TARA uuendustest

Priit Parmakson
Riigi Infosüsteemi Amet

TARA uuendustest

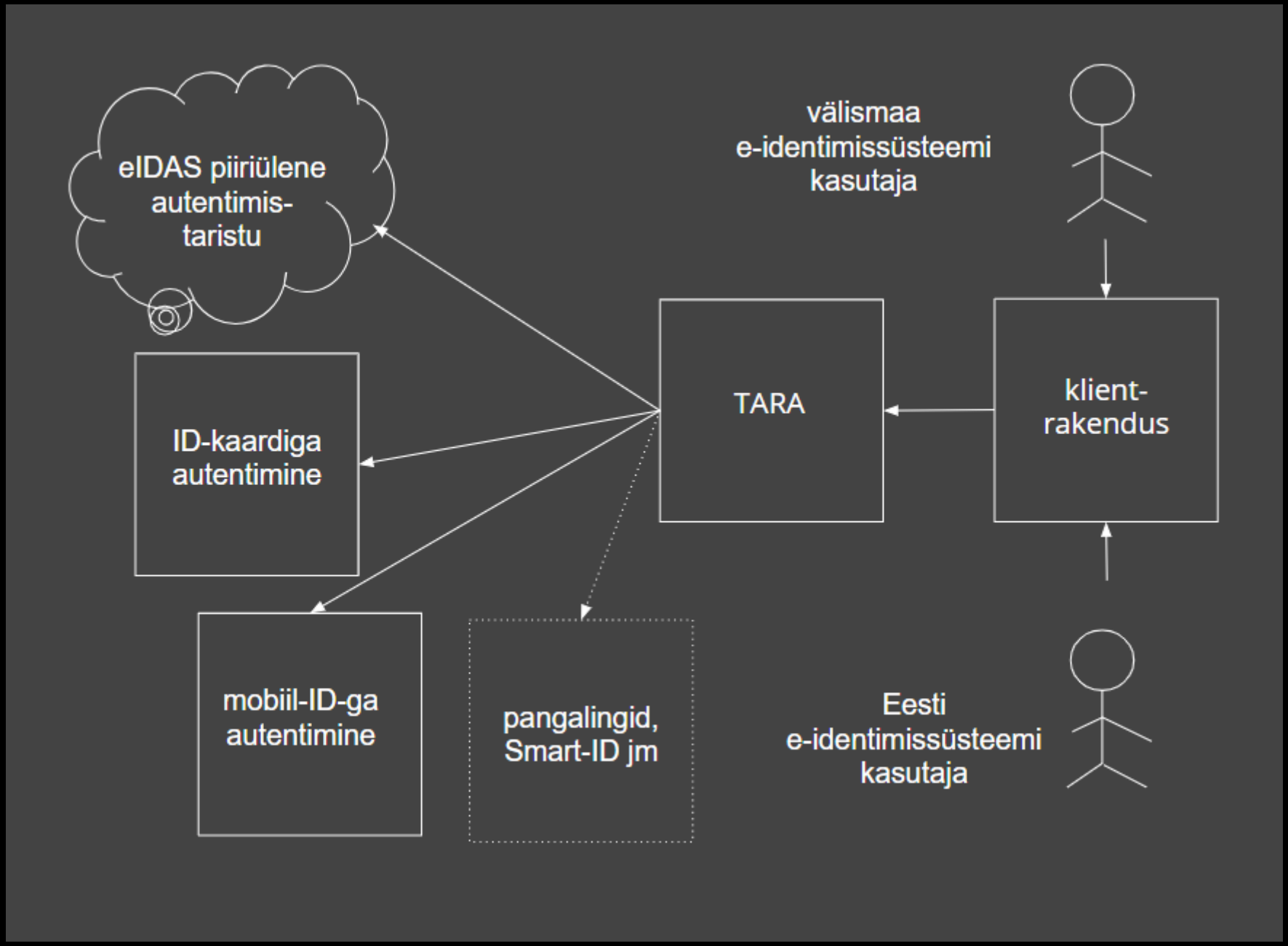
- Eesmärk
- Seis
- Muutusvajadused – välismaised
- Hea ja töötava säilitamine
- Keskse nuripunkti vältimine
- Kindlam protokoll
- Turvalisem platvorm
- Seansihalduse (SSO) lisamine
- Atribuutide pakkumine
- Uute autentimismeetodite tugi

Eesmärgid

- Pakume teenust, millega Eesti asutus saab autentida nii siseriikliku kui ka teisest EL riigist tuleva kasutaja -
- erinevate autentimismeetoditega
- ja turvaliselt.

