# Tänased teemad

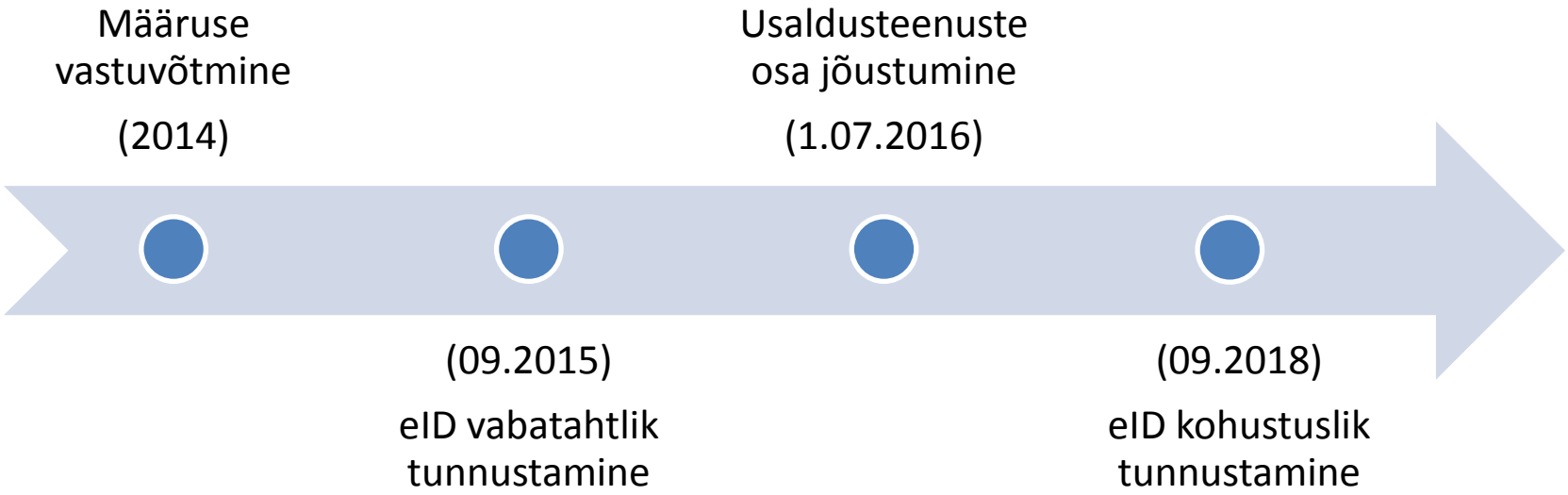
- Laura Kask, MKM
  - eIDAS regulatsioon
  - Piiriülene autentimisvahendite tunnustamine
  - Erinevad e-allkirjad ja nende kasutamine
- Margus Arm, RIA
  - RIA eID valdkond
  - E-allkirjade valideerimine
  - SHA-1 ja vanad formaadid
  - TeRa

# eIDAS

eID

usaldusteenused
(digiallkiri jm)

# eIDASe rakendumise ajajoon



# eID piiriülene tunnustamine

(avalikus sektoris)

- **Määrus reguleerib piiriülest koosvõimet – millist eID-d tuleb teistest liikmesriikidest aktsepteerida.**

- **Kui kuskil kasutatakse autentimist, siis peab sinna ligi laskma ka teiste riikide samaväärse või kõrgema tasemega eID kasutajaid teistest riikidest.**

- **Ligi peab laskma neid eID vahendeid, millest riigid on teada andnud (teavitanud).**

# USALDUSTEENUSED

## (digiallkiri ja muu)

- **Alates 1.07.2016 ühtne tururegulatsioon teenuseosutajatele EÜ majanduspiirkonnas.**

- **Kui kuskil avalikus sektoris aktsepteeritakse e-allkirjaga dokumente, siis tuleb aktsepteerida ka teistest riikidest ja teiste teenuseosutajate abil allkirjastatud samaväärse allkirja tasemega dokumente.**

