

RIA koostööpartnerite infopäev

Üritust korraldab Riigi Infosüsteemi Amet Euroopa Liidu struktuuritoetuse toetuskeemist "Infoühiskonna teadlikkuse tõstmine", mida rahastab Euroopa Regionaalarengu Fond.



RIIGI INFOSÜSTEEMI AMET



Euroopa Liit
Euroopa
Regionaalarengu Fond



Eesti
Tuleviku Heaks

TARK



e-RIIK





RIIGI INFOSÜSTEEMI AMET



Euroopa Liit
Euroopa struktuuri-
ja investeerimisfondid



Eesti
tuleviku heaks

Riiklik SSO (single-sign-on) ja Riigi autentimisteenus (TARA)

Helen Raamat
eID tootejuht

17.11.2020

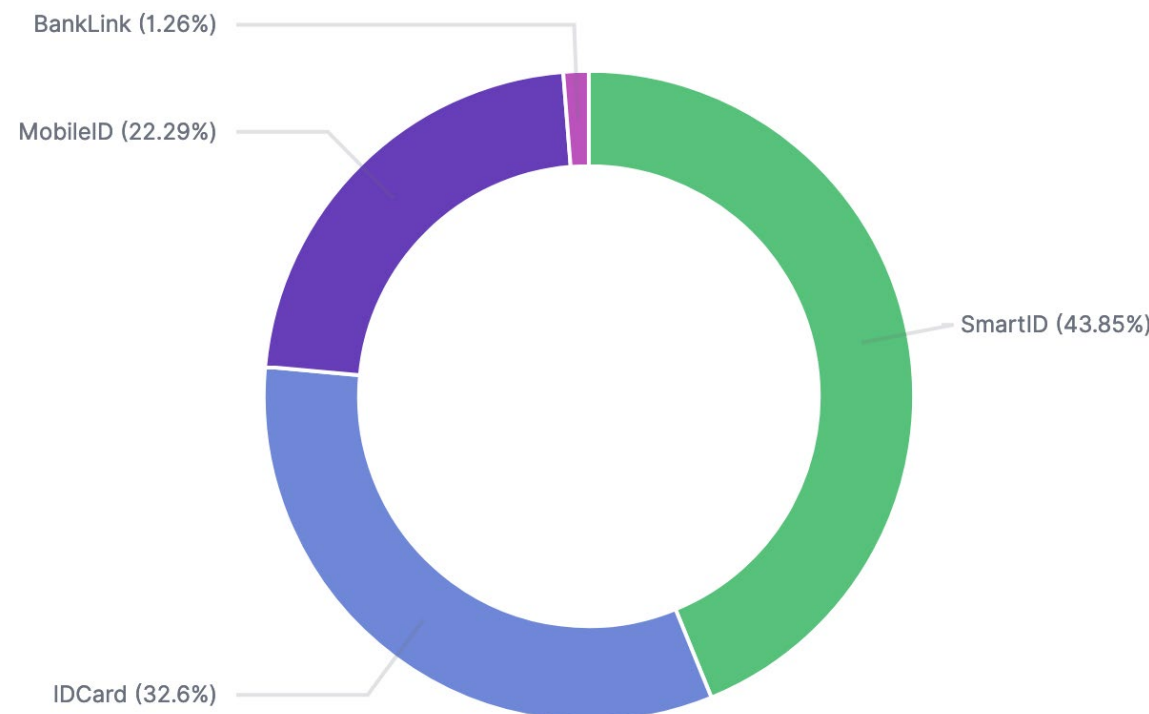
Riigi autentimisteenus (TARA)

- ca **1,9 mln** autentimispäringut kuus (oktoober 2020)
- Liitumisi
 - **46** asutust
 - **271** klientrakendust testkeskkonnas
 - **189** klientrakendust toodangukeskkonnas

- Jaotus autentimisvahendite lõikes

Edukaid autentimisi oktoobris:

- ID-kaart: **601 285**
- Mobiil-ID: **411 030**
- Smart-ID: **808 700**
- Pangalink: **23 172**
- EL eID: **94**



SF projekt: Riikliku SSO tehniline analüüs ja PoC

Eesmärk

Selgitada välja, milline ühekordse sisselogmise (SSO) tehniline lahendus täidaks riigiasutuste ärivajadusi, mis oleks turvaline keskses autentimisteenuses kasutusele võtmise tehnilist võimekust arvestades.

