RIIGI INFOSÜSTEEMI AMET

Riigi autentimisteenus (TARA)

tehniline tutvustus ja tulevikuvaade

Priit Parmakson (Riigi Infosüsteemi Amet)

Rasmus Sööt (AS Nortal)

Millest räägime?

1. Riigi autentimisteenuse tutvustus
2. TARA tehniline ülevaade
3. TARA tehnilisest suunast
    1. Üleminek mikroteenusarhitektuurile
    2. Ühekordse sisselogimise (SSO) lisamine
4. eIDAS otseautentimise demo (Rasmus Sööt)
5. Kogukonna arendustest

1 Riigi autentimisteenuse tutvustus

- Keskne autentimisteenus avaliku ülesande täitjale, kes soovib:
  - oma e-teenuses pakkuda kasutajatele laia valikut autentimismeetodeid, ise neid meetodeid teostamata
  - lisada oma e-teenusele piiriülese autentimise toe (eIDAS määruse järgselt kohustuslik avalikele e-teenusetele 29. septembrist 2018).
- Siseriiklik autentimine:
  - ID-kaart, mobiil-ID, pangad (kuni 2019 IV kv lõpuni), Smart-ID (alates 2019 IV kv keskpaigast).
- Piiriülene (eIDAS) autentimine:
  - Hispaania, Saksamaa, Itaalia, Belgia, Luksemburg
  - lähitulevikus lisanduvad ka teised teavitatud eID skeemidega riigid (Horvaatia, Portugal, Suurbritannia).

Riigi autentimisteenus

- Riigi autentimisteenuse tarkvara tehniline nimi on TARA.
- Riigi keskset autentimisteenust pakub Riigi Infosüsteemi Amet.
- https://e-gov.github.io/TARA-Doku/

Kuidas liituda?

- E-teenus liidestatakse TARAga OpenID Connect protokolli kohaselt.
- Liitumiseks tuleb:
  - välja selgitada, kas ja millistes e-teenustes TARA soovitakse kasutada
  - teostada arendus
  - esitada RIA-le taotlus teenusega liitumiseks
  - testida liidest RIA testteenuse vastu
  - eduka testimise järel taodelda ühendamist toodanguteenusega.
- Liitumise info RIA veebis: https://www.ria.ee/et/riigi-infosusteem/eid/partnerile.html#tara.

Riigi autentimisteenus numbrites (1)

Teenuse kasutajad:

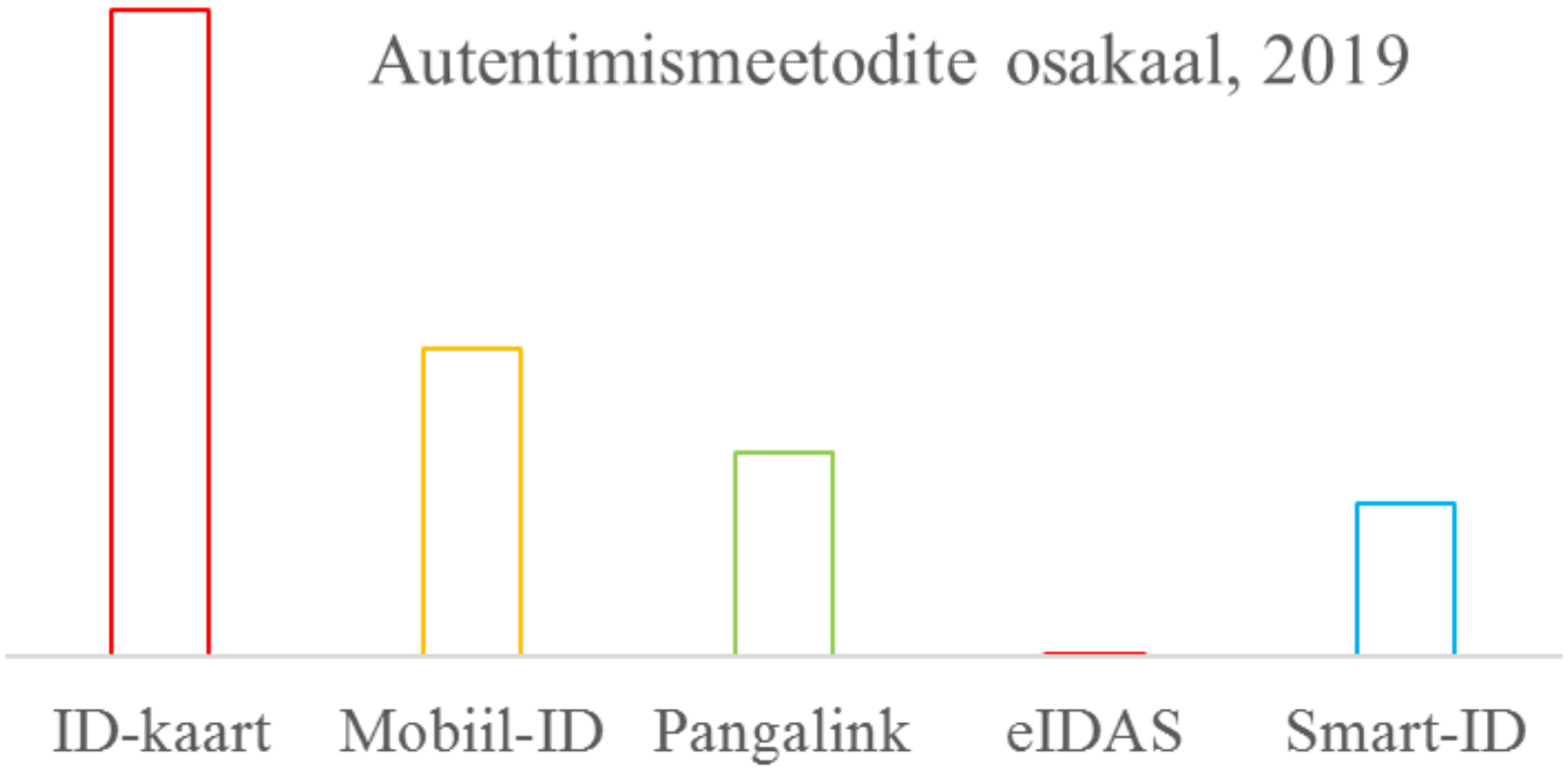
- 23 asutust (toodangus)
- 140 klientrakendust liitunud testkeskkonnaga
  - sh CAS halduses 187
- 60 klientrakendust liitunud toodangukeskkonnaga
  - sh CAS halduses 81.

Keskmiselt 23 kasutajatoe pöördumist kuus.

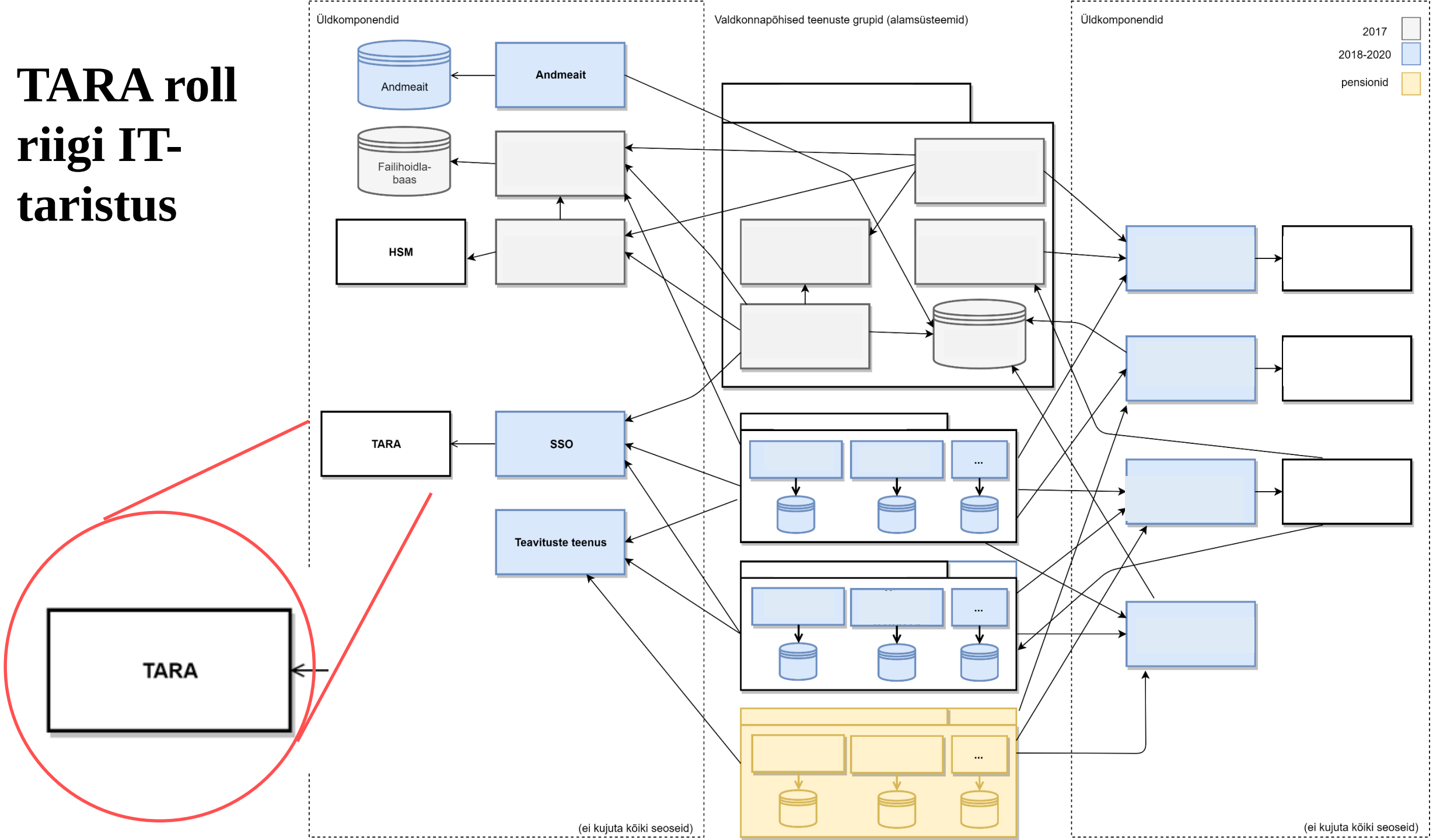
Riigi autentimisteenus numbrites (2)

