RIIGI INFOSÜSTEEMI AMET

e-Allkirjad Euroopas ja nende käsitlemine Eestis

Juhend ja nõuanded e-allkirjade käsitlemiseks

Versioon 1.3
(1606)

Mark Erlich

juuni 2016

Sisukord

Kokkuvõte

Käesolev juhis kirjeldab eIDAS määrusest tulenevaid kohustusi avalikule sektorile piiriüleste e-allkirjade (digitaalallkirjade) tunnustamiseks. Juhises selgitatakse erinevaid e-allkirjade tasemeid, standardeid ja vorme mida EL õigusruumis tuleb käsitleda.

Juhise eesmärk on anda ülevaade mh infosüsteemide halduritele võimalike tegevuste üle, loomaks võimekus teiste EL liikmesriikide e-allkirjade töötlemiseks.

Käesolevat juhist uuendatakse regulaarselt ning selle viimane versioon on leitav Riigi Infosüsteemi Ameti lehelt: https://www.ria.ee/ee/eid-info-ja-juhendid.html

Sissejuhatus

Kuna Eesti kontekstis eeldame enamasti, et e-allkiri on võrdväärne omakäelise allkirjaga (ehk Eesti õigusruumis „digitaalallkiri"), siis on ülimalt oluline, et oleks kasutusel lahendused, millega on võimalik lihtsal viisil tuvastada, kas tegemist on sellise e-allkirjaga või mitte. Käesolev dokument selgitab kuidas on võimalik sellist tuvastust teostada ning milliseid lahendusi on võimalik selleks kasutada. Kokkuvõtva tabeli tegevustest ja tähtaegadest leiab käesoleva dokumendi Lisa 1.

2016 aasta 1. juulist hakkab kehtima eIDAS[1] määruse nõue usaldusteenuste (sh e-allkirjade) piiriüleseks tunnustamiseks. eIDAS määrus (jõustus septembris 2014) on Euroopa Liidu määrus, mis on liikmesriikidele otsekohalduv. eIDAS määrusega seatud nõuded on kohustuslikud avalikule sektorile ja avaliku sektori avalikele teenustele.

Määruse kohaselt peavad liikmesriikide avaliku sektori asutused / teenuse osutajad aktsepteerima e-allkirju mis vastavad nende poolt määratud tasemele või sellest tugevamale tasemele. Eesti kontekstis tähendaks see seda, et kui asutus on ära määranud, et dokument / fail peab olema digitaalallkirjastatud (kvalifitseeritud e-allkirjaga) või allkiri peab vastama omakäelise allkirjaga võrdselt, siis ei pea asutus vastu võtma muid allkirju kui kvalifitseeritud e-allkirju.

Kokkuvõtvalt jagab eIDAS määrus e-allkirjad järgmistesse klassidesse:

- **Kvalifitseeritud e-allkirjad (kasutatakse ka akronüümi QES – qualified electronic signature):** on määruse/seaduse mõistes võrdsed omakäelise allkirjaga. Sellised allkirjad on täiustatud e-allkirjad (kirjeldus ülejärgmises punktis), mis põhinevad kvalifitseeritud sertifikaatidel (kvalifitseeritud sertifitseerimisteenuse osutaja poolt väljastatud) ja on antud kvalifitseeritud allkirjaandmise vahendiga (varasemalt tuntud kui turvaline allkirja andmise vahend). Kvalifitseeritud sertifikaat on kui garantii, et sertifikaadi väljastamisel tuvastati füüsilise isiku identiteet. Kvalifitseeritud allkirja andmise vahend on kui garantii, et allkirja loomiseks kasutatavad andmed (privaatvõti) on kindlalt allkirjastaja ainukontrolli all.
- **Täiustatud e-allkirjad kvalifitseeritud sertifikaatidega (kasutatakse ka akronüümi AdES/QC – advanced electronic signature with qualified certificates):** on täiustatud e-allkirjad, mis põhinevad küll kvalifitseeritud sertifikaadel, kuid ei kasutata kvalifitseeritud allkirja andmise

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

vahendit. See tähendab, et allkirjastamise andmed (privaatvõti) võib olla paigaldatud näiteks kasutaja arvutisse. Samas võib võti olla ka kiipkaardil, kuid seda vahendit ja selle loomist/jagamist pole auditeeritud ega sertifitseeritud (puudub garantii).