- Miks?
 - Riigiasutuse e-teenuse pakkujate ja kasutajate nõudlus riikliku keskse ja turvalise SSO teenuse järele
 - Halduskulude optimeerimiseks riigis dubleerivate SSO lahenduste ja autentimispäringute kulude arvelt
 - Tõsta kesksete teenuste (Riigi autentimisteenus) kvaliteeti ja turvalisust

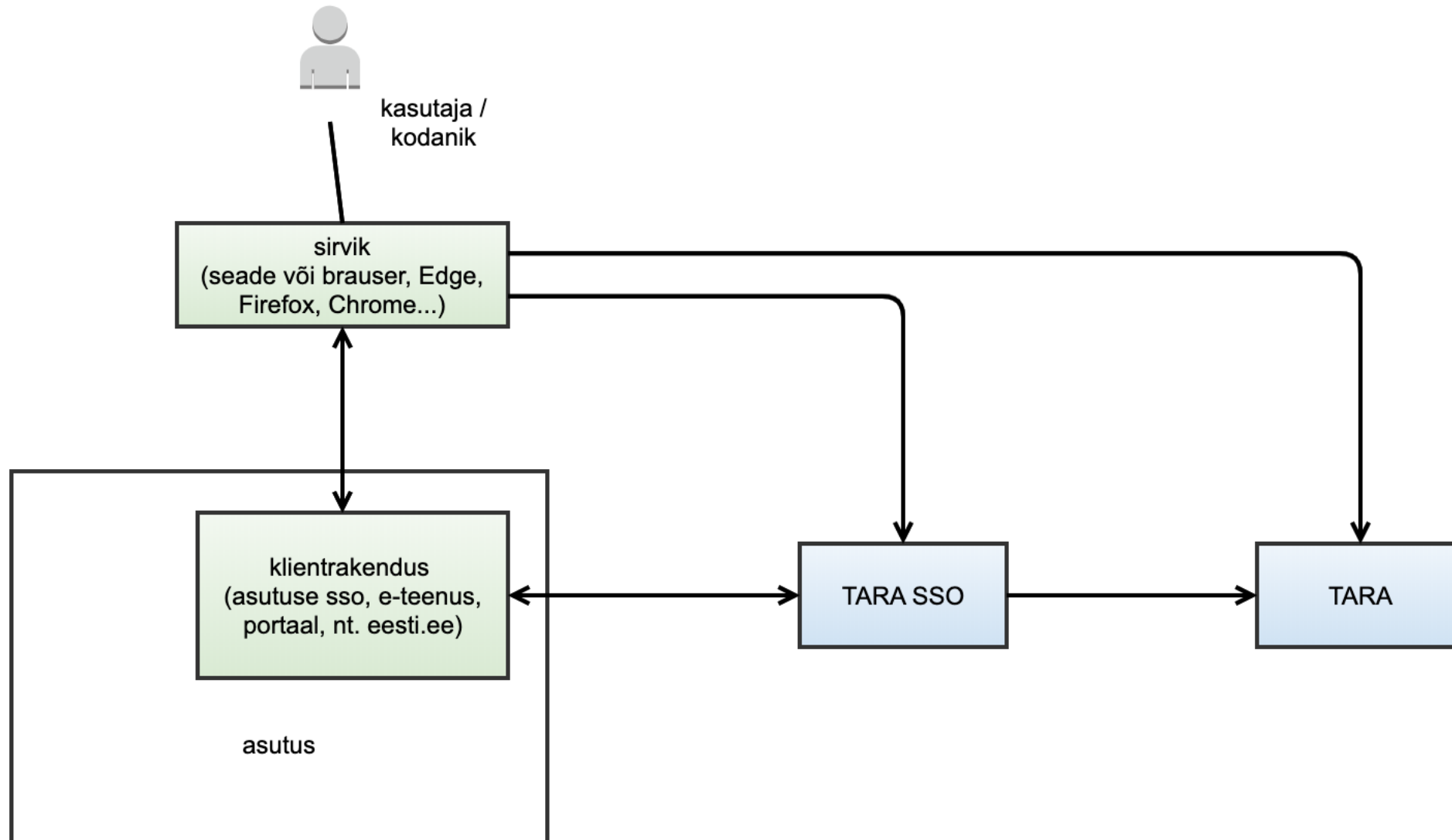
SF projekt: Riikliku SSO tehniline analüüs ja PoC