Autentimiste statistika (2019. a 11 kuud)

- ID-kaart: 1 712 219
- mobiil-ID: 815 371
- pangalink: 542 592
- Smart-ID: 403 395
- eIDAS: 240



TARA roll riigi IT-taristus



2 TARA tehniline ülevaade

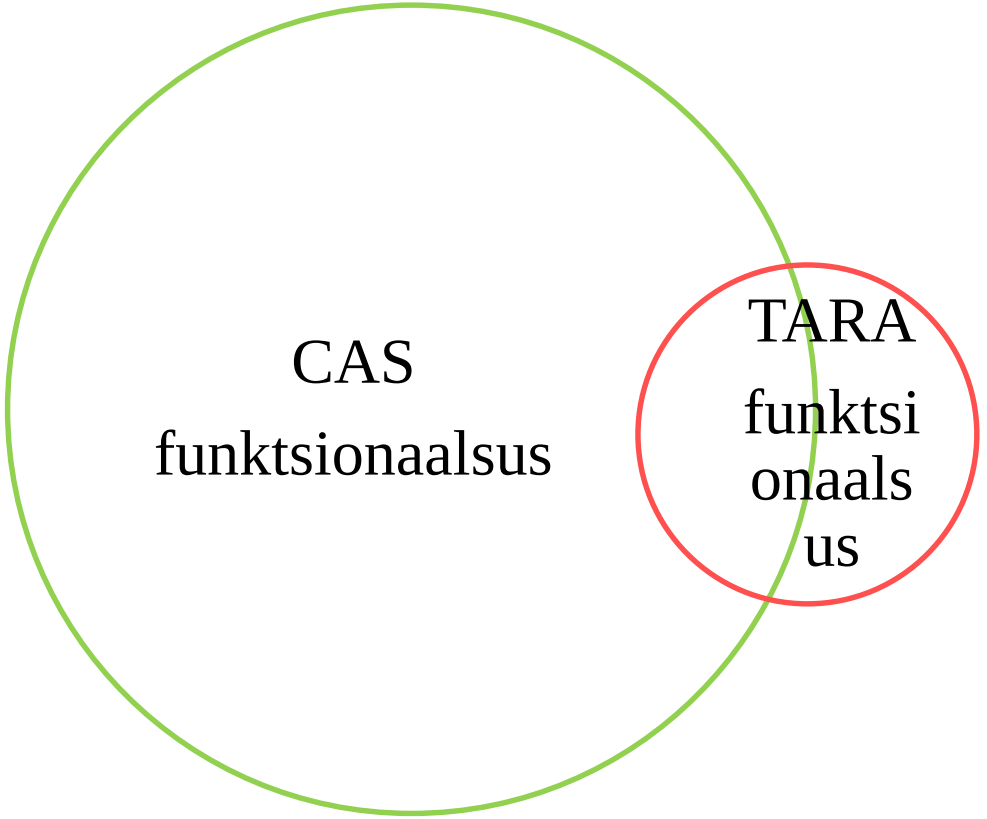
(https://e-gov.github.io/TARA-Doku/TehnilineKirjeldus abil)

