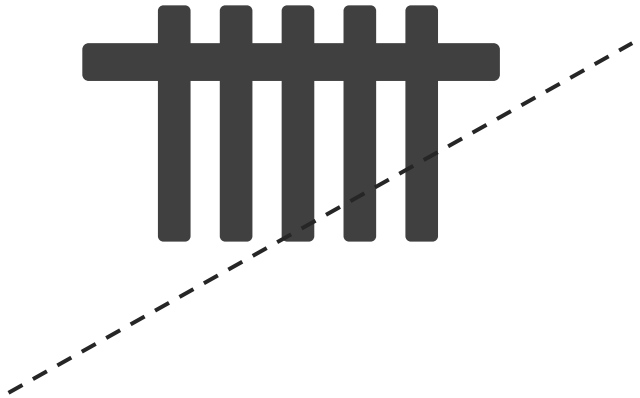
Piiriülene autentimine

tehniline lahendus



Priit Parmakson, RIA

Usaldusteenuste infopäev 15.11.2017

Oleme üles ehitanud sadade avalike teenustega e-riigi.

riigiteenused.ee-s on kirjeldatud 1560
avalikku teenust

Kasutaja autentimist on vaja praktiliselt igas e-teenuses.

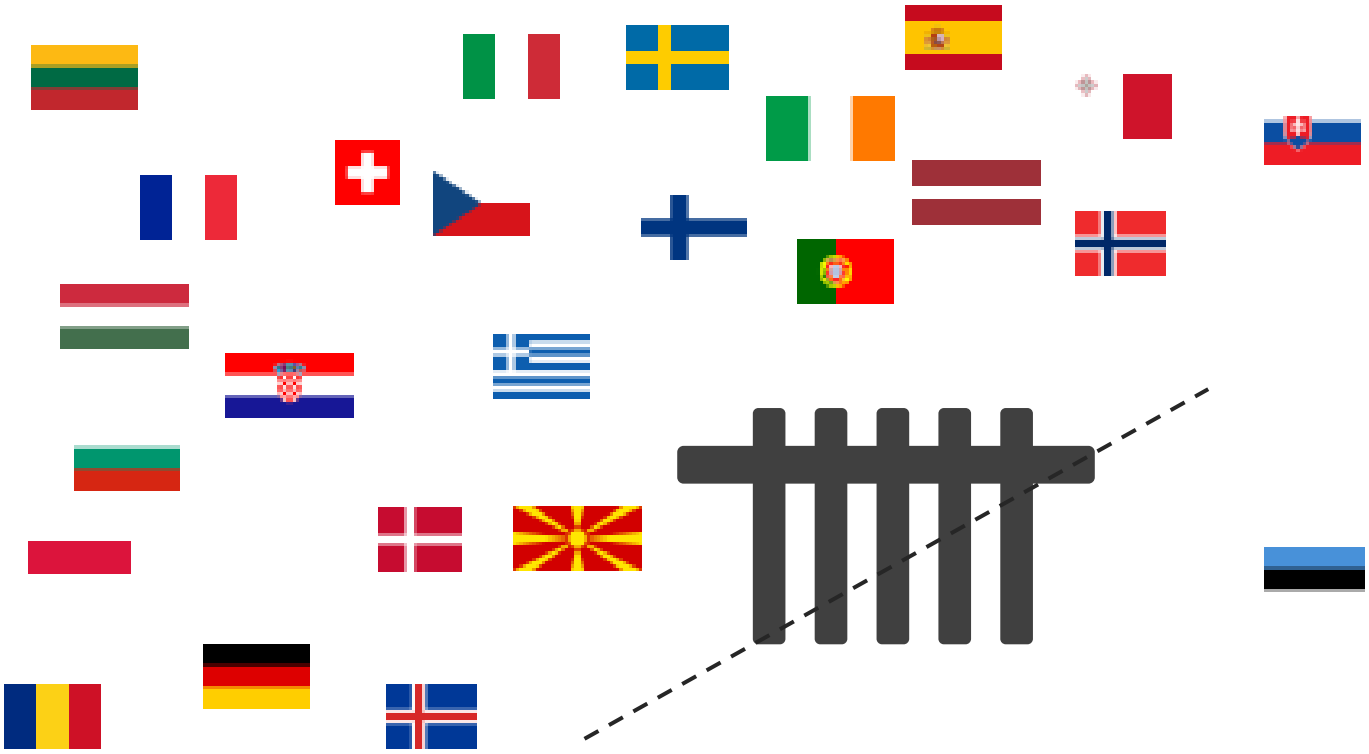
Kuid seni suudavad meie teenused tuvastada ainult

Eesti identiteedisüsteemi (ID-kaart, mobiil-ID)

kasutajaid.

