Teaduste akadeemia küberturvalisuse komisjoni pika plaani tutvustus

Dan Bogdanov, PhD

Dan Bogdanov, akadeemik ja küberturvalisuse komisjoni esimees

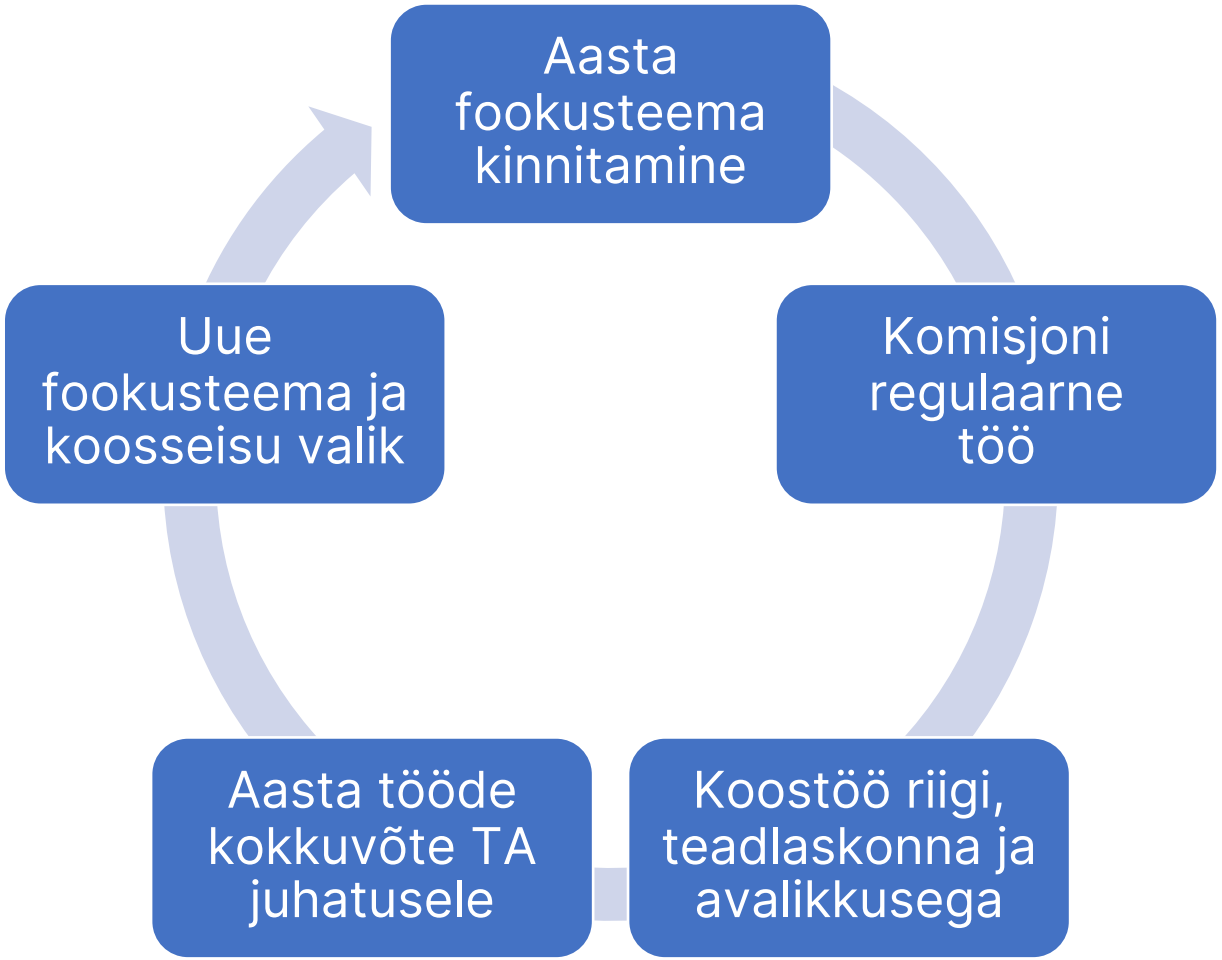
Komisjoni tutvustus

Ajaloost ja uuest mandaadist

- TA küberkaitse komisjon loodi 200x. aastal (juht Leo Mõtus), kuid see ei olnud mitmeid aastaid enam aktiivne
- 15. detsembril 2022 andis akadeemia juhatus akad Bogdanovile ülesandeks komisjon taaskäivitada
- 20. juunil 2023 kinnitas akadeemia juhatus uue küberturvalisuse komisjoni koosseisu
- Uus küberturvalisuse komisjon kohtus esimest korda 14. augustil 2023

