

Maa- ja metsätalousministeriön tietopalvelukeskus

Valtiovarainministeriö

VIITE:VM:N LAUSUNTOPYYNTÖ 5.9.2013 VM008:00/2013, MMM DNRO 356/601/2013

MAA- JA METSÄTALOUSMINISTERIÖN TIETOPALVELUKESKUKSEN LAUSUNTO KANSALLISEN PALVELUVÄYLÄN VIITEARKKITEHTUURISTA SEKÄ SEN ALUSTAVASTA TOTEUTUSSUUNNITELMASTA

Yleistä

Ehdotuksessa kuvatut yhteentoimivuusmekanismit ja arkkitehtuurivalinnat heijastavat yleisesti hyväksi pidettyjä malleja. Mallista on löydettävissä selkeitä yhtäläisyyksiä, jopa teknisten valintojen tasolla siihen, miten maa- ja metsätalousministeriön hallinnonalalla laajasti käytössä oleva sovellusarkkitehtuuri on mallinnettu. Viitearkkitehtuuri-nimestään huolimatta dokumenteissa menttiin suhteellisen syvälle toteutusyksityiskohtiin. Tästä johtuen lausunnossa kommentoidaan osaksi teknisiäkin asioita.

Yleiset kommentit

Palveluväylän jalkautumiseksi hankkeen tulee kyetä houkuttelemaan riittävästi palveluja, jotta väylän käyttöönotosta koetaan saatavan riittävää hyötyä. Tämä on hankkeen merkittävin riski, sillä väylän millään muulla ominaisuudella ei ole väliä, mikäli väylä ei tarjoa riittävästi palveluja. Riski on tunnistettu, mutta se ei mielestämme heijastu riittävästi lausuntomateriaalissa esitettyyn priorisointiin. Lausuntopyyntömateriaalista puuttui toteuttamissuunnitelmassa viitattu "Kansallinen Palveluväylä, Hallinta-, palvelutuotanto- ja liiketoimintamallit", jonka perusteella olisi pystynyt paremmin arvioimaan miten laajasti tätä riskiä on käsitelty.

Organisaatiot, jotka tarvitsevat tietoja perusrekistereistä ovat tehneet integraatiot jo olemassa oleviin rekisteripalveluihin. On vältettävä sitä, että näiden integraatioiden vaihtaminen palveluväylään olisi kustannus ilman lisäarvoa. Ilman lisäarvoa organisaatioiden sisäinen priorisointi suosii väistämättä uusia kehityshankkeita ja välttämättömiä ylläpitotoimenpiteitä. Tämä voi johtaa mm. Virtun ja Asiointitilin kohtaamaan tilanteeseen, missä toimivan järjestelmän käytön laajeneminen pysähtyy tai jopa estyy, koska järjestelmä ei ole saavuttanut kriittistä massaa.

Tästä riskistä johtuen jatkotyöstössä tulisi omistautua käyttökynnyksen matalamiseen. Tämä koskee sekä kynnystä käyttää palveluita palveluväylän välityksellä että kynnystä tarjota palveluita väylän kautta. Keskeisiä onnistumistekijöitä ovat kustannukset, selkeät ja yhdenmukaiset käyttöehdot, lisäarvon tarjoaminen nykyisiin rajapintoihin nähden sekä väylän palveluiden helppokäyttöisyys. Väylän käyttökustannusten tulisi olla vähintään kilpailukykyiset nykyään käytettyjen rekisteripalveluiden kanssa.

Julkisten tietojen ja tilastojen tarjoaminen väylän kautta toisi väylälle sen paljon tarvitsemaa käyttöä, näkyvyyttä sekä osaamista. Helppokäyttöisellä väylärajapinnalla olisi mahdollista houkutella avoimen datan sovelluskehittäjiä ja rakentaa osaamispoolia, jota hyödyntämällä voisi kasvattaa väylän käyttöä.

Palveluväylän hallintamallin monimutkaisuus vaikuttaa myös merkittävästi käyttöönottokynnykseen. Hallintaan osallistuvien osallistujien määrästä johtuen tämä on realistinen riski. Mallin kehityksessä on syytä kiinnittää huomiota siihen, miten määritellyt prosessit näkyvät niiden loppukäyttäjille, eli väylän käyttäjille ja väylässä palveluita tarjoaville organisaatioille. Kankea malli aiheuttaa lisäkustannuksia hallintaorganisaatiolle ja vaikuttaa negatiivisesti väylän käytön laajenemiseen.

