Tallinna Tehnikaülikool

Infotehnoloogia teaduskond

Informaatikainstituut

Infosüsteemide õppetool

Eesti haridus- ja teadusasutustevahelise autentimise ja autoriseerimise taristu äriprotsesside analüüs rahvusvahelise liidestuse võimaldamiseks eduGAINi vahendusel

bakalaureusetöö

Üliõpilane: Piiu Pilt

Üliõpilaskood: 073831 IABB

Juhendaja: Enn Õunapuu

Tallinn 2015

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

_____ _____

(kuupäev) (allkiri)

Annotatsioon

Töö eesmärk on viia läbi analüüs Eesti haridus- ja teadusasutustevahelise autentimise ja autoriseerimise taristu hetkeolukorrast ja soovitud tulemusest pärast rahvusvahelise liidestamise võimaldamist eduGAINi vahendusel. Seejärel esitatakse lahendus soovitud tulemuse saavutamiseks väljaarendamist või kasutuselevõttu vajava tarkvara nimistuna ning arendustööks vajalikud kulud.

Töö tulemusena esitati mõlemad analüüsid teostati nii tekstiliselt kui Bizagi diagrammidena ning leiti sobivad tarkvaralahendused või vajaminevad arendustööd tekkinud probleemide lahendamiseks.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 37 leheküljel, 4 peatükki, 12 joonist.

Abstract

The aims of the thesis is to analyze the business processes of Estonian Academic Authentication and Authorization Infrastructure both in current situation and after enabling interfederating through eduGAIN, followed by list of necessary software or developments and their cost.

The results of the thesis include both analysis' both in text and Bizagi diagram form and list of suitable software for achieving the wanted result and in case there is no excising software, the need for software developments.

The thesis is in Estonian and contains 37 pages of text, 4 chapters, 12 figures, etc.

Lühendid ja mõisted

AAI	*Authentication and Authorization Infrastructure* Autentimise ja autoriseerimise taristu võimaldab ühes asutuses olevaid kasutajakontosid kasutada asutuseväliste teenuste kasutamiseks
ARP	*Attribute Release Policy* Deklaratsioon atribuutidest, mida teenus soovib AAI vahendusel vastu võtta
BPMN	*Business Process Model and Notation* Äriprotsesside modelleerimise standard
eduGAIN	Riiklike identiteediföderatsioone koondav konföderatsioon
EENet	Eesti Hariduse ja Teaduse Andmesidevõrk HITSA struktuuriüksus
GNTB	*GÉANT Trust Broker*
HITSA	Hariduse Infotehnoloogia Sihtasutus
IdP	*Identity Provider* Identiteedipakkuja on asutus, kelle kasutajad on identiteediföderatsiooni lõppkasutajad, saades ligipääsu AAI teenustele. Töös kasutatakse ka terminit „koduasutus”, mis viitab identiteedipakkujale, mille juures lõppkasutajal konto on.
SAML 2.0	*Security Assertion Markup Language 2.0*
SP	*Service Provider* Teenusepakkuja on föderatsiooni kuuluva teenuse haldaja.
SSO	*Single sign-on* Ühekordset sisselogimine üle mitme teenuse
TAAT	Eesti haridus- ja teadusasutustevahelise autentimise ja autoriseerimise taristu on Eesti akadeemiline identiteediföderatsioon