Komisjoni tsükkel on ühe aasta pikkune

- Komisjoni mandaat on uurida digitaalsete teenuste riskide analüüsi metoodikaid
- Uurimisobjektid valitakse Eesti e-riigi teenuste seast (digitaalne identiteet, valimised, andmepõhised teenused)



Esimene fookusteema on valimised

- Esimeseks teemaks valis esimees valimiste (nii paberil kui internetis) turvalisuse analüüsi metoodikate uurimise.
- Teema valiku põhjendused on järgmised.
  1. Valimiste tehnoloogilised valikud on ühiskonnas aktuaalne teema.
  2. Peame algatama arutelu selle üle, kuidas valimisi mõjutab arvutustehnika pikaajalisem areng (võimalikud kvantarvutid).
  3. Valimiste turvamudeli tehakse väiteid ja küsitakse küsimusi, vaja oleks ühtset metoodikat neile vastamiseks.
- Selle teemaga võib tööd jätkuda mitmeks aastaks.

Komisjoni koosseis 2023–2024

- Esimees: Dan Bogdanov (akadeemik, Cybernetica AS teadusdirektor)
- Alo Einla (RIA valimiste osakonna juht)
- Arne Koitmäe (Riigi valimisteenistuse juht)
- Kristjan Krips (Cybernetica AS teadur)
- Ivo Kubjas (ConsenSys vanemteadusinsener)
- Liisa Past (MKM riikliku küberturvalisuse osakonna juhataja)
- Teet Raidma (VVK liige, IS Audit OÜ juhtaudiitor, RIA vanemekspert)
- Mihkel Solvak (Tartu Ülikooli tehnoloogiauuringute kaasprofessor)
- Ahto Truu (Guardtime tarkvaraarhitekt)
- Tarmo Uustalu (akadeemik, Reykjaviki ülikooli professor, TalTech juhtivteadur)
- Priit Vinkel (e-Riigi Akadeemia SA vanemekspert e-valitsemise alal)
- Jan Willemson (Cybernetica AS vanemteadur)

Komisjoni tööplaan 2023–2024

- August-september 2023 – istungid ja eesmärgistamine
- Oktoober 2023 – konverents, plaanide tutvustamine ja tagasiside kogumine
- November 2023-mai 2024 – istungid ja sisuline töö
- Juuni 2024 – kokkuvõtted ja uued plaanid
- Juuli 2024 – komisjon puhkab

