

Kanta JSON Web Token

v. 1.4.0

1.10.2025

Kanta-palvelut

Julkinen

Muutoshistoria

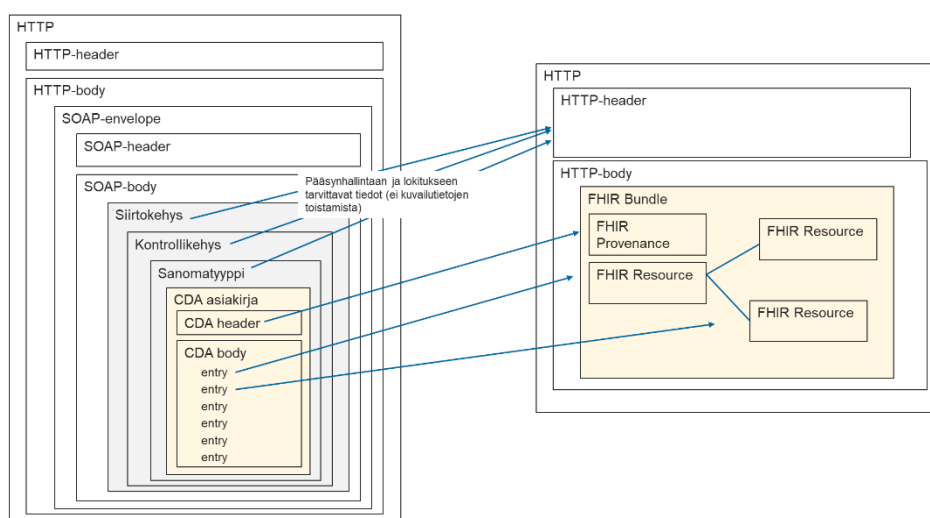
Versio	Muutos	Tekijä	PVM
0.8	Ensimmäinen julkaistava draft-versio kommentointia varten	Kanta-palvelut	23.10.2023
1.0.0	Virallinen julkaisuversio.	Kanta-palvelut	20.12.2023
1.1.0	Korjattu luvun 4.2.2 skeemasta ja luvun 4.2.3 esimerkeistä practitioner_authentication_method → authentication_method Lisäksi lisätty skeemaan puuttuva iss property.	Kanta-palvelut	13.3.2024
1.2.0	Lisätty claimeja RES-käyttöön ja puolesta-asiointiin ja täsmennetty oid-tietojen esittäminen JWT:n sisällössä	Kanta-palvelut	19.12.2024
1.3.0	Selkiytetty luvun 1 Tausta kohtaa missä palveluissa JWT käytössä. Selkiytetty luvun 4.1 Kanta JWT:n otsikkotietue kenttien selitteitä (mm. enkoodaus ja x5c kentän sisältö). Päivitetty palveluista käytettävät nimet läpi dokumentin. JTW tietosisältö: lisätty esimerkkejä, lisätty uusi Resepti-palvelu-kohtainen kenttä hospital sairaala-apteekkeja varten.	Kanta-palvelut	19.2.2025
1.4.0	Lisätty määrittelyyn palvelut Kysely- ja välityspalvelu (KVP) ja Kanta-yhteinen tahdonilmaisupalvelu (TIP). Poistettu määrittelystä Omatietovarannon ammattilaiskäytön osuudet. Luvussa 2 oli virhe JWT:n JSON-tietueen enkoodauksesta, dokumentissa oli base64 kun sen pitää olla RFC 7519 mukaisesti base64url. Lukuun 4.2.1 JWT:n tietosisältö: - Lisätty uudet palvelut KVP ja TIP. - Poistettu OTV - Lisätty uusi kenttä connection_model yhteisliittymismallia varten - Lisätty uusi kenttä extensive_search_reason SHA:n laajan tiedonsaantioikeuden käytön perustelu - Lisätty kenttään request_purpose - kentän käyttö Sosiaalihuollon asiakastietovarannossa. - Tarkennettu kenttien selitteitä ja mahdollisesti pakollisuuksia. - Tarkennettu kentissä käytettäviä koodistoja Luvun 4.2.2 skeemaan päivitetty oikeat kirjoitusasu register ja register_specifier (olivat registry ja reqistry_specifier)	Kanta-palvelut	1.10.2025

Sisällys

1	Tausta	1
2	JSON Web Token (JWT) tekninen rakenne.....	2
3	Kanta JWT:n käyttö	2
4	Kanta JWT	3
4.1	Kanta JWT:n otsikkotietue	3
4.2	Kanta JWT:n tietosisältö, skeema ja esimerkki	4
4.2.1	Kanta JWT:n tietosisältö	4
4.2.2	Kanta JWT:n tietosisällön skeema	1
4.2.3	Kanta JWT:n tietosisältö-esimerkki	4
4.3	Kanta JWT:n allekirjoitus	6

1 Tausta

Kanta-palvelujen FHIR toteutuksissa HL7 V3 Medical Records (MR)-sanomataso tulee korvautumaan REST-rajapinnan http headeriin vietävillä tiedoilla. MR-sanomatasolla tarkoitetaan alla olevassa kuvassa 1.1 esitettyjä siirtokehystä, kontrollikehystä ja sanomatyyppiä. Kuvassa näkyviä CDA R2 asiakirjan rakenteiden esittämistä FHIR-resursseilla ei käsitellä tässä määrittelyssä.



