Kanta FHIR sähköinen allekirjoitus

v. 1.2.0

30.1.2025

Kanta-palvelut

Julkinen

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta tjänsterma
PB 450, 00056 FPA

www.kanta.fi
kanta@kanta.fi

Muutoshistoria

Versio	Muutos	Tekijä	PVM
0.8	Ensimmäinen julkaistava draft-versio kommentointia varten	Kanta-palvelut	23.10.2023
1.0.0	Ensimmäinen virallinen julkaisu	Kanta-palvelut	20.12.2023
1.1.0	Poistettu lukujen 1.3 ja 3.1 teksti pitkäaikaisten allekirjoitusten tukemisesta ja päivitetty lukuun 3.1 oikea profiili JAdES-B-B	Kanta-palvelut	29.02.2024
1.1.1	Korjattu viittaukset JAdES 1.1.1 versiosta 1.2.1 versioon. Korjattu standardissa muuttuneet kohdat skeemassa: - sigT otsikkoparametrin poisto. sigT:n sijasta käytetään iat otsikkoparametria. - sigD -taulukkoon lisätty pakollisena kenttänä ”pars” Lisätty luvun 2.1 tietoihin ”type” -kentässä käytettävät tunnisteet. Poistettu kohdan 6.2.1 esimerkistä ”x5t” -otsikkoparametri. Korjattu luvussa 6.2.2 Signature-objektin esimerkissä json taulukon alkumerkin ”[” väärä sijainti.	Kanta-palvelut	09.10.2024
1.2.0	Korjattu sigD -otsikkoparametrin pakollinen pars -kenttä mukaan allekirjoitukseen. Lisätty pars -kentän viittaus ”/Bundle” -resurssiin. Lisätty version -otsikkoparametri Kanta laajennuksena JAdES -allekirjoitukseen. Tarkennettu version -otsikkoparametrin käyttö. Kirjoitusasua tarkennettu dokumentin laajuisesti.	Kanta-palvelut	30.1.2025

Sisällys

1 Johdanto

FHIR (Fast Healthcare Interoperability Resources) on HL7:n (Health Level Seven) julkaisema datarakennestandardi, joka määrittelee, miten terveystietoja voidaan lähettää ja jakaa eri IT-järjestelmien välillä. FHIR-standardi edistää terveydenhuollon tietojen yhteensopivuutta ja saatavuutta, mahdollistaen tehokkaamman tiedonvaihdon eri terveydenhuollon toimijoiden välillä.

FHIR-resurssit tulee allekirjoittaa, jotta voidaan varmistua, että FHIR-data säilyy muuttumattomana myös pitkäaikaisesti säilytettynä ja että tieto on peräisin oikealta taholta ja tietoa ei ole muutettu Kanta-palveluissa tai tiedon välityspisteissä. Resursseille tehtävä JWS-allekirjoitus perustuu digitaaliseen allekirjoitukseen, joka varmentaa tiedon eheyden ja lähettäjän identiteetin.

Tämä dokumentti tarjoaa ohjeet JWS-allekirjoituksen luomiseen FHIR-resursseille sekä esittää keinot allekirjoituksen tarkastamiseksi. Näin varmistetaan, että FHIR-muotoisten terveystietojen vaihto tapahtuu luotettavasti ja turvallisesti eri toimijoiden välillä.

1.1 Dokumentin rakenne

Tämä dokumentaatio määrittelee tavan luoda ja lisätä digitaalinen allekirjoitus HL7 FHIR Specification (v4.0.1: R4 - STU) mukaisiin sähköisiin resursseihin. Tätä voidaan jatkossa soveltaa myös HL7 FHIR Specification (v5.0.0: R5 - STU) mukaisiin resursseihin.

Dokumentti määrittelee FHIR-resurssien sähköisiin allekirjoituksiin käytettävät käytännöt ja toteutuksen.

Dokumentti määrittelee JSON Digital Signatures [5] tyyppisen allekirjoituksen käytön HL7 FHIR-resurssien digitaaliseen allekirjoitukseen [1] FHIR Specification (v4.0.1: R4 - STU) 6.1.2 Digital Signatures.

Dokumentissa käsitellään vain JSON Digital Signatures [5] tyyppisen sähköisen allekirjoituksen käyttö FHIR JSON (FHIR Specification (v4.0.1: R4 - STU ja v5.0.0: R5 - STU) resurssien allekirjoitukseen.

Luvut 1, 3 ja 5 ovat normatiivisia. Luku 2 käsittelee yleisemmin FHIR-rakennetta ja luku 3 määrittää allekirjoitusrakennetta koskevat asiat. Luku 4 sisältää konkreettisia esimerkkejä allekirjoituksen luonnista, sen tarkastuksesta ja selitykset JWS otsikoille. Luku 5 sisältää normatiivisen kuvauksen allekirjoitusprosessista.

1.2 Sähköisen allekirjoituksen yleiset periaatteet

Yleisellä tasolla digitaaliset allekirjoitukset toimivat siten, että allekirjoituksen luoja luo julkisen ja yksityisen avaimen parin ja jakaa julkisen avaimensa allekirjoitetun resurssin vastaanottajalle.

Allekirjoitus perustuu resurssin tiivisteen (hash) laskemiseen ja yksityisellä avaimella salaamiseen. Jos allekirjoitettava data on JSON-formaatissa, se tulee myös kanonikalisoida eli yhtenäistää ennen tiivisteen laskemista.

Resurssin vastaanottaja käyttää julkista avainta purkaakseen allekirjoituksen salauksen ja tarkistaakseen tiivisteen eheyden. Tämän jälkeen vastaanottaja laskee resurssista tiivisteen ja vertaa sitä tiivisteeseen, jonka hän sai purkaessaan allekirjoitusta. Jos tiivisteet ovat identtisiä, allekirjoitus on validi eli resurssi ei ole muuttunut allekirjoituksen jälkeen.

1.3 Sähköiset FHIR-resurssien allekirjoitukset Kanta-palveluissa

Digitaaliset allekirjoitukset ovat eräs sähköisen allekirjoituksen muoto. Ne käyttävät salaustekniikkaa ja sertifiointiviranomaisen (Certification Authority, CA) myöntämää varmennetta (digital certificate). CA:n myöntämä varmenne varmistaa, että allekirjoituksen aitouteen ja kiistämättömyyteen voi luottaa.

Digitaaliset allekirjoitukset täyttävät seuraavat toiminnalliset vaatimukset:

- Autentikaatio – Niillä voi varmistaa allekirjoittajan identiteetin.
- Eheyden varmistaminen – Niillä voidaan taata, että allekirjoitettua asiakirjaa ei ole muutettu allekirjoittamisen jälkeen.
- Kiistämättömyys – Allekirjoittaja ei voi kiistää allekirjoituksen tekemistä.