Toimittajariippumattomuutta ei ole nostettu korkeimmalle prioriteetille arkkitehtuuriperiaatteista. Sitä ei kuitenkaan pidä nähdä pelkästään arkkitehtuuriperiaatteena, vaan myös olennaisena mekanismina riskien hallintaan. Korkeimmalle prioriteetille asetetut tavoitteet vikasietoisuudesta, korkeasta käytettävyydestä, laajennettavuudesta ja skaalautuvuudesta sisältävät todellisen riskin epäonnistumisesta. Riskin aktualisoituessa, ilman toimittajariippumattomuutta, on hyvin vaikea tehdä korjausliikkeitä. Näiden riskien hallitsemiseksi suosittelemme arvioimaan uudestaan toimittajariippumattomuuden prioriteettia verrattuna yllä mainittuihin tavoitteisiin.

Lisäksi ehdotamme, että toteutus suunnitelman yhteydessä luodaan strategia suunnitelmalliselle käyttönotolle ja sen tukemiselle. Strategiassa tulisi ottaa kantaa kustannus yms. -hyötyjen tarjoamiselle, etteivät kansallisen palveluväylä käyttönoton tukitoimenpiteet jäisi hajanaisiksi tai satunnaisiksi toimenpiteiksi.

Tekniset kommentit

Tuotettavat ympäristöt

Viitearkkitehtuurissa on otettu huomioon tarve testiympäristölle. Sovelluskehitys on usein vähintään kolmiportaista (kehitys, testi ja tuotanto). Vetuma- ja KATSO-palveluihin liittyvässä käytännön kehitystyössä erillisen kehitysympäristön puute on aiheuttanut merkittäviä ongelmia. Palveluväylän kohdalla yhden sovelluksen kehitystyö jakautuu useaan organisaatioon, koska vastuu kehitettävästä loppukäyttäjän sovellusta ja sen käyttämistä uusista tai muokatuista rajapinnoista voi olla hajautunut. Tästä johtuen, palveluväylälle tarvitaan testiympäristöstä erillinen kehitysympäristö.

Lisäksi tuotantoonvientien tukemiseksi tulisi olla täysin tuotantoa vastaava koe-käyttöympäristö. Palveluväylän ympärillä tulee tapahtumaan jatkuvaa rinnakkaisesta kehittämisestä. Tästä johtuen testiympäristössä, sekä itse väylässä että sen palveluissa, tulee olemaan uusia ominaisuuksia ja muutoksia vanhoihin ominaisuuksiin, joita tuotantoympäristössä ei vielä ole. Koekäyttöympäristöllä voidaan taata uuden sovelluksen tai päivityksen olevan yhteensopiva tuotantoympäristön kanssa. Tämän kaltainen koekäyttö on tärkeää, oli sitten kyseessä päivitys palveluita käyttävään sovellukseen, väylään tai tarjottavaan palveluun. Lisäksi tuki moniportaiselle sovelluskehitykselle yhdistettynä kattavaan ja anonymisoituun testiaineistoon toisi merkittävää lisäarvoa palveluväylälle verrattuna useaan nykyiseen rekisterirajapintaan.

Liityntäpalvelin

Liityntäpalvelimien välillä käytettävän protokollan tulee pohjautua avoimiin standardeihin ja yleisesti käytettyihin tekniikoihin. Kansallisesti tärkeän tekniikan jatkuvuuden ja laadun kannalta on välttämätöntä, että on olemassa mahdollisuus kehittää rinnakkaisia toteutuksia liityntäpalvelimesta. Toimittajaloukkuongelmien välttämisen lisäksi avoimet standardit mahdollistavat kilpailun liityntäpalvelintuotteiden ominaisuuksilla ja vaihtoehdot antavat organisaatioille mahdollisuuden valita heidän ympäristöönsä sopivimman tuotteen.

Organisaation omien tietojärjestelmien ja liityntäpalvelimen välillä oleva rajapinta on ymmärrettävästi jätetty pois viitearkkitehtuurista. Tämän rajapinnan toimivuus on kuitenkin kriittinen menestystekijä ja tulisi nostaa esiin merkittävänä riskitekijänä liityntäpalvelinohjelmiston toteutukselle. Rajapinnan toimivuus tässä yhteydessä koostuu muun muassa joustavuudesta, yhteensopivuudesta käytössä olevan teknologian kanssa, luotettavuudesta ja helppokäyttöisyydestä.

Tietoturva

Viitearkkitehtuurissa mainitaan useassa paikkaa MD5 tiivisteiden käyttö. Vaikka maininnat ovatkin esimerkinomaisia, viitteet tiivistealgoritmiin tulisi korvata paremmalla algoritmilla, kuten SHA256:lla. MD5 on jo lähes kymmenen vuotta sitten todettu riittämättömäksi tietoturvakäyttöön¹. Näin huonoon tiivistealgoritmiin viittaaminen nostaa dokumentin uskottavuuden tietoturva-asioissa kyseenalaiseksi.