- **Täiustatud e-allkirjad (kasutatakse ka akronüümi AdES – advanced electronic signature): vastavad järgnevatele nõuetele:**
    1) Allkiri on seotud ainuüksi allakirjutajaga
    2) Allkirja abil on võimalik tuvastada allakirjutaja isikut
    3) Allkiri on loodud allkirjastamiseks vajalike andmetega, mille salastatuse kõrge tasemega tagatakse, et need on ainult allkirjastaja ainukontrolli all
    4) Allkiri on seotud allkirjastatud andmetega sellisel viisil, et hilisemad andmete muudatused on tuvastatavad.
- **Muud e-allkirjad:** on kõik ülejäänud lahendused, mis ei vasta ülaltoodud nõuetele. Sellisteks lahendusteks võivad olla näiteks teenusepõhised allkirjad (näiteks EchoSign – toetatud Adobe Acrobat Readeris) kui ka puutetundlikule ekraanile käega/pulgaga joonistatud allkiri.

eIDAS määruse rakendamiseks on loodud ka rakendusaktid, millest e-allkirju käsitlev rakendusakt[2] viitab selgelt ETSI (European Telecommunications Standards Institute) standarditele, millele vastavaid e-allkirju peavad Euroopa liikmesriigid olema võimelised käsitlema/menetlema. Standarditele mitte vastavate e-allkirjade puhul jääb nende menetlemise piiriülese võimekuse tagamine nende allkirjade looja riigile. Sisuliselt tähendab see seda, et kui allkirjad on standardsed, siis nende automaatne verifitseerimine/lahti võtmine peab olema võimalik igas riigis ja muude allkirjade puhul saavad liikmesriigid neid diskrimineerida.

Standardid ja nende realiseerimine praktikas

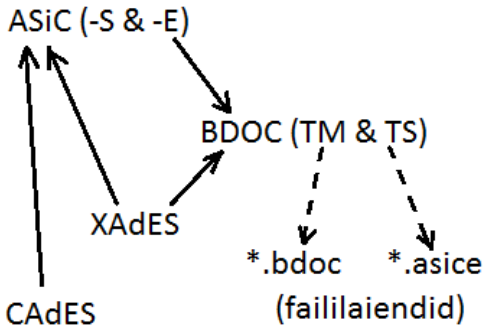
Standardid millele vastavaid e-allkirju peavad liikmesriigid olema võimelised käsitlema:

- XML Advanced Electronic Signature (XAdES) Baseline Profile – ETSI TS 103171 v.2.1.1[3]
- CMS Advanced Electronic Signature (CAdES) Baseline Profile – ETSI TS 103173 v.2.2.1[4]
- PDF Advanced Electronic Signature (PAdES) Baseline Profile – ETSI TS 103172 v.2.2.2[5]
- Associated Signature Container (ASiC) Baseline Profile – ETSI TS 103174 v.2.2.1[6]

Eestis kasutatakse BDOC[7] allkirjavorm põhineb ASiC konteineri ja XAdES allkirja standarditel (ASiC konteiner-failiformaat, mille sees on kasutatud XAdES (XML) allkirja). Allkirja andmise aja fikseerimiseks kasutatakse kolmanda osapoole aega, mille fikseerimiseks saab eelnimetatud standardite kohaselt kasutada kas ajamärgendit (TM – timemark) või ajatemplit (TS – timestamp). Ajatemplil on olemas oma standard mida kasutatakse maailmas laialdaselt. Ajamärgend on aga

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006
[3] http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
[4] http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
[5] http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf
[6] http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf
[7] http://www.id.ee/public/bdoc-spec212-est.pdf

rahvusvaheliselt defineerimata (sellel puudub rahvusvaheline standard või spetsifikatsioon). Kuna Eesti digitaalallkiri on vanem kui ajatempel, siis ajaloolistel põhjustel on tänaseni Eestis enimlevinud lahenduseks ajamärgend. See on Eesti enda „leiutatud“ lahendus, kus allkirjastatavad andmed seotakse sertifikaadi kehtivuspäringuga ning päringu vastuse kellaaega tõlgendatakse kui ajamärgendid. Selline lahendus on matemaatiliselt ja tehniliselt briljantne, kuid kuna muu maailm seda ei kasuta siis pole see suures plaanis jätkusuutlik. Selle tõttu on BDOC formaadis toetatud ka ajatempel. Kasutajatele vahe tegemise lihtsustamiseks muudeti 2015. aastast faililaiendeid vastavalt aja profiilile kas *.bdoc või *.asice (lõppkasutajale on see seadistatav Digidoc3 rakenduse seadetest).



Siiski tuleb mainida, et standardite kaasajastamine, et vastata ajakohastele nõuetele, on pidev protsess. Seega ka tänane lahendus muutub ajas. 2016. aasta aprilli lõpus valmisid eelnimetatud standardite kaasajastatud versioonid(http://www.etsi.org/technologies-clusters/technologies/security/digital-signature). Uutest versioonidest on ajamärgend (TM) eemaldatud. See tähendab omakorda, et tagada Eesti digitaalallkirja vastavust ETSI standarditele, tuleb meil tulevikus TM teenus viia võimalusel vastavusse TS teenuste nõuetele või eemaldada TM profiili tugi rakendustest millega luuakse digitaalallkirju. See ei tähenda nüüd kohest muudatust 2016 aastal, sest me peame järgima eIDAS määrust, mis viitab aga täna kehtivatele standarditele. Kindlasti aga saame rääkida uutele standarditele ülemineku kavast 2016 aasta II poolaastal, kui Euroopa Komisjon otsustab millal viiakse sisse uute standardite kohustus eIDAS määrusesse.

