



RIIGI INFOSÜSTEEMI AMET

Tulevikukrüptograafia

Digiühiskonna väljakutsed ja riigi roll

Lauri Tankler, RIA



Kvantkindel ühiskond

Riigi Infosüsteemi Amet on riiklik kompetentsikeskus, kes kujundab ja kindlustab Eesti digiühiskonna alustalasid: arendame ja haldame digiriigi keskseid tehnoloogilisi platvorme ning tagame riigi küberturvalisuse.

- Valimised kui digiühiskonna teenuste tipp
 - Autentimine, andmevahetus, allkirjastamine jne kõik koos
- Kvantarvuti potentsiaal ja oht on tõsine, nõuab tähelepanu kõigis etappides
- Nii tehniline kui ka sotsiaalne usaldus nõuab tähelepanu



VAJALIKUD TEENUSED

- TEHIKu veebilehed
- Sündmusteenused
- Koodivaramu
- Keskkonnaportaali
- Keskkonnaregister

OLULISED TEENUSED

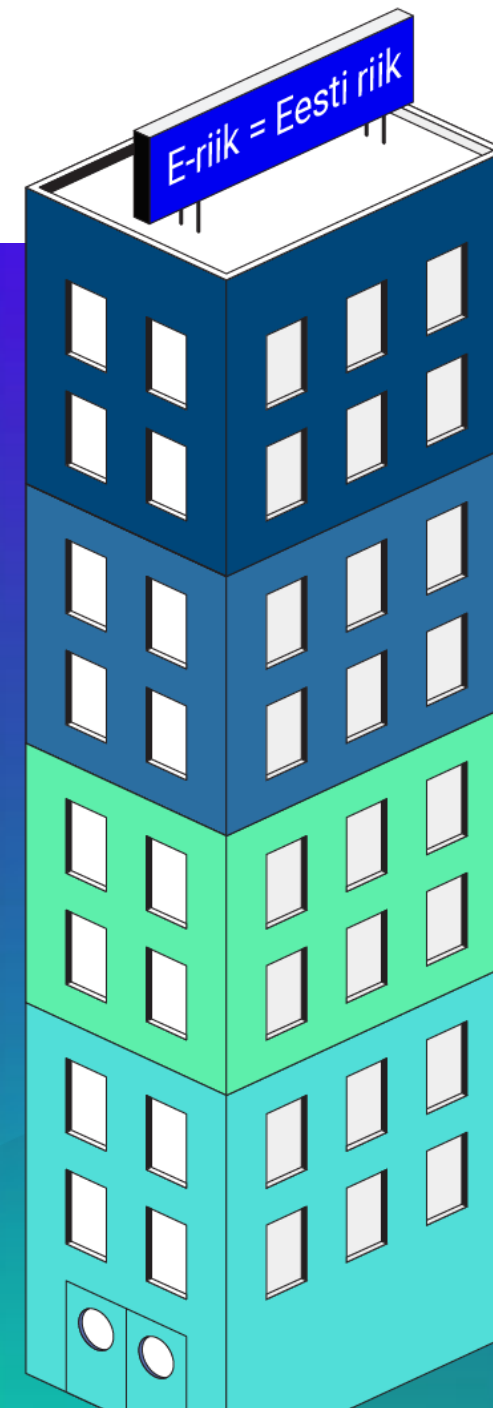
- KEMIT andmehaldus
- Riigiportaali
- Infoturbestandardi haldus
- Maksukohustuste täitmise teenused
- EELIS – Eesti looduse infosüsteem
- Tööelu infosüsteem

KRIITILISED TEENUSED

- e-toimik
- kinnistusraamat
- äriregister
- Riigi Teataja
- maakataster
- riigikassa infosüsteem
- maksukohuslaste register
- rahvastikuregister
- isikut tõendavate dokumentide register
- riiklik pensionikindlustuse register
- autentimise teenus (TARA)

ALUSTEENUSED

- X-tee
- Riigivõrk
- Elektrooniline identiteet (eID)
- Küberturvalisus





Kvantkindel ühiskond

Riigi Infosüsteemi Amet on riiklik kompetentsikeskus, kes kujundab ja kindlustab Eesti digiühiskonna alustalasid: arendame ja haldame digiriigi keskseid tehnoloogilisi platvorme ning tagame riigi küberturvalisuse.

- **Eesmärk:** Eesti ühiskond on valmis olukorraks, kus kvantarvuti abil murtakse lahti seni kasutusel olevad krüptograafilised algoritmid, mistõttu muutuvad need edaspidi kasutuks



Kvantkindel ühiskond

Riigi Infosüsteemi Amet on riiklik kompetentsikeskus, kes kujundab ja kindlustab Eesti digiühiskonna alustalasid: arendame ja haldame digiriigi keskseid tehnoloogilisi platvorme ning tagame riigi küberturvalisuse.

On see lihtne või keeruline?

- Inventuur (mis algoritme ja kus praegu kasutame?)
- Plaan (mis ressursse nõuab kvantkindlaks muutmine?
Nt töötunnid, senise süsteemi paralleelselt toimiva hoidmine)
- Muutuse juhtimine (testimine, läbiviimine, tugi)



RIIGI INFOSÜSTEEMI AMET

Täna kuulamast!

Lauri Tankler

RIA

