Tehnoloogiline profiil

Dokument	Tehnoloogiline profiil
Identifikaator (OID)	1.3.6.1.4.1.19974.12.3.1.3
Versioon	1.3
Viimati muudetud	05.09.2012

1 Kasutatav tehnoloogia

Autentimis- ja autoriseerimisandmete vahetus Föderatsioonis toimub SAML 2.0 (või sellega ühilduvat) protokolli kasutades.

1.1 SimpleSAMLphp

TAATi keskne teenus kasutab andmete vahendamiseks SimpleSAMLphp-d ja lähtub sellest ka juhendite koostamisel. SimpleSAMLphp on soovituslik tarkvaralahendus Identiteedi- ja Teenusepakkujatele.
SimpleSAMLphp on vabavaraline tarkvara, mis on leitav lehet http://simplesamlphp.org/.

1.2 Muud lahendused

Lubatud on kasutada ka teisi tarkvaralisi lahendusi (nt Shibboleth), kui need on ühilduvad TAATiga, sealhulgas atribuutide teisendamine on erilahendust kasutava Identiteedi- või Teenusepakkuja ülesanne.

1.3 Haldusvahend JANUS

Identiteedi- ja Teenusepakkuja haldab JANUSes ise oma metaandmeid ning on kohustatud hoidma neid ajakohasena.
Identiteedipakkuja võib JANUSe abil keelata endaga seotud Lõppkasutajal teatud teenus(t)e kasutamise.
Identiteedipakkuja võib valida, milliste teenuste puhul näidatakse temaga seotud Lõppkasutajatele andmete edastamise kinnitusvormi.
Teenusepakkuja võib JANUSe abil keelata teatud Identiteedipakkuja(te) Lõppkasutajatel oma

teenuse kasutamise.

2 Ühenduse staatused

Identiteedi- ja Teenusepakkujate ühendused TAATiga jagunevad kolme staatusesse: test, kvaliteeditagamine ja produktsioon.

- Teststaatus on avatud kõigile Föderatsiooniga liituda soovijatele. Ühenduste üles seadmine ja süsteemide häälestamine (sh uuendamine) toimub alati selles staatuses.
- Kvaliteeditagamises kontrollib EENet teenuse või identiteedipakkuja sisulist ja tehnilist valmisolekut Föderatsiooniga liitumiseks ning ühenduse toimimist.
- Produktsioonis on ainult lepingulised TAAT teenuse kasutajad. Muudatuste tegemine süsteemides ei ole lubatud.

Iga staatusel on oma jaotur (*hub*) ja vastavas staatuses olevad ühendused teiste jaoturitega ühenduses olijaid ei näe.

2.1 Protseduurid

Föderatsiooniga liituda sooviv teenus või identiteedipakkuja ühendub testjaoturiga ning ühenduse staatuseks on “test”. Kui ühendus on seadistatud ja toimiv, määrab liituda soovija oma staatuseks JANUSes “kvaliteeditagamise ootel”.

Kui liituja vastab Föderatsioonipoliitikaga määratud liitumistingimustele, määrab EENet ühenduse staatuseks “kvaliteeditagamine”. Kui ühendus on toimiv ja kõik atribuudid saadetakse korrektselt, sõlmitakse leping ja staatuseks määratakse “produktsioon ootel”.

Produktsiooni minemise hetke määrab identiteedi- või teenusepakkuja ise muutes oma staatuseks JANUSes “produktsioon”.

Kõik edasised testimised sooritatakse teststaatuses, kusjuures produktsioonitasandi süsteem jääb paralleelselt töösse. Muudetud ühendus peab produktsiooni jõudmiseks läbima kõik sammud (v.a lepingu sõlmimine).

3 TAATi kaudu saadetavad atribuudid

Igal autentimisel väljastab Identiteedipakkuja selle isiku andmed Föderatsioonis kokku lepitud atribuutide väärtustena. TAAT võtab vastu ainult punktides 3.1 ja 3.2 kirjeldanud atribuudid.

Kõik esitatud atribuudid peavad vastama nii vormilt kui semantikalt käesolevale dokumendile. Atribuudid esitatakse tekstistringina UTF-8 kodeeringus.

Atribuutide nimeformaadiks (NameFormat) on urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

3.1 Kohustuslikud atribuudid

Kohustuslikud atribuudid peab iga Identiteedipakkuja väljastama. Teenusepakkuja võib eeldada, et need atribuudid on alati olemas iga Lõppkasutaja kohta.

- sn – perekonnanimi vastavalt isikut tõendavale dokumentile
- cn – täisnimi vastavalt isikut tõendavale dokumentile
- eduPersonPrincipalName – läbi ajaloo unikaalne kasutajatunnus või muu identifikaator koduasutuses, kujul identifikaator@domeen. Atribuudi alusel genereeritakse TAATi poolt tunnus eduPersonTargetedID.
- mail – e-postiaadress, võib olla mitu
- displayName – ekraaninimi / kasutaja eelistatud nimi. Kui pole teada, tuleb väljastada eesnimi.
- eduPersonAffiliation – roll koduasutuses, võib olla mitu. Lubatud rollid kirjeldatud punktis 3.4.

3.2 Valikulised atribuudid

Valikulised atribuudid, mida Identiteedipakkuja võib välja saata. Teenusepakkuja peab arvestama, et valikulised atribuudid võivad puududa.

