

## Kanta JSON Web Token

v. 1.1.0

13.3.2024

Kanta-palvelut

Julkinen

## Muutoshistoria

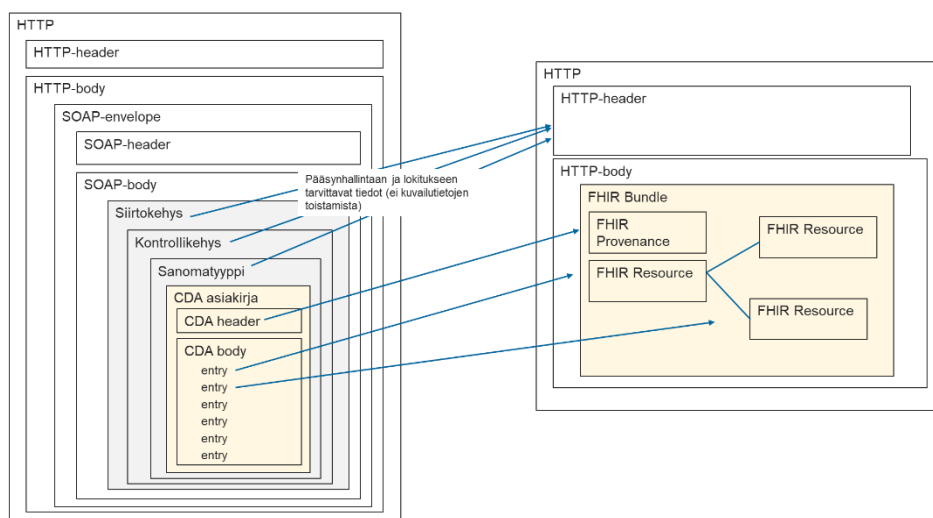
Versio	Muutos	Tekijä	PVM
0.8	Ensimmäinen julkaistava draft-versio kommentointia varten	Kanta-palvelut	23.10.2023
1.0.0	Virallinen julkaisuversio.	Kanta-palvelut	20.12.2023
1.1.0	Korjattu luvun 4.2.2 skeemasta ja luvun 4.2.3 esimerkeistä practitioner_authentication_method → authentication_method Lisäksi lisätty skeemaan puuttuva iss property.	Kanta-palvelut	13.3.2024

## 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 .....	11
4.2.3	Kanta JWT:n tietosisältö-esimerkki .....	14
4.3	Kanta JWT:n allekirjoitus .....	15

## 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.



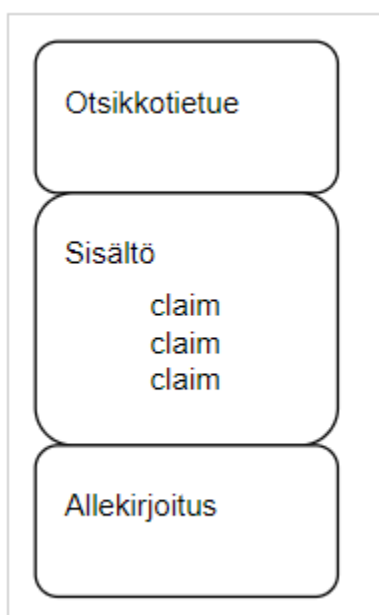
Kuva 1.1 Medical Records-sanomatason korvautuminen REST-rajapinnan http header:lla.

Pääsynhallintaan ja lokitukseen tarvittavat tiedot, joiden osalta halutaan varmistaa oikeellisuus ja muuttumattomuus, vietään JWT:hen ([RFC 7519: JSON Web Token](#)). Kanta JWT:tä käytetään Potilastiedon arkiston (PTA) ja Sosiaalihuollon asiakastiedon arkiston (SHA) uusissa FHIR rajapinnoissa. Jatkossa Kanta JWT:n käyttö laajenee muihin rajapintoihin kuten Reseptin lääkityslista FHIR rajapintaan. Omatietovarannossa (OTV) Kanta JWT:tä käytetään OAuthin assertiona OTV:n tietojen ammattilaiskäyttörajapinnassa.

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 base64 enkoodataan merkkijonoksi ja osat yhdistetään toisiinsa pisteellä.