# E-allkirja „tasemed“

- **Kvalifitseeritud e-allkiri – kvalifitseeritud serdiga antud ja kasutatud selleks turvalist vahendit (kiipkaaart vmt.), sert on olnud kehtiv allkirjastamise ajal. = meie digiallkiri.**

- **Täiustatud e-allkiri kvalifitseeritud serdiga – igasugu soft-serdiga jmt. 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 ei pruugi ka kvalifitseeritud olla.**

- **Lihtsalt e-allkiri – igasugu vigurid, mida e-allkirjaks annab nimetada (pulgaga ekraanil antud vmt.)**

# Õiguslik tähendus

- **Omakäelise allkirjaga võrdväärse allkirja tähendus DAS § 3 kohaselt digitaalallkirjale;**

- **eIDAS määruse artikkel 25 (2) kohaselt on kvalifitseeritud e-allkirjal on käsitsi kirjutatud allkirjaga samaväärne õiguslik toime.**

- **Elektroonilisi allkirju ja nende tasemeid on erinevaid, kuid omakäelisega on võrdväärne on vaid kvalifitseeritud e-allkiri ehk digitaalallkiri.**

# Erinevaid allkirja tasemete näiteid Eestist

- **Digitaalallkiri ehk ID-kaardiga või muu isikut tõendavate dokumentide seaduses sätestatud kaardiga antud allkiri;**
- **Smart ID uus võimalus autentimiseks ning ka e-allkirja andmiseks;**
- **… (muid elektroonilisi allkirju).**

# Kus ja kuidas kasutada erasektoris?

- **Eraõiguslikes suhetes vormivabaduse põhimõte- tahteavalduste vahetamine;**

- **Juhul, kui seaduses ei ole erinõuet, siis võibki olla tehing allkirjastatud ükskõik mis tasemega allkirjaga;**

- **Juhul, kui seaduses on nõue omakäeliseks allkirjaks, siis see saab olla üksnes kvalifitseeritud e-allkiri ehk digitaalallkiri.**

# Kus ja kuidas kasutada avalikus sektoris?

- **Juhul, kui avaliku sektori protsessis on vajalik elektrooniliselt midagi esitada, sobivad kõik e-allkirja tasemed.**

- **Juhul, kui on nõutud, et dokument/avaldus vms tuleb esitada ning allkirjastada omakäeliselt või digitaalselt, siis tuleks kasutada digitaalallkirja ehk kvalifitseeritud e-allkirja.**

RIIGI INFOSÜSTEEMI AMET

# eID

Margus Arm
eID valdkonnajuht

20.09.2017

# RIA eID valdkonna eesmärgid

**RIA eID valdkonna põhieesmärgiks on:**

- olla keskne elektroonilise identiteedi (eID) valdkonna eestkõneleja ja seisukohtade kujundaja Eestis;
- tagada Eestis maailmatasemel, turvalise eID infrastruktuuri toimimine ja olemasolu kaasaegsetel tehnoloogiatel
- tagada eID kasutamiseks vajamineva tark- ja riistvara jätkusuutlik toimimine ja laialdane kasutamine (sh piiriülene)

# SiVa – signatuuride verifitseerimine

- Võimaldab:
  - Kontrollida EE olemasolevaid allkirju (ddoc, bdoc, x-tee jms)
  - eIDAS  PDF allkirja (PaDES)
- Avatud lähtekoodiga (LGPL) rakendus allkirjade kehtivuse kontrollimiseks, igaüks saab endale püsti panna ja kasutada.
- Lõppkasutaja/kodaniku jaoks liidestus DigiDoc klienti.
- https://siva-arendus.eesti.ee/ - eelkõige masinsuhtluseks
- Kasutatud EL DSS rakendus + kohalikud Eesti teegid