Avalike e-teenuste piiriülene kasutamine nõuab piiriülest autentimist.

Piiriülene autentimine tähendab seda, et teise riigi identiteedisüsteemi kasutajat ei tohi enam jätta ukse taha.



Alates septembrist 2018.

Piiriülene autentimine nõuab õiguslikku, organisatsioonilist ja tehnilist lahendust.

Õigusraamistik

Piiriülene võrgustik

eIDAS tehnilised spetsifikatsioonid

tarkvara

Autentimine on lihtne:

- *tulemus on 0/1 – isik kas on tuvastatud või ei ole.*

Autentimine ei ole nii lihtne:

- *autentimismeetodeid on > 1*
- *uued autentimisviisid, sh mitmeteguriline*
- *„hägusautentimine“, identity matching*
- *infosüsteemi omanik soovib koos autentimisega pääsuhaldust jm lisateenuseid*
- *autentimine on olemuselt usaldusteenus*
- *autentimine ei ole ühekordne akt, vaid ajas moduleeruv (turva)omadus kasutaja sujuval liikumisel ühtses e-teenuste ruumis*
- *autentimine peab olema piiriülene (eIDAS).*

Kuidas see käib?

Põhimõtteliselt on kolm kasutuslugu:

1 Anu tahab kasutada välismaa e-teenust

Anu on ID-kaardi kasutaja

2 Leif tahab kasutada Estonia e-teenust

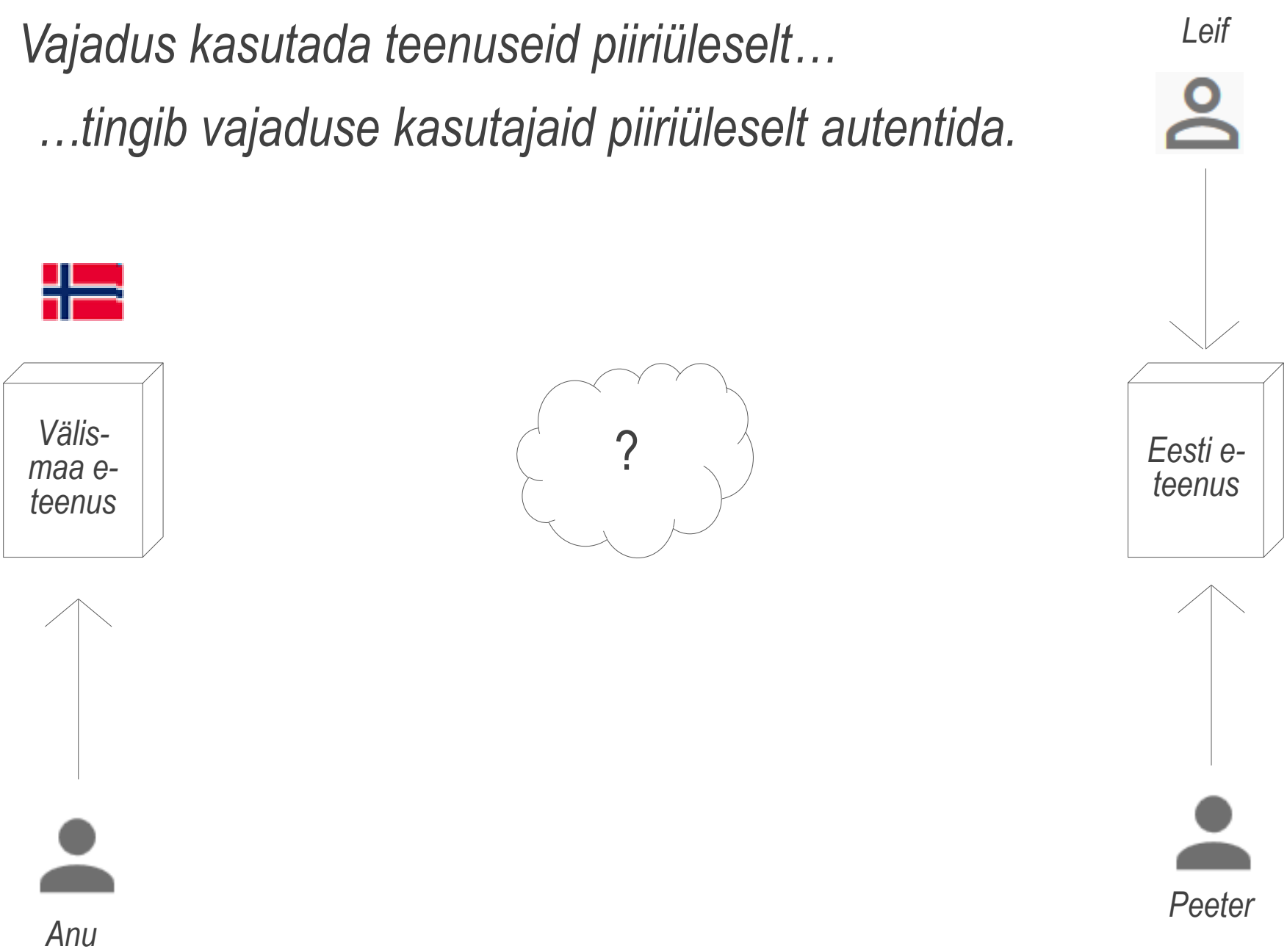

Leif on Norra eID kasutaja

3 Peeter tahab kasutada Eesti e-teenust

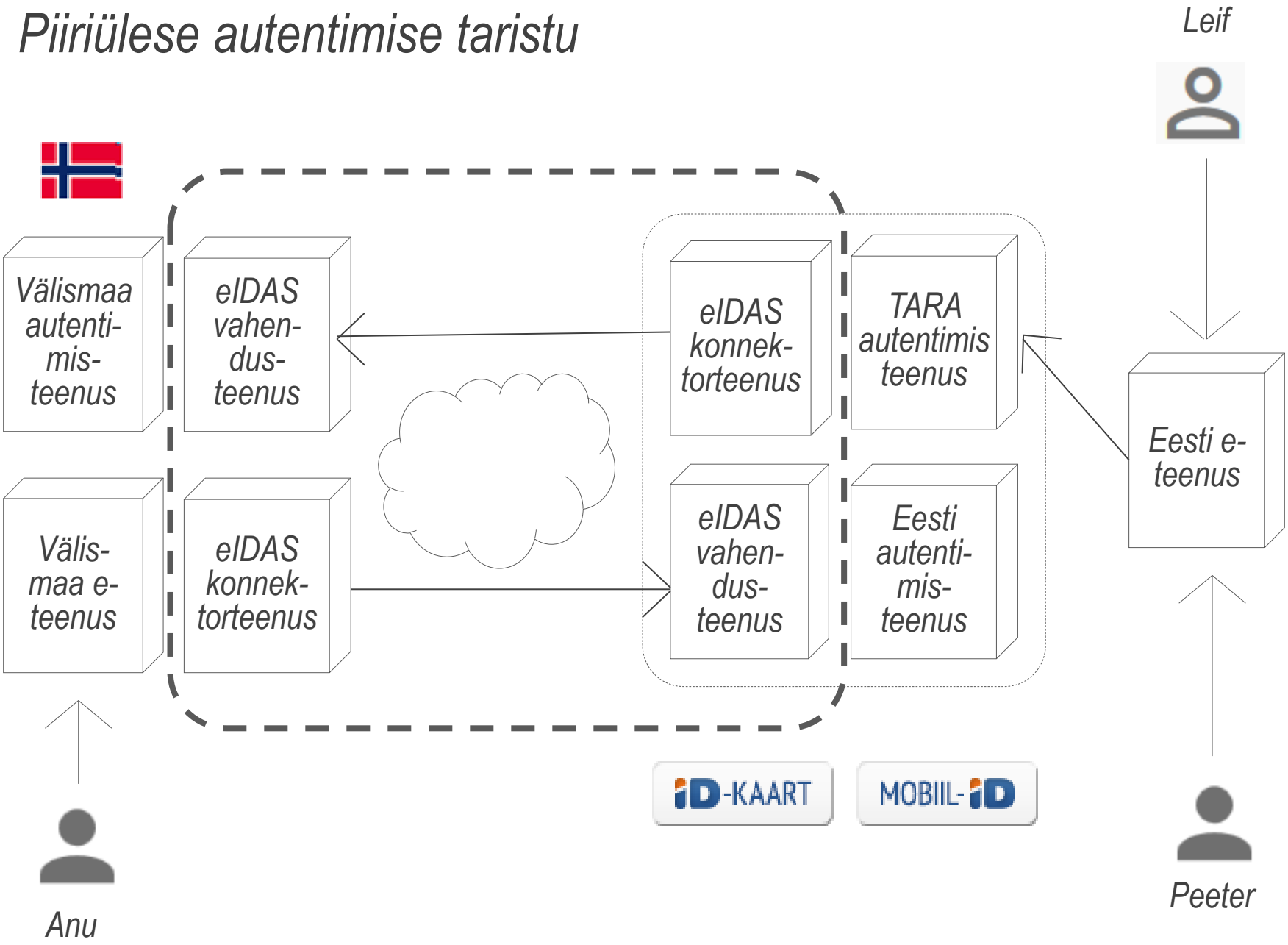
Peeter on m-ID kasutaja

Vajadus kasutada teenuseid piiriüleselt…

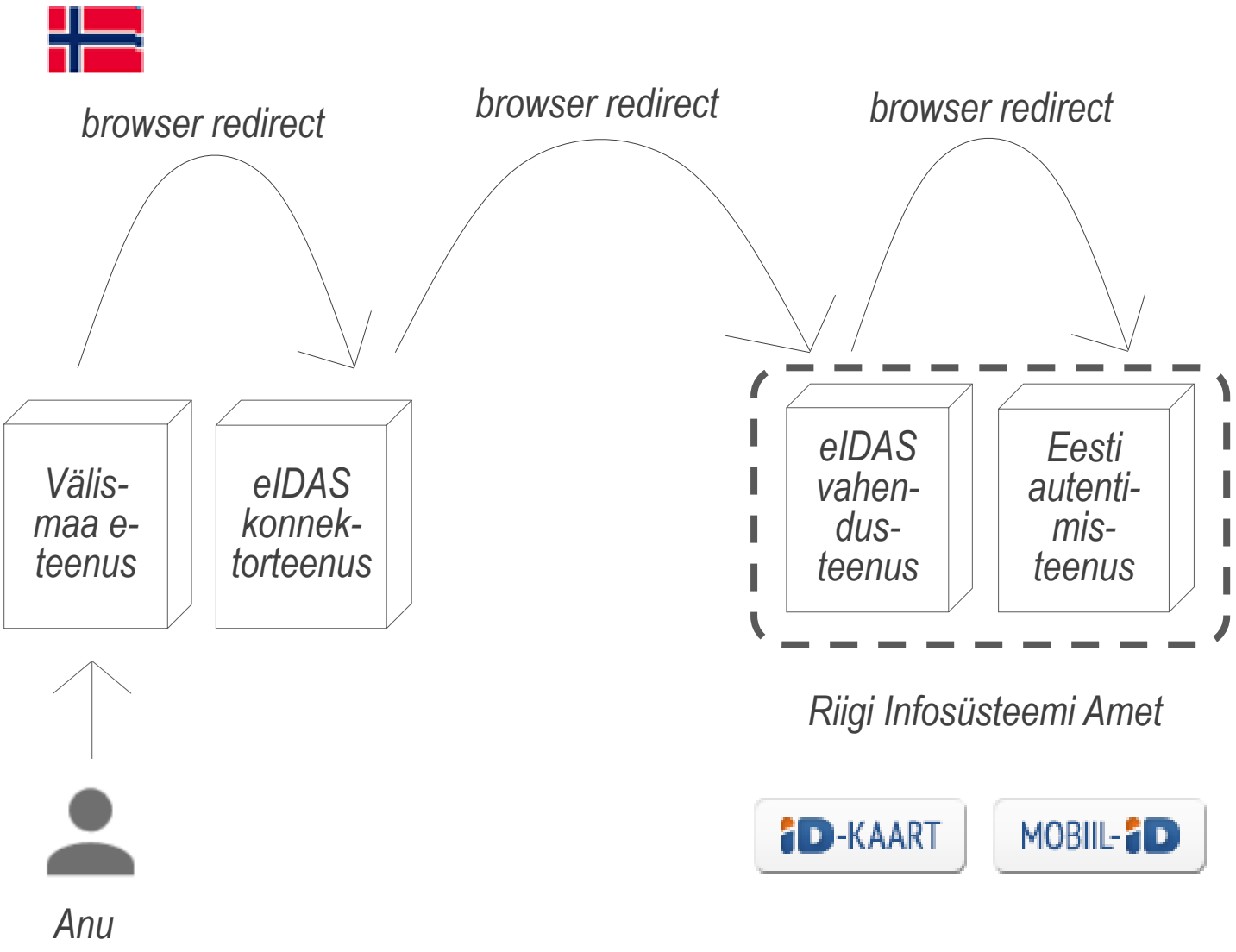
…tingib vajaduse kasutajaid piiriüleselt autentida.