3.1 TARA tehnilisest suunast: Üleminek mikroteenusarhitektuurile

- Praeguse TARA platvormi väljakutsed
- Kuidas leida sobiv alternatiiv?
- Ülevaade sobivatest lahendustest
- Kuidas alternatiive rakendada?
- Millised on järeldused?

TARA platvormi väljakutsed

- Funktsionaalselt ebasobiv karbitoode
- Muudetud karbitoode = hooldamise probleem



Kuidas leida sobiv alternatiiv?

- Alternatiivi sobivuse hindamine on keeruline.
- Kokkuvõttes peab alternatiiv olema:
  - vaba tarkvara nõuetele vastav
  - OIDC standardit järgiv
  - tagasiühilduv TARA praeguste klientide jaoks
  - RIA MFN-i järgiv.

Tarkvaratoodete võrdlemise metoodika (1)

- 29 kriteeriumi, rühmitatud 4 rühma (üldomadused, funktsionaalsus, hooldatavus, töökindlus).
- Detailseks hindamiseks valiti 6 toodet (ORY Hydra, Node oidc-provider, MITREId-Connect, KeyCloak, IdentityServer, OpenAM).

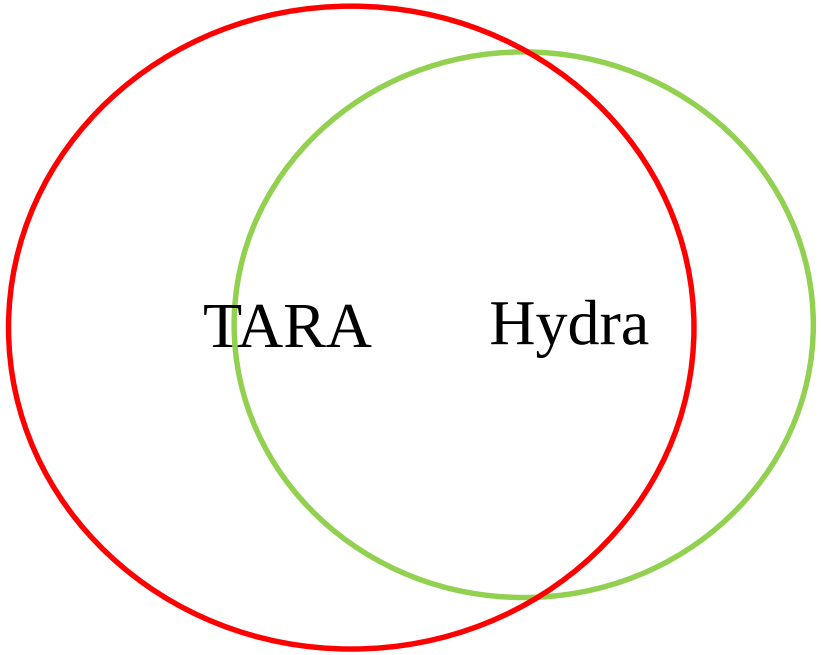
- Üldomadused
  - 0.1 Litsents - 0.2 Keel - 0.3 Vastutav arendaja? - 0.4 Kuidas raha teenitakse?
- Funktsionaalsus
  - 1.1 Protokolli tagasiühilduvus - 1.2 OIDC/OAuth 2.0 lisafunktsionaalsus - 1.3 Mittevajalik lisafunktsionaalsus - 1.4 Vastab OIDC spetsifikatsioonile - 1.5 Haldusliidese olemasolu - 1.6 Andmemudeli sobivus - 1.7 Autentimisskeemide täiendatavus - 1.8 HSM toe võimaldamine.

