Autentimisprotokolli turvauuring

Lähteülesanne

27.02.2018 v 1.0

1 Eesmärk

Uuringu eesmärk on autentimisteenuse TARA protokolli hindamine ja soovituste andmine protokolli täiendamiseks ja tehnilisteks valikuteks protokolli teostamisel.

2 Lähtekohad

2.1 Autentimine käesoleva dokumendi mõistes on avaliku sektori e-teenust kasutava isiku, edaspidi – kasutaja (samasuse) tuvastamine. Isikusamasuse tuvastamine on enamiku e-teenuste kasutamise eeldus. Autentimislahenduste arendamine ja haldamine on oluline kulu. Paljud e-teenused on autentimise lahendanud iseseisvalt. Teised kasutavad asutusesiseseid või valdkondlikke, erinevatele e-teenustele ühiseid autentimisteenuseid. Avalikus sektoris kasutatavate autentimisteenuste „ökosüsteemi“ iseloomustavad järgmised nähtused:

1. autentimismeetodite mitmesus (ID-kaart, mobiil-ID, eIDAS, Smart-ID, pangalingid)
2. vajadus tagada erinevate autentimismeetodite kasutamise võimalus, seda nii kasutajakogemuse kui ka teenuste käideldavuse (vrdl ID-kaardi „kriis“) kaalutlusel
3. autentimismeetodite areng
4. autentimisega seotud osateenuste vajadus (nt kus oled viimati sisse loginud)
5. vahenduse põhimõttel toimivate autentimisteenuste laiem levik
6. pilvepõhiste autentimisteenuste levik
7. vajadus tagada autentimisteenuste väljavahetamise võimalus
8. piiriülese autentimise (eIDAS) lõimimine Eestis seni kasutatud autentimislahendustesse
9. platvormi ebastabiilsus, eelkõige sirvikute suhtlemises kiipkaartidega
10. protokollide paljusus ja alaspetsifitseeritus.

2.2 Ülalnimetatud nähtused on ühest küljest loomulikud – areng, teisest küljest aga problemaatilised, sest toovad asutustele olulisi arendus- ja halduskulusid – millest kõik ei tarvitse olla õigustatud. See on põhjus, miks riik on huvitatud autentimistehnoloogiate ja –teenuste „ökosüsteemi“ mõistmisest ja tehnopoliitika kujundamisest.

2.3 Riigi Infosüsteemi Amet on 2017. a aktiivselt arendanud autentimisteenust TARA [1]. TARA perspektiiv on saada avaliku sektori keskseks autentimisteenuseks, mis pakub e-teenuse kasutajale laia autentimismeetodite valikut ja ühtset kasutajakogemust, e-teenuse osutajale aga kindlust, mugavust ja väikest kulu autentimise lisamisel ja haldamisel oma e-teenuses.

2.4 Autentimisteenus tänapäeva praktikas ei ole enam lihtne teenus, vaid laiem või kitsam kogum funktsionaalsusi. E-teenused ja kasutajad ootavad lisaks elementaarsele isikutuvastustoimingule ka ühekordset sisselogimist (*single sign-on, SSO*) ja sellega seotud seansihaldust, sisselogimiste ajalugu, isikut iseloomustavate tunnuste (atribuutide) pakkumist, turvahoiatusi, ühekordset väljalogimist jm. Seetõttu autentimisteenus, õigemini osateenuste kogum on käsitatav identiteediplatvormi osana. Autentimine on tihti tihedalt (liiga tihedalt) seotud pääsuhaldusega.

3 Uurimisküsimused

3.1 Keskse autentimisteenuse arendamisel on võtmeküsimuseks liidestujatele pakutav protokoll, sellega teostatavad ärilised võimalused, tehniline sobivus, aga samuti turvalisus. TARA protokolli aluseks on OpenID Connect 1.0 protokoll (OIDC) [2]. Tarkvara aluseks on CAS [5].

3.2 TARA arendus on jõudnud seisu, kus vastamist vajavad järgmised küsimused:

1. Hinnang autentimisteenuses TARA teostatud protokolli turvalisusele, OpenID Connect profileerimisel tehtud valikute osas

    1.1. Kas valitud volituskoodi voog (*authorization flow*) on sobiv?

    1.2. Kas klientrakenduste autentimine sümmeetrilise võtme (*client secret*) abil on turvaline? Kas PKI oleks turvalisem?

2. Kas ja millises mahus lisada TARA-teenusele SSO võimekus – nii, et see oleks turvaline?

    2.1. Kas keskse e SSO seansi kehtivuse kontrollimiseks jätta klientrakendustele vabad käed? Kas see oleks turvalisuse seisukohast mõistlik valik? Alternatiiv on SSO seansi kehtivuse päring igal pöördumisel kasutaja sirvikust

    2.2. Kas protokoll tervikuna on asutuseülese SSO tegemiseks sobiv?

    2.3. Kas seni mitmel pool tehtud asutusesisese SSO ja TARA pakutava asutuseülese SSO vahel on turvalisuse seisukohalt oluline erinevus?

    2.4. Kui oluline on "keskse nuripunkti" (*single point of failure*) probleem ja kuidas seda lahendada?

    2.5. Kas kasutaja kokkuvõttes saab aru, millal ja kuhu ta on sisse või välja loginud?

    2.6. Kas protokoll on piisavalt detailiseeritud, et saaks alustada SSO-lahenduse arendusega?

    2.7. Kas SSO-ga liitumine peaks olema kohustuslik (vrdl Soomes on keskse autentimisteenuse kasutamine keskvalitsuse asutustele kohustuslik, kuid SSO-ga liitumine mitte)

    2.8. Kas oleks võimalik määratleda kriteeriume, mille abil piiritleda SSO autentimisprotokolli rakendamiseks sobivate e-teenuste ringi?