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

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

```
.
```

```
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IjEyMzQ1Njc5MCJ9
```

```
.
```

```
KeNzd2Es6XIFQSp59gKjFSxCBmdVIGgi5Es8zg04cmY
```

## 3 Kanta JWT:n käyttö

Kanta JWT:tä käyteen joko suoraan käytettävässä rajapinnassa tai OAuth-token-pyyntöissä. Suoraan käytettävässä rajapinnassa JWT annetaan HTTP headerin Authorization header-kentässä ja sen on tyypiltään Bearer (authentication scheme). OAuth-tokenpyyntö on toistaiseksi käytössä vain OTV:ssa ja siellä JWT annetaan

client\_credentials-flown kaltaisesti assertion-parametrissa. OTV:n osalta asia tullaan dokumentoimaan tarkemmin OTV:n auktorisointioppaaseen (huom. tämä auktorisointioppas ei vielä tämän JWT määrittelyn julkaisun aikaan valmis).

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

```
"Authorization": "Bearer  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJmMjM0NTY3ODkwiibmFtZSI6InRlc3RpliwiaWF0IjoxNTE2MjM5MDIyQy59KjFScCBmdVIGgi5Es8zg04cmY"
```

Alla esimerkki JWT:n sisältävästä OAuth assertion-parametrissa:

```
POST https://phr-auth.kanta.fi/phr-authserver/token HTTP/1.1  
grant_type=urn%3Afi%3Akela%3Akanta%3Aphr%3Aoauth%3Agrant-type%3Afinnish-phr-  
jwt&client_id=ProfessionalClientExample&client_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJmMjM0NTY3ODkwiibmFtZSI6InRlc3RpliwiaWF0IjoxNTE2MjM5MDIyQy59KjFScCBmdVIGgi5Es8zg04cmY
```

## 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 [JWS \(JSON Web Signature\)-standardissa](#).

Allekirjoituksessa käytettävä julkisen avaimen sisältävä varmenne lähetetään JWT:n otsikkotietueen kentässä x5c.

Käytettävä algoritmi kerrotaan otsikkotietueen kentässä alg, algoritmin tarkemmat määrytykset löytyvät Kanta JWS määrittelystä. Version tiedossa annetaan tämän JWT määrittelyn versio.

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

```
{  
  "x5c": [  
    "
```

```
"MIIFGDCCAwACFGrO1cnZGbuVx/Ph7yn/9TFRcib8MA0GCSqGSIb3DQEBAQUAMDgxCz  
AJBgNVBAYTInAkZJMQ0wCwYDVQQKDARLZWxhMRRowGAYDVQQDBFkyYWMgUINBIF  
Rlc3QgQ0EgMTAgFw0yMzA4MjQxNjMjMjM0NTY3ODkwiibmFtZSI6InRlc3RpliwiaWF0IjoxNTE2MjM5MDIyQy59KjFScCBmdVIGgi5Es8zg04cmY"
```

```
nPTf5uwABJGA4qWEMwctdms8U4t53uZv7yehULQAxCq293y/C/RmKFv1UjSrRrCdpr4gOZ
pILH9qQ\ntqjz4cVMLduoFVGIQv7pDiEE60TN914yQNT/RIFFFSQm7+lzxClfW4IBljFHz1Qh
3hstRXxvR18\nOd0CDnN5ChZ3ox1fYB4UiTHhHq7oijEHSx/kca3LbWg0p2sDvNLLqiW39h6
h6v8hxtGZNSrT+2B+\nBPYHIfSXS0nbyn7AO3ZNz6UGP10LD47XOAVIJMvSoB/VNhaZXM
06IM3Q7ChB0h1YCTpN/68ZQYif\nwVpt4DDR4/GqyatWEmFBE3hitXq91/JahpZvnh7DhHb
+pwFeHgLtr3oxcPN/XJT9fOriYwYdDCm\n+zXDv7pTOjBwb54nVdj/GUWuR/tOn460RzlwqU
SaakEkm4gLkUp1lb7yRJ9AwiPPHqDj1ujAtO18\naYRGJPxBygW3wLFDqNxc2h3xncf6V8Z
kJzZjH5cQ2KAr4u1rULE9474JXW81A3bNA7IKBypDCZH\nT2hONddiaDWbF1tBQZiH14ou
Q+DvoEEpGQRBoNCFAGMBAAEwDQYJKoZlhvcNAQENBQADggIBAB5s\nHlrX56mehppx2
ovVJAIUYtYW9fx6rz7RTW6DwiRv5x0/2ZC9ke1SQM/f0LUedFGGRIXHfmdBk5LK\nttp/9au5r
BfHSN4YfYapnrIKs6nzEaV1q0QyD5Zvqp0Q3fM1qDs131PShH5gjVFGk1pzIU2ocYtE\n+INB
+TKgytezR3L8kUGvUojx6CDYBlwwilyc5Nw3GHMpdo26Vi30KIFL/LizDUSlje2M/dcMTIfC\ne
852kjNt0oqOgXrkhPsvX6aAtWibJeTj7iyXwbTTFOW+mD1lm8Zf9PzsOO7xdvAcUm/Mr9D2n
Ydu\n/g7Q7DR8I4bp6yfwzREQBZYtVHNksbToUk30uGBbA9xUhV+eOLzEAGOFp2EdKvSK
ZZHDtoPaehOC\nLTTWhR9Ktw3LMUblmik5MxNu2W5w6R1aNCUf7ADeE+WV0AsjhBEWb
N8zca9NqMpjOIVIZIny6j8+\nYFoelNxmY5jF0/DQj6tYDb9ti7Kpl/g4/B12nXRmwrwj47su57b
CCYnsOCUDq4kOSUyX/YTOM6P\n/5LVz6mMEiHIFhQALFQQz3wXC2uPQObUvUBByO
dIY6BziYrKU2sPh03CdQ9ra7AtHehpHn3G1UN\nHlPTrQd0plxiu5IniNSQgDIHPu00NurXfVZ
E34uDI3yMU2khCdOal7I4I4irykNczfZ23eww"
```

```
],
  "alg": "RS512",
  "version": "1.1.0"
}
```