Sõltumata uutest ja vanadest standarditest on ülimalt oluline, et infosüsteemid ja e-teenused, kus kasutatakse digitaalallkirjastamist võtaksid ajatempli teenuse kasutusele esimesel võimalusel. Ainult nii saame garanteeritult tagada, et meie digitaalallkirjad on ka teistes riikides kasutusel olevates lahendustes verifitseeritavad.

Mis juhtub kui püüda verifitseerida Eesti ajamärgendiga digitaalallkirja mõnes teise riigi lahenduses? – Isegi kui teise riigi lahendus vastab eIDAS määrusele (toetab eelnimetatud standardeid), siis tõenäoliselt pole nende süsteem võimeline automaatselt verifitseerima Eesti ajamärgendi lahendust. Sellisel juhul ei suuda süsteem tuvastada allkirja andmise aja kinnitust ning juriidiliselt ei loeta allkirja võrdväärseks omakäelise allkirjaga. Antud juhul peab allkirja verifitseerimiseks teostama käsitsi toimingu, mis aga praktikas tõenäoliselt ei toimi (sest usaldatakse süsteemi).

Olulised tähelepanekud piiriüleste e-allkirjade puhul

Enamik Eestis kasutatavaid süsteeme on üles ehitatud eeldusel, et teenust osutatakse Eesti

kodanikule või residendile ning et andmed on kindla Eestile omase struktuuriga. Piiriüleste teenuste ja e-allkirjade puhul ei pruugi see nii olla. Nimelt on kõikidel riikidel oma isikukoodi süsteem ning nõuded isikuandmete kättesaadavusele. Sellest tulenevalt ei pruugi alati olla isiku nimi või isikukood koheselt sertifikaadist leitav. Lisaks võivad need andmed (nagu isikukood või muu identifikaator) tunduvalt erineda oma struktuurilt sellest mida me kasutame Eestis.

Ülimalt oluline on siinkohal aru saada milliseid andmeid loetakse e-allkirjast välja ning kasutatakse teenuses või menetlusprotsessis. Seega peab iga infosüsteemi haldur / teenuse omanik kaardistama ära nii menetlusprotsessid kui ka tehnilise võimekuse, et aru saada mida peab muutma.

Sisuliselt tähendab see menetlusprotsesside kirjeldust, kus kasutatakse e-allkirja andmeid nagu allkirjastaja, koht või isikukood (või isikukoodist tulenev sünniaeg). Neid protsesse on vaja täiendada nii, et need kataksid ka olukordi, kus neid andmeid pole võimalik üheselt kätte saada e-allkirja elementidest. Sellisel juhul võib see tähendada kas allkirjastatud dokumendi/faili käsitsi menetlemist (käsitsi avamist ja andmete välja lugemist dokumendi sisust ning käsitsi andmete sisestamist süsteemi) või menetlusvormide muudatust. Tehnilisest aspektist peab ka kontrollima üle, et kasutatavate andmeväljade pikkused ja formaadid (näiteks nõutud ainult numbrid) poleks kindlalt fikseeritud, sest nii isikukood kui ka muud andmed võivad olla pikemad või mõnes muus vabas vormis, kui see mida Eesti elanike puhul rakendatakse.

Kindlasti aga peaks iga menetluse/süsteemi ja e-teenuse haldur endale selgeks tegema kas iga toimingu juures on ilmtingimata allkirjastatud dokumenti vaja ning milleks nõutakse üldse allkirja. Kui tegemist on vaid veendumuses, et antud isik edastas faili või, et isik on olnud seotud toiminguga, siis piisaks ka ainult autentimisest (eeldades, et autentimist turvalogitakse – ehk toimingust jääb jälg maha). Juhul kui allkirja andnud isikuga teostatakse jätkutoiminguid füüsiliselt isikuga kohtudes (näiteks ülikoolide taotlused jms), siis kas ikka on vaja omakäelise allkirjaga võrdsed e-allkirja(?), sest isik saab oma tahet kinnitada füüsilise menetluse juures.

Tegevused EL allkirjade verifitseerimisvõimekuse saavutamiseks

Euroopa Komisjoni poolt on loodud üleeuroopaline e-allkirjade rakendus, tuntud ka kui DSS[8] rakendus. 2015. aasta lõpuks võttis Riigi Infosüsteemi Amet antud rakenduse kasutusele PDF allkirjade verifitseerimiseks. Niinimetatud PDF verifitseerimisteenus[9] on mõeldud teenuste ja rakenduste liidestamiseks[10], sealhulgas Digidoc3 kliendirakendusega. Kuigi tegemist on tehniliselt korrektselt toimiva lahendusega, siis siiski tuleb seda lugeda eksperimentaalseks, kuna teenusel puudub SLA ja seda pakutakse täna kui „*as is*“ teenust.

