

APIt puolesta-asioinnissa

Citrus Solutions oy /

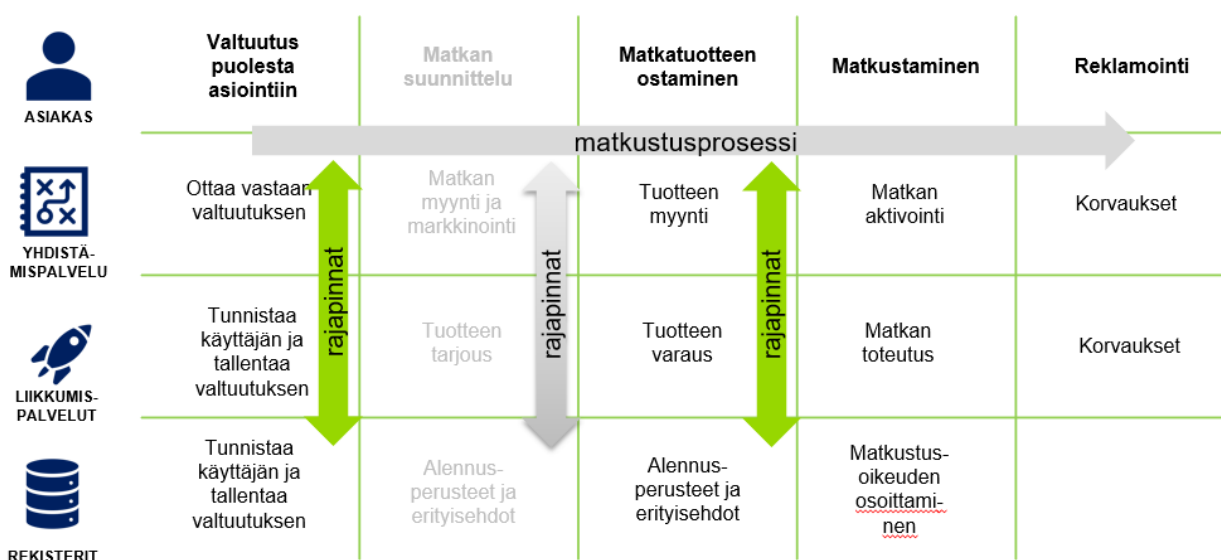
Marjukka Niinioja, Olli Nylander, Tessa Viitanen
20.11.2018

1. Johdanto

Citrus-tiimi on yhdessä projektiryhmän kanssa valmistellut eräitä mahdollisia tapoja puolesta-asioinnin matkaketjujen rajapintojen määrittelyyn ja tietovirtoihin. Lainsäädäntö ei määrittele tarkkaan rajapinnoista, joten periaatteessa on mahdollista ratkaista asiat eri osapuolten kesken usealla eri tavalla. Tässä Citruksen dokumentissa kuvataan ratkaisujen välineitä, jotka ovat osittain teknisiä luonteeltaan.

2. Matkaketjujen osapuolet ja tietovirrat

Rajapintakuvausten pohjaksi on tehty yleinen matkaketjukuva. Osapuolet ovat asiakas, yhdistämispalvelu, liikkumispalvelut ja rekisterit. Matkaketju etenee seuraavissa vaiheissa: asiakas antaa valtuutuksen puolesta asiointiin, matkan suunnittelu (ei kuulu lainsäädännön piiriin, kuvassa harmaana), matkan ostaminen, matkustaminen, reklamointi.