# EL e-allkirjad

- Juhend ja nõuanded e-allkirjade käsitlemiseks
  https://www.ria.ee/public/PKI/EL_e-allkirjade_kasitlemine.pdf
- Ühes riigis aktsepteeritav allkirja tase ei pruugi tagada sama juriidilist jõudu teises riigis
- Erinev standardite tõlgendamine
  http://dss.nowina.lu/validation, allkirjade detailseks analüüsiks
- SiVa2 – 4 kv 2017.
  - täiendavad EU allkirjaformaadid
  - DigiDoc klient valimistejärgne reliis
  - vabavaraliselt kasutatav
  - allkirjade tasemed

# Allkirjad DigiDoc3 kliendis

Kokkulepe:

- **e-allkiri on kehtiv (digitaalallkiri)**
- **e-allkiri on kehtiv (piirangud)**
- **e-allkiri on vigane, ei kehti**

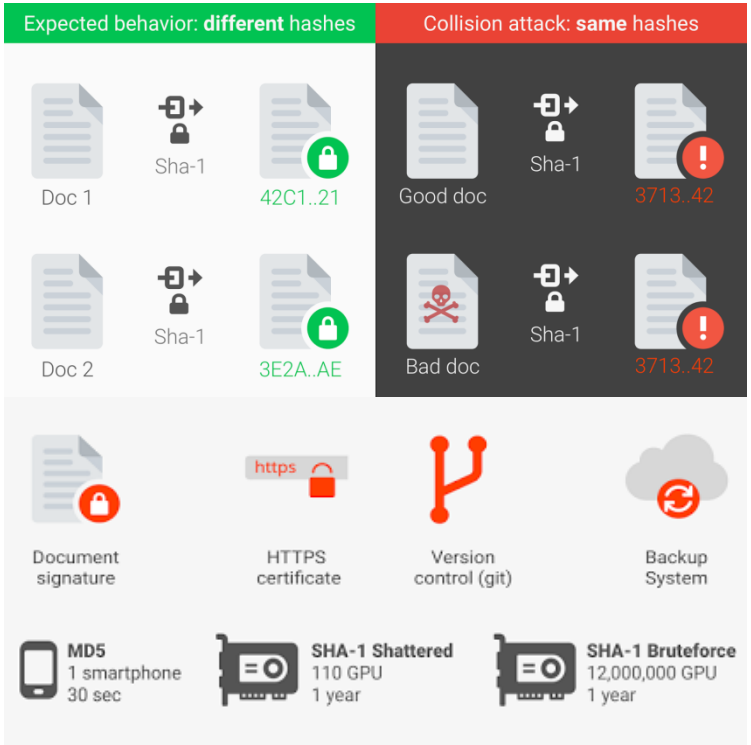
Piirangu kohta kuvatakse (eraldi aknas):

“Tegemist on e-allkirjaga, mis on kasutatav nendes toimingutes, kus ei ole nõutud omakäelise allkirjaga võrdväärset kvalifitseeritud e-allkirja ehk digitaalallkirja.”

DigiDoc Klient järgmine reliis: Juuni 2017

# SHA-1

## Google uudis




## Krüptouuring 2016

**5.4 The cost of chosen-prefix collision attacks against SHA-1**

Considering the estimations based on the techniques used in collision-attack against SHA-1 in 2015 [163], the cost of a collision attack against SHA-1 is between 75,000 and 120,000 US dollars when renting Amazon EC2 cloud over a few months, which is about 100 times lower than estimated in the previous report [12].

## Bruce Schneier (2015 oktoober)

**Abstract**: We present in this article a freestart collision example for SHA-1, i.e., a collision for its internal compression function. This is the first practical break of the full SHA-1, reaching all 80 out of 80 steps, while only 10 days of computation on a 64 GPU cluster were necessary to perform the attack. This work builds on a continuous series of

## Järeldus / Ennustus:

2017 aasta lõpuks on olemasoleva tehnoloogiaga
ja mõnekümne tuhande euroga võimalik mõne nädalaga
võltsida SHA-1 allkirjastatud dokumendi sisu.