- SSO kasutuselevõttuga seotud riskide analüüs, hindamine;
 - riske vähendavate meetmete kava koostamine;
 - avaliku sektori asutuste IT-spetsialistide intervjuueerimine
 - kasutatavuse testide läbiviimine
 - Tulemiks: turvaanalüüs
- Töötati välja ühekordse sisselogimise (SSO) [projektlahendus](#) (tehnilise sobivuse dokument ja protokoll kirjeldus)
 - [tehniline spetsifikatsioon](#)
 - [prototüüp](#) TARA SSO OIDC (OpenID Connect) protokoll testimiseks, SSO kasutusvoogude teostamise kontrolliks, tehniliste ja maksumusriskide maandamiseks

Nõuded

- Turvalisus
 - Riigi autentimisteenuse (TARA) kõrge turvatase peab säilima
- Asutuse nõuetele vastavus
 - OpenID Connect standard
- Kasutusmugavus
- Kasutusjuhud
 - Asutusesisene või asutuste ülene
 - TARA senise voo säilitamine
 - Piiriülene autentimine ja erinevad autentimise tasemed

Arhitektuur



Riikliku SSO OIDC protokoll

- Riigi autentimisteenusest (TARA) sõltumatu OIDC protokoll
- Mitte ainult keskne sisselogimine, vaid ka väljalogimine
- Seansi sünkroniseerimine klientrakenduste ja SSO vahel
 - klientrakenduse seansi aluseks on kehtiv identsustõend
 - tõendit uuendatakse perioodiliselt
- 1 autentimine = 1 seanss
 - SSO ei ole identiteedi süsteem, ei suuda andmeid juurde laadida
 - Autentimisvahend ja usaldustase seansi jooksul ei muutu
- Andmete liikumise / töötlemise selgus kasutajale
 - Ei luba nähtamatult suunata portaalist portaali

Riikliku SSO prototüüp (proof of concept, POC)

- ORY Hydra OIDC server + Java + Spring Security
 - Modulaarne, madal mälu kasutus, suur läbilaskevõime. Riigi autentimisteenus (TARA) plaanitud migreerida Hydra toote peale.
- SSO serveri makett, autentimine TARA testkeskkonnas
- Realiseeritud kasutusjuhud
 - Autentimine, seansi uuendamine ja väljalogimine samas seadmes mitme klientrakenduse vahel. Kasutajate teavituse vahelehed.
- Realiseerimata kasutusjuhud
 - Seansi aegumine SSO poolel (Hydra piirangud), paralleelne autentimine, mitme seadme tugi, TARA täiendused (autentimise taseme tõus).
- <https://github.com/e-gov/TARA-SSO-POC>

