- Tietopyyntöjen hallinta

Nämä yleiset palvelut ovat hyödyllisiä palveluväylään liitettäville varsinaisille substanssipalveluille, ja tukevat siten kansallisen palveluarkkitehtuurin kehittymistä. Toisaalta esim. yleisen tunnistamisratkaisun puute saattaa jopa hidastaa palvelukehitystä.

Yleispalveluiden toteuttaminen on suunniteltava osaksi kansallisen palveluarkkitehtuurin kehittämisohjelmaa sen ensimmäisiksi tehtäviksi kansallisen palveluväylän teknisten ydinpalveluiden toteuttamisen rinnalle.

6.3 Uudet substanssipalvelut

Palveluväylän lisäarvo tulee sen avulla ja kautta saatavista palveluista, joten kehittämistyössä ei voi pitäytyä pelkästään palveluväylän toimintaan saattamisessa ja perustietovarantojen liittämisessä.

Kansallisen palveluväylän arkkitehtuurin kehittämishankkeen yhteydessä hankkeen ohjaus- ja työryhmät listasivat palveluita, joiden kehittämistä on syytä harkita.

Tyypillisesti tällaiset palvelut ovat koosteisia, hallinnonaloja ylittäviä palveluita, joille ei ole selkeää omistajaa. Palveluväylän hyödyllisyyden osoittamiseksi voisi olla hyvä tuottaa ainakin yksi monimutkaisempi palvelu, tuleville hankkeille esimerkiksi.

Esillä on ollut mm:

- Etuustietojen koostepalvelu. Sosiaalialan työntekijät tarvitsevat etuuspäätöksiä tehdessään paljon tietoa eri lähteistä (pankki, vero, tulot/menot, yms.)

- Terveydenhuollon potilaskertomus. Koostaa tietoa niin yksityisen kuin julkisen terveydenhuollon rekistereistä

7 Olemassa olevien vyöhykkeiden liittäminen

Olemassa olevien vyöhykkeiden liittämisessä askeleet ovat pääpiirteissään seuraavat:

- 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

Keskeisimpiä olemassa olevia palveluväyliä ovat VY-verkko, kuntien verkot, TUVE, KanTa ja terveydenhuollon palveluväylät.

Mikäli olemassa oleva palveluväylä ei tarjoa liittymää ulkopuolisille palveluille, väyliä ei luonnollisestikaan voida liittää toisiinsa.

Olemassa olevien väylien liittämisessä vastuu on pääasiassa ko. väylän omistajalla, käytännön asioista myös palveluväyläoperaattori on vastuussa. Aikataulutus on väylän omistajan harkinnassa.

8 Hankkeen riskit

Keskeisimmät aikatauluriskit

Yksittäisten toimeenpanon tehtävien riskien rinnalla kaikkein olennaisimmat hankkeen läpiviennin aikatauluun liittyvät riskit ovat:

1. Valtionhallinnon päätös kansallisen palveluväylän toteutuksen käynnistämisestä ja organisoinnista viivästyy
2. Ratkaisuvalinta viivästyy tai ratkaisu joudutaan kilpailuttamaan
3. Perustietovarantoja ei saada kytkettyä palveluväylään sen alkuvaiheessa

Näiden lisäksi keskeinen koko palvelun hyötyjen realisoitumiseen ja onnistumiseen liittyvä riski on:

A. Kansallisen palveluväylän rahoitusmalli on liittyjille epäedullinen

Riski 1: Valtionhallinnon päätös kansallisen palveluväylän toteutuksen käynnistämisestä ja organisoinnista viivästyy

- Tarkempi kuvaus: Kansallisen palveluväylän ratkaisua ei aleta toteuttaa riittävän nopeasti. Toteuttamisesta ja/tai palveluväylän omistajasta sekä palveluväyläoperaattoria ei saada ratkaistua ja sekä käynnistys että palvelun käynnistys viivästyvät merkittävästi.
- Ennaltaehkäisy: VM ja JulkICT ottaa vahvan vastuun työn käynnistämisestä pikaisesti. VM määrittää kansallisen palveluväylän organisointivastuullisen. Tämän jälkeen toteutuksen ja organisoinnin yksityiskohdat voidaan tarkentaa varsinaisen kehittämishankkeen aikana