# SHA-1 ja Eesti digiallkiri

- SHA-1 on olnud kasutusel:
  - DDOC
  - BDOC1.0
  - Oht ainult siis kui sisuks on PDF fail.
- Ülejäänud Eestis kasutusel olevad allkirjastamise formaadid (bdoc2.1, asice) ei kasuta SHA-1, seega nendega probleeme hetkel ei ole.

# TeRa – Terviklikkuse (tagamise) Rakendus

- Tagamaks digiallkirja pikaajalist terviklikkust (ddoc formaadile ajatempli lisamine)
- ddoc -> ASiCs.
  - otsime vana ddoc,
  - paneme ASiCs konteinerisse,
  - lisame ajatempli.
  - kasutaja otsustab mida, millal ja kuhu
- Ühekordne tegevus
- Ei lisa ega vähenda juriidilist jõudu!
- Desktop rakendus, samuti ka käsurea lahendus
- Arendatud eelkõige kodanikule ja väiksematele ettevõtetele (nn C-ketta omanikele)
- https://tark-e-riik.punkdigital.ee/eidinfopaev2017/presentations

# TeRa


TeRa klient
TeRa KLIENT
Seaded
Abi
Info
Eesti
EESTI VABARIIK
REPUBLIC OF ESTONIA
Teie digiallkirjastatud DDOC failidele lisatakse ajatempel, et kaitsta teid võimalike tulevaste turvanõrkuste eest. Ajatempliga failid on ASICS laiendiga ja asuvad samas kataloogis.
Vaikimisi ajatembeldatakse ainult arvutis asuvaid DDOC faile. Kui soovite võrguketastel asuvaid faile tembeldada või muid seadeid muuta, avage "Seaded" menüü.
Alusta
Euroopa Liit
Euroopa Regionaalarengu Fond
Eesti tuleviku heaks
TeRa klient 0.11.0.164


TeRa klient
TeRa KLIENT
Seaded
Abi
Info
Eesti
EESTI VABARIIK
REPUBLIC OF ESTONIA
Teie digiallkirjastatud DDOC failidele lisatakse ajatempel, et kaitsta teid võimalike tulevaste turvanõrkuste eest. Ajatempliga failid on ASICS laiendiga ja asuvad samas kataloogis.
Vaikimisi ajatembeldatakse ainult arvutis asuvaid DDOC faile. Kui soovite võrguketastel asuvaid faile tembeldada või muid seadeid muuta, avage "Seaded" menüü.
Valmis
DDOC failide tembeldamine on lõppenud
DDOC faile leitud: 9
DDOC faile tembeldatud: 9
Täpsema aruande vaatamiseks vajuta SIIN
Euroopa Liit
Euroopa Regionaalarengu Fond
Eesti tuleviku heaks
TeRa klient 0.11.0.164

# DDOC sõnumid

- Kiri avalikule sektorile 28.04.17.
  - Lisada ajatempel juba eksisteerivatele, **pikaajalist tõestusväärtust** vajavatele DDOC ja BDOC1.0 formaadis dokumentidele
  - Alates 31.03.2018 EI TOHI DDOC ja BDOC1.0 faile enam luua.
  - Pärast 01.07.2018 moodustatud DDOC ja BDOC1.0 allkiri ei ole enam usaldusväärne (ei aktsepteerita avalikus sektoris).
  - TeRa tembeldamislahendus on desktop- ja käsurearakendusena kättesaadav alates 17.04.2017 (https://github.com/open-eid/TeRa/releases/tag/v1.0) koos vajalike juhenditega.
  - Olemasolevad DDOC ja BDOC1.0 failid tuleb üle **ajatembeldada hiljemalt 01.07.2018**.
  - **RIA tagab kõikidele avaliku sektori asutustele TeRa jaoks tasuta ajatempliteenuse kuni 31.12.2017!**
  - RIA jätab endale õiguse nimetatud tähtaegu veelgi lühendada!
- Tavakasutajale koos DigiDoc klient 19.06 reliisiga
  - Saab ASICs faile avada

Riigi Infosüsteemi Amet

# Aitäh!

Küsimusi ?

margus.arm@ria.ee