- Teenusega on lihtne liituda ja liidestuda.

- Teenust pakume "Riigi autentimisteenuse" kaubamärgi all.


eIDAS piiriülene autentimis-taristu
välismaa e-identimissüsteemi kasutaja
ID-kaardiga autentimine
TARA
klient-rakendus
mobiil-ID-ga autentimine
pangalingid, Smart-ID jm
Eesti e-identimissüsteemi kasutaja

Seis

- Liitunud 40 infosüsteemi (toodangus)
- liitumas 90 infosüsteemi (testis)
- piiriülene autentimine töötab (4-5 EL riiki)
- siseriiklik autentimine töötab
- teenuse dok-n, nõustamine, kasutajatugi – töötab.

- 2018. II pa. – 2019. I pa fookus: käideldavus, kasutatavus, turvalisus.

Muutusvajadused - välismaised

- Piiriülene autentimine käib RIAs asuva eIDAS sõlme kaudu.
- Kasutusel on Euroopa Komisjoni tarkvara eIDAS Node.
- Komisjon on eIDAS protokolli muutnud. Senise tugi kaob. Peame kasutusele võtma eIDAS 2.x. See tingib siseriikliku liidestusprotokolli ümbertegemise vajaduse.
- Tehniline prototüüp (POC) 2019 suvel, aasta lõpul teostus.
- TARA klientrakenduse vaatest jääb kõik samaks.
- Kapseldame teie eest Euroopast tuleva keerukuse.

Hea ja töötava säilitamine (I)

- Kõik muutused ei olegi head. Head ja töötavat peab hoidma.
- Tagame TARA protokolli stabiilsuse. Väldime olemasolevat katkitegevaid lisandusi.
- Kui alustasime, võtsime OpenID Connect protokollist ainult minimaalselt vajaliku.
- Selgus, et paljud liidestajad tahavad kasutada teeke, mis eeldavad OpenID Connect laiemat toetust. Oleme lisanud võimalusi (nt `kid`).
- Laiem skoopide valik: `idcard`, `mid`, `banklink`, `smartid`, `eidas`, `eidasonly`. Annab võimaluse valida ainult soovitavad autentimismeetodid.

Hea ja töötava säilitamine (II)

- Tahame hoida teenuse tasuta. Samas teenuse sisendid ei ole tasuta.
- Optimeerime kulusid: AIA kasutuselevõtt, koos dünaamilise ümberlülitamisega tasulisele kehtivuskinnitusteenusele.
- Jätkame tööd teenuse kvaliteedi tõstmisel. Kvaliteeti mõistame kolmemõõtmelisena: käideldavus, turvalisus, kasutatavus.
- Tagame isikuandmete kaitse kõrge taseme jätkuvuse. TARA ei profileeri, müü ega edasta teenuse osutamise käigus tekkivaid isikuandmeid. https://e-gov.github.io/TARA-Doku/Isikuandmed

Keskse nuripunkti vältimine

- Vältida olukorda, kus paljude kriitiliste infosüsteemide töö sõltub ühe keskse teenuse ülevalolekust.
- Infosüsteemi autentimine peaks olema ümberlülitatav asutuse oma autentimislahendusest TARA-le ja vastupidi.
- TARA võiks olla käitatav kahes instantsis.
- Kõik see nõuab standardseid liideseid.

Turvalisem protokoll

- Avaliku sektori standardne autentimisprotokoll on OpenID Connect (mis tugineb OAuth 2.0). Algselt mõeldud sotsiaalvõrgustikele, seetõttu kõigis osistes mitte kõige turvalisem.
- Ilmunud on mitmeid standardikavandeid, kuidas OpenID Connect-i ja OAuth-i turvalisemaks teha. Nt *Open ID Connect Token Bound Authentication*, sertide kasutuselevõtmine sümmeetrilise salasõna asemel jm. Analüüsime neid 2019. a.

