

LAUSUNTO

Valtiovarainministeriö
valtiovarainministerio@vm.fi

20.9.2013

Yhteyshenkilö:
ICT-johtaja, ylijohtaja Timo Valli

Aihe: KANSALLISEN PALVELUVÄYLÄN ARKKITEHTUURIN SUUNNITTELUHANKE
Valtiovarainministeriön pyytämää lausuntoamme Kansallisen palveluväylän
viitearkkitehtuurista sekä sen alustavasta toteutussuunnitelmasta

Lausuntonamme ja vastauksena pyyntöönnne esitämme seuraavaa:

(1)

REST rajapintojen merkitys verrattuna perinteisiin SOAP-pohjaisiin rajapintoihin Web Services integraatioissa on jatkuvasti kasvanut merkityksessä. Tänä päivänä yhä harvemmin enää käytännössä kysytään SOAP-pohjaisia rajapintoja. Viitearkkitehtuurissa todetaankin, että REST on näistä kahdesta suositeltavampi sanomanvälitysmalli. Kuitenkin viitearkkitehtuurista saa sen kuvan että SOAP integraatiot olisivat ensisijainen ja REST integraatiot vasta toissijaisia vaatimuksia. Suosittelemme että 'Palveluväylä tukee REST-palvelurajapintaa' -vaatimus saisi luokituksen 'Välttämätön'.

(2)

Viitearkkitehtuurissa otetaan kantaa moneen tekniseen asiaan myös protokollatasolla. Kuitenkaan tunnistukseen liittyviin teknologioihin ja protokoliin ei ole juurikaan otettu kantaa. Myöskään selkeää tahdonilmaisua ei ole tämän suhteen tehty. Esim. identiteetti- ja pääsynhallinnan standardien käyttö mahdollistaa mm että voi hyödyntää eri kautta tarjolla olevia valmiita integraatiomoduleita ja näin saavuttaa sekä tietoturva- että merkittäviä kustannusetuja.

Tähän perustuen, haluamme korostaa, että on tärkeää varmistaa että valmiita vapaasti tai kaupallisesti tarjolla olevia integraatiomoduleita voi hyödyntää, esim sellaiset jotka tarjoavat SAML SP tai vastaavat WS-Federation tai Oauth toiminnallisuudet.

Huomautamme myös, että viittaus kansainväliseen yhteensopivuuteen, avoimuuteen, sekä luotettavuuteen tarkoittaa tunnistuksen ja identiteettihallinnan osalta käytännössä SAML 2.0 ja WS-Federation protokollien tukea ja sertifioitujen standardien mukaisten ratkaisujen hyödyntämistä.

Viitearkkitehtuurin määrittelyillä voidaan käytännössä, myös ei-tarkoituksellisesti, estää standardien hyödyntäminen ja tuotepohjaisten ratkaisujen käyttö. Tämä merkitsisi että siinä tapauksessa Suomen julkinen sektori joutuisi kustantamaan projektien kautta kaikki suunnittelu-, määrittely ja toteutustyö; sekä lisäksi raskas laadunvarmistus ja sertifiointiprosessi kokonaisuudessaan, sen sijaan että voitaisiin hyödyntää myös valmiita tuotepohjaisia ratkaisuja.

Pahimmillaan koko palvelumallista tulisi näin massiivisen iso julkisen sektorin projektitoimitus (tai palvelu), eikä sellaista pitkäjänteistä tervettä ja kustannustehokasta toimintaa, missä myös tuotepohjaisilla ratkaisuilla ja yksityisellä sektorilla on oma roolinsa ja muuta kuin vain projekti- ja asiantuntijaliiketoimintaa. Standardien hyödyntäminen ja tuotepohjaisten ratkaisujen edellyttää että esim standardien periaatteita ei rikota. Siksi on tärkeää että varmistetaan että hankinnassa voidaan käyttää myös olemassa olevia kaupallisia ratkaisuja.

Kun asetetaan vaatimuksiksi kustannustehokkuus, sekä uuden tunnistusratkaisun tulee olla nykyisiä ratkaisuja edullisempi sekä sähköisten palvelujen tarjoajille että niiden käyttäjille, niin tässä tulee huomioida kokonaiskustannukset ratkaisujen ja palvelujen koko elinkaarelta. Siksi nojautuminen tuotepohjaisiin ja koeteltuihin valintoihin tulee olemaan keskeistä.