Jooniste nimekiri

Sisukord

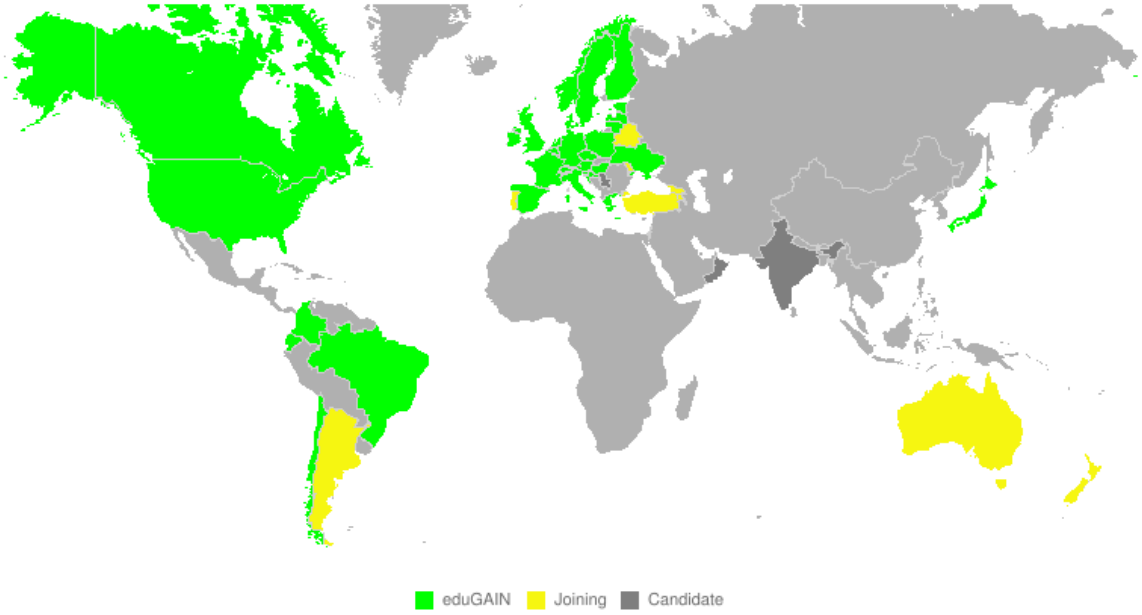
1. Sissejuhatus

Lõputöö teema on seotud autori tööga Eesti Hariduse ja Teaduse Andmesidevõrgus (EENet) ning käsitleb analüüsi EENeti teenusena pakutava Eesti haridus- ja teadusasutustevahelise autentimise ja autoriseerimise taristu (TAAT) rahvusvahelise liidestuse realiseerimiseks eduGAINi vahendusel.

1.1 Taust ja probleem

Akadeemiliste autentimise ja autoriseerimise taristud (AAI) on üle maailma laialdaselt kasutatavad ning võimaldavad isikul, kes omab kasutajakontot mõne (kõrg)haridus- või teadusasutuse (identiteedipakkuja) juures, kasutada seda kontot erinevate haridusalaste teenuste juurde sisse logimiseks ilma täiendavat kontot loomata. Akadeemiline AAI võimaldab lõppkasutajal tõestada oma isikut ja rolli koduasutuses, selle vahendusel on võimalik edastada turvaliselt isikuga seotud andmeid ning see võimaldab ühekordset sisselogimist üle mitme teenuse (SSO). Ühtsetes standardites ja usalduse alustes kokku leppinud asutused moodustavad identiteediföderatsiooni, mis reeglina ühendab ühe riigi identiteedi- ja teenusepakkujaid.

Kuna üks peamisi AAI kasutusalasid on akadeemiline koostöö, mis tihti pole piiratud riigipiiridega, on vajalik võimaldada andmeedastust ka rahvusvahelisel tasandil. Üks ülemaailmne föderatsioon on utoopia, kuna kasutatav tehnoloogia, standardid ja andmeformaadid pole rakendatavad tuhandetele asutustele. Selle asemel koondatakse olemasolevad föderatsioonid kõrgema taseme katus- ehk konföderatsioonidesse. **eduGAIN** on edukas katse koondada riigispetsiifilised akadeemilised AAId nii üleeuroopalises hariduse ja teaduse andmesidevõrgus GÉANT kui kaugemalgi [2].



Joonis 1: eduGAINi liikmed [1]

EENet on Hariduse Infotehnoloogia Sihtasutuse (HITSA) struktuuriüksus, mille peamine eesmärk on tagada teaduse, hariduse ja kultuuri jaoks vajalik infotehnoloogilise taristu areng ja stabiilne toimimine [3]. Oma eesmärkide täitmiseks on EENet välja arendanud Eesti haridus- ja teadusasutustevahelise autentimise ja autoriseerimise taristu (**TAAT**), mis toimib Eesti identiteediföderatsioonina. TAAT on töös alates maist 2012. Seisuga mai 2015 on TAATiga liitunud 12 identiteedipakkujat ja 4 teenust [4]. Lisanduvad teenuse testijad, kelle täpset arvu ei ole võimalik määrata, kuna testkeskkond on avatud kõigile.

TAAT on eduGAINi liige alates maist 2013, kuid puudub tehniline liidestus ning seega ei ole võimalik andmevahetus eduGAINi vahendusel. Identiteedi- ja teenusepakkujatel on võimalik ühenduda eduGAINiga otse, TAATi kasutamata, kuid see meetod nõuab palju tööd ning pidevat suhtlust eduGAINi esindajatega. TAATi tehniliseks ühendumiseks eduGAINiga on vajalik läbi viia TAATiga seotud äriprotsesside analüüs ning määrata arendusvajadus.

1.2 Ülesande püstitus ja metoodika

Töö eesmärk on viia läbi analüüs TAATi hetkeolukorrast ja soovitud tulemusest pärast rahvusvahelise liidestamise võimaldamist. Hetkeolukorra kaardistamine võimaldab teistel EENeti töötajatel saada ülevaadet TAATiga seotud protsessidest, kuna need pole üheselt määratletud TAAT dokumentidega. Soovitud tulemus on dikteeritud eduGAINi standardite poolt ja on lähteülesandeks arendajatele.

Mõlema olukorra kaardistamisel lähtutakse kolmest TAATi põhilisest protsessist:

- Lõppkasutaja föderееritud sisselogimine TAATiga seotud teenusesse
- Identiteedipakkuja (IdP) liitumine TAATiga
- Teenusepakkuja (SP) liitumine TAATiga

Äriprotsessid esitatakse tekstilise kirjeldusena ja seejärel diagrammide kujul kasutades BPMN-i standardeid ja tarkvara Bizagi Modeler.