Tarkvarade võrdlemise metoodika (2)

- Hooldatavus
  - 2.1 Vastab vaba tarkvara põhimõtetele - 2.2 Lähtekood avalik ja versioneeritud - 2.3 Aktiivne arenduskommuun - 2.4 Selge hooldus- ja arendustsükkel - 2.5 Selged ja ajakohased juhised kasutamiseks - 2.6 Paigaldamine täielikult automatiseeritav - 2.7 Andemudeli initsialiseerimine rakenduse väliselt - 2.8 Tugi andmete migreerimiseks versioonivahetusel - 2.9 Sõltuvate infra komponentide väljavahetatavus - 2.10 Logimise täiendatavus - 2.11 OAuth2 parimate turvapraktikate järgmine - 2.12 Programmeerimiskeel.
- Töökindlus
  - 3.1 Testidega kaetus - 3.2 Horisontaalselt skaleeritav - 3.3 Regulaarselt hooldatav - 3.4 Toodangus kasutusel - 3.5 Monitooringuvõimaluste olemasolu.

Toodete uurimine ja hindamine

- Mahukad karbitooted (KeyCloak, IdentityServer, OpenAM, Gluu jt) ei sobi.
- Üks erand - ORY Hydra mikroteenus
  - Erisusi spetsifikatsiooni tõlgendamisel
  - Go keeles
  - Küsitavusi RIA MFN nõuetele vastavuses.



ORY / Hydra

Ülevaade teekidest

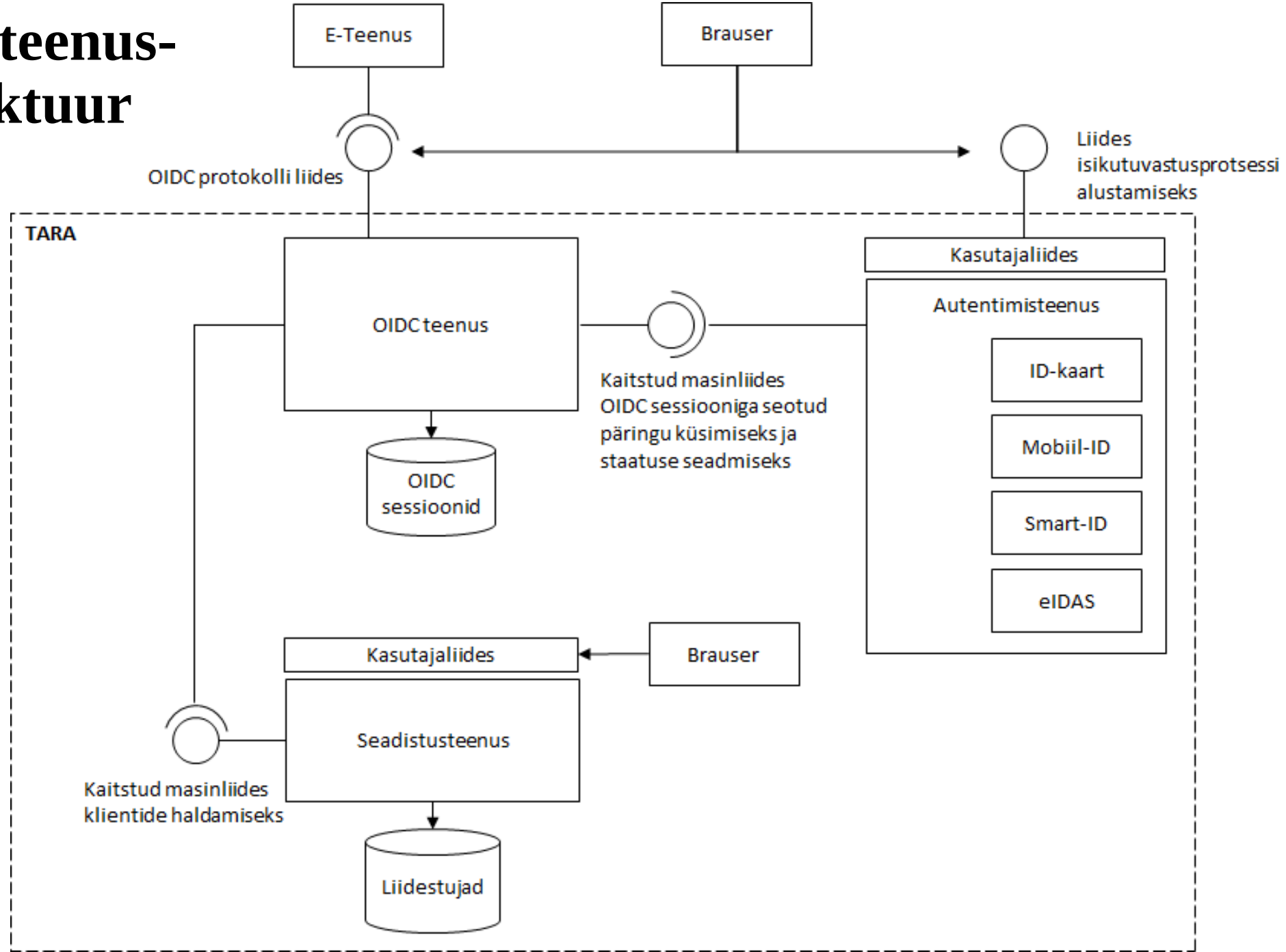
- Java teek – MITREId Connect
  - Käimas suured ümberkorraldused allolevas raamistikus
  - Erisusi spetsifikatsiooni tõlgendamisel.