Kuva 1.1 Medical Records-sanomatason korvautuminen REST-rajapinnan http header:lla.

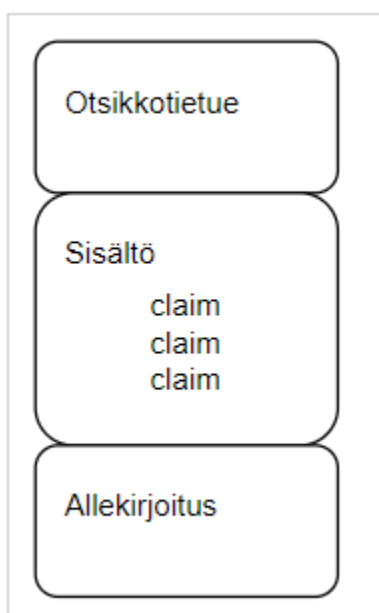
Pääsynhallintaan ja lokitukseen tarvittavat tiedot, joiden osalta halutaan varmistaa oikeellisuus ja muuttumattomuus, viedään JWT:hen ([RFC 7519: JSON Web Token](#)). Kanta JWT:tä käytetään seuraavissa FHIR rajapinnoissa:

- Potilastietovaranto (PTA)
- Resepti-palvelu (RES)
- Sosiaalihuollon asiakastietovaranto (SHA)
- Kysely- ja välityspalvelu (KVP)
- Kanta-yhteinen tahdonilmaisupalvelu (TIP).

JWT:hen sisältyvien tietojen lisäksi MR-sanomatasolla aiemmin siirrettyjä tietoja sijoittuu myös muihin http header-kenttiin, nämä kentät ovat kuvattu erillisessä "Kanta HTTP header"-määrittelyssä.

2 JSON Web Token (JWT) tekninen rakenne

Rakenteeltaan JWT on kolmiosainen: otsikkotietue, tietosisältö ja allekirjoitus. Kanta-palveluissa tarvittavat tietosisällön nimetyt tiedot toimitetaan tämän dokumentin mukaisissa kentissä, jotka ovat JWT:n tietosisällössä täytettynä claimeihin. Osa vaadituista tiedoista sijoittuu JWT:n kuvauksessa ([RFC 7519: JSON Web Token](#)) määriteltyihin yleisiin registered claimeihin, osalle tiedoista on määritelty private claim:eja.



Kuva 2.1 JWT:n kolmiosainen rakenne.

Jokainen JWT:n osa on JSON-muotoinen tietue. Nämä JSON-tietueet base64url enkoodataan merkkijonoksi ja osat yhdistetään toisiinsa pisteellä.

Alla esimerkki JWT:stä (huom. rivinvaihdot eivät sisälly varsinaiseen JWT:hen):

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

```
.
```

```
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpXVCJ9
```

```
.
```

```
KeNzd2Es6XIFQSp59gKjFSxCBmdVIGgi5Es8zg04cmY
```

3 Kanta JWT:n käyttö

Kanta JWT:tä käyteään suoraan käytettävässä rajapinnassa. Suoraan käytettävässä rajapinnassa JWT annetaan HTTP headerin Authorization header-kentässä ja sen on tyypiltään Bearer (authentication scheme).

Alla esimerkki HTTP-headerin JWT:n sisältävästä Authorization header-kentästä:

```
"Authorization": "Bearer  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwiibmFtZSI6InRlc3RpliwiaWF0IjoxNTE2MjM5MDIyQyQ.KeNzd2Es6XIFQSp59gKjFSxCBmdVIGgi5Es8zg04cmY"
```

4 Kanta JWT

Tässä luvussa käydään läpi Kanta JWT:n otsikkotietue, tietosisältö ja sen skeema, sekä allekirjoitus.

4.1 Kanta JWT:n otsikkotietue

Otsikkotietueesta käytetään teknistä nimitystä JOSE-header ja se on kuvattu tarkemmin [RFC 7515 JWS \(JSON Web Signature\)-standardissa](#).