## 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.

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

Tietotyypit noudattavat JWT määrittelyn ([RFC 7519: JSON Web Token](#)) tietotyyppejä tai tämän määrittelyn skeeman tietotyyppejä (Object-II, Object-CV).

Taulukko 4.1 Kanta-palveluiden JWT Claimit.

PTA= Potilastiedon arkisto, SHA = Sosiaalihuollon asiakastiedon arkisto, OTV = Omätietovaranto, RES = Resepti-palvelu

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

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
<b>JWT-standardin mukaiset yhteiset claimit (Registered Claims)</b>						
iss	Kanta-liityntäpisteen tunniste	P	P	P	P	String
sub	Liittyjäorganisaation tunniste (sama arvo kuin subscriber_id kentässä)  OTV: organisaation tunniste, jolle oikeus annettu auktorisointipalvelussa  RES/PTA/SHA: organisaation tunniste, jolle annettu lähetysoikeus (ilmoitettava erikseen osoitteistoon)	P	P	P	P	String
aud	Vastaanottajan tunniste  Tuotanto-ympäristössä:  PTA: 1.2.246.556.18.2  SHA: 1.2.246.556.18.6  RES: 1.2.246.556.18.1  OTV: auktorisointipalvelimen osoite	P	P	P	P	String
exp	JWT:n vanhenemisaika  PTA/SHA/RES: enintään iat + 30 minuuttia  OTV: enintään iat + 5 minuuttia	P	P	P	P	NumericDate
iat	JWT:n luontiaika	P	P	P	P	NumericDate
jti	JWT:n yksilöivä tunniste	E	E	P	E	String
<b>Kanta-tasoiset lisäclaimit (Private Claims)</b>						
application_name	Pyynnön tehneen tietojärjestelmän nimi	P	P	P	P	String
application_version	Pyynnön tehneen tietojärjestelmän versio	P	P	P	P	String



Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
practitioner_id	<p>Pyynnön tehneen ammattihenkilön tunnistenumero</p> <p>Terhikki, suosikki, SV-numero, vrk-yksilöivä tunnus tai henkilötunnus, tunnusten käyttö vastaava kuin Medical Records sanomamäärittelyissä.</p> <p>Annetaan system ja value, molemmat pakollisia.</p> <p>PTA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyynnö</p> <p>SHA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyynnö</p> <p>RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyynnö</p>	eP	eP	P	eP	Object-II:  {s: "1.2.246.21", v: "010186-993N" }
citizen_id	<p>Pyynnön tehneen kansalaisen tunnistenumero</p> <p>Annetaan system ja value, molemmat pakollisia.</p> <p>PTA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyynnö tai puolesta asiointitilanne.</p> <p>SHA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyynnö tai puolesta asiointitilanne.</p> <p>RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyynnö</p>	eP	eP	E	eP	