Kindlam platvorm

- Praegune TARA tarkvara on CAS platvormil, mis sisaldab palju segavat ja mittevajalikku. Analüüsime, kas jätkame senisega või läheme üle uuele platvormile.
- Uuel platvormil (või kui analüüs näitab, et otstarbekas on jätkata senisel) lisame täiendavaid võimalusi (nt klientrakenduste dünaamiline registreerimine).

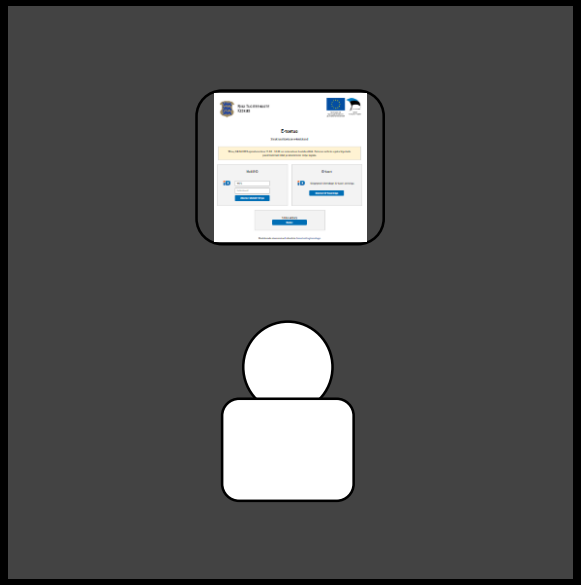
Seansihalduse (SSO) lisamine

- Seni saate TARAst ainult autentimise. Seansi loomine ja pidamine on iga klientrakenduse enda asi.
- Sellel on nii plusse kui ka miinuseid.
- Tuleb arvestada erinevaid *use case*-e.
- Ühekordne sisselogimine (single sign-on, SSO), kui tuleb, ei saa olema kohustuslik. Klientrakendus saab endist viisi võtta TARAst ainult autentimise.
- Üleriiklik SSO nõuab tõenäoliselt ka seansihalduse praktikate teatud ühtlustamist, vähemalt arusaamiste lähendamist. Hakatis on tehtud: https://e-gov.github.io/TARA-Doku/Seansihaldus.

eesti.ee

- Mari kasutab raamatukogu avaliku internetipunkti arvutit. Sulgeb sirviku. Tuleb Jaan. Avab sirviku. Kas seanss tohib olla alles?

e-toetuse süsteem (SFOS)



- Ametnik Mart kasutab süsteemi töökoha arvutist. Sulgeb sirviku ja läheb kohvile. Tuleb tagas ja avab sirviku. Kas ta peab uuesti sisse logima?

Atribuutide pakkumine

- Ahvatlev on autentimisega koos teha päring ühte või teise andmekogusse ja väljastada klientrakendusele lisaks isikut identifitseerivate andmete miinimumkomplektile veel andmeid (nt aadress, e-postiaadress, õigus esindada ettevõtet jne). OpenID Connect protokoll näeb sellist võimalust ette (*UserInfo* otspunkt).
- Praegu oleme konservatiivsed. Väljastame ainult kasutaja eesti.ee aadressi (nt `60001019906@eesti.ee`) ja sedagi ainult ID-kaardiga autentimisel ning mitte *UserInfo* otspunktis, vaid identsustõendis.
- Oleme valmis atribuute pakkuma, kui selleks on piisavalt nõudlust. Seejuures tuleb jälgida, et atribuudil oleks kindel semantika (probleem nt esindusõiguse väljastamisel EL teistesse riikidesse) ja isikuandmete töötlemine oleks põhjendatud.

Uute autentimismeetodite tugi

- Kust king pigistab? Kasutajatoe pöördumiste statistika näitab, et kõige rohkem on muresid ID-kaardiga.
- ID-kaardiga autentimine töötab ilusasti – kui ahela kõik lülid on korralikult seadistatud.
- Sirvikutootjate dünaamilises maailmas ei ole TLS-põhise autentimise stabiilsuse saavutamine lihtne.
- Ootame palju "Web eID" uuringust https://github.com/open-eid/browser-extensions2.