Otsikkotietueessa annetaan seuraavat kentät:

- x5c: allekirjoituksessa käytettävä julkisen avaimen sisältävä varmenne lähetetään JWT:n otsikkotietueen kentässä x5c. Elementtiin laitetaan base64 -enkoodattuna DER muotoinen varmenne (EI base64url -enkoodattu) (RFC 7515 4.1.6).
- alg: käytettävä algoritmi kerrotaan otsikkotietueen kentässä alg, algoritmin tarkemmat määrittelyt löytyvät tämän dokumentin luvussa 4.3 Kanta-palveluiden JWT:n allekirjoittaminen viitatusta "Kanta FHIR sähköinen allekirjoitus" määrittelystä.
- version: version tiedossa annetaan tämän JWT määrittelyn skeeman versio.

Alla esimerkki JWT:n header kentästä (JWT JOSE-header):

```
{  
  "x5c": [  
  
    "MIIFGDCCAwACFGRO1cnZGbuVx/Ph7yn/9TFRcib8MA0GCSqGSIb3DQEBDQUAMDgxGz  
    AJBgNVBAYTInAkZJMQ0wCwYDVQQKDARLZWxhMR0wGAYDVQQDDBFKYWMgUINBIF  
    Rlc3QgQ0EgMTAgFw0yMzA4MjQxLnMjAyNDRaGA8yMTIzMDczMTEyMDI0NFowVzELMAk  
    GA1UEBhMCRkkxDTALBgNVBAoMBEtlbGExHTAbInBgNVBAUTFDEuMi4yNDYuNTU2LjE  
    wMDAxLjM1MR0wGAYDVQQDDDBFSU0EgVGZzdCBPcmcgS2VsYTCCInAilwDQYJKoZIh  
    vCNAAQEBBQADggIPADCCAggCggIBALQtrMq3HUzOrluw2rO4UOdNmesVINnf+Kru\nFdfKfG  
    042MbM0b2xHURwlzjA8Z3u8QN4cbCV9cITiHBf88Li++DNEUagyl5dsI9m+FgOB3WonQKB\  
    nPTf5uwABJGA4qWEMwctdms8U4t53uZv7yehULQAxQc293y/C/RmKFv1UjSrRrCdpr4gOZ  
    pILH9qQ\ntqjz4cVMLduoFVGIQv7pDiEE60TN914yQNT/RIFFFSQm7+lzxClfW4IBljFH  
    z1Qh  
    3hstRXxvR18\nOd0CDnN5ChZ3ox1fYB4UiTHhHq7ojjEHSx/kca3LbWgOp2sDvNLLqiW39h6  
    h6v8hxtGZNSrT+2B+\nBPYHfSXS0nbyn7AO3ZNz6UGP10LD47XOAVIJMvSoB/VNhaZXM  
    06IM3Q7ChB0h1YCTpN/68ZQYif\nnwVpt4DDR4/GqyatWEmFBE3hitXq91/JahpZvnh7DhHb  
    +pwFeHgLTR3oxcPN/XJT9fOrlYwYdDCm\n+zxZDV7pTOjBwb54nVdj/GUWuR/tOn460RzlwqU  
    SaakEkm4gLkUp1lb7yRJ9AwIPPHqDj1ujAtO18\naYRGJPxBygW3wLFdqNxc2h3xnzcf6V8Z  
    kJzZjH5cQ2KAr4u1rULE9474JXW81A3bNA7IKBypDCZH\nT2hONddiaDWbF1tBQZiH14ou  
    Q+DvoEEpGQRBoNCFAGMBAAEwDQYJKoZIhvcNAQENBQADggIBAB5s\nnHlrX56mehppx2
```

```
ovVJAIUYtYW9fx6rz7RTW6DwiRv5x0/2ZC9ke1SQM/f0LUedFGGRIXHfmdBk5LK\http/9au5r
BfHSN4YfYapnrIKs6nzEaV1q0QyD5Zvqp0Q3fM1qDs131PShH5gjVFGk1pzIU2ocYtE\n+INB
+TKgytezR3L8kUGvUojx6CDYBlwwilyc5Nw3GHMpdo26Vi30KIFL/LizDUSlje2M/dcMTIfC\ne
852kjNt0oqOgXrkhPsvX6aAtWibJeTj7iyXwbTTFOw+mD1lm8Zf9PzsOO7xdvAcUm/Mr9D2n
Ydu\n/g7Q7DR8l4bp6yfwzREQBZYtVHNksbToUk30uGBbA9xUhV+eOLzEAGOFp2EdKvSK
ZZHDtoPaehOC\nLTTWhR9Ktw3LMUblmik5MxNu2W5w6R1aNCUf7ADeE+WV0AsjhBEWb
N8zca9NqMpjOIVIZIny6j8+\nYFoelNsumY5jF0/DQj6tYDb9ti7Kpl/g4/B12nXRmwrwj47su57b
CCYnsOCUDq4kOSUyX/YTOM6P\n/5LVz6mMEiHfHqALFQQQz3wXC2uPQObUvUBByO
dIY6BzlYrKU2sPh03CdQ9ra7AtHehpHn3G1UN\nnHIPtrQd0plxu5IniNSQgDIHPuO0NurXfVZ
E34uDI3yMU2khCdOal7I4I4irykNczfZ23eww"
```

```
],
"alg": "RS512",
"version": "1.4.0"
}
```

4.2 Kanta JWT:n tietosisältö, skeema ja esimerkki

Tässä kappaleessa on kuvattu Kanta JWT:n tietosisältö, sille määritelty skeema sekä esimerkki tietosisällöstä.