Turvaanalüüs

- Turvaanalüüsi allikaks on rahvusvahelised standardid, eelkõige OIDC protokollistik, erialane kirjandus, infoturbesüsteem ISKE.
- Kriitiline on SSO seansivõtme kaitse, seansi oleku uuendamine ja seansi õigeaegne lõpetamine – tagada kasutaja mitteaktiivsuse korral seansi aegumine mõistliku aja jooksul.
- OIDC baasil TARA SSO teenuses paratamatult tekib jääkrisk, kui kasutaja seanssi korrektset ei lõpeta. Sarnane risk kaasneb mistahes teises süsteemis SSO rakendamisel.
- Pakutud meetmed aitavad riske maandada kuid ei suuda kõiki riske täielikult elimineerida.
- Tehnilise lahenduse osas peab nii SSO teenusepakkuja kui ka liidestaja rangelt järgima OIDC/OAuth2.0 [parimaid praktikaid](#) (ründemudel [RFC-6819](#) ja selle täiendused).

Kasutatavuse testimine

- Testiti kasutajate arusaamist klientrakenduste vahel liikumisest, seansi alustamisest, seansi lõpetamisest, autentimisest keeldumise erijuhtudest ning SSO volituste vahelehest.
- Peamised järeldused:
 - Kasutajad ei tea mis on Riigi autentimisteenus (TARA), TARA autentimise valikut on klientrakenduses erinevalt käsitletud.
 - Kasutajad ei mõista TARA ja TARA SSO vahelist erinevust – otsus tuleb teha klientarkenduse poolt
 - Kasutajad saavad aru vahelehtede olulisusest. Vaheleht aitab selgitada SSO seansi tausta ja seansi jooksul toimunud sisselogimisi.
 - Kõrgema autentimistaseme nõudmisel oluline kasutajat teavitada.

Evitus ja arendustööde hinnang

- Riikliku SSO teenuse tuumikus mõistlik kasutada OIDF sertifitseeritud karbitoodet - mõjutab arendusmahte ligi kaks korda
- Ajakulu SSO realiseerimiseks: 570-943 tööpäeva
- Ajakulu SSO liidestajale: 16-35 tööpäeva.

RIA hinnang

Projekt aitab kaasa SSO rakendamise eelduseks olevate võimekuste loomisele. Meil on nüüd:

- **eestikeelne terminoloogia** (et saaksime aru, millest räägime)
- eestikeelsed tekstid, mis SSO lahti seletavad
- laiem inimeste ring, kes suudavad lugeda **rahvusvahelisi SSO standardeid ja neid Eestis rakendada**
- laiem ringkond, kes suudavad neid tekste lugeda ja nende mõistete abil mõtteid väljendada
- **konkreetne Eesti tingimustele sobiva SSO protokollide ettepanek**
- **rohkem kui üks arendusfirma, kes suudab SSO-d teostada**
- e-teenuste omanikud, kes suudavad SSO-d oma teenustes kasutusele võtta

Edasine tegevuskava

- Osalemine Arhitektuurinõukogus sügisel 2020 identiteedi- ja pääsuhooduse töörühmas ja avalikes aruteludes
- Riikliku SSO arenduste algus märts 2021
- Riikliku SSO piloteerimine (SMIT, RIA) 2021 lõpp – 2022 algus
- Riikliku SSO live keskkonda viimine 2022 I pa



RIIGI INFOSÜSTEEMI AMET

Aitäh!

Helen Raamat

helen.raamat@ria.ee

TÄNAME OSALEMAST!

"Tark e-riik" ürituste sarja korraldab Riigi Infosüsteemi Amet Euroopa Liidu struktuuritoetuse toetuskeemist "Infoühiskonna teadlikkuse tõstmine", mida rahastab Euroopa Regionaalarengu Fond. Üritust aitas läbi viia Publicon.



RIIGI INFOSÜSTEEMI AMET



Euroopa Liit
Euroopa
Regionaalarengu Fond



Eesti
Tuleviku Heaks

TARK



e-RIIK