Kanta FHIR-allekirjoituksessa täytyy käyttää SOTE järjestelmäallekirjoitusta.

HL7 FHIR resursseja (resources) allekirjoitetaan lisäämällä Bundle-resurssiin irrotettu (detached) JSON signature.

- JSON-digitaaliallekirjoituksen täytyy noudattaa kappaleessa 1.5.1 viitattuja standardeja ja spesifikaatioita (JAdES, FHIR, RFC).
- JSON-digitaaliallekirjoituksen täytyy noudattaa JAdES-standardia tarkennettuna KANTA-osilla tässä määrittelyssä kuvatuilla tavoilla.

1.4 Dokumentissa käytetyt termit, symbolit ja lyhenteet

1.4.1 Lyhenteet

Lyhenne	Selite
JSON	JavaScript Object Notation
JWS	JSON Web Signature
JOSE	JSON Object Signing and Encryption
OCSP	Online Certificate Status Protocol

SHA	Secure Hash Algorithm
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
JCS	JSON Canonicalization Scheme

Taulukko 1: Käytetyt lyhenteet

1.4.2 Terminologia

Tässä asiakirjassa käytetään aina, kun mahdollista, samaa terminologiaa kuin IETF RFC 7515:ssä [2] ja IETF RFC 8259:ssä [1].

Tässä asiakirjassa termi "JSON Web Signature" tarkoittaa IETF RFC 7515:ssä [2] määriteltyä JSON-allekirjoitusrakennetta.

Tässä asiakirjassa käytetään termiä "arvo" ilmaisemaan JSON-objekteja, JSON-taulukoita tai JSON-numeroita tai JSON-merkkijonoja, eli osajoukkoa "JSON-arvon" mahdollisista merkityksistä, jotka esiintyvät nimi-arvoparin arvoina ja on lueteltu IETF RFC 8259:n [1] lausekkeessa 3.

Tässä asiakirjassa käytetään termiä "otsikkoparametri" kuvaamaan JSON-objektia, JSON-taulukkoa, JSON-numeroa tai JSON-merkkijonoa, joka on joko IETF RFC 8259:ssä [1] määritellyn JWS Protected Headerin tai JWS:n suojaamattoman otsikon jäsen.

Tässä asiakirjassa käytetään termejä "kenttä” ja ”jäsen" ilmaisemaan JSON-objektin jäsen (JSON nimi-arvo -pari) IETF RFC 8259:n [1] lausekkeen 4 mukaisesti.

Tässä asiakirjassa käytetään termiä "elementti" tai "taulukon elementti" osoittamaan JSON-taulukon sijainnin sisältöä (määritetty IETF RFC 8259:n [1] lausekkeessa 5).

Tässä asiakirjassa käytetään termiä "JCS" ilmaisemaan standardoitu tapa kuvata JSON dokumentti kanonikalisoidulla muodolla.

Tässä asiakirjassa käytetään termiä "**Täytyy**" ilmaisemaan ehdotonta vaatimusta kaikille toteutuksille.

Tässä asiakirjassa käytetään termiä "**Pitäisi**" ilmaisemaan parasta käytäntöä tai suositusta, joka on otettava huomioon toteutuksen yhteydessä. Saattaa olla päteviä syitä jättää ”Pitäisi” -määriteltyjä kohteita huomioimatta, mutta täytyy ymmärtää ja punnita huolellisesti kaikki seuraukset ennen kuin valitaan toinen vaihtoehto.

Tässä asiakirjassa käytetään termiä "**Voi**" ilmaisemaan valinnaisuus toteutuksessa. Kohde voidaan sisällyttää tai jättää pois toteuttajan päätöksen mukaan ilman seuraamuksia.

Tässä asiakirjassa käytetään termiä "**Ei saa**" ilmaisemaan ehdoton kielto kaikille toteutuksille.

1.5 Viittaukset

Viittaukset lähteisiin ovat joko erityisiä (julkaisupäivän ja/tai painoksen tai versionumeron perusteella) tai epäspesifisiä. Tiettyihin viittauksiin sovelletaan vain lainattua versiota. Epäspesifisiin viittauksiin sovelletaan viitatun asiakirjan viimeisintä versiota (mukaan lukien mahdolliset muutokset).

1.5.1 Normatiiviset viittaukset

[1] FHIR Specification (v4.0.1: R4 - STU): http://hl7.org/fhir/R4/index.html

[2] FHIR Specification (v5.0.0: R5 - STU): http://hl7.org/fhir/R5/index.html

[3] ETSI TS 119 182-1 V1.2.1 (2024-07): Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Technical Specification,

https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf

[4] IETF RFC 8259 (December 2017): "The JavaScript Object Notation (JSON) Data Interchange Format", https://www.rfc-editor.org/rfc/rfc8259.html

[5] IETF RFC 7515 (May 2015): "JSON Web Signature (JWS)", https://www.rfc-editor.org/rfc/rfc7515.html

[6] IETF RFC 7519 (May 2015): JSON Web Token (JWT), https://www.rfc-editor.org/rfc/rfc7519.html

[7] Kyberturvallisuuskeskus Kryptograafiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

[8] DVV Palveluvarmenteet sosiaali- ja terveydenhuollolle, https://dvv.fi/palveluvarmenteet

[9] IETF RFC 8785 (June 2020): JSON Canonicalization Scheme (JCS), https://www.rfc-editor.org/rfc/rfc8785.html

[10] IETF RFC 3986 (January 2005): Uniform Resource Identifier (URI): https://www.rfc-editor.org/rfc/rfc3986.html

[11] ETSI:n TS 119 312 V1.2.1 (2017-05): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites,
https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf

[12] ECMA-262, 10th edition, June 2019 ECMAScript® 2019 Language Specification https://262.ecma-international.org/10.0/

1.5.2 Informatiiviset viittaukset

[i.1] https://www.kanta.fi/jarjestelmakehittajat/sahkoisen-allekirjoituksen-maarittely