Riigi Infosüsteemi Ametis on käimas projekt SiVa (tuletatud sõnadest „signature validation“), mille eesmärk on luua digitaalallkirjade verifitseerimisteenuse raamistik. Tegemist on vabavara lahendusega, mida saab kasutada välise teenusena (masin-masin teenus) või paigaldada seda lokaalse teenusena asutuse või infosüsteemi siseselt. Teenuse algne skoop on oli verifitseerimis-võimekus ajaloolistele (kõik DDOC formaadi põlvkonnad) ja eksootilistele (näiteks x-tee ja PDF)

[8] https://joinup.ec.europa.eu/asset/sd-dss/description
[9] https://validator.eesti.ee/pdf-validator-webapp/wservice
[10] http://open-eid.github.io/pdf-validator/

digitaalallkirjadele. Projekti lõppfaasis oli planeeritud kolida eelnimetatud PDF verifitseerimisteenus arendatud raamistikule. SiVA projekti kavandatud lõpp jääb 2017. aasta 1.-sse kvartalisse.

Lisaks eelnimetatud projektile on Riigi Infosüsteemi Ametil kavas laiendada verifitseerimisvõimekus kõikidele eIDAS määruse poolt nimetatud standarditele vastavatele e-allkirjadele. Selleks integreeritakse DSS rakendus täielikult SiVa lahendusse ning ID-kaardi tarkvara (teegid ja klientrakendused) liidestatakse SiVa teenusega. Kuna SiVa lahendus valmib alles 2017. alguseks, siis täieulatuslik võimekus valmib alles 2017. 1.-sel poolaastal. Sellegi poolest on kavandatud võimalikult varajane teenuste avalikustamine (*proof-of-concept*, beeta test jne), mis jääb tõenäoliselt 2016. aasta viimasesse kvartalisse.

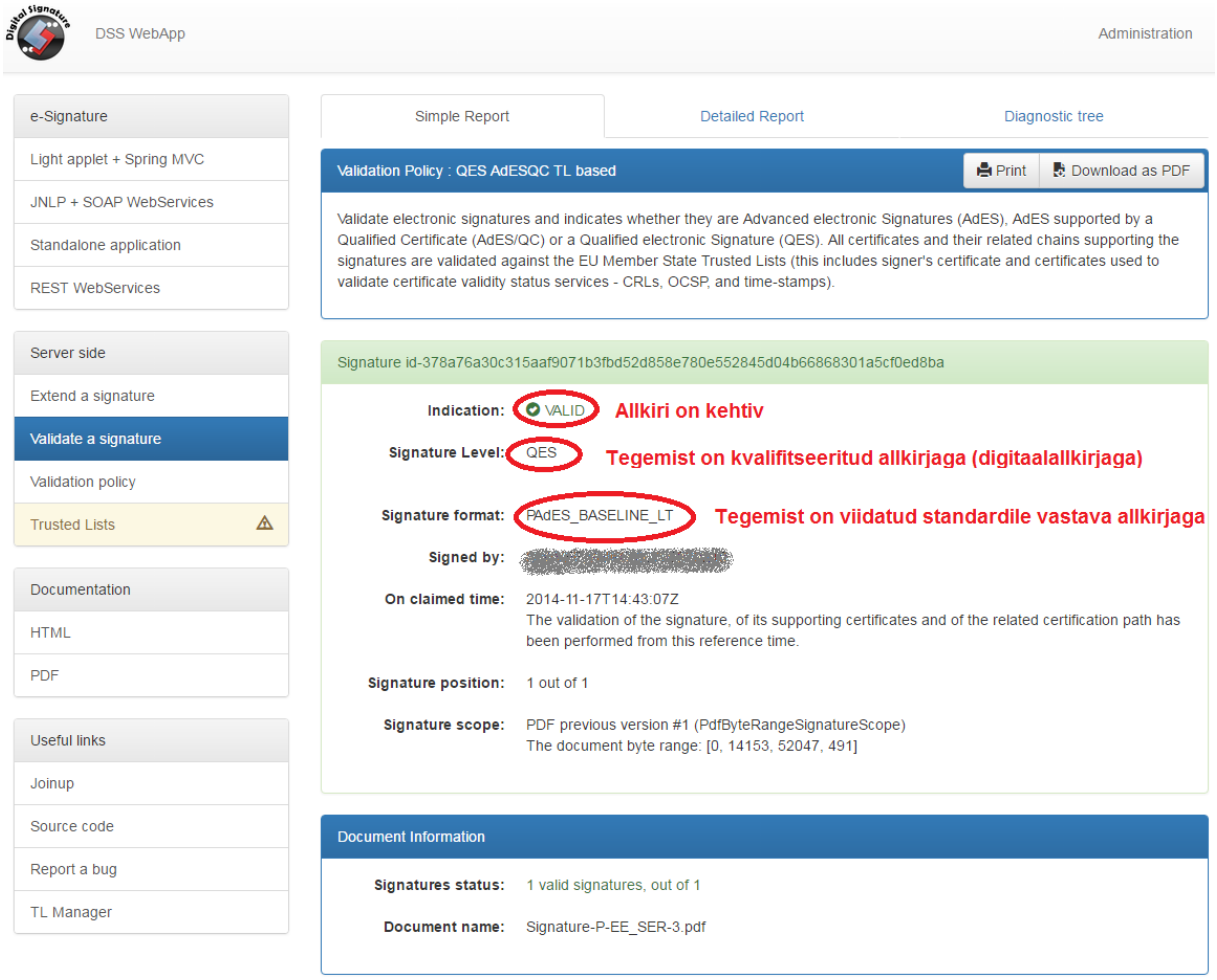
EL allkirjavormid ja nende tuvastusviisid

