# Saate CDA R2 -asiakirjojen sähköisen allekirjoituksen määritykselle ja soveltamisoppaalle

Kanta-palveluissa hyödynnettävän sähköisen allekirjoituksen määritys ja soveltamisopas on yhdistetty alkukesästä 2014 yhdeksi dokumentiksi. Samassa yhteydessä dokumentin sisältöä on päivitetty seuraavien asioiden osalta:

1. Ennen Kanta-arkistoon liittymistä syntyneiden asiakirjojen (”vanhat asiakirjat”) allekirjoittamisen periaate
2. SHA256-tiivistefunktion käyttöönotto varmenteissa
3. SHA256-tiivistefunktion käyttöönotto CDA R2 -asiakirjan sähköisessä allekirjoituksessa
4. Allekirjoituksen kohdistaminen CDA R2-asiakirjassa
   1. PDF-asiakirjat
   2. filter2-kohdistamisen tarkennukset
   3. XPath-kohdistamisen kieltäminen

Muutokset otetaan Kanta-palveluissa käyttöön siten, että:

* 1.2.2015 alkaen Kanta hyväksyy SHA256-tiivistefunktion käytön varmenteissa ja sähköisissä allekirjoituksissa kuitenkin siten, että myös SHA1-tiivistefunktiota (RSAwithSHA1) saa käyttää edelleen.
* viimeistään 31.12.2015 mennessä VRK ryhtyy tuottamaan varmenteet SHA256-tiivisteellä
* 1.2.2016 alkaen
  + Kanta ei enää hyväksy *uusissa asiakirjoissa* SHA1-allekirjoituksia[[1]](#footnote-1)
  + Kanta lakkaa tekemästä järjestelmäallekirjoituksia Kanta-arkistoon tallennettaviin asiakirjoihin[[2]](#footnote-2)
  + Kanta siirtyy tekemään Reseptikeskuksen järjestelmäallekirjoitukset käyttäen SHA256-tiivistefunktiota[[3]](#footnote-3)
  + XPath-kohdistamisen tuki poistuu

Kela tiedottaa myöhemmin tarkemmista aikatauluista, joiden puitteissa uudet piirteet ovat koestettavissa asiakastestausympäristöissä.

Näiden lisäksi sähköisen allekirjoituksen ID-kohdistamiseen liittyen julkaistiin keväällä 2014 tiedote. Tiedotteessa kuvattiin uusien Java-versioiden ja ID-pohjaisen allekirjoituksen kohdistamisen yhteentoimivusongelma ja kyseisen ongelman korjaustapoja. Mikäli kyseinen tiedote ei ole saavuttanut kaikkia allekirjoitustoteutuksia tekeviä tahoja, voi tiedotteen pyytää osoitteesta tekninentuki@kanta.fi.

1. Kanta hyväksyy SHA1-varmenteet niiden viimeiseen voimassaolopäivään saakka [↑](#footnote-ref-1)
2. Ennen Kanta-arkistoon liittymistä syntyneiden asiakirjojen osalta Kanta-arkisto ei tee järjestelmäallekirjoituksia missään vaiheessa [↑](#footnote-ref-2)
3. Apteekki- ja potilastietojärjestelmien pitää hyväksyä Kanta-järjestelmän tekemät SHA1-allekirjoitukset ko. reseptien elinkaaren loppuun saakka [↑](#footnote-ref-3)