Riski 2: Ratkaisuvalinta viivästyy tai ratkaisu joudutaan kilpailuttamaan

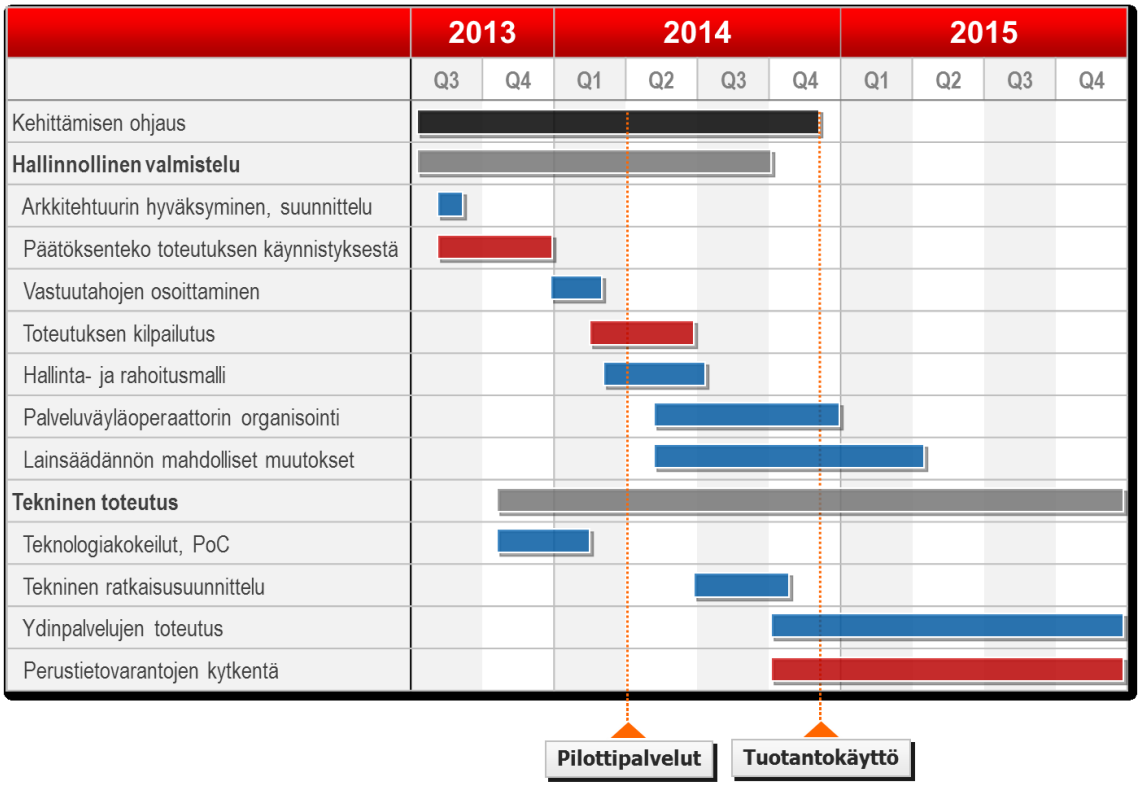
- Tarkempi kuvaus: Arkkitehtuurin lähtötilanteessa ja tavoitetilassa on tunnistettu keskeisimmät olemassa oelvat ratkaisumallit, joiden pohjalta kansallinen palveluväylä voitaisiin toteuttaa. Näitä ei testata teknisissä ja toimitusarvioinneissa (ns. PoC) riittävän nopeasti ja teknistä ratkaisupohjaa ei saada valittua. Mikäli valinta kohdistuu lisensoitavaan tuotteeseen eikä avoimen lähdekoodin ratkaisuun, itse ratkaisu ja/tai sen toteutus voidaan joutua kilpailuttamaan. Kilpailuttaminen viivästyttää aikataulua
- Ennaltaehkäisy: VM / JulkICT määrittää nopeasti arviointiryhmän, joka käy systemaattisesti mutta nopeasti ratkaisuvaihtoehdot läpi. Pohjaratkaisu valitaan ripeästi. Suositaan osana muuta arviointia avoimen lähdekoodin ratkaisuja JHKA-arkkitehtuuriperiaatteiden mukaisesti. Mikäli joudutaan kilpailutuksiin, hyödynnetään jo olemassa olevia puitejärjestelyjä, -sopimuksia ja/tai julkisen hallinnon asiantuntijoita kehittämisessä.