DSS rakendus

Nagu eelnevas peatükis kirjeldatud, on tegemist masin-masin teenuse rakendusega. Seega on selle kasutuselevõtt kindlasti sobilik infosüsteemidel kus on kõrge käideldavuse ja konfidentsiaalsuse nõue. DSS rakendus sisaldab kõiki vajalikke funktsionaalsusi allkirjade verifitseerimiseks vastu eIDAS nõudeid ja tasemeid. Siiski eeldab selle kasutuselevõtt ka mõningast seadistamist, et lõppkasutajal oleks lihtne tuvastada kas tegemist on kvalifitseeritud e-allkirjaga (omakäelisega võrdne allkiri) või ei ole.

DSS rakendus toetab kõiki eelnimetatud standarditele vastavaid e-allkirju ning nende profiile ja tasemeid. Lahendusega tutvumiseks on loodud demo-portaal[11], mis suudab tuvastada täiustatud e-allkirju (AdES standardite perele vastavad allkirjad) ning lisaks kas tegemist on kvalifitseeritud e-allkirjaga (QES, Eesti mõistes ka digitaalallkiri) või kvalifitseeritud sertifikaatidega täiustatud e-allkirjaga (AdES/QC). Siiski tuleb suhtuda sellistesse portaalidesse (näiteks ka Nowina[12] lahendus) reservatsiooniga, kuna lahendus ei ole tavakasutaja sõbralik ning võib anda allkirjast vääriti arusaamist. Näiteks vajab allkirja kehtivus ja vastavus omakäelisele allkirjale arusaamist tehnilistest terminoloogiatest, kas tegemist on korrektse QES allkirjaga (vaata allolevat joonist). Lisaks võib aga detailne info kuvada esmaselt kehtiva allkirja kohta hoiatusi puuduliku informatsiooni kohta, mille tõttu tegelikult ei peaks allkiri olema kehtiv QES allkiri või vastupidi hoiatustest sõltumata peaks allkirja juriidiliselt korrektseks tunnistama.

[11] https://joinup.ec.europa.eu/sd-dss/webapp-demo/validation
[12] http://dss.nowina.lu/validation



Joonis: kuva DSS rakenduse demolehelt, mis kuvab digitaalallkirja kehtivusinfot lihtsustatud kujul koos lisatud selgitustega

Digidoc3 klientrakendusse ning alusteekidesse on planeeritud eIDAS määrusele vastavate allkirjade verifitseerimise tugi läbi SiVa teenuse 2016. aasta lõpuks.

Adobe jm PDF rakendused

PDF lugeriga allkirjade kontrollimisel **ei tohi** usaldada dokumendil kuvatavat allkirja vormi. Tegemist on visuaalse elemendiga mis ei oma allkirja õigsuse kontrollimisel mingit sisu. Allkirjade kontrollimiseks tuleb avada signatuuri/allkirja detailvaade. Siiski on ka detailvaates PDF allkirjade kontrollimine mõneti problemaatiline, kuna kasutaja vaatest on raske vahet teha korrektsete ja ebakorrektsete allkirjade vahel, rääkimata juriidiliselt omakäelise allkirjaga võrdsete ja teiste allkirjade vahel. Iseenesest on rakendustes nagu Adobe Reader kõik vajalikud tehnilised valmidused olemas, küll aga pole selle seadistamine kasutajale jõukohane. Lisaks on Adobe rakendusel oma usaldusahel mis ei ühti Euroopa usaldusnimekirjadega. Ehk sisuliselt ei vasta rakendus eIDAS määrusele. Selline rakendus võib näidata ise tekitatud „võlts identiteediga“ allkirju kehtivatena ja samas korrektseid EL kodaniku allkirju kahtlastena/mitte kehtivatena.