(3)

Mikäli määritellään vain Suomen oloihin ja markkinoille soveltuvia ratkaisuja, niin kaupallisilla toimijoilla ei ole intressejä toteuttaa tuotteistettuja ratkaisuja joilla olisi myös vientimahdollisuuksia. On tärkeää että varmistetaan että onnistunut suomalainen public-private yhteistyö myös käytännössä jatkossakin toimii niin, että kaupallisilla toimijoilla on riittävästi intressejä panostaa omaa tuotekehitystä ja liiketoiminnan kehitystä asian eteen, mikä koituu myös Suomen julkisen sektorin ja suomalaisen yhteiskunnan hyödyksi. Valinnoillaan julkinen sektori voi tärkeänä lisänä osaltaan myös vaikuttaa siihen syntytykö ja onko Suomella tällä alueella myös vientituotteita.

(4)

Kun Kansallisen palveluväylän tukipalveluja suunnitellaan, niin on syytä huomioida että monia näistä toiminnallisista kokonaisuuksista on myös mahdollista hankkia valmiina tuotteina joita voi konfiguroida käyttöön. Tämä on kustannustehokas vaihtoehto sille, että perustetaan mittava ohjelmistokehityshanke joka ja josta pitkässä juoksussa tulee valtionhallinnolle riippakivi ja helposti massiivinen jatkuva projektitoimitus.

Tämä koskee muun muassa seuraavia viitearkkitehtuurin erityisiä toiminnallisia kokonaisuuksia jotka on viitearkkitehtuuridokumentaatioissa mainittu:

- Organisaation tunnistaminen
- Kansalaisen tunnistaminen
- Suostumusten ja tahdonilmaisujen hallinta
- Valtuutusten ja puolesta-asioinnin hallinta

sekä tarkemmin esimerkiksi:

- 'Suostumusten hallinnan keskeiset ominaisuudet' ovat kaikki vakio-ominaisuuksia Ubisecuren CustomerID tuotteessa.
- 'Keskeiset valtuutusten hallintaan liittyvät toiminnallisuudet' ovat kaikki vakio-ominaisuuksia Ubisecuren CustomerID tuotteessa.
- Koskien Toimenpidesuostumuksia, niin Ubisecuren CustomerID tuotteen REST-rajapinnassa olevalla Create Mandate Template-toiminnolla voidaan luoda esivalmisteltuja valtuutus pohjia tiedonluovutusta ja toimenpiteitä varten. Kun valtuutus halutaan antaa vastaanottajalle, niin tarvittava valtuutus pohja liitetään vastaanottajaan (käyttäjä tai organisaatio).
- Yritysten ja organisaatioiden tunnistamisen käyttötapaukset ovat vakio-ominaisuuksia Ubisecuren CustomerID tuotteessa

(5)

Viitearkkitehtuurissa ei selkeästi ilmene miten on tarkoitus hallita sitä mitä tietoja ja mistä käyttäjistä Palveluväylään liitetyt sovellukset saa kysellä tietoja esim käyttäjistä. Palveluväylän arkkitehtuuridokumentin mukaan on olemassa "Sopimuskatalogi" joka osittain viittaa tähän toimintoon. Epäselväksi jää edelleen, onko tämä vain 'export' jostain järjestelmästä tai palvelusta missä sopimuksia varsinaisesti hallitaan, vai onko tämä se osa kokonaisuutta missä näitä tietoja myös primääristi hallitaan. Näiden hallinta tulee olemaan merkittävä haaste kokonaisuuden toimivuuden kannalta.

(6)

Kansallinen palveluväyläarkkitehtuuri –dokumentissa on mainittu joitakin Ruotsissa käytettyjä malleja, mutta ei lainkaan sitä että Ruotsissa ollaan par’aikaa siirtymässä uudempaan malliin (EID2) joka paremmin täyttää myös EU-direktiiviä. Myös terveydenhuollossa ollaan siirtymässä federatiiviseen malliin (SAMBI). On tärkeää että myös Suomessa käytettäisiin federatiivista tunnistusmallia, joka myös mahdollistaa kilpailuttamisen ja eri toimijoiden palvelujen rinnakkaisen toiminnan. Keskitetty malli tunnistuksessa ja muissa identiteetti- ja pääsynhallinnan toiminnoissa ei tulisi olemaan kokonaiskustannusten kustannustehokas tai palvelulaadun kannalta paras malli.

(7)

Jotta Kansallinen Palveluväylä tulee kustannustehokas ja ketterä on myös syytä varmistaa että siinä on mahdollista hyödyntää erilaisia pilvipalveluja ja niiden kautta myös aikaansaada joustavuutta. Nykyisessä muodossaan Viitearkkitehtuuri vaikuttaa joiltakin osin edelleenkin melko keskitetyltä ja raskaalta, kun ideaalimalli olisi ketteryttä ja jatkuvaa kehitystä mahdollistava malli.

Ystävällisin terveisin

UBISECURE SOLUTIONS OY

Charles Sederholm
Toimitusjohtaja