

Kanta JSON Web Token

Draft, v. 0.8

23.10.2023

Kanta-palvelut

Julkinen

Muutoshistoria

Versio	Muutos	Tekijä	PVM
0.8	Ensimmäinen julkaistava draft-versio kommentointia varten	Kanta-palvelut	23.10.2023

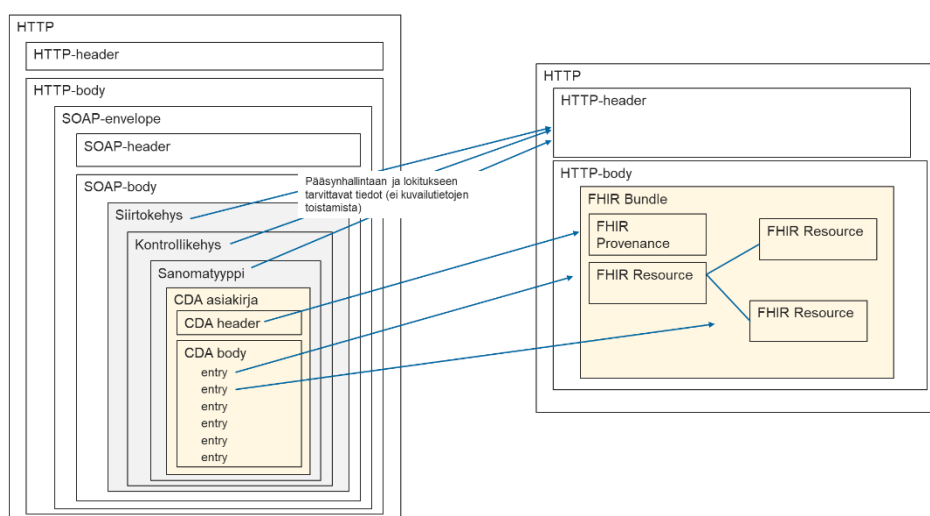
Sisällys

1	Tausta	1
2	JWT:n 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	4
4.3	Kanta JWT:n allekirjoitus	16

23.10.2023

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.



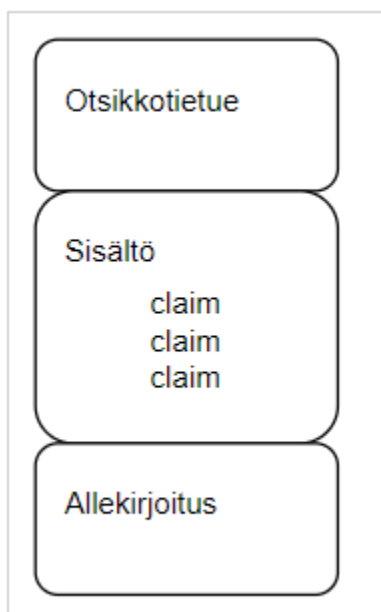
Kuva 1.1 Medical Records-sanomatason korvautuminen REST-rajapinnan *HTTP* header:lla.

Pääsynhallintaan ja lokitukseen tarvittavat tiedot, joiden osalta halutaan varmistaa oikeellisuus ja muuttumattomuus, viedään JWT:hen ([RFC 7519: JSON Web Token](#)). Kanta JWT:tä on tarkoitus käyttää Potilastiedon arkiston (PTA) ja Sosiaalihuollon asiakastiedon arkiston (SHA) uusissa FHIR rajapinnoissa. Jatkossa Kanta JWT:n käyttö laajenee muihin rajapintoihin kuten Reseptin lääketyslista 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 JWT:n tekninen rakenne

JWT:n tekninen rakenne on esitetty kuvassa 2.1. 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:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

.

eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpXVCJ9

.

KeNzd2Es6XIFQSp59gKjFSxCBmdVIGgi5Es8zg04cmY

3 Kanta JWT:n käyttö

Kanta JWT:tä käyteään 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 valmis).