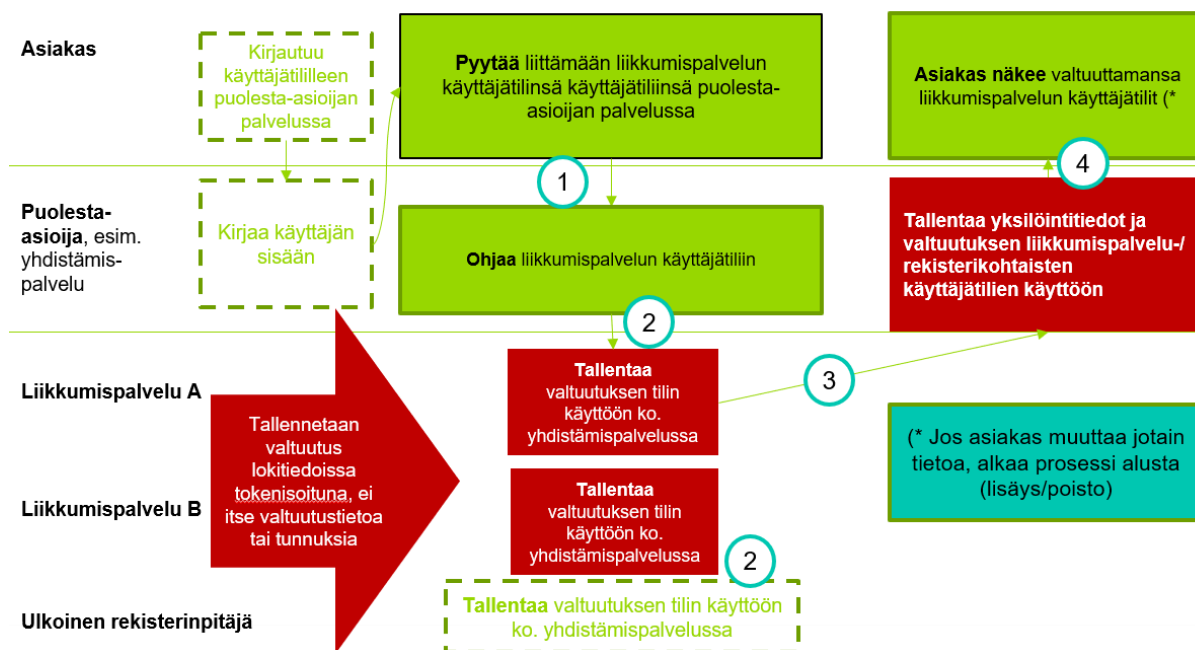


Kuvan mukaisesti rajapintamäärytykset ovat oleellisia valtuutusvaiheessa ja matkan ostamisvaiheessa. Matkaketjun osapuolilla on puolesta asiointissa erilaisia rooleja, jotka on kuvattu seuraavassa:

| Tehtävä /rooli | Asiakas | Puolesta asioija (esim. yhdistämis-palvelu) | Rajapinnan avaaja (esim. kuljetuspalvelu) | Ulkoinen rekisterinpitäjä |
|---|---------|---|---|---------------------------|
| Valtuutus käyttäjälle käyttöön | X | | | |
| Valtuutuksen varmistaminen | | X | X | X |
| Matkaketjuun liittyvien tuotteiden tiedot | | X | X | |
| Palvelujen saatavuus | | | X | |
| Rajapintojen avaaminen | | X | X | (X) |
| Matkatunnistusten tuottaminen | | X | X | |
| (Maksaminen) | X | | | |

3. Valtuutus

Valtuutuksesta on tehty prosessikuvaus. Kuvauksen osapuolet ovat asiakas, puolesta-asioija (esim. yhdistämispalvelu), liikkumispalvelu ja ulkoinen rekisterinpitäjä. Punaisella kuvatut alueet perustuvat erääseen vaihtoehtoiseen ratkaisumalliin, jossa valtuutuksen yksilöintitiedot tallennetaan sekä puolesta-asioijalle että liikkumispalvelun tuottajalle. Lopullinen ratkaisu riippuu osapuolista ja niiden omista sisäisistä tarpeista.



Valtuutuksen rajapinnat on kuvassa ympyröity luvuilla 1-4. Rajapintojen kautta kulkeva tietosisältö on esitetty seuraavassa taulukossa:

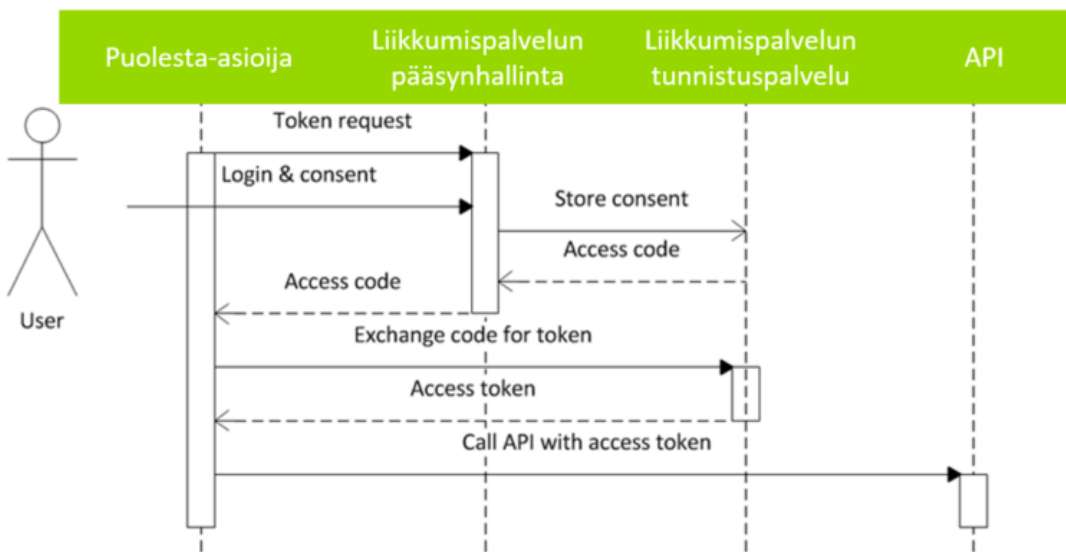
| Valtuutuksen rajapinnat | Tietosisältö |
|--|---|
| 1. Asiakas käynnistää valtuutustoimenpiteen | <ul style="list-style-type: none"> Asiakkaan tunniste yhdistämispalvelussa Liikkumispalvelutieto eli mihin palveluun halutaan yhdistää |
| 2. Käyttäjän tunnistaminen, uuden valtuutuksen tekeminen, aiemman muuttaminen, valtuutuksen voimassaolon tarkistus tai rekisterin tietojen tarkistaminen (KUTSU) | <ul style="list-style-type: none"> Yhdistämispalvelun tunnistetieto (esim. sopimusnumeroon perustuva tieto) Asiakkaan tunnistetieto valtuutetussa palvelussa tai uuden valtuutuksen osalta asiakkaan henkilöön liittyvä tunnistetieto (palvelun erityislainsäädännön ja tietosuojatason mukaisesti) |
| 3. Valtuutus liikkumispalvelun ja käyttäjätilin käyttöön | <ul style="list-style-type: none"> Asiakkaan tunnistetieto valtuutetussa palvelussa (jos tili tai rekisteritieto on olemassa), valtuutuksen mahdollinen voimassaoloaika.*) <p>*) Näistä esitetään OpenID Connectiin ja OAuth2 –standardiin sekä Kansallisen luottamusverkkoon perustuva sekä palvelin pohjaiseen toteutukseen perustuva vaihtoehto</p> |
| 4. Puolesta asioija ilmoittaa asiakkaan valtuuttamat käyttäjätilit ja muut mahdolliset vielä valtuuttamattomat palveluntarjoajat (PALAUTE) | <ul style="list-style-type: none"> Valtuutettujen liikkumispalvelutilien tunnisteet Tarjolla olevat liikkumispalvelukumppanit / matkaketjun osalliset tai rekisteri, joille ei vielä valtuutusta |

Valtuutuksen käytössä ja tallentamisessa voidaan noudattaa seuraavia periaatteita:

- Kyseessä on tietojen luovutus liikkumispalvelulta puolesta-asioijalle
- Liikkumispalvelun tulee tallentaa tieto, että käyttäjä on antanut luvan luovuttaa tietoja.

- Tieto tulee tallentaa vähintään niin kauan kuin tietojen luovutus, tässä tapauksessa valtuutus käyttää käyttäjätilin tietoja on voimassa
- Suppeimmillaan valtuutus on pääsynhallinnan token, jolla on useimmiten voimassaoloaika kymmenistä sekunneista joihinkin tunteihin ja jonka palvelu voi uusia ns. refresh tokenin avulla aina kun käyttäjä käyttää palvelua niin kauan kuin käyttäjä löytyy ja valtuutusta ei ole poistettu. Valtuutuksen päätyttyä tieto on tallentunut lokitietoihin, joista sitä voidaan tarvittaessa tarkastella ristiriita- tai tietoturvatapahtumatilanteissa lokitietojen säilytysajan puitteissa
- Liikkumispalvelu on pääsynhallintapalvelun asemassa ja vastaa siitä, kuinka kauan tunnistus ja valtuutus ovat voimassa.

Kuvassa esitetty malli kuvaa OpenID Connect –pohjaista auktorisointi- ja tunnistamisflowta. Tämä on yksi vaihtoehto.



Käyttäjä valtuuttaa puolesta-asioijan käyttämään liikkumispalvelun käyttäjätiliään. Tästä valtuuttamisesta olemme rakentaneet kaksi vaihtoehtoista mallia, jotka on esitetty seuraavassa kuvassa.