    2.9. Kas seansihalduseks tuleks kasutada postMessage API põhist lahendust, vt [3]?

2.10. Kas ühekordne väljalogimine tuleks teostada OpenID Connect vastavate standardikavandite [4] järgi?

2.11. Kas protseduurilised ja policy aspektid on piisavalt detailiseeritavad, et lahendus oleks turvaline? Nt kas *back-channel logout*-le tuleks kehtestada ühtsed, kohustuslikud seansiaegumisajad?

3. Kas TARA-võiks (riskide hajutamiseks) pakkuda mitmes instantsis, mitme erineva asutuse poolt?

3.1. Mida TARA protokollis tuleks muuta, et see oleks võimalik?

4. Kas oleks tehniliselt ja äriliselt teostatav TARA-s aluseks olev, probleemne CAS [5] tarkvara välja vahetada EMTA autentimislahendusele arendatud OpenID Connect SSO toega tarkvara vastu?

4.1. Alternatiivina, kas EMTA autentimislahendus oleks edasiarendatav, et pakkuda universaalset autentimisteenust ka teistele asutustele?

5. Kuidas tagada haldusalade olemasolevate autentimislahenduste koostalitlusvõime keskse autentimisteenusega?

5.1. Kas selleks on võimalik ja otstarbekas pakkuda tehnilisi reegleid või protokolli?

6. Mõned asutused eelistavad piiriülese autentimise lahendada otseühendusega RIA eIDAS konnektorteenuse [6] külge. Kuidas lahendada SAML-i ja OpenID Connect-i paralleelne kasutamine, nii, et asutustele ei tekiks liigset keerukust?

4 Infoallikad

Töö põhineb järgmistele kirjalikele infoallikatele:

1. autentimisteenuse TARA dokumentatsioon [1][2]
2. RIA eIDAS konnektorteenuse dokumentatsioon [6]
3. standardid [3], [4], [7], vajadusel ka muud
4. EMTA autentimislahenduse dokumentatsioon
5. Soome keskse SSO-autentimisteenuse dokumentatsioon [8]
6. kasutuslood (käesoleva dokumendi lisas).

Lisaks viiakse töö täitmise käigus läbi:

1. algatusseminar
2. vähemalt üks vaheseminar
3. jooksev suhtlus küsimustele vastuste saamiseks
4. lõpuseminar.

5 Väljund

Töö väljund on analüüsi ja soovitusi sisaldav dokument (uuringuaruanne).

Hiljemalt kaks nädalat enne lõpliku uuringuaruande esitamist esitab uuringu teostaja tellijale aruande eelvariandi, millele tellija annab tagasisidet.

6 Viited

[1] Autentimisteenus TARA, https://e-gov.github.io/TARA-Doku/.

[2] [1] RIA SSO autentimisteenuse kavand, https://github.com/ria-eidas/RIA-autentimisteenus/wiki/Teenuse-kontseptsioon.

[3] OpenID Connect Session Management, http://openid.net/specs/openid-connect-session-1_0.html.

[4] OpenID Connect Front-Channel Logout, http://openid.net/specs/openid-connect-frontchannel-1_0.html; OpenID Connect Back-Channel Logout, http://openid.net/specs/openid-connect-backchannel-1_0.html.

[5] CAS OpenID Connect Authentication. https://apereo.github.io/cas/5.1.x/installation/OIDC-Authentication.html.

[6] RIA eIDAS konnektorteenus. https://e-gov.github.io/eIDAS-Connector/.

[7] OpenID Connect Core 1.0, http://openid.net/specs/openid-connect-core-1_0.html.

[8] Suomi.fi e-Identification – Technical interface description, https://esuomi.fi/suomi-fi-services/suomi-fi-e-identification/technical-interface-description/?lang=en.

7 Lisa. Kasutuslood

`K0` ("lihtne autentimine") - kasutaja logib e-teenusesse sisse, kasutab seda mõne aja ja lahkub, kas välja logides või sirvikut sulgedes. Kasutaja võidakse välja logida ka serveri algatusel, seansi aegumise tõttu.

`K1a` ("ühekordne sisselogimine") - kasutaja logib sisse e-teenusesse E1. Mõne aja pärast, E1-st väljumata, soovib ta avada ja siseneda sama sirviku teises sirvimiskontekstis (teises sakis või aknas) e-teenusese E2. Kasutaja ei pea uuesti sisse logima, vaid ta logitakse E2-te automaatselt sisse.

`K1b` ("sessiooni üleandmine") - kasutaja logib sisse e-teenusesse E1. Mõne aja järel soovib (samas sirvimiskontekstis) liikuda e-teenusesse E2. Kasutaja logitakse E2-te liikumisel automaatselt sisse.

`K2a` ("ühekordne väljalogimine") - kasutaja on sisse logitud mitmesse e-teenusesse. Kasutaja logib välja e-teenusest E1. Ühtlasi logitakse ta välja kõigist e-teenustest.

`K2b` ("seansi aegumine") - keskne seanss aegub. Kasutaja logitakse välja.

`K3a` ("pidev kasutaja") - kasutaja (näiteks asutuse töötaja) kasutab e-teenust kogu tööpäeva vältel. Ta ei pea ikka ja jälle sisse logima.

`K3b` ("mitme teenuse pidev kasutaja") - kasutaja (näiteks asutuse töötaja) kasutab erinevaid e-teenuseid kogu tööpäeva vältel. Ta ei pea mitmeid kordi sisse logima.