4.2.1 Kanta JWT:n tietosisältö

Taulukossa 4.1 on kuvattu JWT tietosisällössä käytettävät JWT claimit. JWT claimit koostuvat yhteisistä JWT-standardin claimeista (registered claims), sekä Kanta-tasoisesti määritellyistä lisäclaimeista (private claims). Kunkin claimin osalta on määritelty claimin nimi, selite, pakollisuus eri palveluissa sekä tietotyyppi.

Tietotyypit noudattavat JWT määrittelyn ([RFC 7519: JSON Web Token](#)) tietotyyppejä tai tämän määrittelyn skeeman tietotyyppejä (Object-II, Object-CV). Oid-tyypin arvot annetaan pelkkänä oidina ilman urn:oid: -etuliitettä.

Tyhjiä eikä blankkoja tietosisällön arvoja hyväksytään, vaan tarpeeton claim jätetään kokonaan pois.

Taulukko 4.1 Kanta-palveluiden JWT Claimit.

PTA= Potilastietovaranto, SHA = Sosiaalihuollon asiakastietovaranto, RES = Resepti-palvelu, KVP = Kysely- ja välityspalvelu, TIP = Kanta-yhteinen tahdonilmaisupalvelu

P=Pakollinen, eP = Ehdollisesti Pakollinen, V = Valinnainen, E = ei käytössä

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
JWT-standardin mukaiset yhteiset claimit (Registered Claims)							
iss	Kanta-liityntäpisteen tunniste	P	P	P	P	P	String
sub	Liittyjäorganisaation tunniste (sama arvo kuin subscriber_id kentässä) organisaation tunniste, jolle annettu lähetysoikeus (ilmoitettava erikseen osoitteistoon) SOTE-organisaatiorekisterin toimintayksikkö tai Valvira - Terveystieteiden tutkimuskeskuksen itsenäiset ammatinharjoittajat tunniste tai Fimea - Apteekkirekisterin tunniste	P	P	P	P	P	String
aud	Vastaanottajan tunniste Tuotanto-ympäristössä: PTA: 1.2.246.556.18.2 SHA: 1.2.246.556.18.6	P	P	P	P	P	String

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	RES: 1.2.246.556.18.1 KVP: 1.2.246.556.18.7 TIP: 1.2.246.556.18.8						
exp	JWT:n vanhenemisaika enintään iat + 30 minuuttia	P	P	P	P	P	NumericDate
iat	JWT:n luontiaika	P	P	P	P	P	NumericDate
jti	JWT:n yksilöivä tunniste	E	E	E	E	E	String
Kanta-tasoiset lisäclaimit (Private Claims)							
application_name	Pyynnön tehneen tietojärjestelmän nimi	P	P	P	P	P	String
application_version	Pyynnön tehneen tietojärjestelmän versio	P	P	P	P	P	String
practitioner_id	Pyynnön tehneen ammattihenkilön tunniste	eP	eP	eP	P	eP	Object-II: Terhikki / Suosikki:

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	Terhikki, suosikki, SV-numero, vrk-yksilöivä tunnus tai henkilötunnus, tunnuksen käyttö vastaava kuin Medical Records sanomamäärittelyissä. Annetaan system ja value, molemmat pakollisia. PTA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö SHA, TIP: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyyntö RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö. Tunnisteen tulee olla SV-numero tai Terhikkittunnus.						practitioner_id: {s: "1.2.246.537.26", v: "01234567890"} SV-numero: practitioner_id: {s: "1.2.246.537.25", v: "123456"} Vrk-yksilöivä tunnus: practitioner_id: {s: "1.2.246.537.29", v: "123456789"} Henkilötunnus: practitioner_id: {s: "1.2.246.21", v: "010186-993N"}
citizen_id	Pyynnön tehneen henkilön tunniste (ei ammattihenkilö) Annetaan system ja value, molemmat pakollisia. PTA, SHA, RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön	eP	eP	eP	E	eP	Object-II: {s: "1.2.246.21", v: "010144-955L"}

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	tai hänen puolestaan asioivan käynnistämä hakupyyntö. Tunnisteena tulee käyttää virallista henkilötunnusta. TIP: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön tai hänen puolestaan asioivan käynnistämä haku- tai tallennuspyyntö. Tunnisteena tulee käyttää virallista henkilötunnusta.						
practitioner_given	Pyynnön tehneen ammattihenkilön etunimi PTA, RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö. SHA, TIP: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyyntö.	eP	eP	eP	P	eP	Array<String>
citizen_given	Pyynnön tehneen henkilön etunimet (ei ammattihenkilö) PTA, SHA, RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön tai hänen puolestaan asioivan käynnistämä hakupyyntö.	eP	eP	eP	E	eP	Array<String>