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

```
"Authorization": "Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWUiOiJxMjM0NTY3ODkwIiwibmFtZSI6InRlc3RpliWiaWF0IjoxNTE2MjM5MDIyZS5keS6XIFQSp59gKjFSxCBmdVIGgi5Es8zg04cmY"
```

Alla esimerkki JWT:n sisältävästä OAuth assertion-parametrasta:

```
POST https://phr-auth.kanta.fi/phr-authserver/token HTTP/1.1
grant_type=urn%3Afi%3Aakela%3Aakanta%3Aphr%3Aoauth%3Agrant-type%3Afinnish-phr-jwt&redirect_uri=https%3A%2F%2Flocalhost&client_id=ProfessionalClientExample&client_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWUiOiJxMjM0NTY3ODkwIiwibmFtZSI6InRlc3RpliWiaWF0IjoxNTE2MjM5MDIyZS5keS6XIFQSp59gKjFSxCBmdVIGgi5Es8zg04cmY
```

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 on RSA512 ja se kerrotaan otsikkotietueen kentässä alg. Version tiedossa annetaan tämän JWT määrittelyn versio.

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

```
{
  "x5c": [

    "MIIFGDCCAwACFGrO1cnZGbuVx/Ph7yn/9TFRcib8MA0GCSqGSIb3DQEBDQUAMDgxGz
    AJBgNVBAYTInAkZJMQ0wCwYDVQQKDARLZWxhMR0wGAYDVQQDDBFKYWMgUINBIF
    Rlc3QgQ0EgMTAgFw0yMzA4MjQxLnMjAyNDRAGA8yMTIzMDczMTEyMDI0NFowVzELMAk
    GA1UEBHMCRkkxDTALBgNVBAoMBEtlbGExHTAbInBgNVBAUTFDEuMi4yNDYuNTU2LjE
    wMDAxLjM1MR0wGAYDVQQQDDBFSU0EgVGZvdCBPcmcgS2VsYTCCInAilwDQYJKoZIh
    vCNAQEBBQADggIPADCCAgoCggIBALQtrMq3HUzOrluw2rO4UOdNMesVINnf+KruInF
    dFkfG042MbM0b2xHURwIzjA8Z3u8QN4cbCV9ciTiHBf88Li++DNEUagyl5dsI9m+Fg
    OB3WonQKBInPTf5uwABJGA4qWEMwctdms8U4t53uZv7yehULQAxG293y/C/RmKFv1
    UjSrRrCdpr4gOZpILH9qQInTqpjz4cVMLduoFVGIQv7pDiEE60TN914yQNT/RIFFFS
    Qm7+lzxClfW4BljFH1Qh3hstRXxvR18InOd0CDnN5ChZ3ox1fYB4UiTHhHq7oijEHSx/
    kca3LbWg0p2sDvNLLqiW39h6h6v8hxtGZNSRt+2B+InBPYHIfSXS0nbyn7AO3ZNz6
    UGP10LD47XOAVIJMvSoB/VNhaZXM06IM3Q7ChB0h1YCTpN/68ZQYifInwVpt4DDR
    X4/GqyatWEmFBE3hitXq91/JahpZvnh7DhHb+pwFeHgLT3oxcPN/XJT9fOrlYwYd
    DCmIn+zXDv7pTOjBwb54nVdj/GUWuR/tOn460RzlwQU SaakEkm4gLkUp1lb7yR
    J9AwIPPHqDj1ujAtO18InaYRGJPxBygW3wLFdqNxc2h3xnzcf6V8Z
```

```
kJzZjH5cQ2KAr4u1rULE9474JXW81A3bNA7IKByDCZHnT2hONddiaDWbF1tBQZiH14ou
Q+DvoEEpGQrBoNCFAGMBAAEwDQYJKoZIhvcNAQENBQADggIBAB5s\nHlrX56mehppx2
ovVJAIUYtYW9fx6rz7RTW6DwiRv5x0/2ZC9ke1SQM/f0LUedFGGRIXHfmdBk5LK\http/9au5r
BfHSN4YfYapnrIKs6nzEaV1q0QyD5Zvqp0Q3fM1qDs131PShH5gjVFGk1pziU2ocYtE\n+INB
+TKgytezR3L8kUGvUojx6CDYBlwwilcy5Nw3GHMpd026Vi30KIFL/LizDUSlje2M/dcMTIfC\ne
852kjNt0oqOgXrkhPsvX6aAtWibJeTj7iyXwbTTFOw+mD1lm8Zf9PzsOO7xdvAcUm/Mr9D2n
Ydu\n/g7Q7DR8I4bp6yfwzREQBZYtVHNksbToUk30uGBbA9xUhV+eOLzEAGOFp2EdKvSK
ZZHDtoPaehOC\nLTTWhR9Ktw3LMUblmik5MxNu2W5w6R1aNCUf7ADeE+WV0AsjhBEWb
N8zca9NqMjOIVIZIny6j8+\nYFoelNxmY5jF0/DQj6tYDb9ti7Kpl/g4/B12nXRmwrwj47su57b
CCYnsOCUDq4kOSUyX/YTOM6P\n/5LVz6mMEiHfHqALFQQQz3wXC2uPQObUvUBByO
dIY6BziYrKU2sPh03CdQ9ra7AtHehpHn3G1UN\nHlPTrQd0Plxiu5IniNSQgDIHPuO0NurXfVZ
E34uDI3yMU2khCdOal7I4I4irykNczfZ23eww"
```

```
],
"alg": "RS512",
"version": "1.0.0"
}
```