- JavaScript teek – Node oidc-provider
  - Üks võtmearendaja
  - Volatiilne versioonihalduspoliitika.

Kuidas alternatiive rakendada?

- Arhitektuur peaks olema paremini fokusseeritud TARA vajadustele.
- Muuta OIDC ja autentimisvahendite toe pakkumine eraldi evitatavateks teenusteks.
- OIDC protokolli parem isoleeritus.
- Muudatused protokollis ja autentimisvahendites üksteisest sõltumatuks.
- OIDC spetsiifiiline osa lihtsamini väljavahetatavaks ja keeleagnostiliseks.

Mikroteenus-arhitektuur



Kulude võrdlus

Mikroteenusarhitektuurile üleminek

töömaht inimkuudes

arendaja - 9, testija - 5, kokku **13** inimkuud

Tasuvusaeg u **3** aastat

TARA v1.5 raames uuele CAS põlvkonna (v6.x) tarkvarale üleminek

arendaja - 4, testija - 1, kokku **5** kuud

Tehnilise analüüsi kokkuvõte

- Praeguse lahenduse tehniline võlg jääb suurenema.
- "Hõbekuuli" hooldatavuse osas ei ole - alustooted muutuvad.
- Eelistada rätseplahendust karbitoote täiendamisele.
- Tarkvara arhitektuur peab olema fokusseeritud TARA vajadustele.
- Muudatused kliendi protokolli ja autentimisvahendite osas peaks olema üksteisest sõltumatud.
- Sobivaimad kandidaadid:
  - Hydra teenus ja NodeJS.
- MITREId Connect kasutuselevõtuga tasuks oodata.

3.2 Ühekordse sisselogimise (SSO) lisamine

- SSO protokolli disainimine
- POC
- Kasutatavuse uuring
- Turvauuring

- Teostus
- Evitamine.

4 Kogukonna arendustest: TARA-Go

https://koodivaramu.eesti.ee/e-gov/TARA-Go

TARA klient Go keeles

main.go

```go
package main

import (
  "fmt"
  "log"
  "net/http"
  "os"

  tara "github.com/e-gov/TARA-Go"
)

func main() {
  client, err := tara.NewClient(tara.Conf{
    Issuer:                "https://tara-test.ria.ee",
    AuthorizationEndpoint: "https://tara-test.ria.ee/oidc/authorize",
    TokenEndpoint:         "https://tara-test.ria.ee/oidc/token",
    JWKSURI:               "https://tara-test.ria.ee/oidc/jwks",
    RedirectionURI:        "",
    ClientIdentifier:      "",
    ClientSecret:          "",
    Scope:                 []string{"idcard", "mid", "smartid"},
    RequestLogger:         log.New(os.Stdout, "tara: ", log.LstdFlags),
  })
  if err != nil {
    panic(err)
  }
```

Kogukonna arendustest: TARA-Mock

https://github.com/e-gov/TARA-Mock

TARA-Mock on teenus, mis teeb TARA autentimise suvalise testkasutajaga, kui vaja, siis ka inimese sekkumiseta.