RIIGI NFOSÜSTEEMI AMET

EESTI.EE AUTENTIMISTEENUS

X-tee kogukonna seminar

04.05.2017

Priit Raspel

eIDAS määrus reguleerib, meie teeme…

- 19. september 2018. a.
- need, kes pakuvad avalikkusele suunatud ja avalikus võrgus kättesaadavaid teenuseid, peavad võimaldama teostada autentimist oma infosüsteemi(desse) samade reeglite järgi.
- riigi ja KOV asutustele kohustuslik, teistele vabatahtlik.
- kui paljudele kohustuslik, siis miks mitte teha seda samade vahenditega ?
- ühiseks kasutamiseks loodud vahendite kasutamine on vabatahtlik – kõike võib teha ka ise.

Lahendus: eesti.ee autentimisteenus

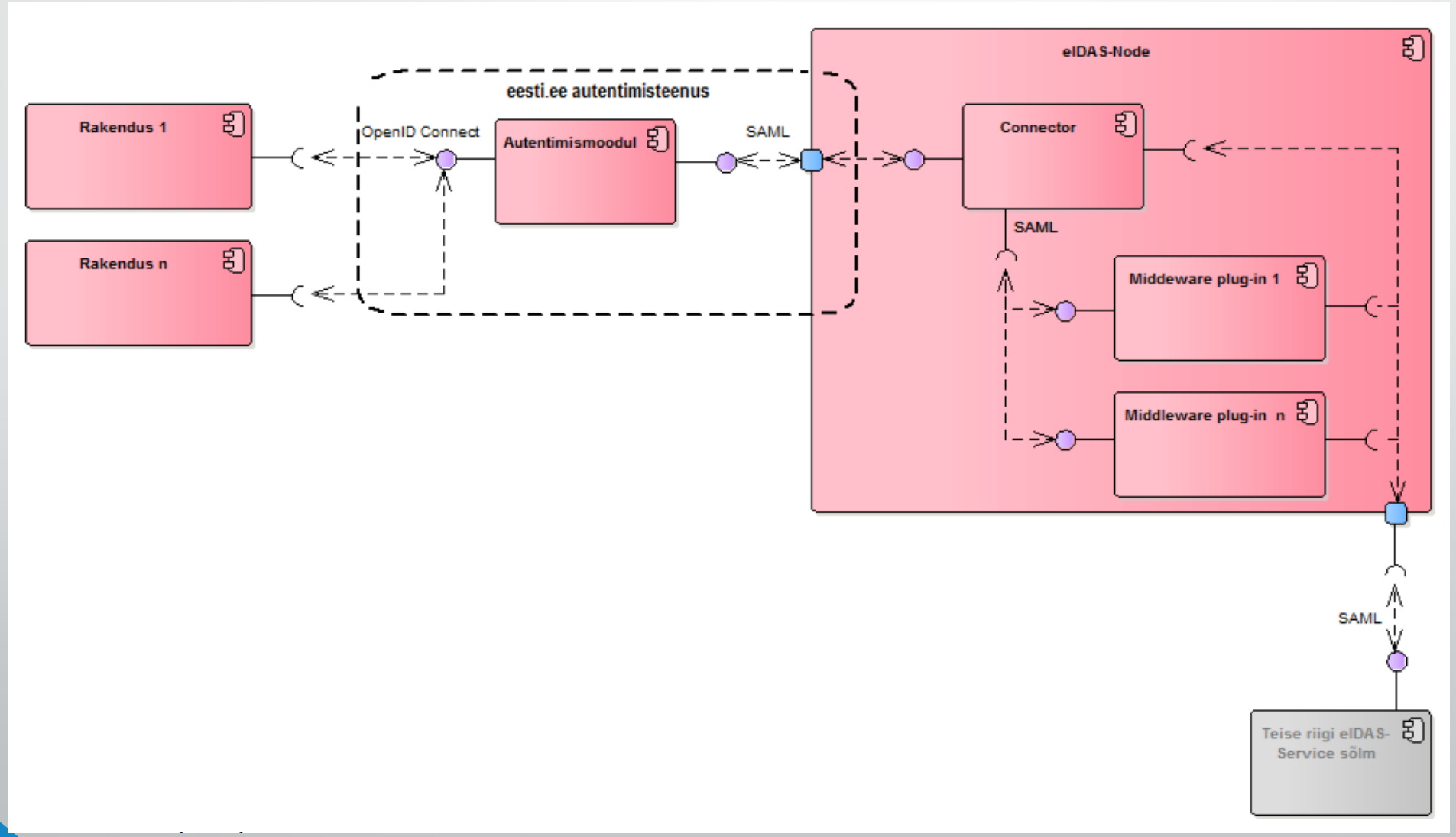
- Eesti Vabariigi elektrooniliste identiteetide kasutamine autentimiseks
- Teiste EL liikmesriikide elektrooniliste identiteetide kasutamine autentimiseks läbi eIDAS infrastruktuuri
- Kasutatav kui teenus läbi OpenID Connect protokolli
- SSO

Milliste vahenditega ja keda autendime

Grupp	Autentimisvahend
Eesti kodanik	EE eID, mID, pangalink
Eesti resident (elamisluba, mittekodanik)	EE eID, mID, pangalink
e-resident	EE eID, mID, pangalink
EL liikmesriigi kodanik või resident, kes on ühtlasi Eesti resident	eIDAS
EL liikmesriigi kodanik või resident, kes ei ole Eesti resident	eIDAS

vt. ka EESTI VABARIIGI INFOSÜSTEEMIS AUTENTIMISLAHENDUSTELE KEHTIVAD NÕUDED (autentimisnormatiiv)