Riski 3: Perustietovarantoja ei saada kytkettyä palveluväylään sen alkuvaiheessa

- Tarkempi kuvaus: Perustietovarantoja ei saada mukaan kansalliseen palveluväylään joko teknisistä tai poliittisista syistä. Palveluväylään ei synny palveluja, jotka houkuttelevat varsinaisia substanssi- ja liiketoimintapalveluja mukaan. Tällöin on vaarana, että kansallisen palveluväylän käyttö jää vähäiseksi tai käyttö käynnistyy hyvin hitaasti
- Ennaltaehkäisy: Käytetään VM:n normi- ja/tai budjettiohjausta perustietovarantojen kytkemiseksi kansalliseen palveluväylään. Mikäli perustietovarantojen taustajärjestelmät eivä kykene palvelurajapintoihin, priorisoidaan kytkettäviä perustietovarantoja, esim.
    - VTJ

- KTJ
- YTJ
- Muut perustietovarannot

Mikäli edellä kuvatut riskit realisoituvat, aikataulu voi helposti venyä seuraavasti:



Kuvaan on punaisella merkitty viivästyvät osat edellisten riskien realisoituessa lievästi. Mikäli edellä kuvatut riskit realisoituvat kokonaisuudessaan, aikatauluviive voi olla vielä ylläkin kuvattua selvästi merkittävämpi.

Riski A: Kansallisen palveluväylän rahoitusmalli on liittyjille epäedullinen

1. Tarkempi kuvaus: Rahoitusmalli määritetään viitearkkitehtuurisuositusten vastaisesti sellaiseksi, että kansallisen palveluväylän käyttö ja siihen kytkeytyminen on liittyjille maksullista. Tämä vähentää merkittävästi kansallisen palveluväylän houkuttelevuutta ja vähentää sen käyttöä olennaisesti.
2. Ennaltaehkäisy: Kansallinen palveluväylä nähdään nykyaikaisen tietoon perustuvan yhteiskunnan perusinfrastruktuuri, joka mahdollistaa tuottavuuden kasvattamisen sekä sähköisen asioinnin merkittävän kehittämisen. VM tunnistaa tämän perustarpeen ja rahoittaa kansallisen palveluväylän kehittämisen ja perusoperoinnin budjettivaroin.

Varsinaisen hankkeen läpiviennin yleiset riskit

Edellä on kunkin toteuttamistehtävän kohdalle lueteltu kyseiseen tehtävään liittyviä riskejä. Niiden lisäksi on tunnistettu seuraavat koko hankkeeseen liittyvät hanketason ja käyttöönoton riskit:

Palveluväylän suuren toteuttamiskokonaisuuden koordinointi epäonnistuu

Toteutukset eivät synny oikea-aikaisesti. Yksittäiset toteutukset eivät muodosta toimivaa kokonaisuutta. Palveluntuottajat tekevät omia yhteen sopimattomia ratkaisujaan. Palveluväylän rakentaminen epäonnistuu.

Ennalta ehkäisy: Laaditaan riittävän tarkka toteutussuunnitelma kokonaisuudelle ja luodaan toteutukselle toimivat ohjaus- ja koordinointirakenteet. Vastuutetaan eri osapuolet riittävästi ja selkeästi.

Organisaatiot eivät valmistaudu ajoissa väylän käyttöönottoon

Palveluväylän laajamittaiseen käyttöön saaminen hidastuu. Kriittisen massan muodostumisen viivästyminen saattaa pilata koko käyttöönoton.

Ennalta ehkäisy: Laaditaan kuvaus siitä, miten palveluväylään liitytään ja mitä se edellyttää organisaatioilta. Julkisten organisaatioiden on sisällytettävä väylän käyttöönotto toimintasuunnitelmiinsa ja budjetteihinsa heti ensi tilassa.

Kansallista yhteistä tunnistamisratkaisua ei synny

Yhteinen tunnistamisratkaisu on yksi palveluväylän käytön kannalta olennainen yleispalvelu. Epäonnistuminen tässä ratkaisussa vaikuttaa suuresti väylän käyttöön.

Ennalta ehkäisy: Haetaan yhteistä ratkaisua yhdessä eri toimijoiden kanssa.

9 Referenssit

/1/ Kansallinen Palveluväylä, viitearkkitehtuuri
/2/ Nykytila-arvio, yhteenveto
/3/ Kansallinen Palveluväylä, Hallinta-, palvelutuotanto- ja liiketoimintamallit