Federoitu tunnistautuminen

1. Käyttäjä kirjautuu myös liikkumispalvelun tilille.
2. Kirjautumisen jälkeen käynnistyy valtuutusprosessi, jolloin puolesta-asioija välittää liikkumispalvelulle käyttäjän tiiltä löytyvän liikkumispalvelun rajapinnan tuntemaan tunnisteen, joka on riittävällä tasolla, mutta ei suoraan myös liikkumispalvelun tiedossa.
3. Toteutustapa tyypillisesti OAuth2 ja sen päälle tehty OpenID Connect-ratkaisu, jossa standardin mukainen access code, joka vaihdetaan tokeniin, johon on tallennettu käyttäjän identiteetin tunnistee, kuten sähköpostiosoite, myös muita käyttäjän perustietoja voidaan välittää (yleensä ainakin nimi, mahdollisesti puhelinnumero ja muita tietoja) käyttäjän suostumuksella.
4. Suositellaan käytettäväksi PPID:tä (Pairwise Pseudonymous Identifiers) selväkielisten tunnisteen sijaan, jotta eri palveluiden keräämää dataa ei ole suoraan mahdollista yhdistää.

Järjestelmätason tunnistautuminen

1. Käyttäjä antaa tunnisteen (ei kirjautu liikkumispalvelun tilille itse), jolla puolesta-asioija käy tekemässä sopimuksen mukaan kyselyn liikkumispalvelun rajapintaan: sähköpostiosoite, puhelin, kanta-asiakastunniste, matkakortin tunnistee.
2. Tämä vaihtoehto ei ole suositeltava siksi, että siinä kuka tahansa, jolla on sekä käyttöoikeus rajapintaan että käyttäjän tunnistee voi luoda valtuutuksen käyttäjän tietämättä.

OpenID Connect protokolla pohjautuu OAuth2 (RFC 6749) -standardiin <https://tools.ietf.org/html/rfc6749> . OpenID Connect on federoituun eli jaettuun tunnistautumiseen OAuth2 –päälle rakennettu suositus: https://openid.net/specs/openid-connect-core-1_0.html . OpenID Connect on turvallisempi kuin pelkkä OAuth2 tai SAML ja soveltuu JSON-muotoisiin rajapintoihin paremmin kuin SAML, joka taas soveltuu erityisesti SOAP-rajapintoihin. Suurin osa suosituista tunnistamiseen käytetyistä palveluista maailmalla käyttää OpenID Connectia tai SAMLia, myös Suomessa käytetty pankkien TUPAS tunnistautuminen ollaan korvaamassa niillä. Siirtymäaika loppuu 2019 syksyyn mennessä TUPAS-luottamusverkostoon kuuluvilta: <http://www.finanssiala.fi/uutismajakka/Sivut/Luottamusverkosto,-TUPAS-ja-tunnistamisen-muutokset.aspx> . Viestintävirasto on tehnyt suositukset 212/2018 S (SAML) ja 213/2018 S (OIDC) Kansallisen luottamusverkoston rajapinnoista. Suomalainen tunnistautumisen kenttä on muuttunut OpenID Connectin suuntaan vuoden 2018 aikana.

Mm. LIPPU –projektin 1 vaiheessa on käytetty OAuth2 –mukailevaa toteutusta mutta ilman OpenID Connectin suosittamia käytäntöjä. Mm. 1. Vaiheen APIssa <https://github.com/finnishtransportagency/lippu-api> on käytetty räätälöityä X- Authorization –headeria, kun taas suositus on käyttää API-kutsuissa standardia Authorization-headeria Bearer –tokenilla. Esimerkki käyttäjän tietojen hakemisesta, jos liikkumispalvelu tarjoaa suosituksessa mainitun /userinfo -rajapinnan

GET /userinfo HTTP/1.1

Host: server.example.com

Authorization: Bearer SIAV32hkKG

Myös 1. vaiheen rajapinnan login – endpointit ovat toiminnaltaan ja nimiltään erilaisia kuin suosituksen mukaiset /authorize ja /token. Esimerkitoteutuksessa ei ole ollut mukana puolesta-asiointin vaatimusta, eli käyttäjätiliä ja sen käyttäjän tunnistamista. 1. vaiheen rajapinnassa tunnistautunut rajapinnan käyttäjä ei ole käyttäjätilin omistaja vaan rajapintaa käyttävä sovellus. Matkustajan tiedot välitetään selväkielisinä, ei pseudonymisoituina. Suosituksesta poikkeaminen aiheuttaa yleensä ylimääräistä määrittelyä, suunnittelua, toteutusta, testausta ja tietoturvan varmistamista rajapinnan käyttäjiltä ja saattaa muodostaa ylimääräisen esteen ja kustannuksen rajapinnan käyttöön.