[i.2] https://www.rfc-editor.org/rfc/rfc6901

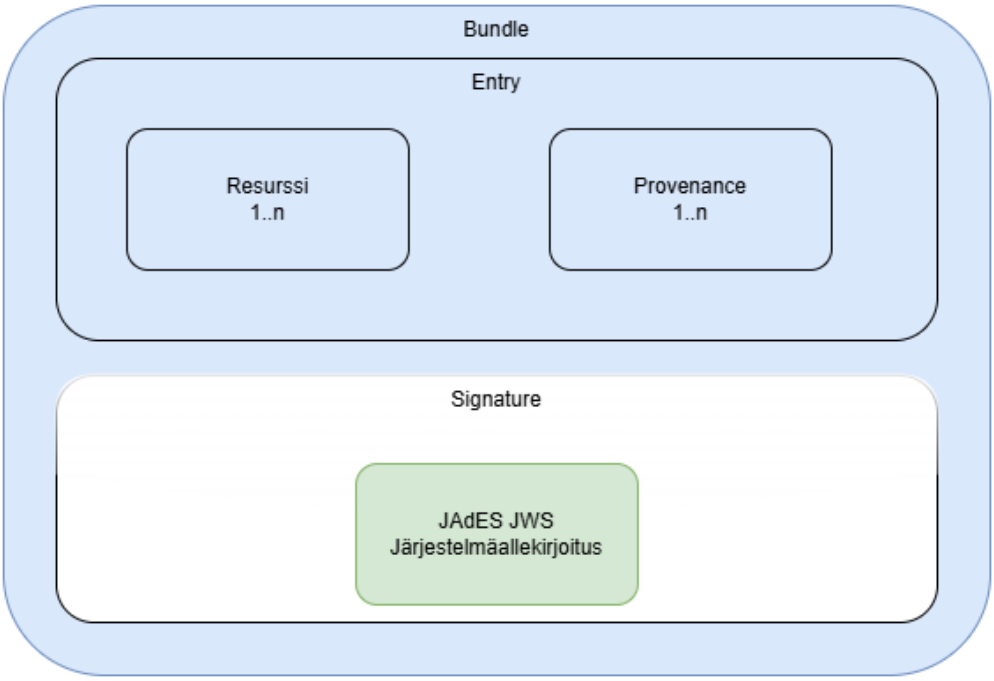
[i.3] DSS (Digital Signature Service) version : 5.12.1 - 2023-03-15, https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Signature+Service+-++DSS

[i.4] https://hl7.org/fhir/R4/datatypes-definitions.html#signature

2 FHIR-resurssien sähköinen allekirjoitus

2.1 FHIR resurssien allekirjoituksen rakenne

Tämä kappale sisältää esimerkin FHIR spesifikaation mukaisista JSON resurssista. Kanta-FHIR-resurssien allekirjoituksissa tuetaan ensimmäisessä vaiheessa koko Bundle-resurssin allekirjoitusta, jolloin Signature-objekti sijaitsee Bundle-resurssissa. Tulevaisuudessa uusien käyttötarpeiden osalta (useampi allekirjoitus, moniallekirjoitus usealle yksittäiselle resurssille resurssikohtaisesti) määrittelyitä täydennetään tämän dokumentin uusiin versioihin.



Kuva 1: FHIR Bundlen rakenne allekirjoituksen kanssa

FHIR Signature on JSON-objekti, johon JWS allekirjoitus sisällytetään. Kanta JWS allekirjoitukset tehdään FHIR Bundle-resursseista. Luotu allekirjoitus lisätään Signature-objektin data-kentän arvoksi.

Allekirjoituksen kohdistuminen käsitellään luvussa 4.3.

```
{
  // from Element: extension
  "type" : [{ Coding }], // Syy allekirjoitukselle
  "when" : "<instant>", // Allekirjoituksen ajankohta
  "who" : { Reference(Device|Organization|Patient|Practitioner|PractitionerRole|Related-
Person) }, // Allekirjoituksen luoja
  "onBehalfOf" : { Reference(Device|Organization|Patient|Practitioner|Practitioner-
Role|RelatedPerson) }, // Allekirjoitusta edustava taho
  "targetFormat" : "<code>", // Allekirjoitettavien resurssien tekninen formaatti
  "sigFormat" : "<code>", // Allekirjoituksen tekninen formaatti
  "data" : "<base64Binary>" // Allekirjoitus merkkijonona
}
```

Esimerkki 1: FHIR Signature-elementin rakenne

Yllä on esitetty FHIR R4 -standardin mukainen Signature -tyyppisen objektin schema [i4] (FHIR Specification (v4.0.1: R4 - STU) 2.24.0.17 Signature). Yllä olevassa skeemassa FHIR Specification (v4.0.1: R4 - STU) pakollisia kenttiä ovat type, when ja who, muut Signature objektin kentät ovat optionaalisia. Standardin R5-versiossa on väljennetty kenttien pakollisuutta. Allekirjoituksen kenttien pakollisuuteen voidaan ottaa kantaa myös Kanta-palveluiden profiloinnilla.

JWS allekirjoitus sisällytetään FHIR Signature.data -kenttään BASE64 enkoodattuna eli BASE64(”JAdES -allekirjoitus JWS Compact Serialization muodossa ilman payload osiota”).

```
BASE64((BASE64URL(UTF8(JWS Protected Header))..BASE64URL(JWS Sig-
nature))
```

Allekirjoitusten kentissä tulee huomioida BASE64 ja BASE64URL enkoodauksien ero.

Signature-objektissa:

- type = Lisätietoja allekirjoituksesta. Kanta FHIR-transaktiossa käytetään ”Review Signature” -arvoja FHIR standardin [1] FHIR Specification (v4.0.1: R4 - STU) https://www.hl7.org/fhir/valueset-signature-type.html mukaisesti.
    - "system" : "urn:iso-astm:E1762-95:2013", allekirjoitettaessa Kanta FHIR-transaktiota
    - "code" : "1.2.840.10065.1.12.1.13", palvelimen allekirjoitettaessa Kanta FHIR-transaktiota järjestelmäallekirjoitusvarmenteella
    - "display" : "Review Signature", palvelimen allekirjoitettaessa Kanta FHIR-transaktiota järjestelmäallekirjoitusvarmenteella
- when = Ajankohta allekirjoituksen luonnille UTC-formaatissa.
- who = Allekirjoituksen luojan tunniste.