Viitearkkitehtuurin kappaleen 6.2.2 kutsuprotokolla on kuvattu hyvin tarkalle tasolle. Tällä tasolla suunniteltaessa keskeistä tietoturvamekanismia, tulisi protokollan lähde ilmetä – onko tämä yleisesti tunnettu, tutkimukseen perustuva protokolla vai dokumentin kirjoittajan esimerkinomainen kuvaus mahdollisesta toimenpidesarjasta? Luotamme siihen, että palveluväylän kutsumekanismien tarkka suunnitelma ja protokollat julkaistaan myöhemmin lausunnoille sekä annetaan auditoitaviksi tietoturva-alan ammattilaisille ennen lopullisen toteutuksen aloittamista.

Päätös käyttää lyhytaikaisia varmenteita liityntäpalvelimien välisen liikenteen suojaamiseksi on kiitettävä. Aktiivisesti päivittyviin sulkulistoihin ja tarkistuspalveluihin perustuva varmenteiden tarkistaminen on käytännössä mahdotonta tehdä oikein.

MMM:n hallinnonalan näkökulma

Maa- ja metsätalousministeriön tietopalvelukeskuksen (Tike) kehittämä ja käyttämä sovellusarkkitehtuuri vastaa kuvattua autentikoidun verkoston arkkitehtuuria. Palvelupyynnöt tehdään yhdenmukaisella mekanismilla sovellusten ja tietovarantojen välillä ja toimintaa koordinoi yhteinen autentikointi ja palveluhakemisto. Tätä teknologiaa käyttää miltei 40 viranomais- ja asiointisovelluksesta. Tiken sovellusarkkitehtuurin mukaiset sovellukset sopisivat alkuvaiheessa osaksi palveluväylää yhtenä vyöhykkeenä.

Tike tarjoaa usealle kolmannen osapuolen toimijalle ja sovellukselle integrointeja ympäristön sisällä oleviin tietovarantoihin ja prosesseihin. Integraatioihin käytetään vastaavaa teknologiaa, kuin mitä palveluväylän viitearkkitehtuurissa hahmoteltiin. Kommunikaatio tapahtuu SOAP-viestein ja molemmat keskustelu-

¹ <http://eprint.iacr.org/2004/199.pdf>

kumppanit tunnistavat vastapuolen tämän tarjoaman varmenteen perusteella. Tämä vastaa pitkälti viitearkkitehtuurissa kuvatun vyöhykkeen roolia. Palvelupyynnöt sekä vyöhykkeen sisällä että integraatorajan yli ovat täysin jäljitettävissä.

Tikellä on siis tekniset valmiudet tarjota palveluväylälle asiakasorganisaatioidensa sovellusten palveluita ja prosesseja näin yhdessä sovittaessa. Koska Tiken kehittämä ja käyttämä arkkitehtuuri on lähestulkoon yhteensopiva itse palveluväylän vaatimuksien kanssa, olisi järkevää hyödyntää tätä kokemusta palveluväylän jatkokehityksessä. Tikellä on ainutlaatuista osaamista tämäntyyppisen yhteentoimivan autentikoidun verkoston kehityksestä ja ylläpidosta ja voi siksi tarjota merkittävää panosta palveluväylän jatkotyöstössä.

Muita huomioita

Viitearkkitehtuurissa loppukäyttäjiä ei ole määritelty johdonmukaisesti. Osassa loppukäyttäjäksi lasketaan ainoastaan asioijat, ja toisaalla dokumentissa loppukäyttäjiksi lasketaan isompi käyttäjäryhmä mukaan lukien esim. viranomaiset.

Viitearkkitehtuurissa esitellään ristiriitaisia kommentteja dokumentin abstraktiotasosta. Näiden tarkentaminen ja yhtenäistäminen olisi tarpeen, jotta dokumentin taustalla oleva visio välittyisi selvemmin. Osassa dokumenttia arkkitehtuuri kuvataan runkona tarkemmalle suunnittelulle ja toisaalla esitetään reunaehto että dokumentin valmistumisen jälkeen toteutus voidaan käynnistää heti.

Muilta osin Tikellä ei ole lausuttavaa luonnoksesta.

Lisätietoja Tiken lausunnosta antaa yksikön päällikkö Johanna Knekt (puh. 040 8400340, johanna.knekt@mmmtike.fi).

Toimialueen päällikkö
Ylijohtajan sijaisena

Päivi Kasurinen

Yksikön päällikkö

Terhi Wainio-Biese