Valtuutus on mahdollista antaa myös suostumuksen perusteella¹. Esimerkinä mm. Dittmar & Ingreniuksen tekemän tietosuojaselvityksen suostumukseen perustuvan valtuutuksen antamista listaamme tässä OpenID Connect suosituksen tarjoamat vakiotavat käyttäjän kanssa vuorovaikutukseen. Rajapinnan tarjoajan kannattaa huomioida kuitenkin, että suostumus on vain yksi valtuutuksen hankintatavoista. OpenID Connect -pohjaista ratkaisua käytettäessä **liikkumispalvelun** tulisi toteuttaa, kun käyttäjä asioi puolesta-asiointia tarjoavan palvelun kautta ja puolesta-asioija kysyy suostumusta käyttäjän puolesta

- none: sopii siihen, että tarkistetaan, onko olemassa olevaa valtuutusta, palautetaan vain virheet

¹ Suostumuksella ei tässä välttämättä tarkoiteta oikeudellista suostumusta henkilötietojen käsittelyyn vaan yleisesti käyttäjän tietoisena pitämistä.

- Login: pyydetään käyttäjää kirjautumaan uudelleen, jos kirjautuminen ei ole enää voimassa
- Consent: pyydetään suostumusta tietojen käyttöön (edellyttää kirjautumista)
- Select account: Pyydetään käyttäjää valitsemaan käyttäjätili, jonka käyttöön hän haluaa valtuuttaa puolesta-asioijan (käyttäjällä saattaa olla tunnuksia ja voimassa oleva käyttäjäistunto useampaan tiliin, esim. yritys, henkilökohtainen, lapsen tili jne.)

OpenID Connect määrittelee joitakin vakiotietoja, joita käyttäjistä voi jakaa käyttäjän suostumuksella. Huom! Vaikka käyttäjistä olisi saatavissa kaikki vakiotiedot, tulee suostumus pyytää ja tietoja jakaa vain sen verran, mitä puolesta-asiointiin ehdottomasti tarvitaan. Mm. asiakasnumero tai henkilötunnus vaativat lisäyksiä standardiin.

| Member | Type |
|-----------------------|-------------|
| sub | string |
| name | string |
| given_name | string |
| family_name | string |
| middle_name | string |
| nickname | string |
| preferred_username | string |
| profile | string |
| picture | string |
| website | string |
| email | string |
| email_verified | boolean |
| gender | string |
| birthdate | string |
| zoneinfo | string |
| locale | string |
| phone_number | string |
| phone_number_verified | boolean |
| address | JSON object |
| updated_at | number |

Kansallisessa luottamusverkostossa OpenID Connectiin (ja SAMLiin) on määritelty seuraavassa kuvassa esitetyt lisäkentät. (Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0. FICORA Recommendation. 213/2018

https://www.viestintavirasto.fi/attachments/suosituksset/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf)²

² Viestintäviraston spesifikaatio koskee vahvan tunnistuksen tarjoajien välistä tietosisällöltään säädettyä rajapintaa. Puolesta-asioinnissa on arvioitava henkilötietojen käsittelyoikeus.

| Claim Name | FriendlyName (not used in OIDC) | eIDAS MDS Attribute | Comments, Example value(s) in Courier New |
|--|---------------------------------------|------------------------|--|
| urn:oid: 2.5.4.4 | FamilyName | Current Family Name | Meikäläinen von Essen |
| urn:oid: 1.2.246.575.1.14 | FirstNames | Current First Names | Matti Elmeri Valdemar Anna-Liisa Hilikka (all known current first/given names, space separated) |
| urn:oid: 1.3.6.1.5.5.7.9.1 | DateOfBirth | Date of Birth | 1971-06-28 (YYYY-MM-DD) |
| urn:oid: 1.2.246.21 | HETU HENKILÖTUNNUS | - | 220750-999Y 141002A909X (Finnish personal identity code, henkilötunnus) * |
| urn:oid: 1.2.246.22 | SATU SOISIAALITURVA-TUNNUS | - | 99999999D (Finnish Unique Identification Number, sähköinen asiointitunnus) * |
| http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier | PersonIdentifier | Unique Identifier | XX/YY/123456ABCDEF (as defined by eIDAS SAML Attribute Profile [eIDASTech], subject to change) * |

* One of these three claims is mandatory, the rest are OPTIONAL to include in a claims token. It is up to the FTN Broker and IdP to agree which identifier between them is used as the mandatory claim. The eIDAS PersonIdentifier is not expected to be commonly used nationally within the FTN, but is referred to here in case eIDAS cross-border authentication becomes relevant to the FTN.