- targetFormat = Allekirjoitettujen resurssien tekninen formaatti. Tämän täytyy olla aina **application/fhir+json**.
- sigFormat = Allekirjoituksen tekninen formaatti. Tämän täytyy olla aina **application/jose**.
- data = JWS allekirjoitus. BASE64-enkoodattuna.

```
"signature" : {
  "type" : [{
    "system" : "urn:iso-astm:E1762-95:2013",
    "code" : "1.2.840.10065.1.12.1.13",
    "display" : "Review Signature"
  }],
  "when" : "2022-02-08T10:16:32.000+10:00",
  "who": {
      "identifier" : {
           "system" : "urn:ietf:rfc:3986",
           "value" : "urn:oid:1.2.246.xxxx.yyyy.10"
    },
    "display" : "Organisaation nimi"
  },
  "targetFormat" : "application/fhir+json",
  "sigFormat" : "application/jose",
  "data" : "UEQ5NGJXd2dkbVZ5YzJsdmJqMGlNUzR3SWlCbGJt
TnZaR2x1WnowaVZWUkdMVGdpLi4xY21VK0Nqd3ZSVzUyWld4dmNHVStJQT09"
}
```

Esimerkki 2: Esimerkki Signature-objektista, joka sisältää JWS-allekirjoituksen

2.2 FHIR-resurssin allekirjoittaja who-rakenteessa

Bundlen allekirjoittaja ilmaistaan who-kentässä viittauksella käyttäen loogista viittausta ja display-arvoa. Allekirjoitus tehdään liittyjäorganisaation järjestelmäallekirjoitusvarmenteella. Jos allekirjoituksen tekee muu taho kuin liittyjäorganisaatio, annetaan tiedoissa allekirjoittavan vastuuorganisaation (Kanta-välittäjä) tunniste.

```
"who": {
      "identifier" : {
           "system" : "urn:ietf:rfc:3986",
           "value" : "urn:oid:1.2.246.xxxx.yyyy.10"
    },
    "display" : "Organisaation nimi"
}
```

3 Sähköisen allekirjoituksen vaatimukset Kanta-palveluissa

3.1 Sähköisiä allekirjoituksia koskevat sitovat vaatimukset

[1] FHIR Specification (v4.0.1: R4 - STU) 2.24.0.17 Signature mukaiset vaatimukset digitaalisille allekirjoituksille:

1. FHIR bundlen Signature.data -kentän arvo on base64 enkoodattu JWS-allekirjoitus [5] IETF RFC 7515 (May 2015)
2. Allekirjoitus on irrallinen (allekirjoitus on irrallaan itse allekirjoitettavasta sisällöstä)
3. Kun FHIR resurssi on allekirjoitettu, allekirjoitus on tehty resurssin kanonikalisessa JSON-muodossa. Kanonikalisointivaatimukset on esitetty luvussa 4.4.
4. Allekirjoituksen pitäisi käyttää minimissään tiivistealgoritmia SHA256. Allekirjoituksen vahvistuskäytäntö koskee allekirjoitusta ja määrittää hyväksyttävyyden.
5. Allekirjoitus täytyy sisältää "srCms signer commitments" -objektin allekirjoituksen "tarkoitusta" varten. Tarkoitus voi olla todistettu toiminto tai allekirjoitukseen liittyvä rooli. Arvon tulee olla standardista ASTM E1762-95(2013). srCms-objekti sisältää samat tiedot rakenteessaan kun Signature.type -objekti.
6. FHIR määrityksen suosituksesta poiketen Kanta-palveluissa allekirjoituksena käytetään JAdES-B-B -profiilia tarkennettuna tässä määrittelyssä kuvatuilla tavoilla.

Vaatimukset allekirjoituksen tarkistamiselle [1] (FHIR Specification (v4.0.1: R4 - STU) 2.1.28.0.18.2 JSON Signature rules):

1. Tarkastaa, että digitaalisesti allekirjoitettu tieto on eheä JWS-allekirjoituksen avulla
2. Vahvistaa, että allekirjoittajan varmenne on tunnistettu, voimassa ja sopii allekirjoituksen tarkoitukseen
3. Vahvistaa, että allekirjoitettava sisältö on muokkaamaton

Allekirjoitusten kanonikalisointi vaatimukset [1] (FHIR Specification (v4.0.1: R4 - STU) 2.1.6.4.5 Canonical JSON):

Allekirjoitettava sisältö (payload) kanonikalisoidaan luvun 4.4 Allekirjoitettavan tiedon kanonikalisointi mukaisesti.

3.1.1 Käytetyt tiivistealgoritmit

Liikenne- ja viestintävirasto Traficomin/Kyberturvallisuuskeskuksen ohje [7] (Kyberturvallisuuskeskus Kryptograafiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen) sisältää kryptografiset vähimmäisvaatimukset turvallisuusluokitellun tiedon

suojaamiseen. Ohje määrittelee digitaalisia allekirjoituksia varten eri suojaustasoilla käytettävät tiivistealgoritmit.

JAdES standardi [3] (ETSI TS 119 182-1 V1.2.1 (2024-07): Electronic Signatures and Infrastructures (ESI)) määrittelee myös allekirjoituksiin käytettävät kryptografiset tiivistealgoritmit kohdassa Annex E (normative): Digest algorithms identifiers for JAdES signatures. JAdES standardin mukaan kryptografiset vahvuusvaatimukset voidaan korvata kansallisilla vaatimuksilla.

FHIR resurssien allekirjoituksissa täytyy käyttää tiivisteiden laskemisessa ohjeen [7] (Kyberturvallisuuskeskus Kryptograafiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen) mukaisia, kansalliset määräykset turvallisuustasolla IV täyttäviä, tiivistealgoritmeja.

Kanta-palveluiden FHIR-allekirjoituksissa täytyy käyttää alla olevassa taulukossa listattua tiivistealgoritmia:

Algoritmi	Tarkenne/Kuvaus
SHA-2: SHA-256	Minimivaatimus Kansallinen turvallisuusluokka/kryptovahvuus TL IV. Tiiviste-funktio, käyttötarkoitus digitaaliset allekirjoitukset ja "hash-only" -sovellukset. Toteutusten **TÄYTYY** tukea tiivistealgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea tiivistealgoritmia allekirjoitusten tarkastamisessa.
SHA-2: SHA-384	Tiivistefunktio, käyttötarkoitus digitaaliset allekirjoitukset ja "hash-only" -sovellukset. Toteutusten **TÄYTYY** tukea tiivistealgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea tiivistealgoritmia allekirjoitusten tarkastamisessa.
SHA-2: SHA-512	Tiivistefunktio, käyttötarkoitus digitaaliset allekirjoitukset ja "hash-only" -sovellukset. Toteutusten **TÄYTYY** tukea tiivistealgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea tiivistealgoritmia allekirjoitusten tarkastamisessa.

Taulukko 2: käytettävät tiivistealgoritmit

3.1.2 Allekirjoitusalgoritmit ja menetelmät

Liikenne- ja viestintävirasto Traficomin/Kyberturvallisuuskeskuksen ohje [7] (Kyberturvallisuuskeskus Kryptograafiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen) sisältää kryptografiset vähimmäisvaatimukset turvallisuusluokitellun tiedon suojaamiseen. Ohje määrittelee digitaalisia allekirjoituksia varten eri suojaustasoilla käytettävät allekirjoitusalgoritmit.