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	TIP: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön tai hänen puolestaan asioivan käynnistämä haku- tai tallennuspyyntö.						
practitioner_family	Pyynnön tehneen ammattihenkilön sukunimi PTA, RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö. SHA, TIP: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyyntö.	eP	eP	eP	P	eP	String
citizen_family	Pyynnön tehneen henkilön sukunimi (ei ammattihenkilö) PTA, SHA, RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön tai hänen puolestaan asioivan käynnistämä hakupyyntö. TIP: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön tai hänen puolestaan asioivan käynnistämä haku- tai tallennuspyyntö.	eP	eP	eP	E	eP	String

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
authentication_method	Pyynnön tehneen henkilön tunnistautumismenetelmä Käytettävä koodisto 1.2.246.537.5.40128.2006 (KanTa-palvelut - Tunnistautumistapa) PTA, SHA, TIP: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö.	eP	eP	P	P	eP	Object-CV {c: "2", s: "1.2.246.537.5.40128.2006"}
requested_record	Pyynnön kohde (potilas, asiakas) PTA: ehdon pakollisuus: pakollinen, kun toiminto kohdistuu yhden henkilön tietoihin. Tieto ei saa toistua. SHA: Tieto toistuu, jos kyseessä on sosiaalihuollon yhteiseen asiaan liittyvä tallennus, versiointi tai mitätöinti. KVP, TIP: tieto ei saa toistua. Annetaan system ja value, molemmat pakollisia. Object-II tietotyyppillä voi antaa vain yhden pyynnön kohteen tiedot. Array<Object-II> tietotyyppillä voi antaa	eP	P	E	P	P	Object-II / Array<Object-II>: Object-II: {s: "1.2.246.21", v: "010144-955L" } Array<Object-II> [{s: "1.2.246.21", v: "010144-955L" }, {s: "1.2.246.21", v: "010107A937F" }] Tilapäinen yksilöintitunnus:

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	yhden tai useamman pyynnön kohteen tiedot. Array<Object-II> tietotyyppi on lisätty versiosta 1.4.0 lähtien käyttöön. Object-II on edelleen tuettuna taaksepäin yhteensopivuuden vuoksi.						{s: "1.2.246.10.1234567.22.2025", v: "150180-9999"}
subscriber_id	Liittyjäorganisaation tunnus SOTE-organisaatiorekisterin toimintayksikkö tai Valvira - Terveystieteiden tutkimuskeskus - ammatinharjoittajat tunniste tai Fimea - Apteekkirekisterin tunniste	P	P	P	P	P	String
subscriber_name	Liittyjäorganisaation nimi	P	P	P	P	P	String
subscriber_unit_id	Liittyjäorganisaation palveluyksikön tunnus ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	E	V	eP	eP	String
subscriber_unit_name	Liittyjäorganisaation palveluyksikön nimi ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	E	V	eP	eP	String

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
requester_id	Pyynnön tehneen organisaation tunniste SOTE-organisaatiorekisterin toimintayksikkö tai Valvira - Terveystieteiden tutkimuskeskus - Terveystieteiden tutkimuskeskus - Apteekkirekisterin tunniste Yhteisliittymistilanteessa pyynnön tehneen vuokralaisen organisaation tunniste	P	P	P	P	P	String
requester_name	Pyynnön tehneen organisaation nimi	P	P	P	P	P	String
requester_unit_id	Pyynnön tehneen organisaation palveluyksikön tunniste PTA, KVP, TIP: ehdon pakollisuus: pakollinen yhteisliittymistilanteessa RES: ehdon pakollisuus: pakollinen yhteisliittymistilanteessa ja vain potilas-tietojärjestelmissä. Yhteisliittymistilanteessa pyynnön tehneen vuokralaisen organisaation palveluyksikön tunniste	eP	P	eP	eP	eP	String
requester_unit_name	Pyynnön tehneen organisaation palveluyksikön nimi	eP	P	eP	eP	eP	String

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	PTA, KVP, TIP: ehdon pakollisuus: pakollinen yhteisliittymistilanteessa. RES: ehdon pakollisuus: pakollinen yhteisliittymistilanteessa ja vain potilastietojärjestelmissä.						
requester_custodian	Pyynnön tehneen rekisterinpitäjän yksilöivä tunniste PTA, TIP: ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	P	E	P	eP	String
requester_custodian_name	Pyynnön tehneen rekisterinpitäjän nimi PTA, TIP: ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	P	E	P	eP	String
register	Hakevan rekisterinpitäjän rekisteritunnus ehdon pakollisuus: pakollinen vain hakupyynnöissä Käytettävä koodisto: 1.2.246.537.5.40150.2009 (KanTa-palvelut - Potilasasiakirjan rekisteritunnus)	eP	E	E	eP	eP	Object-CV: {c: "2", s: "1.2.246.537.5.40150.2009"}