4.2 Kanta JWT:n tietosisältö

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

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 datamuoto.

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

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

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
JWT-standardin mukaiset yhteiset claimit (Registered Claims)						
iss	Kanta: liityntäpisteen tunniste / sertifikaatin serial number	P	P	P	P	String
sub	JWT:n tuottaneen järjestelmän tunniste	P	P	P	P	String

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
aud	JWT: The "aud" (audience) claim identifies the recipients that the JWT is intended for 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	P	P	P	P	NumericDate
jti	JWT:n yksilöivä tunniste	P	P	P	P	String
iat	JWT:n luontiaika (max. 5 min. menneisyydessä)	V	V	P	V	NumericDate
Kanta-tasoiset lisäclaimit (Private Claims)						
application_name	Pyynnön tehneen tietojärjestelmän nimi	P	P	P	P	String
application_version	Pyynnön tehneen tietojärjestelmän versio	P	P	P	P	String
practitioner_id	Pyynnön tehneen ammattihenkilön käyttäjätunniste Terhikki, suosikki, SV-numero, vrk-yksilöivä tunnus tai henkilötunnus. Huom. tarkennettava mikä missäkin palvelussa sallittu. Annetaan system ja value, molemmat pakollisia. PTA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyynnö SHA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyynnö	eP	eP	P	eP	Object-II: {s: "1.2.246.21", v: "010186-993N" }

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
	RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö					
citizen_id	Pyynnön tehneen kansalaisen tunniste PTA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö SHA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö	eP	eP	E	eP	
practitioner_given	Pyynnön tehneen ammattihenkilön etunimi PTA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö. SHA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyyntö. RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö.	eP	eP	P	eP	List<String>
citizen_given	Pyynnön tehneen kansalaisen etunimet PTA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö. SHA: ehdon pakollisuus: pakollinen, jos kyseessä	eP	eP	E	eP	List<String>