JAdES standardi [3] (ETSI TS 119 182-1 V1.2.1 (2024-07): Electronic Signatures and Infrastructures (ESI)) määrittelee, että digitaalisten allekirjoitusten luomiseen ja täydentämiseen käytettävien algoritmit ja avainten pituudet tulee olla standardin [11] (ETSI TS 119 312 V1.2.1 (2017-05)) mukaisia. Lisäksi JAdES standardin mukaan [11] (ETSI TS 119 312 V1.2.1 (2017-05)) standardissa määritellyt kryptografiset vahvuusvaatimukset voidaan korvata kansallisilla vaatimuksilla.

FHIR resurssien allekirjoituksissa täytyy käyttää ohjeen [7] (Kyberturvallisuuskeskus Kryptograafiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen) ja Digi- ja väestötietovirasto (DVV) [8] (DVV Palveluvarmenteet sosiaali- ja terveydenhuollolle) -ohjeen mukaisia ja tuettuja SOTE-varmenteita.

Kanta-palveluiden FHIR-allekirjoituksissa täytyy käyttää alla olevassa taulukossa listattua allekirjoitusalgoritmia:

Algoritmi (Äärellisen kunnan koko)	**Tarkenne/Kuvaus**
ECDSA[256]	**Minimivaatimus** Kansallinen turvallisuusluokka/kryptovahvuus TL IV Elliptic Curve Digital Signature Algorithm, allekirjoitus epäsymmetrisellä menetelmällä (esim. RSA) - "vaativat allekirjoitukset" Tuettu algoritmi ECDSA ES256 (EC P-256 DSA with SHA-256) Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tarkastamisessa.
ECDSA[384]	Elliptic Curve Digital Signature Algorithm, allekirjoitus epäsymmetrisellä menetelmällä (esim. RSA) - "vaativat allekirjoitukset" Tuettu algoritmi ECDSA ES384 (EC P-384 DSA with SHA-384) Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tarkastamisessa.

RSA[3072]	**Minimivaatimus** Kansallinen turvallisuusluokka/kryptovahvuus TL IV Allekirjoitus epäsymmetrisellä menetelmällä (esim. RSA) - "vaativat allekirjoitukset" Tuettu algoritmi RS256, RS384 ja RS512 (RSASSA-PKCS1-v1_5) Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tarkastamisessa.
RSA[4096]	Allekirjoitus epäsymmetrisellä menetelmällä (esim. RSA) - "vaativat allekirjoitukset" Tuettu algoritmi RS256, RS384 ja RS512 (RSASSA-PKCS1-v1_5) Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tuottamiseen. Toteutusten **TÄYTYY** tukea allekirjoitusalgoritmia allekirjoitusten tarkastamisessa.

Taulukko 3: Allekirjoitusalgoritmit

4 JWS allekirjoitus

4.1 JWS allekirjoitus

JSON Web Signature (JWS) on IETF:n ehdottama standardi (RFC 7515) kaikenlaisen tiedon allekirjoittamiseen. HL7 FHIR standardi suosittelee JWS signaturen käyttöä FHIR resurssien digitaalisiin allekirjoituksiin.

HL7 FHIR allekirjoituksissa JWS on JSON compact serialization -muodossa, joka sisältää seuraavat osat, mutta ei hyötykuormaa:

- Otsikko (Header), joka sisältää arvon BASE64URL(UTF8(JWS Protected Header))
- ”..” Tyhjällä merkkijonolla korvattu data-osio erotetaan pisteillä otsikosta ja allekirjoituksesta
- Allekirjoitus (Signature), joka sisältää arvon BASE64URL(JWS Signature)

JWS otsikko (JWS Protected Header) sisältää JSON otsikkoparametreja, jotka ilmaisevat allekirjoitukseen käytetyt parametrit ja tiedot allekirjoitettavasta sisällöstä ja/tai sisällöstä muodostetut tiivisteet.

JWS-otsikko, tyhjällä merkkijonolla korvattu data-osio ja allekirjoitus ketjutettuna järjestyksessä pisteillä ('.') osien välissä tuottaa serialisoidun JWS irroitetun (detached) allekirjoituksen.

HL7 FHIR allekirjoituksissa JWS hyötykuormaa (payload) ei sisällytetä serialisoituun esitys- ja tallennusmuotoon.

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9..dBjftJeZ4CVPmB92K27uhbUJU1p1r_wW1gFWFOEjXk
```

Taulukko 4: esimerkki JWS-allekirjoituksesta

4.2 FHIR Bundlen allekirjoitus

Kanta-palveluissa FHIR-resurssit allekirjoitetaan allekirjoittamalla Bundle, jossa ne siirretään ja tallennetaan.

JWS:n otsikon täytyy sisältää alg, iat, typ, b64, crit, x5c, sigD, srCms ja version otsikkoparametrit.

SigD otsikkoparametri on JSON-objekti, jonka täytyy sisältää mId, pars ja ctys -kentät.

srCms otsikkoparametri on JSON-objekti, jonka täytyy sisältää commId ja commQuals - kentät. FHIR spesifikaation [1] FHIR Specification (v4.0.1: R4 - STU) mukaan allekirjoituksen täytyy sisältää srCms-kenttä.

version otsikkoparametri sisältää Kanta FHIR sähköinen allekirjoituksen versionumeron, esimerkiksi ”kanta-fhir-1.0”.

```
// BASE64URL(UTF8(JWS Protected Header))
{
  "alg": "<Allekirjoitusalgoritmi esim. RS256, RS384, RS512, ECDSA P-256 tai EC-
DSA P-384>",
  ”iat”: ”<RFC7519:n mukainen aikaleima [NumericDate]>”,
  "typ": "<JOSE, jos JWS or JSON signature>",
  // b64 on true, kun mId = ObjectIdByURI
  "b64": true,
  // crit parametrissa tulee olla kaikki JWS/JAdES allekirjoituksen parametrit
  "crit": [{"alg",”iat”,"b64","typ","x5c","sigD","srCms",”version”}],
  "x5c": [
     "<DER-muotoisen X.509 varmenteen BASE64 arvo>"
  ],
  "srCms": [
    {
      "commId": "<oId yksilöi allekirjoittajan tekemän sitoumuksen>",
      "commQuals": ["<sitoumusta koskevat lisätiedot. Taulukko objekteja>"],
    }
  ],
  "sigD": {
      // Jos mId = http://uri.etsi.org/19182/ObjectIdByURI, HashM ja HashV ei
tule headeriin; pars sisältää viittauksen allekirjoituksen kohteeseen, tässä
vaiheessa Bundle-viittaus (/Bundle); ctys sisältää payloadin sisältötyyppin
(content type)
      "mId": "<URI identifioi hyötykuormaan viittauksiin käytetyn mekanismin>",
      ”pars”: [”<URI allekirjoituksen kohteeseen>”],
      "ctys": ["<Hyötykuorman sisältötyyppi (content type)>"]
  },
```