- eduPersonScopedAffiliation – roll grupis, võib olla mitu. Lubatud esitusvormid on kirjeldatud punktis 3.5.
- preferredLanguage – eelistatud keel, võib olla mitu. Keeletähised on kahetähelised vastavalt ISO 3166 standardile.
- schacPersonUniqueID – Eesti isikukood. Kui Eesti isikukoodi ei ole, jäetakse atribuut edastamata. Isikukood esitatakse üheteistkohalise numbrina vastavalt "Isikukood. EV ST 585-90" standardile, mille ette lisatakse koolonitega eraldatult riigi ja ID tüübi tähis, Eesti puhul "ee:EID:"

3.3 TAAT atribuudid

Atribuudid, mille koostab TAAT ning edastab Teenusepakkujale iga päringu puhul

- schacHomeOrganization – koduasutuse ID, domeeninime kujuline
- eduPersonTargetedID – üle Föderatsiooni unikaalne mitteisikustav ID, erinev iga Lõppkasutaja ja teenuse paari puhul. Atribuut esitatakse alati 75-märgilise stringina.

3.4 Rollid

Lubatud rollid, mida võib saata eduPersonAffiliation või eduPersonScopedAffiliation atribuudiga:

- **student** – õppur
- **faculty** – õppejõud / teadustöötaja
- **staff** – tehniline või administratiivne töötaja
- **affiliate** – asutusega (ka ajutiselt) seotud isik, kellel pole spetsiifilisi õigusi
- **library-walk-in** – isik, kes kasutab asutuse võrgus arvutit
- **alum** – vilistlane

Lisaks eelnimetatutele, peab Identieedipakkuja lisama ka järgnevad rollid, kui need vastavad ühendi tingimustele:

- **employee** – liitroll, mis on ühend rollide **staff** ja **faculty** liikmetest
- **member** – liitroll, mis on ühend rollide **student**, **staff** ja **faculty** liikmetest

3.5 Grupid

Atribuuti eduPersonScopedAffiliation kasutatakse kujul <roll>@<grupp>.<nimeruumitähis>, kus:

- roll on määratud punktis 3.4
- grupp omab ühest tähendust oma nimeruumis
- nimeruumitähis määrab semantika ning on Identiteedi- või Teenusepakkuja spetsiifiline või kehtivad üle Föderatsiooni. Nimeruumitähis on domeeninime kujuline.

Identiteedipakkuja peab koostama ning avaldama enda poolt kasutatavate gruppide nimistu.
Üle Föderatsiooni kehtivad TAAT nimeruumitähisega grupid:

- roll@<õppetase>.studylevel.taat.edu.ee, kus lubatud õppetasemed ja nende tähendused on kirjeldatud punktis 3.6. Kasutamiseks ainult student rolliga. Ühe õppekohaga võib olla seotud ainult üks õppetase.
- roll@<üksus.---.üksus>.ou.taat.edu.ee, kus üksus on asutuse allüksus, kusjuures üksusi võib olla mitu, kui tagatud on hierarhiline järjekord, nii et iga mainitud üksus on endast parempoolse alamüksus või suurim võimalik. Minimaalse suurusega üksus on õppekava või eriala tähis. Atribuut peab sisaldama vähemalt ühte üksust. Üksuste tähised peavad olema minimaalsel kujul ja asutusesiseselt alati samad.

3.6 Õppetasemed

Lubatud on kasutada järgnevaid õppetaseme tähistusi:

- **dok** – doktoriõpe
- **mag** – magistriõpe
- **bak** – bakalaureuseõpe
- **int** – bakalaureuse- ja magistriõppe integreeritud õppekavadel põhinev õpe, seal hulgas arstiõpe, loomaarstiõpe, proviisoriõpe, hambaarstiõpe, arhitektiõpe, ehitusinseneriõpe ja klassiõpetaja õpetajakoolitus
- **rak** – rakenduskõrghariduse omandamine
- **kursus** – kursustel või täiendkoolitusel osalemine, millega ei omandata kindlat kraadi või taset ning millega ei ole seotud õppekohta
- **gymn** – üldkeskhariduse omandamine
- **kutse** – kutsekeskhariduse omandamine
- **keskeri** – keskerihariduse omandamine

Õppetasemete definitsioonid vastavad Eesti Vabariigi haridusseadusele.

4 Metaandmed

TAAT on kõigile Identiteedi- ja Teenusepakkujatele väliste (remote) metaandmete allikaks. Identieedi- ja Teenusepakkuja peab lisama oma väliste metaandmete nimistusse kõigi kolme TAAT jaoturi metaandmed.
Iga Identiteedi- ja Teenusepakkuja peab JANUSes registreerima oma sisemised (hosted) metaandmed.
Metaandmed esitatakse XML või SimpleSAMLphp formaadis ning minimaalselt peavad olema määratud järgmised atribuudid:

- entityID – teenuse või autentimissüsteemi unikaalne URI, kasutatakse selle Identiteedi- või Teenusepakkuja identifitseerimiseks kõikides süsteemides, väga tundlik muutuste suhtes
- certData – Base64-kodeeritud sertifikaat
- OrganizationName – teenuse või identiteedipakkuja unikaalne nimi. Kohustuslik esitada eesti (et) ja inglise (en) keeles, kuid võib lisada ka rohkem keeli.
- OrganizationDisplayName – teenuse või identiteedipakkuja nimi, mida näidatakse Lõppkasutajale. Kohustuslik esitada eesti (et) ja inglise (en) keeles, kuid võib lisada ka rohkem keeli.
- OrganizationURL – Teenuse või Identiteedipakkuja infoleht. **NB!** Domeeniosa peab iga Identiteedipakkuja puhul olema unikaalne (sellest genereeritakse schacHomeOrganization).
- name – nimi, mida näidatakse JANUSes, domeeninimekujuline
- SingleSignOnService – URL sisselogimise asukohaga (SAML endpoint). Ei ole kasutusel Teenusepakkujate puhul.
- SingleLogoutService – URL kasutaja väljalogimise asukohaga (SAML endpoint)