Täiendavalt on maailmapraktikas kasutusjuhtusid kus allkirja loomisel selle õigsust ei kontrollita (ei võeta sertifikaadi kehtivuskinnitust, ei kontrollita usaldusahelat, ega kinnitata ajatempliga) vaid tehakse seda hiljem allkirjade valideerimisel. See aga tähendab, et rakendused teostavad mh sertifikaadi kehtivuse kontrollimist iga kord dokumendi avamisel. Selline lahendus näitab allkirja

kehtivana vaid sertifikaadi eluea jooksul – ehk hilisem (kui sertifikaat juba kehtivuse kaotanud) dokumendi avamine annab allkirja kohta mitte kehtiva teate.

Riigi Infosüsteemi Amet on loonud võtnud kasutusele pilootteenuse, millega saab kontrollida PDF formaadis allkirjade kehtivust. Teenus on liidestatud Digidoc3 kliendi rakendusega ning seadistatud nii, et kasutajale kuvataks kas tegemist on kehtiva digitaalallkirjaga (QES – omakäelise allkirjaga võrdne allkiri). Detailsem juhis on käesoleva dokumendi Lisa 2.

Eelkirjeldatud puudustest tulenevalt on soovitatav PDF allkirjade valideerimisel kasutada eIDAS võimekusega rakendust nagu DSS või Digidoc3 klient rakendust.

Lõppsõna

Kui seni me elasime suhteliselt suletud maailmas, milles valitsesime ise, siis tänaseks on maailm jõudnud meile järgi ja me oleme osa suurest ökosüsteemist. See tähendab, et meie senised saavutused ja murede lahendamine e-ühiskonnas oli suuresti meie enda teha, siis tänase seisuga peame seda tegema koos teiste Euroopa riikidega.

Eesti kindel eesmärk on olnud ja jätkuvalt on Eesti kodanikele tagada võimalikult mugav ja kiire teenindamine riigi poolt ning Euroopa kontekstis sõltumatult millise riigi poolt. Eesti riigis on meil selleks kasutusel nii ID-kaart kui ka e-teenused. Euroopa vaatest peame sellise ambitsiooni saavutamiseks tegema koostööd liikmesriikide vahel. See aga tähendab vastastikust e-allkirjade ja seonduvate teenuste tunnustamist. eIDAS määrus on sellise koosvõime loomiseks põhivundament, mis ühtlasi mitte ainult ei arenda Euroopa turgu sisemiselt vaid tugevdab Euroopa majandust maailmaturul.

Tegelik elu pole nii must-valge nagu pelgalt tunduda võib – me ei saa kindlalt väita, et üks või teine süsteem on loodud ainult Eesti elanikele ning selle pärast pole selles vaja tegeleda piiriüleste küsimustega nagu e-allkirjad. Tänane EL võimaldab nii tööjõu kui ka teenuste vaba liikumist, mis tähendab, et e-allkirjad mis on loodud mõne EL liikmesriigi lahendusega võivad tulla mõnelt Eestis resideerivalt EL kodanikult, kes kasutab enda koduriigi lahendust e-allkirjastamiseks. Seega saab öelda, et eIDAS määruse rakendumisest pole meil Eestis ainult „meie vahendiga“ e-Residendid vaid võivad olla ka e-Residendid kellel on mõne teise EL liikmesriigi „vahend“.

Teenuseid kus me tõesti saame välistada teiste EL liikmeriikide e-allkirju on ainult need, mis on mõeldud ainult Eesti kodakondsusega isikutele.

Täiendavate küsimuste puhul ja nõuande saamiseks palume pöörduda Riigi Infosüsteemi Ameti kasutajatoe poole: help@ria.ee

Lisa 1

Tegevuste ja teadaolevate tähtaegade tabel (täiendatakse jooksvalt):

Muutus /tegevus	Valmimise/jõustumise tähtaeg	Mõju
eIDAS usaldusteenuste piiriülene tunnustamine	2016-07-01	Digitaalallkirjade piiriülene tunnustamine kõikides avalikes teenustes
Verifitseerimisteenus (SiVa), mis suudab verifitseerida mh EL liimesriikides loodud digitaalallkirju	1.kv. 2017	Baastarkvara (sh digidoc teegid) toetavad liidest SiVa teenusega. Liidese loomine infosüsteemidesse, kus verifitseeritakse digitaalallkirju
ETSI uute standardite versioonide avalikustamine	Aprill 2016	Digitaalallkirjastamise rakenduste vastavusse viimine (arendus) uute standarditega
Uute ETSI standardite kasutuselevõtt eIDAS määruses	3.kv.2017	Infosüsteemide kaasajastamine (uusi standardeit toetavate rakenduste uuendamine infosüsteemides)