```
  ”version”: ”<Kanta FHIR sähköinen allekirjoituksen versionumero, esim. ”kanta-fhir-1.0”>”
}
.
// BASE64URL(payload)
{
  "<Hyötykuorma (payload)>”
}
.
// BASE64URL(JWS signature)
{
 "Allekirjoitus"
}
```

Yllä on esitelty JWS:n rakenne, kun allekirjoitus kohdistuu Bundle-resurssiin.

4.3 Allekirjoituksen kohdistaminen

FHIR allekirjoitus kohdistetaan koko Bundle-resurssiin, jossa Signature-objekti sijaitsee.

JAdES standardin [3] (ETSI TS 119 182-1 V1.2.1 (2024-04) 5.2.8.3.1 General requirements) -lauseke määrittelee mekanismit (mechanism Id), jotka käyttävät URI:ita viitattaessa JWS-hyötykuormaan.

FHIR Bundle-resurssin allekirjoitukseen käytetään mekanismia "http://uri.etsi.org/19182/ObjectIdByURI" (sigD-objektin mId-kenttä). Allekirjoitettava bundle on aina JWS hyötykuormassa (payload) ja sigD-objektin pars-taulukon elementissä viitataan FHIR Bundle-resurssiin ”/Bundle”.

4.4 Allekirjoitettavan tiedon kanonikalisointi

JSON-kanonikalisointi eli JCS (JSON Canonicalization Scheme) on menetelmä, joka varmistaa yksiselitteisen esityksen JSON-rakenteelle. JCS määrittelee säännöt, joiden avulla JSON sarjallistetaan, ja sen avulla voidaan taata, että JSON on standardoitu ennen tiivisteen tai allekirjoituksen luomista. Tässä dokumentissa viitataan IETF JSON Canoncalization Scheme-standardiin.

JSON kanonikalisointivaatimukset on määritelty RFC 8785 JSON Canonicalization Scheme (JCS) [8] -dokumentissa. Allekirjoitettavien JSON-muotoisten FHIR resurssien kanonikalisointiin täytyy käyttää IETF RFC 8785 JSON Canonicalization Scheme (JCS) [9] mukaista toteutusta.

JCS [8] (Luku 3.2) kanonikalisointisäännöstö:

1. JSON-kenttien osien väliin ei saa jättää välilyöntejä.

2. Alkeistyyppien sarjallistus: Joidenkin alkeistyyppien arvot voivat muuttua, kun ne sarjallistetaan ES6-standardin mukaisesti.

- Literaalit: JSON literaalit "null", "true" ja "false" eivät muutu sarjallistamisen johdosta.
- Merkkijonot: Jos jokin merkki kuuluu ASCII-merkkialueeseen (U+0000 - U+001F), se on sarjallistettava käyttäen pientä heksadesimaalista Unicode-merkintää (\uhhhh). Tähän on poikkeuksena valmiiksi määritellyt JSON-ohjausmerkit U+0008, U+0009, U+000A, U+000C tai U+000D, jotka täytyy sarjallistaa vastaavasti \b, \t, \n \f ja \r. Jos merkki ei kuulu ASCII-merkkialueeseen, se täytyy sarjallistaa sellaisenaan. Lisäksi merkit U+005C tai U+0022 täytyy sarjallistaa vastaavasti \\ ja \". Lisäksi, tuloksena olevan Unicode-koodipisteiden sekvenssin täytyy olla ympäröity kaksinkertaisilla lainausmerkeillä (").
- Kokonaisluvut: RFC-standardin mukaan kokonaisluvut täytyy serialisoida ECMA-262 spesifikaation kohdan 7.1.12.1 mukaisesti [12]. RFC-standardi suosittelee sarjallistuksen esimerkki-implementaationa RYU, jolla on tehty JCS open-source Java implementaatio.

3. Kanonikalisen JSONin vaatimuksiin kuuluu, että JSON-objektin kentät ovat aakkosjärjestyksessä. Aakkosjärjestykseen kuuluu seuraavat säännöt

- JSON-objektin kentät täytyy järjestää rekursiivisesti. Tämä tarkoittaa sitä, että myös JSON-lapsiobjektien kentät täytyy järjestää.
- JSON-taulukon elementtien järjestystä ei saa muuttaa.
- Kun JSON-objektin kentät järjestetään, täytyy noudattaa seuraavia sääntöjä:
  - Järjestysprosessi koskee merkkijonoja niiden "raakana" muotona. Esimerkiksi rivinvaihtomerkkiä \n kohdellaan merkkinä U+000A.
  - Järjestettävät JSON-objektit formatoidaan taulukkoina UTF-16 mukaan. UTF-16 arvot järjestetään suoraan kokonaislukuina riippumatta kieliasetuksista.
  - JSON-objektin kentät järjestetään nimien mukaan nousevaan aakkosjärjestykseen seuraavasti: "", "a", "aa", "ab"..

4. UTF-8 Koodaus: Jotta voidaan varmistua alustariippumattomasta esityksestä, JSON-data täytyy koodata UTF-8 muotoon.

Huom. RFC 8785 [8] standardissa kohdassa 3.2.3 on esitetty esimerkki, jonka mukaisesti kanonikalisoinnin tulee toimia.

Kanonikalisointi voidaan suorittaa ulkoisella kanonikalisointiohjelmistolla tai -kirjastolla:

1. Luo allekirjoitettava JSON.

2. Käytä kanonikalisointiohjelmistoa järjestämään ja muuntamaan data kanonikalisoituun muotoon.
3. Allekirjoita kanonikalisoitu JSON.
4. Lisää tuloksena oleva allekirjoitusarvon alkuperäiseen JSON-resurssiin sille määritettyyn rakenteeseen.
5. Järjestä valmis JSON käyttäen työkalua.

Yhteensopiva allekirjoituksen varmistusjärjestelmä:

1. Käsittelee ja parsii allekirjoitetun JSON resurssin käyttäen JSON työkalua.
2. Lukee annetusta rakenteesta allekirjoituksen.
3. Poistaa allekirjoituksen käsitellystä JSONista.
4. Järjestää jäljellä olevat JSONin kentät käyttäen JSON-työkalua.
5. Antaa ulkopuolisen kanonikalisointiohjelmiston järjestää ja palauttaa tietoa.
6. Varmistaa, että kanonikalisoidut tiedot vastaavat tallennettua allekirjoitusta käyttämällä allekirjoituksen luomiseen käytettyä algoritmia ja yksilöityä varmenteesta löytyvää avainta.

4.5 JWS otsikon (headerin) otsikkoparametrit

JWS, FHIR ja JAdES spesifikaatiot sisältävät vaatimuksia JWS-otsikon otsikkoparametreille. FHIR pakollisia JWS-otsikon otsikkoparametreja ovat alg, iat, typ ja x5c.

JAdES standardin [3] ETSI TS 119 182-1 V1.2.1 (2024-07) mukaisesti Kanta-allekirjoitusten tapauksessa (JAdES-B-B) pakollisia ovat myös sigD, b64, crit ja srCms -otsikkoparametrit.

Kanta laajennuksena pakolliseksi määritellään myös version -otsikkoparametri.

JSON Web Token (JWT) spesifikaation [5] IETF RFC 7519, mukaisia otsikkoparametreja esim. issuer, exp ja aud voi lisätä JWS otsikkoon, mutta ne eivät ole pakollisia JAdES ja FHIR spesifikaatioissa, joten niitä ei käytetä.

4.5.1 alg

alg (algoritmi) otsikkoparametri identifioi JWS:n suojaamiseen käytetty allekirjoitusalgoritmin. Kanta HL7 FHIR allekirjoituksissa käytettävät algoritmit ovat tämän dokumentin luvussa 3.1.2 . alg-otsikkoparametrilla on oltava IETF RFC 7515:n [5] kohdassa 4.1.1 määritetty muoto ja arvo. Tämä otsikkoparametri on pakollinen.

4.5.2 iat

iat (allekirjoitusaika) otsikkoparametri määrittää JWS:n luontiajan RFC7519:n mukaisen aikaleiman [NumericDate]. iat määrittää ajan sekunteina ajanhetkestä 1970-01-01T00:00:00Z UTC eteenpäin. Aika on IEEE Std 1003.1 mukainen (Unix epoch time).

4.5.3 typ

typ (tyyppi) otsikkoparametri määrittää JWS:n mediatyypin [IANA.MediaTypes]. typ otsikkoparametrin arvolla "jose" ilmaistaan, että tämä objekti on JWS, JWS Compact Serialization -muodossa. FHIR bundlen allekirjoituksessa typ parametrin arvo on ”jose”.

4.5.4 b64