Komisjoni üks ettepanek:
ühtlustatud turbeohtude kataloog ja analüüsi metoodika

Valu kirjeldus ja võimalik lahendus

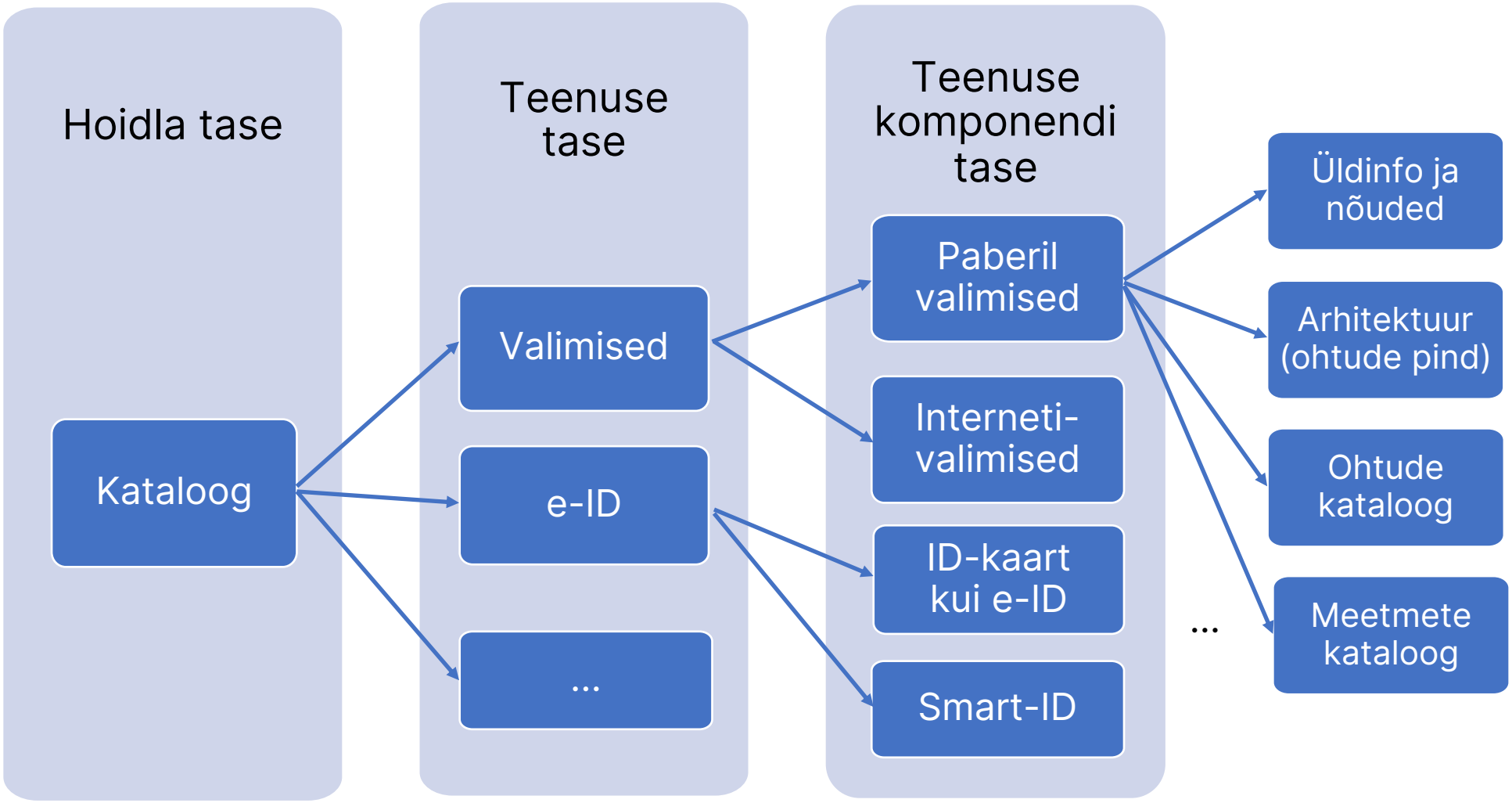
“Minu teenuse turbehalduse süsteem nõuab, et mul oleks kirjeldatud süsteem ja selle ohud.”

“Ma pean otsustama, millised ohud ähvardavad minu teenust uute tehnoloogiate arenedes.”

“Minult oodatakse, et oskan kiiresti vastata kõikidele küsimustele oma teenuse turvalisuse kohta.”

Süsteemi kirjeldaus ja ohtude kataloog

Esialgne infoarhitektuur



Kuidas kataloog võiks sündida?

- TA küberturvalisuse komisjon töötaks välja kataloogi infoarhitektuuri, tehnilise struktuuri ja kasutamise juhised
- Valitakse välja pilootteenus, mille jaoks teeb komisjon koostöös teenuse omaniku ning teadlastega ära esmase analüüsi.
- Teenuse omanik ning teised teadlased hindavad metoodikat ning pilootteenuse analüüsi.
- Hinnangute põhjal täiendatakse metoodikat.
- Metoodika avaldatakse ning võetakse kasutusele.

Kuidas saaks kataloogi kasutada?

- Kui teenuse omanik teeb ise turvaanalüüsi, või tellib seda teadlastelt või turbeteenuse andjatelt, palutakse võtta aluseks kataloog ning esitada töö selle täiendusena.
- Kui teenuse omanikul on vaja vastata nt avalikkuse päringutele, teeb ta seda kataloogile tuginedes.
- Kui tekib päring, mille kohta kataloogis sissekannet pole, siis küsimusele vastamise käigus täiendatakse kataloogi (nii et järgmine kord oleks vastamine kiirem).
- Teenuse omanik võib otsustada kataloogis enda teenuse turvaanalüüsi ka kasutada.

Mis saab edasi?

Mis saab pärast konverentsi?

- Komisjon jätkab ohtude kataloogi struktuuri ja metoodika arendamisega.
- Kui näeme, kataloogi ideel on jumet, korraldame pilootuuringu.
  - Leiame riigiga koostöös pilootteenuse ja selle uuritava komponendi.
  - Leiame ohtude kataloogi arendamiseks sobivad tehnilised tööriistad.
  - Koostame esimese turvaanalüüsi ning anname selle teenuse omanikule üle.

Mis saab pikas plaanis?

- Tulevikus saab komisjon tööd teha kindlasti tehisintellekti ja andmepõhiste süsteemide küberturvalisusega
- Digitaalse identiteediga on RIA juba väga head tööd teinud, põnevaks teemaks saab postkvant-krüptograafia
- Usun, et komisjoni töö väärtus saab selgemaks viie-kuni-kümne tööaasta jooksul

- Tänan kõiki konverentsile tulijaid!