

[Skip to Content \(Press Enter\)](#)

Uudised

Ülevaade: uus digidokumendi formaat BDOC ja selle eelised praeguse ees

13.11.2014

Nii nagu kogu tehnoloogia on pidevas muutumises, on ka digidokumendi formaadi muutumine osa normaalsest arengust. Kui soovime ajaga kaasas käia, peame uuendama digidoci krüptograafiat.

Selleks võetakse Eestis kasutusele uus digitaalallkirjastatud dokumendi formaat BDOC, mis hakkab asendama seni kasutusel olnud formaati DDOC.

Miks tuttav DDOC välja vahetatakse?

Selleks on mitmeid põhjuseid. Esiteks on oluline ühilduvus ülejäänud maailmaga. 2002. aastal kasutusele võetud DDOC oli toona mõeldud ennekõike kasutamiseks Eesti-siseselt.

See formaat on meid hästi ja veatult teeninud. Nüüd, tosin aastat hiljem, elame uues maailmas, kus seni kehtinud reeglid ja standardid tuleb üle vaadata. Nüüd soovime, et kõik Eestis antud allkirjad oleksid ka rahvusvaheliselt standardsed.

Teiseks ei toeta formaat DDOC kaasaegsemaid räsi- ja krüptoalgoritme. DDOC vastab kõikidele täna kehtivatele krüptograafiastandarditele, ent üleminek peab toimuma enne kui need aeguvad.

Kolmandaks võetakse 2015. aasta alguses kasutusele uue krüptograafiaga Mobiil-ID ja 2017. aastast ka uus ID-kaart. Et saaksime nendega digiallkirju anda, peab kasutusele võtma uue formaadi ehk BDOCi.

Miks on BDOC parem?

Lühidalt öeldes on BDOC nagu DDOC, ainult et veel parem ja turvalisem. BDOC formaadis failile saab anda allkirja kõikide seni välja antud ID-kaartidega ja nii olemaoleva kui ka uuest aastast väljastatava Mobiil-ID-ga.

Muudatus võrreldes DDOC-iga on näiteks see, et .bdoc-faili näol on tegemist ZIP-konteineriga, mis sisaldab allkirjastatud faile, allkirju ja juhtinfot ning mida saab põhimõtteliselt avada kõikide ZIP-formaati tundvate programmidega.

Kuna ZIP on kokku pakitud vorming, võivad BDOC failid olla võrreldes DDOC failidega (mis on XML tekstifailid) oluliselt väiksemad.

Lisaks on positiivne, et nii BDOC kui ZIP formaadis failide e-posti teel edastamine on paremini toetatud. (DDOC formaadis dokumentide e-postiga edastamisel on olnud probleeme, sest osa meiliserveritest filtreeris DDOC formaadis e-kirja manused välja.)

Mis muutub?

- Alates 2015. aastast on DigiDoc3 klient rakenduses vaikimisi loodav digiallkirjastamise

formaad BDOC. DigiDoc Portaalis on juba alates käesoleva aasta juunist vaikimisi formaat BDOC.

- BDOC formaadis faile saab avada, allkirju verifitseerida ja allkirjastada DigiDoc3 klientrakendusega, mille versiooninumber on vähemalt 3.8.
- On oluline, et organisatsioonid ja nende infosüsteemid, mis inimestelt digiallkirjastatud dokumente vastu võtavad, sellega arvestaksid ja valmis oleksid.

Kui kasutate alati kõige uuemat ID-kaardi tarkvara, siis ei ole muretsemiseks põhjust.

Arvutis oleva ID-kaardi tarkvara versiooninumbrit saate kontrollida nii, et avate DigiDoc3 kliendi, vajutate nuppu Info ja avanemas aknas kuvataksegi versiooninumber. Kui see on madalam kui 3.8, tuleb tarkvara uuendada. Seda saab teha aadressil www.id.ee.

Küsimuste ja probleemide korral on soovitatav kõigepealt uuendada oma ID-kaardi tarkvara ning seejärel võtta ühendust Sertifitseerimiskeskuse ööpäevaringse abiliiniga numbril 1777.

Kokkuvõtteks

Uues formaadis on tehtud tehnilised uuendused, mis on vajalikud parima turvalisuse tagamiseks ning kasutusmugavuse tõstmiseks.

- Seni kasutusel olnud formaadi faililaiend oli .ddoc. Uue formaadi puhul on faililaiend .bdoc.
- BDOC konteineri formaat on ZIP. Senise DDOC konteineri formaat oli XML.
- Kuna ZIP on kokku pakitud vorming, võivad BDOC failid olla võrreldes DDOC failidega (mis on XML tekstifailid) oluliselt väiksemad. See muudab failide töötlemise kiiremaks.
- Allkirja formaat on endiselt XAdES, kuid BDOC kasutab XAdES versiooni 1.4.2 senise 1.2.2 asemel ja konteinervormingu puhul on kasutusel ASiC baasprofiil
- Toetatud räsi- ja krüptoalgoritmide hulk suureneb.

Allikas: [Forte](#)

KÜSI ABI

Kui sa ei leidnud oma küsimusele vastust, kirjuta meie meeskonnale.

- **Nimi**
- **E-post**
- **Teema**
- **Sisu**

- **Laadi ekraanipilt või diagnostika fail**
[Vaata juhendit](#)

Ühtegi faili ei ole valitudVali fail(id)

•

- **Hinda oma arvutikasutusoskust, et saaksime anda paremaid juhiseid**

☐ vähene ☐ keskmine ☐ hea

- Vigane kontrollsõna

KontrollsõnaLoo uus kontrollsõna

Kuidas saame artiklit parandada, et sellest rohkem abi oleks?

Saada Sulge