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
register_specifier	Hakevan rekisterinpitäjän rekisterin tarkenne ehdon pakollisuus: kun register arvo on 4 (=työterveys) Jos y-tunnus annetaan s-kentässä on sen arvo normalisoitava eli etunolla poistettava ja yhdysmerkki poistettava (suositus on käyttää eroteltuna system ja value kenttiin).	eP	E	E	eP	eP	Object-II: Y-tunnus: registry_specifier: {s: "1.2.246.10", v: "123456-7"} Henkilötunnus: register_specifier: {s: "1.2.246.21", v: "010144-955L"} Y-tunnukseton työnantajayritys: register_specifier: {s: "1.2.246.537.30", v: "2345678.11"}
service_event_id	Viittaus palvelutapahtumaan PTA ehdon pakollisuus: annettava luovutushakupyynnöissä, annettava ajanvarauksen arkistoinnissa RES ehdon pakollisuus: pakollinen potilastietojärjestelmän tehdessä hakuja, jos haku tehdään palvelutapahtuman yhteydessä	eP	E	eP	E	E	String

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
special_reason	Tietojen haun erityinen syy Käytettävä koodisto: 1.2.246.537.6.240.2012 (THL - Asiakastietojen katselun erityinen syy) PTA: ehdon pakollisuus: Pakollinen hauissa tilanteessa, jossa potilastietojärjestelmä ei pysty automaattisesti todentamaan hoitosuhteen olemassaoloa, kun ammattilaiskäyttäjä hakee tietoja Potilastietovarannosta. Lisäksi hätähakutilanteissa erityisenä syynä ilmoitetaan koodiarvo "Hätähaku". SHA: ehdon pakollisuus: pakollinen hauissa, jos hakua ei perustella tietoja hakevan ammattihenkilön ja haun kohteena olevan asiakkaan välisellä asiayhteydellä.	eP	eP	E	E	E	Object-CV / Array<Object-CV>: Object-CV: <pre>{c: "2", s: "1.2.246.537.6.240.2012"}</pre> Array<Object-CV> <pre>[{c: "2", s: "1.2.246.537.6.240.2012"}, {c: "3", s: "1.2.246.537.6.240.2012"}]</pre>
special_reason_explanation	Tietojen haun erityinen syy – perustelu Perustelun maksimipituus 256 merkkiä	eP	eP	E	E	E	String

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	PTA, SHA: ehdon pakollisuus: pakollinen hauissa, joissa tietojen haun erityisen syyn koodiarvoksi annettu "Muu syy".						
usage_situation	Puolesta asiointitilanne Ilmoitetaan koodistolla 1.2.246.537.6.882.201501 (Ajanvaraus - Yhteyshenkilön tyyppi) PTA ehdon pakollisuus: pakollinen, kun pyynnön tehnyt kansalainen on muu kuin potilas itse. SHA, TIP: ehdon pakollisuus: pakollinen, kun OmaKannan käyttäjä on muu kuin kansalainen itse. RES ehdon pakollisuus: kun OmaKannan käyttäjä on muu kuin kansalainen itse tai kun haetaan alle 18-vuotiaan potilaan lääkityslista koostetta tai jäljennöstä ulkomaanmatkaa varten ja hakijana on muu kuin potilas itse 1.2.0 versiosta lähtien	eP	eP	eP	E	eP	Object-CV: {c: "2", s: "1.2.246.537.6.882.201501"}

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
request_purpose	Kyselyn syy tai pyynnön lähettämisen käyttötilanne RES: Käytettävä koodisto: 1.2.246.537.5.40110.2006 (Sähköi- nen lääkemääräys - Reseptikyselyn syy) RES: ehdon pakollisuus: pakollinen hauissa RES: 1.2.0 versiosta lähtien SHA: Käytettävä koodisto: 1.2.246.537.6.1289.201901 (Sosiaali- huolto - Asiakastiedon arkiston käyt- tötilanne) SHA: ehdon pakollisuus: pakollinen, kun pyyntö koskee muuta kuin sosi- aalihuollon luovutusilmoituksen tallen- tamista. SHA: 1.4.0 versiosta lähtien	E	eP	eP	E	E	Object-CV {c: "2", s: "1.2.246.537.5.40110.2006"} {c: "2", s: "1.2.246.537.6.1289.201901"}
consent_type	Suostumuksen tyyppi	E	E	eP	E	E	Object-CV