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
practitioner_given	<p>Pyynnön tehneen ammattihenkilön etunimi</p> <p>PTA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyynnö.</p> <p>SHA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyynnö.</p> <p>RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyynnö.</p>	eP	eP	P	eP	Array<String>
citizen_given	<p>Pyynnön tehneen kansalaisen etunimet</p> <p>PTA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyynnö.</p> <p>SHA: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyynnö.</p> <p>RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyynnö.</p>	eP	eP	E	eP	Array<String>
practitioner_family	<p>Pyynnön tehneen ammattihenkilön sukunimi</p> <p>PTA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyynnö.</p> <p>SHA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyynnö.</p>	eP	eP	P	eP	String

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
	RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö.					
citizen_family	<p>Pyynnön tehneen henkilön sukunimi</p> <p>PTA: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyyntö.</p> <p>SHA: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyyntö.</p> <p>RES: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyyntö.</p>	eP	eP	E	eP	String
authentication_method	<p>Pyynnön tehneen henkilön tunnistautumismenetelmä</p> <p>Käytettävä koodisto 1.2.246.537.5.40128.2006 (KanTa-palvelut - Tunnistautumistapa)</p> <p>PTA ja SHA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö.</p>	eP	eP	P	P	Object-CV  {c: "2", s: "1.2.246.537.5.40128.2006"}
requested_record	<p>Pyynnön kohde (potilas, asiakas)</p> <p>PTA ehdon pakollisuus: pakollinen, kun toiminto kohdistuu yhden henkilön tietoihin.</p>	eP	P	P	E	Object-II:  {s: "1.2.246.21", v: "010144-955L" }
subscriber_id	Liittyjäorganisaation tunnus	P	P	P	P	String
subscriber_name	Liittyjäorganisaation nimi	P	P	P	P	String

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
subscriber_unit_id	Liittyjäorganisaation palveluyksikön tunnus  ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	E	eP	V	String
subscriber_unit_name	Liittyjäorganisaation palveluyksikön nimi  ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	E	eP	V	String
requester_id	Pyynnön tehneen organisaation tunniste	P	P	P	P	String
requester_name	Pyynnön tehneen organisaation nimi	P	P	P	P	String
requester_unit_id	Pyynnön tehneen organisaation palveluyksikön tunniste  ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	P	eP	V	String
requester_unit_name	Pyynnön tehneen organisaation palveluyksikön nimi  ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	P	eP	V	String
requester_custodian	Hakeva rekisterinpitäjä  ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	P	eP	E	String
requester_custodian_name	Hakevan rekisterinpitäjän nimi  ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	P	eP	E	String
register	Hakevan rekisterinpitäjän rekisteritunnus  ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	E	eP	E	Object-CV:  {c: "2", s: "1.2.246.537.5.4015.0.2009"}

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
	Käytettävä koodisto: 1.2.246.537.5.40150.2009 (KanTa-palvelut - Potilas- asiakirjan rekisteritunnus)					
register_specifier	<p>Hakevan rekisterinpitäjän rekisterin tarkenne</p> <p>ehdon pakollisuus = kun register: arvo on 4 (=työ-terveys)</p> <p>Jos y-tunnus annetaan s-kentässä on sen arvo normalisoitava eli etunolla poistettava ja yhdysmerkki poistettava.</p> <p>Y-tunnus:</p> <p>registry_specifier: {s: "1.2.246.10", v: "123456-7" }</p> <p>Henkilötunnus:</p> <p>registry_specifier: {s: "1.2.246.21", v: "010144-955L" }</p> <p>Y-tunnukseton työnantajajayritys:</p> <p>registry_specifier: {s: "1.2.246.537.30", v: "2345678.11" }</p>	eP	E	eP	E	Object-II:  {s: "1.2.246.10", v: "123456-7" }
service_event_id	<p>Viittaus palvelutapahtumaan</p> <p>PTA ehdon pakollisuus = annettava luovutushakupyynnöissä, annettava ajanvarauksen arkistoinnissa</p> <p>OTV ehdon pakollisuus = annettava Omatietovarannon ammattilaischauissa</p>	eP	E	eP	eP	String