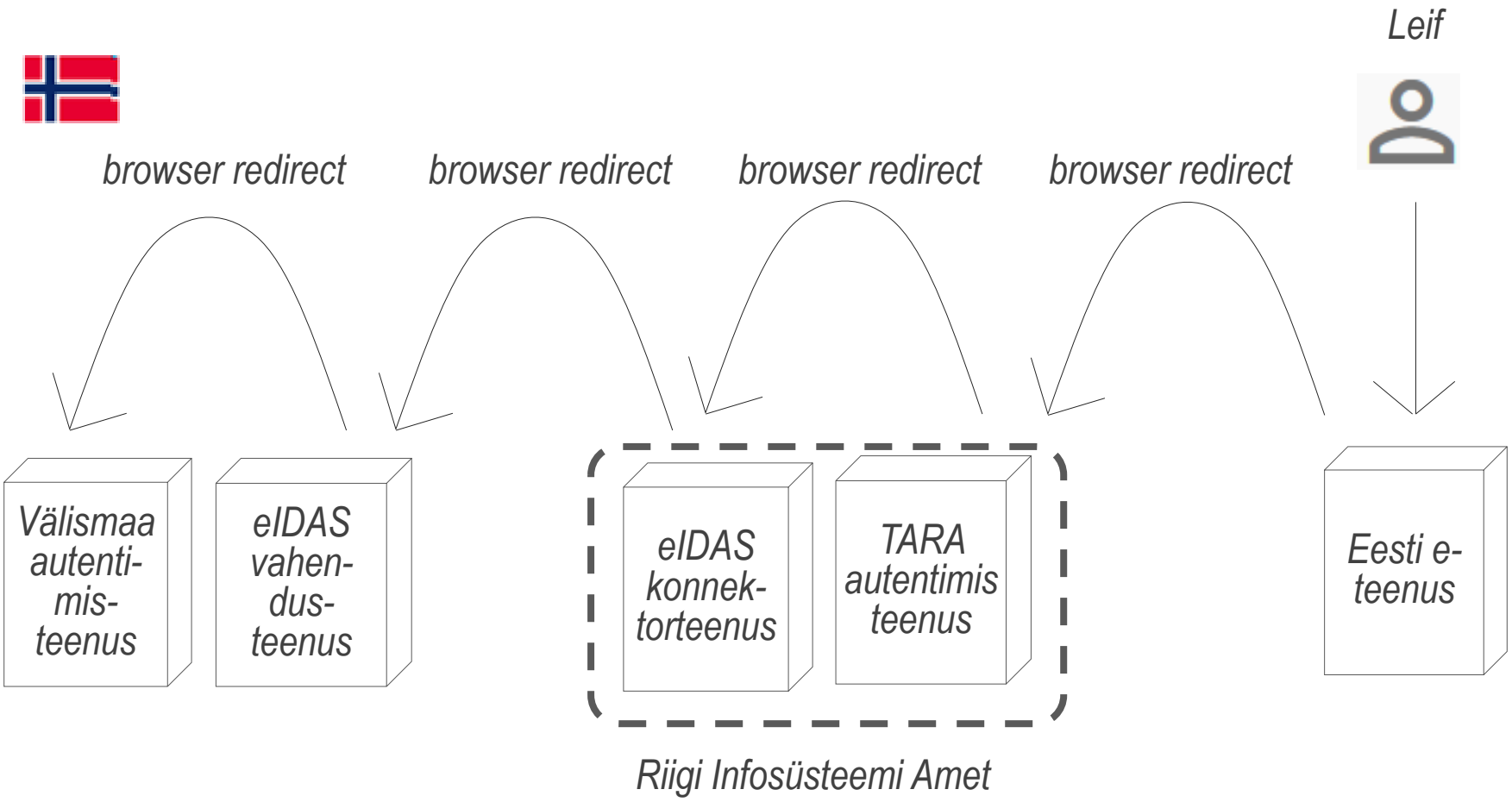
Piiriülese autentimise taristu



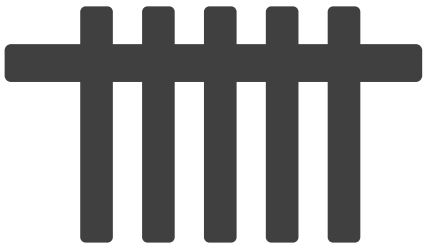
Eestlane välismaa e-teenuses

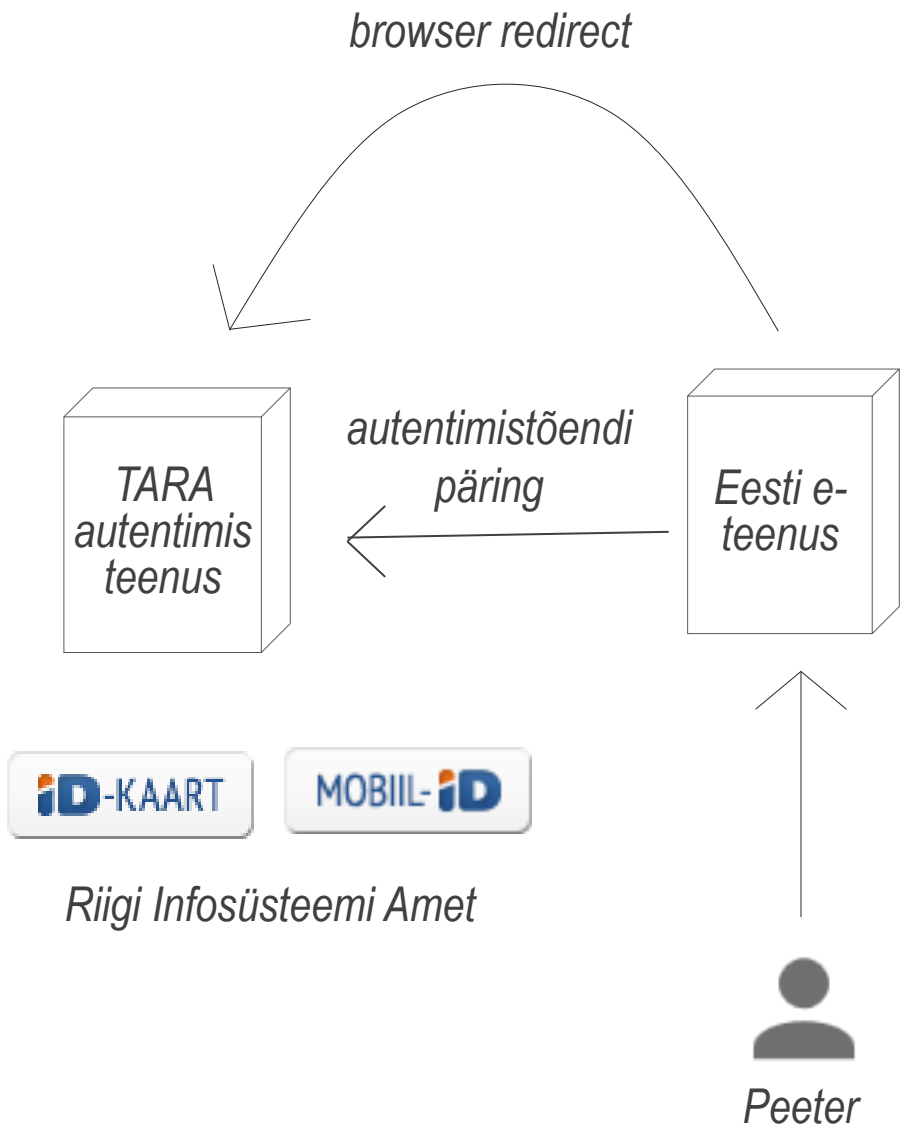


Välismaalane meie e-teenuses



Eestlane Eesti e-teenuses





Kasutaja autentimist on vaja peaaegu igas süsteemis.

riigiteenused.ee-s on kirjeldatud 1560 avalikku teenust

kõik need vajavad autentimist. Hinnanguliselt paarsada erinevat autentimislahendust.

Autentimine ei ole rakendusespetsiifiline funktsioon.

Mõistlik oleks autentimine lahendada out-of-the-box.

Autentida ühe lahendusega, ühes kohas ja anda autentimise tulemus – autenditud kasutaja – e-teenusele.

Out-of-the-box lahendust ei ole tekkinud.

Minu kogemus 4-5 autentimislahenduse arendamisega erinevatele süsteemidele viimase 1,5 a jooksul:

Autentimise tehnilised lahendused ei ole piisavalt standarditud.

ID-kaart on tugeval tasemel. Meil on autentimisnormatiiv, mis annab raamid, kuid ei anna out-of-the-box lahendust.*