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	Käytettävä koodisto: 1.2.246.537.5.40119.2006 (Sähköi- nen lääkemääräys - Suostumustyytit) RES: ehdon pakollisuus: pakollinen hauissa 1.2.0 versiosta lähtien						{c: "2", s: "1.2.246.537.5.40119.2006"}
hospital	Palvelunantajan tunnus, jonka alai- suudessa sairaala-apteekki tai lääke- keskus toimii RES: ehdon pakollisuus: pakollinen vain sairaala-apteekeille ja lääkekes- kukselle 1.3.0 versiosta lähtien	E	E	eP	E	E	String "1.2.246.10.48484666998.19.10.0
connection_model	Yksityisen toimijan liittymismalli Kanta-palveluihin PTA, SHA, KVP, TIP: ehdon pakolli- suus: pakollinen, kun pyynnön on lä- hettänyt yksityinen terveydenhuollon tai sosiaalihuollon organisaatio Käytettävä koodisto: 1.2.246.537.5.40200.2014 (Kanta-	eP	eP	E	eP	eP	Object-CV {c: "2", s: "1.2.246.537.5.40200.2014"}

Claim	Selite	PTA	SHA	RES	KVP	TIP	Datamuoto
	palvelut - Yksityisten toimijoiden liittymismallit) Versiosta 1.4.0 lähtien						
extensive_search_reason	Laajan tiedonsaantioikeuden käytön perustelu Käytettävä koodisto: 1.2.246.537.6.1299.202101 (Sosiaali-huolto - Laajan tiedonhaun peruste) SHA: ehdon pakollisuus: pakollinen, kun asiakastietoja haetaan toisen rekisterinpitäjän rekisteristä palvelunantajan laajalla tiedonsaantioikeudella tai viranomaisen laajalla tiedonsaantioikeudella. Versiosta 1.4.0 lähtien	E	eP	E	E	E	Object-CV {c: "4", s: "1.2.246.537.6.1299.202101"}

4.2.2 Kanta JWT:n tietosisällön skeema

Tietosisällön skeema:

```
{
  "$schema": "http://json-schema.org/schema#",
  "$id": "https://kela.fi/kanta.jwt.schema.json",
  "title": "Kanta JWT",
  "description": "Kanta JWT schema versio 1.4.0",
  "type": "object",
  "properties": {
    "iss": {
      "type": "string",
      "maxLength": 64
    },
    "aud": {
      "type": "string",
      "maxLength": 512
    },
    "exp": {
      "type": "integer"
    },
    "sub": {
      "type": "string",
      "maxLength": 64
    },
    "iat": {
      "type": "integer"
    },
    "jti": {
      "type": "string"
    },
    "application_name": {
      "type": "string",
      "maxLength": 512
    },
    "application_version": {
      "type": "string",
      "maxLength": 512
    },
    "citizen_id": {
      "$ref": "#/$defs/ii"
    },
    "citizen_given": {
      "type": "array",
      "minItems": 1,
      "items": {
        "type": "string"
      }
    },
    "citizen_family": {
      "type": "string",
      "maxLength": 128
    },
    "practitioner_id": {
      "$ref": "#/$defs/ii"
    },
    "practitioner_given": {
```

```
        "type": "array",
        "minItems": 1,
        "items": {
            "type": "string"
        }
    },
    "practitioner_family": {
        "type": "string"
    },
    "authentication_method": {
        "$ref": "#/$defs/cv"
    },
    "requested_record": {
        "type": [
            "object",
            "array"
        ],
        "items": {
            "$ref": "#/$defs/ii"
        }
    },
    "subscriber_id": {
        "type": "string",
        "maxLength": 64
    },
    "subscriber_name": {
        "type": "string",
        "maxLength": 256
    },
    "subscriber_unit_id": {
        "type": "string",
        "maxLength": 64
    },
    "subscriber_unit_name": {
        "type": "string",
        "maxLength": 256
    },
    "requester_id": {
        "type": "string",
        "maxLength": 128
    },
    "requester_name": {
        "type": "string",
        "maxLength": 256
    },
    "requester_unit_id": {
        "type": "string",
        "maxLength": 64
    },
    "requester_unit_name": {
        "type": "string",
        "maxLength": 256
    },
    "requester_custodian": {
        "type": "string",
        "maxLength": 64
    },
    "requester_custodian_name": {
```

```
        "type": "string",
        "maxLength": 256
    },
    "registry_specifier": {
        "$ref": "#/$defs/ii"
    },
    "registry": {
        "$ref": "#/$defs/cv"
    },
    "service_event_id": {
        "type": "string",
        "maxLength": 64
    },
    "special_reason": {
        "type": [
            "object",
            "array"
        ],
        "items": {
            "$ref": "#/$defs/cv"
        }
    },
    "special_reason_explanation": {
        "type": "string",
        "maxLength": 512
    },
    "usage_situation": {
        "$ref": "#/$defs/cv"
    },
    "request_purpose": {
        "$ref": "#/$defs/cv"
    },
    "consent_type": {
        "$ref": "#/$defs/cv"
    },
    "hospital": {
        "type": "string",
        "maxLength": 64
    },
    "connection_model": {
        "$ref": "#/$defs/cv"
    },
    "extensive_search_reason": {
        "$ref": "#/$defs/cv"
    }
},
"required": [
    "iss",
    "aud",
    "exp",
    "sub",
    "iat",
    "application_name",
    "application_version",
    "subscriber_id",
    "subscriber_name",
    "requester_id",
    "requester_name"
```

```
],
"$defs": {
  "ii": {
    "description": "Identifier",
    "type": "object",
    "properties": {
      "s": {
        "description": "Identifier",
        "type": "string",
        "maxLength": 64
      },
      "v": {
        "description": "System for the identifier",
        "type": "string",
        "maxLength": 128
      }
    },
    "required": [
      "s"
    ]
  },
  "cv": {
    "description": "Coded value",
    "type": "object",
    "properties": {
      "c": {
        "description": "Code",
        "type": "string",
        "maxLength": 64
      },
      "s": {
        "description": "System for the code",
        "type": "string",
        "maxLength": 64
      }
    },
    "required": [
      "c",
      "s"
    ]
  }
}
```