4. Matkan ostaminen eli ns. myyntirajapinta

Myyntirajapinnassa vaatimukset minimissään toiminnallisuudesta ovat seuraavat:

- Liikkumispalvelu tarjoaa rajapinnan vähintään varausten/tilausten vastaanottamista varten (Matkaketjujen tietovirrat – matkan ostaminen).
- Jotta puolesta-asioija voi tehdä tilauksen, sen tulee tietää riittävät reitti-, pysäkki-, aikataulu-, hinta- ja saatavuustiedot sekä esteettömyystiedot rajapintojen kautta (käytännössä 2 luku 1§ 1 mom. luetellut olennaiset tiedot ovat välttämättömiä niin normaalihintaisen kuin 2a§ puolesta-asioinnin alennuksen, korvauksen tai erityisehdon mukaisiin matkustusoikeuksiin) (vrt. Matkaketjujen tietovirrat – matkan suunnittelu).
- Puolesta-asioinnin ehtona on, että hyödynnetään "käyttäjän olemassa olevalla käyttäjätilillä olevia tunniste- ja käyttäjätietoja" (2a§ 1 mom.). Rajapinnassa matkan ostamiseen käytetyn käyttäjätilin tiedot ja mahdolliset muiden matkustajien henkilötiedot tulisi välittää pseudonymisoituna ja vain niiltä osin kuin matkustusoikeuden kirjaamiseen ja tarkistamiseen liittyen on tarpeellista.

Rajapinnan käytön erot Lippu 1.-vaiheessa ja Lippu 2. vaiheessa (puolesta asiointi) ovat seuraavat:

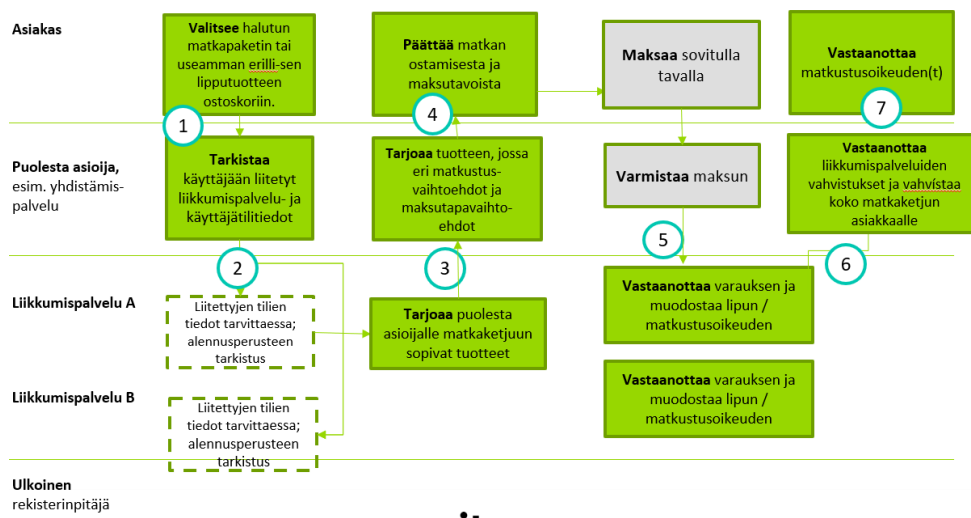
1. Vaiheessa

- Hae tuotteet (Products)
- Hae saatavuus tuotteille (Availability)
- Tee varaus (Reservation)
- Käsittele matkustusoikeutta (Travel entitlement)

2. Vaiheessa

- **Valtuuta puolesta-asioija (Consent / Delegation)**
- Hae käyttäjälle soveltuvat tuotteet (Products)
- Hae saatavuus tuotteille (Availability)
- Tee varaus (Reservation)
- Käsittele matkustusoikeutta (Travel entitlement)

Matkan ostaminen voidaan kuvata vastaavalla tavalla kuin valtuutus. Osapuolina ovat asiakas, puolesta asioija, liikkumispalvelu ja ulkoinen rekisterinpitäjä. Kuvassa on maksaminen esitetty harmaalla, koska toimintona siitä ei mainita laissa mitään.



Kuvassa on rajapinnat numeroitu 1-7. Alla olevassa taulukossa on avattu rajapinnat ja niiden tietosisällöt.