- tellija ei oska detailset ülesannet püstitada

- arendaja ei saa tööga hakkama

- happy path tehakse valmis, veaolukordade käsitlus jääb puudulikuks

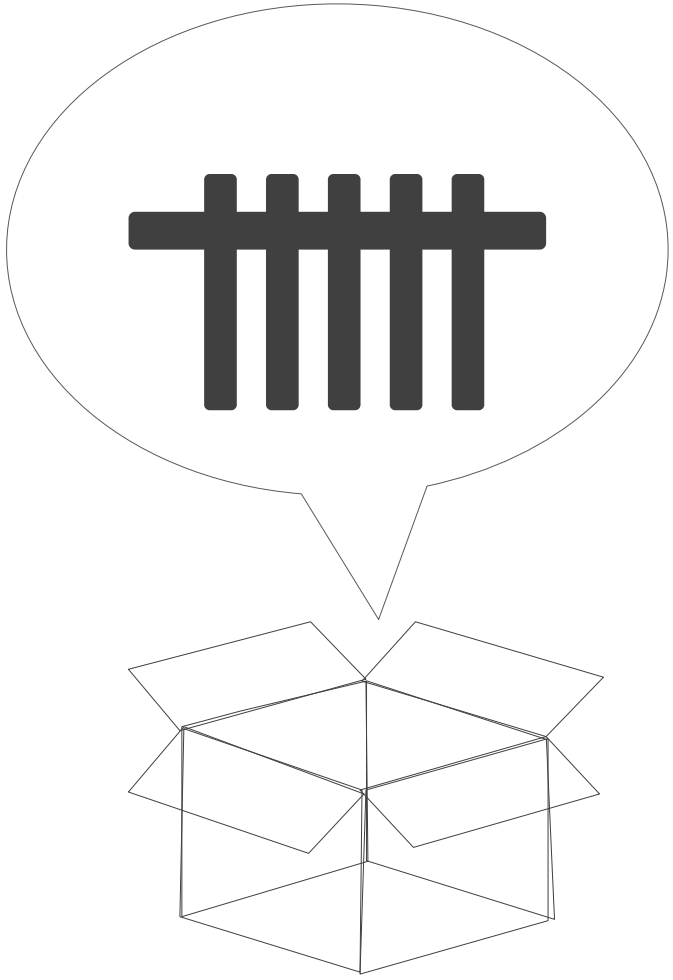
- admin ei ole konfimise üle õnnelik

Autentimislahenduste arendus on kulukas ja aeganõudev.

** Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded, v 1.0, https://www.ria.ee/public/PKI/Autentimislahendustele-kehtivad-nouded.pdf, Riigi Infosüsteemi Amet, 2017.*

TARA idee:

autentimine keskse teenusega
- lihtsalt kasutatav, out-of-the-box lahendus
- ühitab siseriikliku ja piiriülese
- platvorm täiendavatele teenustele.



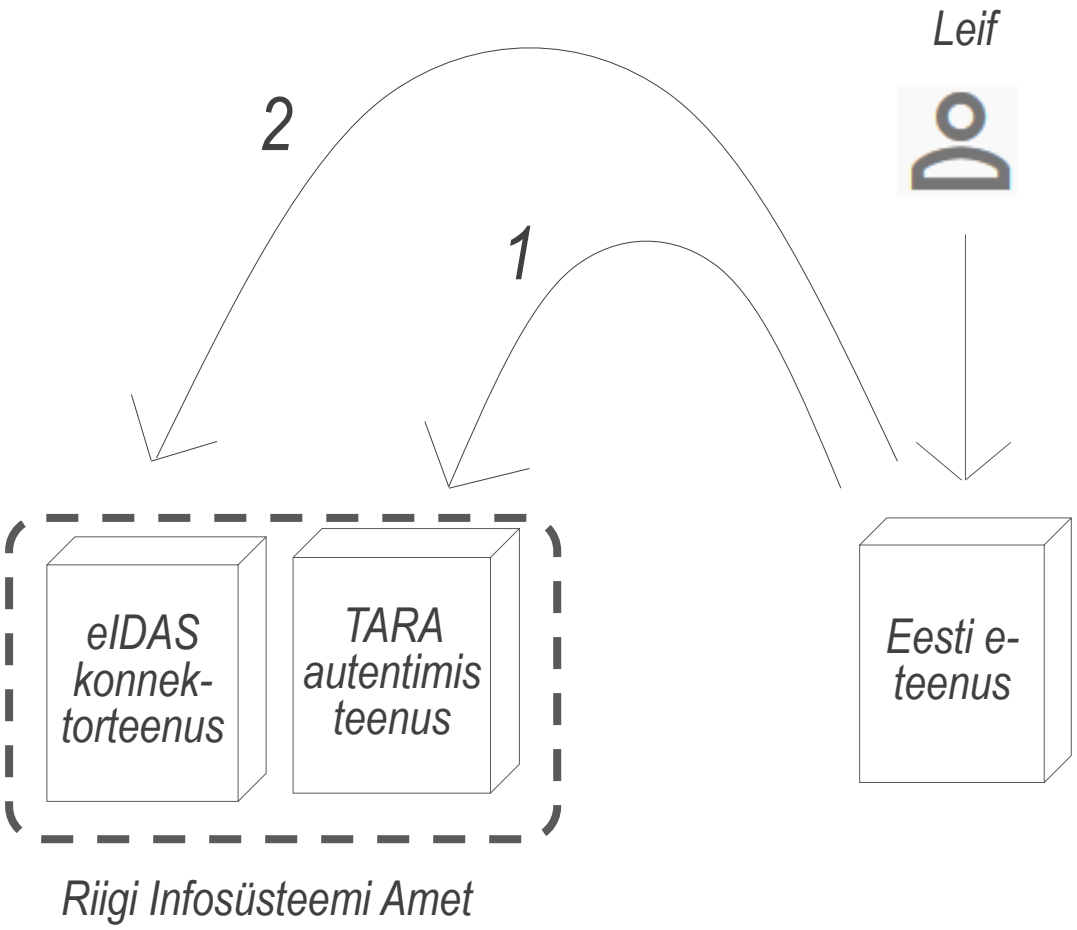
Kaks võimalust liidestumiseks

1

TARA külge

2

otse eIDAS konnektorteenuse külge



RIA pakub – Eesti asutustele:

- *TARA autentimisteenus*
  - *OpenID Connect protokoll*
  - *nii siseriiklik kui ka piiriülene autentimine*
  - *ID-kaart, m-ID, kavas lisada teisi meetodeid*
  - *sobib kõigile, ka väikestele asutustele*
- *eIDAS konnektorteenus*
  - *SAML protokoll*
  - *suurtele asutustele, kes soovivad autentimise UI ise lahendada*

RIA pakub – välismaa asutustele:

- *välismaa e-teenust kasutava eestlase autentimist*
  - *eIDAS taristu kaudu*
  - *ID-kaart, m-ID*
  - *esindusõiguste päring Äriregistrisse*

Tegemisel ja tehtu

TARA autentimisteenus

test	*avatud* ✓
toodang	*kui esimene liidestuja on valmis*
ID-kaart, m-ID	*valmis* ✓
eIDAS	*valmib veebruar-märts 2018*

eIDAS konnektorteenus

test	*avatud* ✓
toodang	*kui esimene liidestuja on valmis*

TARA autentimisteenus

www.ria.ee/ee/autentimisteenus-tara.html

eIDAS konnektorteenus

https://github.com/ria-eidas/eidas-node/blob/master/eIDAS-Konnektorteenus.md

Demo

https://tara-client-py.herokuapp.com/

http://samategev.herokuapp.com

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

Teekaart *(mida kõike võiks teha)*

A/B testimise valimiteenus

teadete sundusliku kättetoimetamise teenus

SAP-i integratsioon?

kasutaja nõusoleku võtmise teenus

kasutusstatistika tootmise teenus

kasutajat kirjeldavate atribuutide väljastamise teenus

kasutaja rollide väljaselgitamise teenus

rolli valimise teenus

ühekordne sisselogimine (SSO)

ühekordne väljalogimine

Pangalingid

Smart-ID

eksootiliste autentimismeetodite teenus

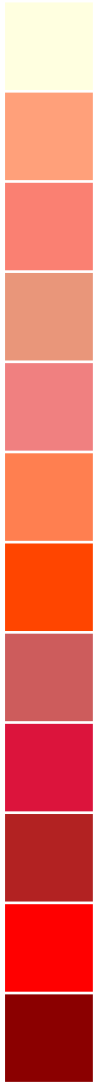
eIDAS

Platvorm: OpenID Connect, ID-kaart, m-ID

Autentimisteenuse turvauuring, kavas 2018

Riskid:

Uuringu fookus



1 teenuse järele ei ole reaalset vajadust

2 kasutaja ei saa teenusest aru

3 asutuste võimekus (organisatsiooniline, finantsiline, tehniline) teenust kasutusele võtta on madal

4 valitud tehniline kontseptsioon osutub ebaturvaliseks

5 valitud tehniline kontseptsioon osutub mitteteostatavaks

6 valitud tehniline kontseptsioon osutub mittejätkusuutlikuks

7 turul ei leidu kompetentset, huvitatud arendajat

8 turul ei leidu kompetentseid liidestuste arendajaid

9 RIA võimekus teenuse arendust tellida osutub ebapiisavaks

10 RIA võimekus teenust käitada osutub ebapiisavaks

11 teenus kokkuvõttes ei tasu end ära.

TARA autentimisteenuse demo

TARA on teenus, millega avaliku sektori asutus saab e-teenuses autentida nii Eesti kui ka teisest EL riigist tulnud kasutaja.

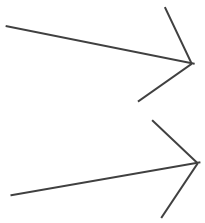
Tere, `PRIIT PARMAKSON`!

Autentimistõend:

```
{ aud: 'ParmaksonResearch',
  iss: 'https://tara-test.ria.ee',
  jti: '267c097a-71ca-41d4-98fb-d6159676b2e
  exp: 1510614185,
  iat: 1510585385,
  nbf: 1510585085,
  sub: 'EE36107120334',
  profile_attributes:
    { family_name: 'PARMAKSON'
      given_name: 'PRIIT',
      mobile_number:
    },
  amr: [ 'AcceptUsersAuthenticationHandler'
  state: 'msTeDi9GREgJnUA0',
  nonce: ''
}
```

Autentimise kohta väljastatav tõend

Turvaelemendid



Head autentimist!