b64 otsikkoparametri ilmaisee onko JWS hyötykuorma base64url enkoodattu tai enkoodamaton. b64 arvolla true, hyötykuorman täytyy olla base64url enkoodattu. b64-otsikkoparametrilla on oltava IETF RFC 7797 [14]:n lausekkeessa 3 määritelty muoto ja arvo. b64 -arvon täytyy olla true, jos mId -kentän arvo on "http://uri.etsi.org/19182/ObjectIdByURI".

FHIR bundlen allekirjoituksessa b64 otsikkoparametrin arvo on true.

4.5.5 crit

crit otsikkoparametri on JSON-taulukko, jossa pitää olla kaikkien FHIR-pakollisten ja Kanta-allekirjoituksessa käytettävien JAdES-allekirjoituksien otsikkoparametrien nimet, kuten alg, iat, typ ja x5c sekä sigD, b64, srCms ja version. crit-otsikkoparametrilla on oltava IETF RFC 7797 [14]:n lausekkeessa 4.1.11 määritelty muoto ja merkitys.

4.5.6 x5c

x5c (X.509 Certificate Chain) otsikkoparametri on JSON-taulukko, jonka ensimmäisen elementin tulee olla allekirjoitukseen käytetty varmenne. Jokainen taulukon elementti on base64-koodattu DER [ITU.X690.2008] PKIX-sertifikaatin arvo ([RFC4648]:n luku 4 – koodauksessa ei saa käyttää base64url-koodausta).

4.5.7 sigD

sigD otsikkoparametri on JSON-objekti, joka avulla viitataan yhteen tai useampaan hyötykuorma-tieto-objektiin. sigD määrittää miten viittaukset hyötykuorma-objekteihin käsitellään ja mekanismin edellä mainitujen vaatimuksen täyttämiseksi. sigD-kentän Mechanism Id (mId) arvolla 'http://uri.etsi.org/19182/ObjectIdByURI' pitää sisältää mId, pars ja ctys -kentät.

- mId - URI, joka identifioi käytettävän mekanismin, jota käytetään hyötykuorma-tietoobjekteihin viitattaessa ja niiden käsittelyssä hyötykuorman rakentamiseen.
- pars - JSON-taulukko, joka sisältää URI -viitauksen allekirjoitettavaan objektiin. FHIR bundlen allekirjoituksessa listassa on yksi arvo: ”/Bundle”.

- ctys - JSON-taulukko, jonka elementit sisältävät jokaisen hyötykuorma-tieto-objektien sisältötyypin, joihin pars-taulukon elementeissä viitataan. FHIR bundlen allekirjoituksessa hyötykuorman sisältötyyppi on ”text/json”.

4.5.8 srCms

srCms otsikkoparametri on JSON-objekti, joka määrittää allekirjoittajan allekirjoituksen yhteydessä tekemän sitoumuksen. Sitoumus voi olla määritelty osaksi allekirjoituspolitiikkaa tai se voi olla rekisteröity tyyppi. Ennalta määritettyjen sitoumustyyppitunnisteiden luettelo on ETSI TS 119 172-1 [i.7] määrittelyssä. srCms tietojen tulee vastata FHIR Signature -objektin type-kentän tietoja. FHIR spesifikaation [1] (FHIR Specification (v4.0.1: R4 - STU)) mukaan allekirjoituksen täytyy sisältää srCms otsikkoparametri.

- srCms on JSON-taulukko, joka sisältää JSON-kenttiä:
- commId - OId-tyyppinen tieto, jonka arvona täytyy olla URI, joka yksilöi allekirjoittajan tekemän sitoumuksen. "commId": "1.2.840.10065.1.12.1.13".
- commQuals - Taulukko sitoumusta koskevista lisätiedoista (objekteja).
  - "system": "urn:iso-astm:E1762-95:2013"
  - "display": "Review Signature "

4.5.9 version

version otsikkoparametri on KANTA-spesifinen lisäys JWS-allekirjoituksen versioimiseen. Versioinnin seurantaa tarvitaan, koska FHIR-allekirjoitus ja JAdES -standardit ovat vielä muuttumassa. version otsikkoparametri määrittää minkä Kanta FHIR sähköinen allekirjoitus -määrityksen mukaista mekanismia allekirjoitusten luonnissa ja tarkistuksessa tulee käyttää.

KANTA FHIR sähköinen allekirjoitus -teknisen määritysdokumentin versio	**JWS-allekirjoituksen version otsikkoparametrin arvo**	**Määrittely voimassa (alkaa – päättyy)**
1.2.0 (30.1.2025)	”version” : ”kanta-fhir-1.0”	30.1.2025 – toistaiseksi voimassa

5 Allekirjoituksessa käytetyt prosessit (normatiivinen)

5.1 Allekirjoituksen muodostaminen

Yhden FHIR bundlen allekirjoituksen muodostaminen (ObjectIdByURI -menetelmä)

1. Valmistele JWS otsikko
2. Poista FHIR bundlen Signature-objekti allekirjoitettavasta bundlesta
3. Kanonikalisoi allekirjoitettava bundle vaatimusten mukaisella JSON kanonikalisointiohjelmalla
4. Base64url enkoodaa kanonikalisoitu bundle (hyötykuorma) vaatimusten mukaisella base64UrlEncode-ohjelmalla
5. Kanonikalisoi JWS otsikko vaatimusten mukaisella JSON kanonikalisointiohjelmalla
6. Base64url enkoodaa kanonikalisoitu JWS otsikko vaatimusten mukaisella base64UrlEncode-ohjelmalla
7. Luo allekirjoitus yksityisellä avaimella ja vaatimusten mukaisella allekirjoitusalgoritmilla
8. Luo irroitettu (detached) allekirjoitus poistamalla hyötykuorma JWS:stä
9. Lisää irroitettu (detached) allekirjoitus alkuperäisen FHIR bundlen Signature.data -kenttään base64-enkoodattuna FHIR-määrittelyn mukaisesti
10. Lisää Signature-objekti takaisin bundleen

5.2 Allekirjoituksen tarkastaminen

Allekirjoitus tarkistetaan seuraavasti:

Bundlen allekirjoituksen tarkistus (ObjectIdByURI -menetelmä)

1. Pura Base64-enkoodattu JWS allekirjoitus tarkistettavan resurssin Signature.data -kentästä
2. Poista Signature-objekti tarkistettavasta resurssista
3. Kanonikalisoi tarkistettava nykyinen bundle vaatimusten mukaisella JSON kanonikalisointiohjelmalla (IETF JSON Canonicalization Scheme (JCS))
4. Base64url enkoodaa kanonikalisoitu bundle vaatimusten mukaisella base64UrlEncode-ohjelmalla
5. Muodosta tarkistettava JWS alkuperäisestä JWS-otsikosta, nykyisestä resurssista ja alkuperäisestä JWS:n allekirjoitusosasta

6. Pura tarkistukseen käytettävä varmenne ja sen julkinen avain JWS-otsikon x5c otsikkoparametrista
7. Tarkista JWS:n allekirjoitus varmenteen julkisella avaimella

Allekirjoituksen muut tarkistukset:

- Allekirjoitusalgoritmi (alg otsikkoparametri) on sallittu (luku 3 Sähköisen allekirjoituksen vaatimukset Kanta-palveluissa)
- typ parametrin arvo on ”jose”
- tarkista crit otsikkoparametrin parametrilistassa mainitut parametrit (alg, iat, b64, x5c, sigD, typ, srCms ja version) ovat JWS-otsikossa oikein
- tarkista version otsikkoparametrin arvo ja tee allekirjoituksen tarkistus version mukaisen määrityksen perusteella
- tarkista ,että x5c parametrin varmenne on hyväksytty ja varmenteen myöntäjä (Issuer) on luotettu DVV:n SOTE -varmenne
- tarkista, että sigD rakenne on oikein ja sisältää vaaditut parametrit vaaditussa muodossa
- Allekirjoitusvarmenteen (x5c otsikkoparametri) 'Validity Not Before' on vanhempi kuin allekirjoituksen aikaleima (iat otsikkoparametri)
- Allekirjoitusvarmenteen (x5c otsikkoparametri) 'Validity Not After' on myöhempi kuin allekirjoituksen aikaleima (iat otsikkoparametri)
- Allekirjoitusvarmennetta ei ole revokoitu

6 Esimerkit (ei normatiivisia)

6.1 FHIR bundle -resurssin allekirjoitus

6.1.1 JAdES JWS-allekirjoitus