4.2.3 Kanta JWT:n tietosisältö-esimerkki

Esimerkki JWT:n tietosisällöstä:

```
{
  "aud": "1.2.246.556.18.2",
  "exp": 1692962672,
  "sub": "1.2.246.10.48484841.10.0",
  "iat": 1692960872,
  "iss": "1.2.246.10.48484841.10.0.13.1",
  "jti": "12d3a0f7-a8a5-478b-8100-e75325f2d1ee",
  "application_name": "Ammattikäytön testisovellus",
  "application_version": "123",
```

```
"practitioner_id": {
  "s": "1.2.246.21",
  "v": "010186-993N"
},
"practitioner_given": [
  "Testi",
  "Nimi"
],
"practitioner_family": "Testisukunimi",
"practitioner_authentication_method": {
  "c": "2",
  "s": "1.2.246.537.5.40128"
},
"requested_record": {
  "s": "1.2.246.21",
  "v": "010144-955L"
},
"subscriber_id": "1.2.246.10.48484841.10.0",
"subscriber_name": "Liittyjän nimi",
"subscriber_unit_id": "1.2.246.10.48484841.10.1",
"subscriber_unit_name": "Liittyjän palveluyksikön nimi",
"requester_id": "1.2.246.10.48484666.10.0",
"requester_name": "Pyynnön tehneen organisaation nimi",
"requester_unit_id": "1.2.246.10.48484666.10.1",
"requester_unit_name": "Pyynnön tehneen yksikön nimi",
"requester_custodian": "1.2.246.10.48484666.19.0",
"register_specifier": {
  "s": "1.2.246.10",
  "v": "123456-7"
},
"register": {
  "c": "4",
  "s": "1.2.246.537.5.40150.2009"
},
"service_event_id": "1.2.246.10.48484666.10.0.14.2009.432006",
"special_reason": {
  "c": "2",
  "s": "1.2.246.537.6.240.2012"
},
"special_reason_explanation": "Viranomaisen OrganisaatioX pyytämä
selvitys henkilön terveystiedoista",
"usage_situation": {
  "c": "2",
  "s": "1.2.246.537.6.882.201501"
},
"request_purpose": {
  "c": "2",
  "s": "1.2.246.537.5.40110.2006"
},
"consent_type": {
  "c": "2",
  "s": "1.2.246.537.5.40119.2006"
},
"hospital": "1.2.246.10.48484666998.19.10.0",
"connection_model": {
  "c": "2",
  "s": "1.2.246.537.5.40200.2014"
},
}
```

```
    "extensive_search_reason": {  
      "c": "5",  
      "s": "1.2.246.537.6.1299.202101"  
    }  
  }
```

4.3 Kanta JWT:n allekirjoitus

Kanta JWT allekirjoitetaan JWS-määrittelyn ([RFC 7515: JSON Web Signature](#)) ja JWT-määrittely ([RFC 7519: JSON Web Token](#)) mukaisesti käyttäen JWT otsikkotietueessa annetun varmenteen yksityistä avainta.

Varmenteen on oltava Digi- ja väestöviraston (DVV) myöntämä SOTE-varmenne (palvelinvarmenne tai järjestelmäallekirjoitusvarmenne). Varmenteella on pystyttävä tekemään sähköinen allekirjoitus.

Käytössä olevat algoritmit on kuvattu dokumentin "Kanta FHIR sähköinen allekirjoitus" luvuissa 3.1.1 (Käytetyt tiivistealgoritmit) ja 3.1.2 (Allekirjoitusalgoritmit ja menetelmät).