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
	on kansalaisen käynnistämä hakupyyntö. RES: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö.					
practitioner_family	Pyynnön tehneen ammattihenkilön sukunimi PTA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö. SHA: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä tallennus- tai hakupyyntö. RES: ehdon pakollisuus: pakollinen, jos kyseessä on ammattihenkilön käynnistämä hakupyyntö.	eP	eP	P	eP	String
citizen_family	Pyynnön tehneen henkilön sukunimi PTA: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyyntö. SHA: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyyntö. RES: ehdon pakollisuus: pakollinen, jos kyseessä on kansalaisen käynnistämä hakupyyntö.	eP	eP	E	eP	String
authentication_method	Pyynnön tehneen henkilön tunnistautumismenetelmä PTA ja SHA: ehdon pakollisuus: pakollinen, jos kyseessä on henkilön käynnistämä hakupyyntö.	eP	eP	P	P	Object-CV {c: "2", s: "1.2.246.537.5.40128"}

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
requested_record	Pyynnön kohde (potilas, asiakas) PTA ehdon pakollisuus: pakollinen, kun toiminto kohdistuu yhden henkilön tietoihin.	eP	P	P	E	Object-II: {s: "1.2.246.21", v: "010144-955L" }
subscriber_id	Liittyjäorganisation tunnus	P	P	P	P	String
subscriber_name	Liittyjäorganisation nimi	P	P	P	P	String
subscriber_unit_id	Liittyjäorganisation palveluyksikön tunnus ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	E	eP	V	String
subscriber_unit_name	Liittyjäorganisation palveluyksikön nimi	eP	E	eP	V	String
requesting_id	Pyynnön tehneen organisaation tunniste	P	P	P	P	String
requesting_name	Pyynnön tehneen organisaation nimi	P	P	P	P	String
requesting_unit_id	Pyynnön tehneen organisaation palveluyksikön tunniste ehdon pakollisuus: pakollinen yhteisliittymistilanteessa	eP	P	eP	V	String
requesting_unit_name	Pyynnön tehneen organisaation palveluyksikön nimi	eP	P	eP	V	String
requesting_custodian	Hakeva rekisterinpitäjä ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	eP	eP	E	String
requesting_custodian_name	Hakevan rekisterinpitäjän nimi ehdon pakollisuus: pakollinen vain hakupyynnöissä	eP	eP	eP	E	String

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
register	Hakevan rekisterinpitäjän rekisteritunnus ehdon pakollisuus: pakollinen vain hakupyynnöissä Koodisto: 1.2.246.537.5.40150.2009	eP	E	eP	E	Object-CV: {c: "2", s: "1.2.246.537.5.40150.2009"}
register_specifier	Hakevan rekisterinpitäjän rekisterin tarkenne ehdon pakollisuus = kun registry_type: arvo on 4 (=työterveys) Jos y-tunnus annetaan s-kentässä on sen arvo normalisoitava eli etunolla poistettava ja yhdysmerkki poistettava. Y-tunnus: registry_specifier: {s: "1.2.246.10", v: "123456-7" } Henkilötunnus: registry_specifier: {s: "1.2.246.21", v: "010144-955L" } Y-tunnukseton työnantajajäritys: registry_specifier: {s: "1.2.246.537.30", v: "2345678.11" }	eP	E	eP	E	Object-II: {s: "1.2.246.10", v: "123456-7" }
service_event_id	Viittaus palvelutapahtumaan PTA ehdon pakollisuus = annettava luovutushakupyynnöissä, annettava ajanvarauksen arkistoinnissa	eP	E	eP	E	String

Claim	Selite	PTA	SHA	OTV	RES	Datamuoto
	OTV ehdon pakollisuus = annettava Omatietovaranon ammattilaishauissa					
special_reason	Tietojen haun erityinen syy PTA: ehdon pakollisuus: pakollinen hauissa, tarkempi määrittely vielä tekemättä, OTV:hen tulee sama ehto SHA: ehdon pakollisuus: pakollinen hauissa, jos hakua ei perustella tietoja haakevan henkilön ja haun kohteena olevan asiakkaan välisellä asiayhteydellä.	eP	eP	eP	E	Object-CV: {c: "2", s: "1.2.246.537.6.240"}
special_reason_explanation	Tietojen haun erityinen syy - perustelu PTA: ehdon pakollisuus: pakollinen hauissa, tarkempi määrittely vielä tekemättä, OTV:hen tulee sama ehto SHA: ehdon pakollisuus: pakollinen hauissa, jos hakua ei perustella tietoja haakevan henkilön ja haun kohteena olevan asiakkaan välisellä asiayhteydellä.	eP	eP	eP	E	String