Lisa 2

PDF formaadis allkirjade kehtivuse kontrollimine Digidoc3 rakenduse abil

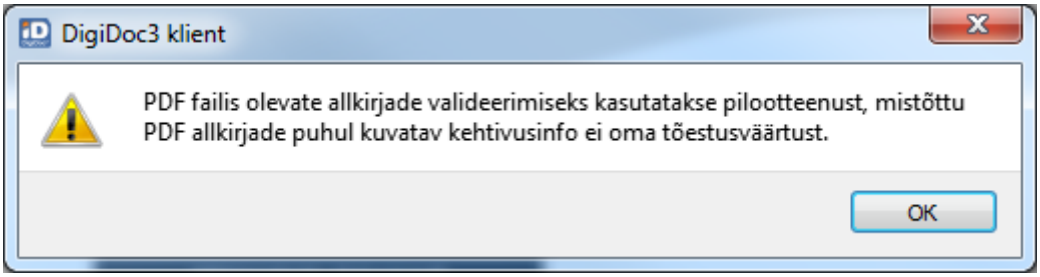
Alates Digidoc tarkvara versioonist 3.12.3 (avaldatud mais 2016)[13] on toetatud PDF failide sisemiste allkirjade kehtivuse kontroll.

PDF sisese allkirja kontrollimiseks tuleb avada Digidoc3 klientrakendus ning valida allkirjastatud dokumendi avamine (vaata allolevat joonist) ning valida PDF formaadis fail mille allkirja soovitakse kontrollida

Joonis:Digidoc3 klint rakenduses allkirjastatud dokumendi avamine

[13] https://installer.id.ee

PDF allkirjaga dokumendi avamisel kuvatakse hoiatusteade (vaata allolevat joonist), et tegemist on pilootteenusega ning, et allkirja kehtivusinfo ei pruugi olla piisav tõendamaks allkirja kehtivust.