```
// JAdES JWS Header
{
  "alg": "RS256",
  ”iat”: 1698068273000,
  "typ": "jose",
  "b64": true,
  "crit": [
    "b64",
    "alg",
    ”iat”,
    "typ",
    "x5c",
    "sigD",
    "srCms",
```

```
    "version"
  ],
  "x5c": [
    "MIIEtDCCApygAwIBAgIFHyPzaocwDQYJKoZIhvcNAQELBQAwgZsxCzAJBgNVBAYTAkl
FMRAwDgYDVQQIDAdLSUxEQVJFMGvnaV2c2UhFqIAo156r41Dnjng3qiZNc="
  ],
  "sigD": {
    "mId": "http://uri.etsi.org/19182/ObjectIdByURI",
    "pars": [
      "/Bundle"
    ]
    "ctys": [
      "text/json"
    ]
  },
  "srCms": [
    {
      "commId": "1.2.840.10065.1.12.1.13",
      "commQuals": [
       {"system":"urn:iso-astm:E1762-95:2013","display":"Review Signature"}
      ]
    }
  ]
  "version": "kanta-fhir-1.0"
}

// Payload
{
    "resourceType": "Bundle",
    "id": "ab71e831-3e8e-40c5-b005-cbbbf6f30423",
    "type": "collection",
    "entry": [
       ...
    ]
}


// Serialized Detached Signature
          BASE64URL(UTF8(JWS Header) || '..' || BASE64URL(JWS signature)
```

6.1.2 FHIR Signature -objekti

```
"signature" : {
    "type" : [{
      "system" : "urn:iso-astm:E1762-95:2013",
      "code" : "1.2.840.10065.1.12.1.13",
      "display" : "Review Signature"
    }],
    "when" : "2022-02-08T10:16:32.000+10:00",
    "who": {
      "identifier" : {
           "system" : "urn:ietf:rfc:3986",
           "value" : "urn:oid:1.2.246.xxxx.yyyy.10"
      },
      "display" : "Organisaation nimi"
    },
    "targetFormat" : "application/fhir+json",
```

```
    "sigFormat" : "application/jose",
    "data" : "UEQ5NGJXd2dkbVZ5YzJsdmJqMGlNUzR3SWlCbGJtTnZaR2x1WnowaVZWUkdMVGdp
Li4xY21VK0Nqd3ZSVzUyWld4dmNHVStJQT09"
}
```