| Matkaketjun vaihe | Tietosisältö |
|---|---|
| 1. Puolesta asioija vastaanottaa matkavalinnan asiakkaalta (KUTSU) | Reitti, matkustaja, esteettömyystarpeet |
| 2. Puolesta asioija selvittää matkavalintaan liittyvät palveluntarjoajat ja asiakkaan valtuutukset kunkin toimijan tilien käyttöön (KUTSU), selvittää sopivat tuotteet ja maksutapoihin liittyvät ehdot | Matkaketju ja siihen liittyvät tuotteet, palveluntarjoajat, matkustajan valtuutukset; alennusperusteet, maksutavat |
| 3. Liikkumispalvelu tekee tarjouksen puolesta asioijalle omasta osuudestaan matkaketjua (PALAUTE) | Matkaketju, käyttäjätilit, alennus- ja erityisehdot, tuotteet |
| 4. Puolesta asioija tekee matkaketjutarjouksen asiakkaalle, joka tilaa ja antaa tarvittavat lisätiedot (esim. avustustarve matkan aikana) (PALAUTE) | Matkaketju ja siihen liittyvät tuotteet |
| 5. Puolesta asioija välittää asiakkaan tilausvahvistuksen pohjalta tilaukset liikkumispalveluille (KUTSU) | |
| 6. Liikkumispalvelu vahvistaa tilauksen omalta osaltaan puolesta asioijalle ja toimittaa tiedot matkustusoikeuden osoittamista varten (PALAUTE) | Matkaketju, tilausvahvistus, sis. Matkan, matkustajan ja esteettömyystiedot, matkustusoikeuden osoittamiseen liittyvät tiedot |
| 7. Puolesta asioija yhdistää tarvittaessa tilausvahvistus- ja matkustusoikeustiedot matkaketjun osista ja välittää ne asiakkaalle (PALAUTE) | Kuin edellä, mutta tarvittaessa yhdistelmänä koko ketjulle |

Myyntirajapinnan tietoarkkitehtuuri ja vertailu 1.-vaiheeseen on esitetty seuraavassa taulukossa. Myyntirajapinnan osapuolet ovat puolesta asioija, tilaaja, maksaja ja matkustajat. Sarakkeet ovat seuraavat:

1-2. sarakkeessa tietoarkkitehtuuri on esitetty loogisella tasolla

3. Sarakkeessa on viitattu 1. vaiheessa tehtyyn esimerkkitoeteutukseen ja kuvattu miten sen rajapinnassa on toteutettu ko. tietokenttä.

4. Sarakkeessa on esitetty suositus, kuinka tieto tulisi esittää, jotta se toteuttaisi puolesta-asioinnin vaatimukset ja olisi muuten mahdollisimman standardi.

| Tieto | Kommentti | 1. vaiheen esimerkkirajapinnassa | Suositus 2. vaiheessa |
|----------------------------------|--|--|---|
| Puolesta-asioija | <u>Puolesta-asioijan</u> ja valtuuttajan tietoja ei tulisi käsitellä erillisinä, jotta valtuutuksen eheys säilyy | X-initiator (?) | Authorization –header, Bearer –token, johon liikkumispalvelu on myöntäessään kirjoittanut myös puolesta-asioijan claimin |
| Tilaaaja, käyttäjätilin omistaja | Tilaaajan tietona tulisi välittää valtuutuksen yhteydessä annettu identiteettitieto | <u>CustomerInfo</u> (selväkielinen nimi, sähköposti ja puhelinnumero), ei erillistä tilaajaa/matkustajaa | <u>Authorization –header Bearer-token</u> , johon tilaaajan pseudonymisoidut tunnisteen (esim. <u>sposti</u> tai asiakasnumero) |
| Maksaja (jos eri kuin tilaaja) | Maksaja voi olla puolesta-asioija, käyttäjätilin omistaja tai muu taho. | - | Ks. edellä |
| Matkustajat | Matkalla voi olla myös muita matkustajia, vähintään lakiin perustuva avustaja. Käyttäjätilin omistaja ei välttämättä ole itse matkustaja. Riippuu käyttäjätilin ja valitun matkustustavan ehdoista voiko matkaan lisätä muita matkustajia ja mitä tietoja heistä tarvitaan | - | <u>Passengers</u> –elementti ja matkustajan tyyppi, vähintään tukemaan lakisäätöistä avustajaa |

Seuraavassa taulukossa on määritelty myyntirajapinnan tietosisältö matkustusoikeuden osalta.

| Tieto | Kommentti | 1. vaiheen esimerkkirajapinta | Suositus 2. vaiheessa |
|--|--|---|---|
| Matkustusoikeuden alkamis- ja loppumisajankohdat | Päivämäärä, kellonaika ja aikavyöhyke | "validFrom": "2018-10-20T07:15:31.495Z", "validTo": "2018-10-20T07:15:31.495Z" | Sama kuin 1. vaihe |
| Matkustusoikeuden alkamis- ja päättymispaikat | Matkasta ja tuotteesta riippuen saatetaan tarvita tarkka sijainti tai alue. Tarkka sijainti ei välttämättä ole <u>ostohetkellä</u> tiedossa, esim. vyöhyke-, sarja- tai kuukausiliput | <u>Availability</u> –kutsussa käytetty koordinaatteja tai paikkaa, matkan ostamisessa tai matkustusoikeudessa ei <u>sijaintitietoja</u> | <u>Distance</u> (etäisyys), <u>FromLocation</u> (lähtöpaikka), <u>ToLocation</u> (saapumispaikka), <u>Location</u> (paikka) Kaikki paikat voidaan tunnistaa paikan tunnistella (esim. tietty asema), postiosoitteella, koordinaateilla tai tekstinä. |
| Esteettömyys ja avustutarve | Matkustaja voi vapaaehtoisesti tai liikennepalvelun ehtojen mukaisesti varata avustajalle paikan (ks. Matkustajat), ilmoittaa pyörätuolista (voi olla myös erillinen lipputyppi) tai saattajan tarpeesta asemilla. | "accessibility": [{ "title": "WHEELCHAIR" ... | Liikennepalvelusta ja sen erityisehdoista johtuen riittävä kohta avustustarpeen ilmoittamiselle. Huomioitava tietosuoja ja henkilön rajoitteet, yksityiskohdat usein parempi käsitellä suullisesti |

