



RIIGI INFOSÜSTEEMI AMET

ID-tarkvara tulevikuplaanid

Margus Arm
eID valdkonnajuht

03.11.2016

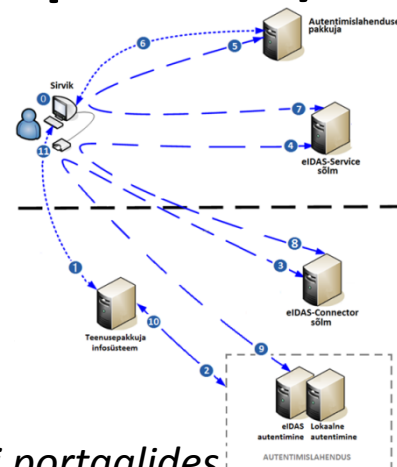
SiVa – signatuuride verifitseerimine

- Võimaldab:
 - Kontrollida EE olemasolevaid allkirju (ddoc, bdoc, x-tee jms)
 - eIDAS PDF allkirja (PaDES)
- Avatud lähtekoodiga (LGPL) veebiteenus allkirjade kehtivuse kontrollimiseks, igaüks saab endale püsti panna ja kasutada.
- Lõppkasutaja/kodaniku jaoks liidestus DigiDoc3-ga.
- Tähtaeg: Dets 2016.
- SiVa2 – 2 kv 2017.
 - täiendavad EU allkirjaformaadid



eIno – eIDAS NODE (Eesti sõlmpunkt)

- Piiriülene autentimislahendus
- EL koosvõime projekt – CEF rahastus
- Eestis 2 teenust:
 - eIDAS Service
 - võimaldab eestlasel autentida teiste EL riikide portaalides
 - eIDAS Connector
 - võimaldab EL riikide kodanikel enda vahendiga autentida Eesti portalides
- Avaliku sektori avalikele teenustele kohustuslik 19.08.2018
- Kasutatav ka erasektorile
- Tähtaeg: 02.2017



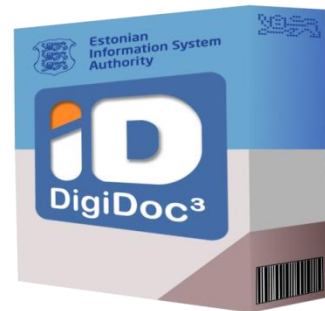
TeRa – Terviklikkuse (tagamise) Rakendus

- Tagamaks digiallkirja pikaajalist terviklikkust (ddoc formaadile ajatempli lisamine)
- ddoc -> ASiC.
 - otsime vana ddoc,
 - paneme ASiC konteinerisse,
 - lisame ajatempli.
 - kasutaja otsustab mida, millal ja kuhu
- Ühekordne tegevus – rakendust ei uuendata
- Desktop rakendus, samuti ka käsurea lahendus
- Tähtaeg: 02.2017



eID klienditarkvara

- **Komponendid:**
kaardi driverid, kaardi halduse rakendus, allkirja teegid (C++, Java), allkirja klient (digidoc3, pluginad), krüpteerimise rakendus
- Paketi värskendus 4x aastas (järgmine reliis dets 2016) + vahereliisid kui vaja
- Uued arenduspartnerid
- Suund BT 4.0
 - Uus kasutajaliides (puutetundlik)
 - All-in-one (allkiri, küpto, haldusvahend)
 - Kaasajastatud kustuslood



Mopp – Mobiilsete platvormide tugi

- Ei ole ainult digiallkirja äpp!
- Baastarkvara tugi Android ja iOS.
- Driverid ja alusteegid
- Arendajate juhised ja tugi
- Väliste kiipkaardilugejate tugi (Bluetooth, micro USB)
- Tähtaeg: 2 kv 2017



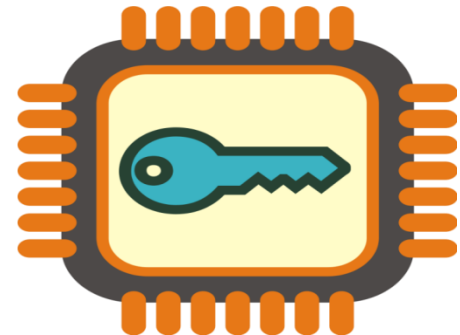
Euroopa Liit
Euroopa struktuuri-
ja investeerimisfondid



Eesti
tuleviku heaks

ID-kaardi hange

- PPA-ga koostöö uues ID-kaardi hankes
- Uus põlvkond ID-kaarte (ka digi-ID ja eResident)
- Uued kaardid alates 2019
- CA nõuded uues hankes
- Riistvara nõuete haldus
- eIDAS nõuetele vastav lahendus



Tegevustest veel (1)

- KONT – uus krüptoformaad
 - Tehniline lahendus olemas
 - Toetab rohkem algoritme, kaasajastamine
 - Juurutamine 2017, reliisitakse koos mõne BT-ga
- eIDAS määruse rakendamine
 - Qualified signature vs advanced signature. Mis me Eestis tahame?
 - „digitaalallkiri“ on kvalifitseeritud e-allkiri!
 - §24 „E-identimise ja e-tehingute usaldusteenuste seadus (EUTS)“



Tegevustest veel (2)

- Autentimisnormatiiv
 - Juhend/reeglistik autentimislahendustele
- Uued eID lahendused
 - eSIM?
 - SK uus eID lahendus?
 - Veel midagi huvitavat?
- Usaldusteenuse pakkujatele nõuete defineerimine.
 - QSCD-de seadmete nimekiri
 - Puudutab ka finantsasutusi, kes kasutavad digitempleid



Arendusmudel

- Riigi poolt tellitud eID tarkvara on avatud lähtekoodiga tarkvara, "avatud turul" koos kõigi teiste sarnastega
- saavutada maksimaalne tulemus investeeritud raha eest ja pikaajaline jätkusuutlikus (sealhulgas ilma võimaliku RIA rahastuseta)
- Strateegiline huvi vältida „Forkide“ teket ja maksimaalselt kaasata kolmandaid osapooli (nii Eesti erasektoris kui ka üle maailma)
- Turul on olemas ja on tekkimas alternatiivseid lahendusi

Rollid

- PPA – füüsilised isikut tõendavad dokumendid
 - Isikute identiteedihaldus
 - Füüsiline dokument
 - Turvaelemendid
 - Väljastamine
- RIA – kõik eID-ga seonduv
 - Kiip
 - Rakendused kiibil
 - Usaldusteenuste regulatsioon (ca CA ja PKI nõuded)
 - eID tarkvara





RIIGI INFOSÜSTEEMI AMET

Aitäh!

Küsimusi ?

margus.arm@ria.ee

Digiallkirjadest lähemalt



- **Kvalifitseeritud e-allkiri (võrdne käsitsi antud allkirjaga)** – põhineb kvalifitseeritud sertifikaadil (mis on olnud kehtiv allkirjastamise ajal) ning antud turvalise vahendiga (kiipkaart jms. QSCD seade) = **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.)