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
	RES ehdon pakollisuus = pakollinen potilastietojärjestelmän tehdessä hakuja, jos haku tehdään palvelutapahtuman yhteydessä					
special_reason	<p>Tietojen haun erityinen syy</p> <p>Käytettävä koodisto: 1.2.246.537.6.240.2012 (THL - Asiakastietojen katselun erityinen syy)</p> <p>PTA ja OTV: ehdon pakollisuus: pakollinen hauissa, tarkempi määrittely vielä tekemättä</p> <p>SHA: ehdon pakollisuus: pakollinen hauissa, jos haku ei perustella tietoja hakuvan henkilön ja haun kohteena olevan asiakkaan välisellä asiayhteydellä.</p>	eP	eP	eP	E	Object-CV:  {c: "2", s: "1.2.246.537.6.240.2012"}
special_reason_explanation	<p>Tietojen haun erityinen syy - perustelu</p> <p>PTA ja OTV: ehdon pakollisuus: pakollinen hauissa, tarkempi määrittely vielä tekemättä</p> <p>SHA: ehdon pakollisuus: pakollinen hauissa, jos haku ei perustella tietoja hakuvan henkilön ja haun kohteena olevan asiakkaan välisellä asiayhteydellä.</p>	eP	eP	eP	E	String

#### 4.2.2 Kanta JWT:n tietosisällön skeema

Tietosisällön skeema:

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "https://kela.fi/kanta.jwt.schema.json",

```

```
"title": "Kanta JWT",
"description": "Kanta JWT schema",
"type": "object",
"properties": {
  "iss": {
    "type": "string"
  },
  "aud": {
    "type": "string"
  },
  "exp": {
    "type": "integer"
  },
  "sub": {
    "type": "string"
  },
  "iat": {
    "type": "integer"
  },
  "jti": {
    "type": "string"
  },
  "application_name": {
    "type": "string"
  },
  "application_version": {
    "type": "string"
  },
  "citizen_id": {
    "$ref": "#/$defs/ii"
  },
  "citizen_given": {
    "type": "array",
    "items": [
      {
        "type": "string"
      }
    ]
  },
  "citizen_family": {
    "type": "string"
  },
  "practitioner_id": {
    "$ref": "#/$defs/ii"
  },
  "practitioner_given": {
    "type": "array",
    "items": [
      {
        "type": "string"
      }
    ]
  },
  "practitioner_family": {
    "type": "string"
  },
  "authentication_method": {
```

```
        "$ref": "#/$defs/cv"
      },
      "requested_record": {
        "$ref": "#/$defs/ii"
      },
      "subscriber_id": {
        "type": "string"
      },
      "subscriber_name": {
        "type": "string"
      },
      "subscriber_unit_id": {
        "type": "string"
      },
      "subscriber_unit_name": {
        "type": "string"
      },
      "requester_id": {
        "type": "string"
      },
      "requester_name": {
        "type": "string"
      },
      "requester_unit_id": {
        "type": "string"
      },
      "requester_unit_name": {
        "type": "string"
      },
      "requester_custodian": {
        "type": "string"
      },
      "requester_custodian_name": {
        "type": "string"
      },
      "registry_specifier": {
        "$ref": "#/$defs/ii"
      },
      "registry": {
        "$ref": "#/$defs/cv"
      },
      "service_event_id": {
        "type": "string"
      },
      "special_reason": {
        "$ref": "#/$defs/cv"
      },
      "special_reason_explanation": {
        "type": "string"
      }
    }
  },
  "required": [
    "iss",
    "aud",
    "exp",
    "sub",
    "iat",
```



```
    "application_name",
    "application_version",
    "subscriber_id",
    "subscriber_name",
    "requester_id",
    "requester_name"
  ],
  "$defs": {
    "ii": {
      "description": "Identifier",
      "required": [
        "s"
      ],
      "type": "object",
      "properties": {
        "s": {
          "description": "Identifier",
          "type": "string"
        },
        "v": {
          "description": "System for the identifier",
          "type": "string"
        }
      }
    },
    "cv": {
      "description": "Coded value",
      "required": [
        "c",
        "s"
      ],
      "type": "object",
      "properties": {
        "c": {
          "description": "Code",
          "type": "string"
        },
        "s": {
          "description": "System for the code",
          "type": "string"
        }
      }
    }
  }
}
```

#### 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",
"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"
}
```

### 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. 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).