Lahenduse arhitektuur



Erinevad võimalused

- **Valik 1.** Liituda RIA-s loodud eesti.ee autentimisteenusega
- **Valik 2.** Paigaldada oma infrastruktuurile eesti.ee autentimisteenus ja kasutada eIDAS autentimismehhanismiga liitumiseks RIA-s paigaldatud eIDAS Connector sõlme.
- **Valik 3.** Luua ise autentimisteenus ja kasutada eIDAS autentimismehhanismiga liitumiseks RIA-s paigaldatud eIDAS Connector sõlme.
- (**Valik 4.** Luua kogu autentimislahendus ise sh. paigaldada eIDAS Connector server)

Tegevused erinevate vallikuvariantide puhul

Tegevus	1	2	3	4
Eesti.ee autentimisteenusega liitumine rakenduse administraatori juures	+	-	-	-
Eesti.ee autentimisteenuse poole pöördumise liidese implementeerimine oma infosüsteemis	+	-	-	-
Autentimislahenduse tarkvara loomine	-	-	+	+
Autentimislahenduse paigaldamine oma infrastruktuurile	-	+	+	+
eIDAS Connector serveri teenusega liitumine RIA rakenduse administraatori juures	-	+	+	-
Autentimislahenduse häälestamine ühendumiseks RIA eIDAS Connector serveriga	-	+	+	-
eIDAS Connector serveri paigaldamine oma infrastruktuurile	-	-	-	+
Turvasertifikaatide vahetamine kõikide Euroopa Liidu liikmesriikide eIDAS Service serveri haldajatega ja sertifikaatide hilisem haldamine	-	-	-	+
Eesti.ee autentimisteenusega liidestumise (OpenID Connect ver. 1.0) ja autentimisprotsessi toimimise testimine	+	-	-	-
eIDAS Connector serveriga liidese (SAML ver. 2.0) ja autentimisprotsessi toimimise testimine	-	+	+	+
RIA-st aktsepti saamine autentimislahenduse kasutamiseks	+	+	+	-

Millal saab kasutama hakata?

- **Valik 4.** Kohe
- **Valik 3.** Kohe
- **Valik 2.** 1. kvartal 2018
- **Valik 1.** 1. kvartal 2018

Tulemused sammhaaval …

- Avalik arendus GitHub-is
- Tulemuste välja andmine iga etapi valmimisel:
  - ülesanne (mai 2017)
  - spetsifikatsioon (september 2017)
  - OpenID Connect koos fikseeritud token’i genereerimisega (oktoober-november 2017)
  - autentimine Eesti autentimisvahenditega (detsember 2017 – jaanuar 2018)
  - autentimine eIDAS vahenditega (1. kvartal 2018)
  - (täiemõõduline SSO (hiljem))
- Tulemuste valmimisest teavitamine

Ongi kõik?

Kindlasti mitte…

Kasutajate jagamine rollidesse

Grupp	Autentimisvahend	Õiguste tase (autoriseerimine)	Liigitamise alus
Eesti kodanik	EE eID , mID, pank	kodanik	eID
Eesti resident (elamisluba, mittekodanik)	EE eID , mID, pank	resident	eID ja rahvastikuregister (vastus „on elamisloaga“ või „on mittekodanik“)
e-resident	EE eID, mID, pank	mitte-resident	eID
EL liikmesriigi kodanik või resident, kes on ühtlasi Eesti resident	eIDAS	resident	eIDAS ja rahvastikuregister (vastus: „on EE resident“)
EL liikmesriigi kodanik või resident, kes ei ole Eesti resident	eIDAS	mitte-resident	eIDAS ja rahvastikuregister (vastus: „ei ole EE resident“)

Teenustele ligipääsu muutmine

- **Teenuste inventuuri tegemine ja otsustamine, milliseid teenuseid saab pakkuda milliste tasemete kasutajatele.** Iga teenuse juures peavad olema määratud kõik need kasutajate tasemed, kelledele antud teenust pakkuda saab. Seda sama tuleb teha ka kõigi tulevikus loodavate teenustega.

- **Teenustele juurdepääsu piiramine sõltuvalt autoriseerinud kasutaja tasemest.** Kui teenuse poole pöördub isik, kes kuulub tasemele, mida konkreetse teenuse puhul ei ole kirjeldatud, siis lükatakse teenuse poole pöördumise soov tagasi.

… ja muidugi isikukood

- Eesti infosüsteemides kasutatakse isikute unikaalse identifikaatorina 11-kohalist isikukoodi.
- eIDAS infrastruktuuri kaudu autentimisel saabub token'i sees eIDAS identifikaator, mille pikkus on riigiti erinev
- on võimalik, et mõnedes riikides isikute eIDAS identifikaator võib muutuda
- eIDAS autentimismehhanismi kaudu Eesti infosüsteemis autentinud ja teenust saanud isikutel tuleb isikukoodi asemel kasutada eIDAS identifikaatorit, millele on lisatud prefiksina riigi kahekohaline kood (ISO-2)
- Andmebaasides tuleb üle kontrollida isikukoodi välja pikkus ja muuta seda vajadusel selliselt, et sinna mahuks sisse pikem väärtus kui 11 kohta
- Isikukoodi välja soovituslik minimaalne pikkus on 64 sümbolit.

Tänan tähelepanu eest!

KUNI 12.05.2017: priit.raspel@ria.ee
ALATES 15.05.2017: priit.raspel@tehik.ee