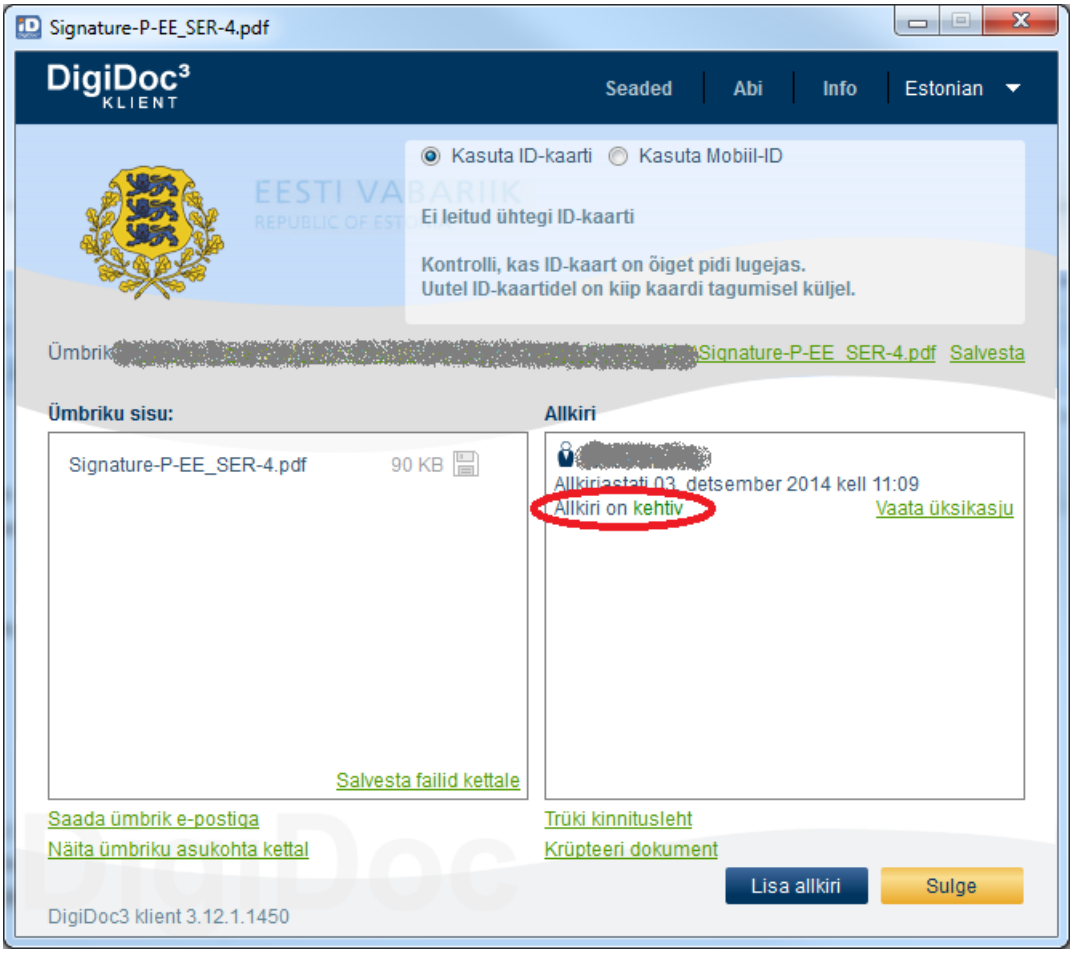


Joonis: hoiatus pilootteenuse osas

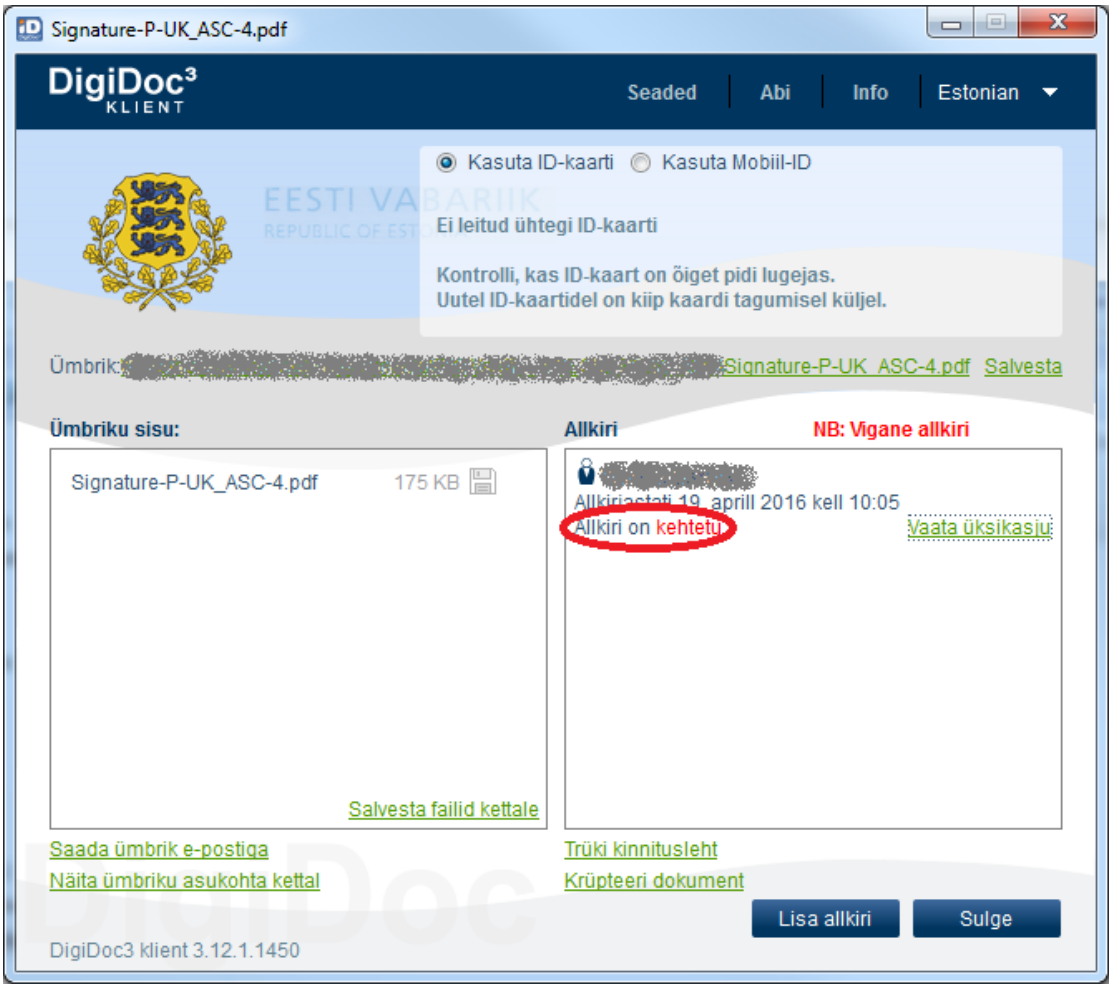
Selline hoiatusteade kuvatakse kuni (hiljemalt) 30. juunini 2016, kuna mais ja juunis 2016 on käimas EL liikmesriikide vaheline e-allkirjade ristkasutatavuse testimine. Selle testimise käigus võib tekkida vajadus teenuse korrigeerimiseks ja täiendamiseks ning seega kuvatakse hoiatusteadet testimise lõpuni.

Digidoc3 klient rakenduses kuvatakse allkirja kehtivana juhul kui allkiri vastab PAdES standardile ning täidab kõik eIDAS määrusest tulenevad kvalifitseeritud allkirja nõuded. Nõuete mitte täitmisel või mõne nõutud elemendi puudumisel hoiatusi ei kuvata, vaid näidatakse allkirja kui mitte kehtivat.

Allolevad joonised illustreerivad kehtivat ja kehtetut allkirja:



Joonis: kehtiva digitaalallkirjaga PDF fail Digidoc3 klient rakenduses



Joonis:kehtetu digitaalallkirjaga (allkiri kas ei vasta nõuetele või on vigane) PDF fail Digidoc3 klient rakenduses