Seuraavassa taulukossa on kuvattu myyntirajapinnan tiedot tuotteista ja hinnoista.

| Tieto | Kommentti | 1. vaiheen esimerkkirajapinnassa | Suositus 2. vaiheessa |
|-----------|---|--|---|
| Tuotteet | Matkavarauksen liittyvät liikkumispalvelun tuotteiden tunnisteet | "productType": "PRODUCT-SINGLE-TICKET" "extraServices" {} | Lisätään tuotteet alennus- ja korvausryhmille, sekä erityisehtoja sisältäviin tuotteisiin |
| Hinta | Hinta per tuote, kokonaishinta, veron sisältyminen, alennukset | "fare": { "currency": "string", "amount": 0, "vatPercent": 0} | Sama kuin 1. vaiheessa, schema.org käyttää "price" ja "priceSpecification" |
| Määrä | Matkustaja tai matkakohtainen tai muu määrä per tuoterivi | Ks. Hinta (amount) | Määrä (Quantity), ei pakollinen, jos kulutukseen perustuva. MinPrice, MaxPrice tai sarjalipuissa yhden osan hinta ja yksikkö (unitCode) |
| Valuutta | | Ks. Hinta (currency, ISO standarilla) | Sama kuin 1. vaiheessa |
| Maksutapa | Loppuasiakkaan maksutavalla voi olla merkitystä hintaan tai ehtoihin, esim. reklamaatioihin | | PaymentType tarvittaessa |

Seuraavassa taulukossa on kuvattu myyntirajapinnan tekniset tunnisteet.

| Tieto | Kommentti | 1. vaiheen esimerkkirajapinnassa | Suositus 2. vaiheessa |
|--------------------|---|----------------------------------|--|
| Kieli | | Accept-Language | Sama |
| Sanoman tunniste | Kutsujan luoma uniikki id, jokaiselle kutsulle jota käytetään virhetilanteiden selvitykseen | X-Message-Id | Sama, mutta uniikkiuden varmistamiseksi ja aikaleiman tallennusta varten sanoman tunnisteeseen tulisi sisältää aikaleima (esim. RFC2822) |
| Varauksen tunniste | Uniikki rajapintaa kutsuvan toimijan luoma id, joka pysyy samana kaikkien yhden matkan ostamiseen liittyvien transaktioiden ajan. | X-Transaction-Id | Sama, mutta uniikkiuden varmistamiseksi ja aikaleiman tallennusta varten transaktioid:n tulisi sisältää aikaleima, jolloin koko matkaketjun ostaminen on aloitettu |

5. Rajapinnan fyysinen toteutustapa

Laissa ei ole suoraan määritelty rajapinnan toteutustapaa. Toteutustavalla on vaikutusta myös siihen, mitä standardeja tunnistautumiseen ja valtuutuksiin voi soveltaa. Reaaliaikaisuuden ja vakiotietomuodon vaatimus toteutuu kuitenkin usein hyvin moderneilla ratkaisuilla kuten REST _arkkitehtuuriperiaatteisiin perustuvat API:t. GraphQL _rajapintoja tai muuntotyypisiä rajapintoja (gRPC tms.) ei toistaiseksi ole nähty julkisten tai kumppanikäyttöön tarkoitettujen (avointen rajapintojen) toteutukseen tarpeeksi hallittaviksi, mutta teknologian ja käytäntöjen kehittyessä nekin voivat olla vaihtoehtoja. Näiden vakiotietomuoto on JSON ja JSON schema, jossa voidaan hyödyntää eri sanastoja, usein kaupallisissa tarkoituksissa schema.orgia. Myös XML:ää ja XML-schemaa voidaan hyödyntää REST- ja SOAP-ratkaisuissa.