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" : {
```

```
"aud" : {
  "type" : "string"
},
"exp" : {
  "type" : "integer"
},
"sub" : {
  "type" : "string"
},
"iat" : {
  "type" : "integer"
},
"jti" : {
  "type" : "string"
},
"application_name" : {
  "type" : "string"
},
"practitioner_id" : {
  "$ref" : "#/$defs/ii"
},
"practitioner_given" : {
  "type" : "array",
  "items" : [{
    "type" : "string"
  }]
},
"practitioner_family" : {
  "type" : "string"
},
"practitioner_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"
},
"requesting_id" : {
  "type" : "string"
},
"requesting_name" : {
  "type" : "string"
},
"requesting_unit_id" : {
  "type" : "string"
},
"requesting_unit_name" : {
  "type" : "string"
},
"requesting_custodian" : {
  "type" : "string"
},
"requesting_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",
    "application_name",
    "application_version",
    "requested_record",
    "subscriber_id",
    "subscriber_name",
    "requesting_id",
    "requesting_name",
    "requesting_custodian",
    "requesting_custodian_name",
    "register"
  ],
  "$defs" : {
    "ii" : {
      "description" : "Identifier",
      "required" : [
        "s"
      ],
      "type" : "object",
      "properties" : {
```



```
      "s" : {
        "description" : "System for Identifier",
        "type" : "string",
      },
      "v" : {
        "description" : "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",
        }
      }
    }
  }
}
```

Esimerkki JWT:n tietosisällöstä:

```
{
  "aud" : "1.2.246.556.18.2",
```

```
"exp" : 1692962672,
"sub" : "1.2.246.556.10001.35",
"iat" : 1692960872,
"jti" : "12d3a0f7-a8a5-478b-8100-e75325f2d1ee",
"application_name" : "Ammattikäytön testisovellus",
"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" : "1.2.246.556.10001.35",
"subscriber_name" : "Liittyjän nimi",
"subscriber_unit_id" : "1.2.246.556.10001.35",
"subscriber_unit_name" : "Liittyjän palveluyksikön nimi",
"requesting_id" : "1.2.246.556.10002.2",
"requesting_name" : "Pyynnön tehneen organisaation nimi",
"requesting_unit_id" : "1.2.246.556.10002.32",
"requesting_unit_name" : "Pyynnön tehneen yksikön nimi",
"requesting_custodian" : "1.2.246.556.10001.35",
"register_specifier" : {
    "s" : "1.2.246.10",
    "v" : "123456-7"
},
"register" : {
    "c" : "4",
    "s" : "1.2.246.537.5.40150.2009"
},
"service_event_id" : "1.2.200.200.2008.20.20.20.2034980283.23",
"special_reason" : {
```

```
        "c" : "2",
        "s" : "1.2.246.537.6.240"
    },
    "special_reason_explanation" : "Viranomaisen OrganisaatioX pyytämä selvitys
henkilön terveystiedoista"
}
```

4.3 Kanta JWT:n allekirjoitus

Kanta JWT allekirjoitetaan JWS-standardin mukaisesti käyttäen JWT otsikkotietueessa annetun varmenteen yksityistä avainta.

Varmenteen on oltava SOTE-varmenne. Varmenteen osalta on vielä tarkennettava, mitä varmennetta on käytettävä tai minkä varmenteen käyttö on sallittua. Joka tapauksessa varmenteella on pystyttävä tekemään sähköinen allekirjoitus.

Allekirjoitus on kuvattu tarkemmin dokumentissa Kanta JSON allekirjoitus.