



RIIGI INFOSÜSTEEMI AMET

eIDAS ja Digitaalallkirjad

Mark Erlich

eID koosvõime ekspert

18.05.2016

e-allkirjad eIDAS määruses



Otsekohalduv kõikidele avalikus sektoris:

- Digiallkirjadest peab aksepteerima „kõiki”.
- **1. juuli 2016** jõustub rakendusakt mis käsitleb elektrooniliste allkirjade ja e-templite formaate
- Kui nõutakse käsitsi antud allkirja siis saab piirduda kvalifitseeritud e-allkirja nõudmisega.
- Eestis tuleb eIDAS määruse rakendamise seadus
 - Tühistab digitaalallkirja seaduse
 - Kvalifitseeritud e-allkiri = Digitaalallkiri

Digiallkirjadest lähemalt



- **Kvalifitseeritud e-allkiri (võrdne käsitsi antud allkirjaga)** – põhineb kvalifitseeritud sertifikaadil (mis on olnud kehtiv allkirjastamise ajal) ning antud turvalise vahendiga (kiipkaart jms.) = **meie digitaalallkiri.**
- **Täiustatud e-allkiri kvalifitseeritud serdiga**
– igasugu soft-serdiga jms. allkirjad, mis tekitavad tõsiseltvõetava seose allkirjastatud asja ja allkirja andja vahel, serdi kehtivuse kontroll allkirjastamisel ei ole tingimata nõutav.
- **Täiustatud e-allkiri** – sama, kuid sert pole kvalifitseeritud.
- **Lihtsalt e-allkiri** – igasugu vigurid, mida ka hea fantaasia korral e-allkirjaks annab nimetada (pulgaga ekraanil antud, muud standardid jne.)

Eesti allkirjad (BDOC) ja eIDAS



- Standardseid e-allkirjade formaate peavad kõik aktsepteerima – AdES (sh PDF) ja ASiC
- BDOC on ASiC ning põhineb XAdES standardil, aga...
 - Uues (2016) standardi versioonis puudub ajamärgend (TM)
 - Valik: ajatempel (TS) või ajamärgend (TM)
 - Ajatempel = allkirjastamisel 1 tehing rohkem
- Eksootilisi formaate tuleb aktsepteerida, kui on kättesaadavaks tehtud võimalus neid valideerida.
 - Ebastandardised allkirju saab diskrimineerida, ehk keeruline on teistele tõestada, et me pole „kaamelid“

Eesti allkirjade tulevik?



- Kui pole kindel kas allkirjastatud dokumenti võidakse kasutada/edastada väljaspool Eestit – kasutage TS profiili (*.asice laiendiga allkirjastatud fail)
- Tänapäevane TM kaob/muutub põhivoolu tarkvarast (vanade allkirjade kontrollimise võimekus säilitatakse)
- Püüame vältida kõrvalekaldeid standarditest Standardite muudatused ei tohi mõjutada rakenduste API-d
- Hügieen tagab minimaalse muudatuste mõju hooldus igapäevaseks – uuendage tarkvara regulaarselt

Teiste allkirjad EL-is



- Usaldus läbi Usaldusnimekirja – TL
 - Eesti Baastarkvara toetab juba täna
- Euroopa Komisjoni tarkvara „DSS”
<https://joinup.ec.europa.eu/asset/sd-dss/home>
 - Võimeline valideerima tervet „issanda loomaaeda”
 - Java rakendus mida saab kasutada juba täna.
- 2016/2017 valmib valideerimisteenus „SiVa”
 - Algselt mõeldud Eesti ajaloole ja eksootikale (X-tee jms)
 - Võimalikult varakult EL allkirjade tugi
 - Digidoc kliendi liides

Tänased toimetused?



- **jdigidoc** kasutajad asendage see ASAP **digidoc4j** teegiga
 - Vana jdigioc ei toeta TS-i
 - jdigidoc-il puudub tugi ja jätkusuutlikus
- Vaadake üle digiallkirjadega seotud protsessid
 - Mis andmeid ja mis formaadis loete/salvestate allkirjast
- Looma ja haldame juhiseid
 - <https://www.ria.ee/ee/eid-info-ja-juhendid.html#EL>
- Piloteerime lahendusi Digidoc3 kliendis
 - Kasutaja vaade: Kas allkiri on võrdne omakäelise allkirjaga

Mis juhtub peale 1. juulit 2016



- Rakendub usaldusteenuste (sh digiallkirjade) kohustuslik tunnustamine.
 - Elu läheb edasi: seni on imbunud Eestisse mõnikümmend allkirja aastas
- Valmistume võimalikult varakult
 - Kellel võimalik saab proovida DSS rakendust juba täna demo: <https://joinup.ec.europa.eu/sd-dss/webapp-demo/validation>
 - Soovitav piloteerida SiVa teenusega (2016 lõpp)
- Mõelge ja planeerige protsesside ning rakenduste muudatusi juba täna



RIIGI INFOSÜSTEEMI AMET

Tänan!

Mark Erlich

mark.erlich@ria.ee