Seejärel esitatakse lahendus soovitud tulemuse saavutamiseks väljaarendamist või kasutuselevõttu vajava tarkvara nimistuna ning arendustööks vajalikud kulud. Võimalusel hoidutakse majasisesest arendusest ning kasutatakse valmisolevat tarkvara.

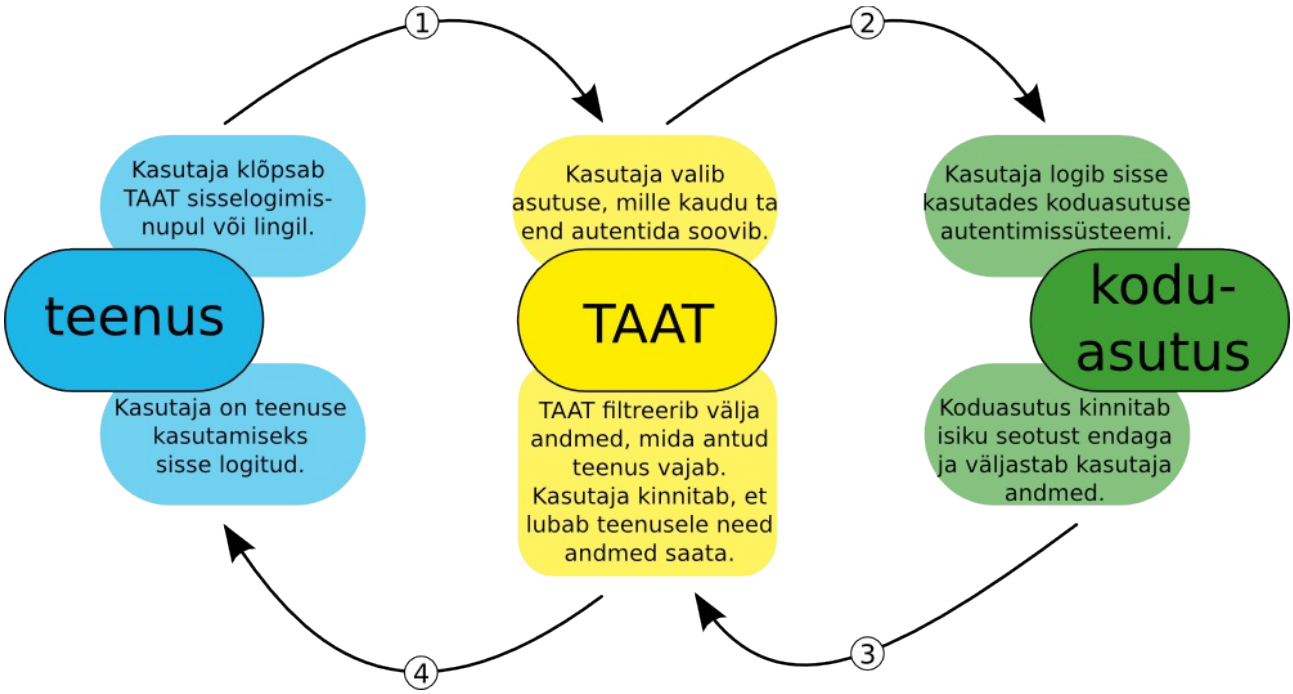
2. Hetkeolukord

TAATi toimimist reguleerib Föderatsioonipoliitika, mis defineerib föderatsiooni olemuse, haldamise ja struktuuri, määrates protseduurid ja tingimused, mis korraldavad teenuse- ja identiteedipakkujate vahelist autentimise ja autoriseerimise info edastamist [5]. Kõik tehtavad muudatused peavad olema Föderatsioonipoliitika ja Eestis kehtivate õigusaktidega kooskõlas.

2.1 Kasutatav tehnoloogia

TAAT on *hub-and-spoke* stiilis identiteediföderatsioon, mis tähendab, et kõik andmed liiguvad läbi TAAT keskse jaoturi. Mudel valiti Eesti jaoks parima variandina, kuna võimaldab rohkem hallatavust ja turvalisust kui otseühendus identiteedi- ja teenusepakkuja vahel. Andmete hulk, mis teenusepakkujani jõuab, on minimeeritud vastavalt teenuse vajadusele. Kaks teenusepakkujat ei saa isikuga seotud andmete vahel seost leida ilma kolmanda osapoole abita. Identiteedipakkuja ei tea, mis teenuseid temaga seotud isik kasutab ilma kolmanda osapoole abita [6].

TAAT keskne jaotur vastutab selle eest, et isikuandmeid ei edastataks kolmandatele osapooltele ilma isikult nõusolekut küsimata [7], kuvades nõusolekuvormi koos saadetavate andmetega igal autentimisel, kui kasutaja ise pole valinud teisiti, ning tagab, et teenusele ei saadetaks minimaalsest vajalikust rohkem isikuandmeid.



Joonis 2: TAAT tööpõhimõte [4]

SAML 2.0

SAML 2.0 (*Security Assertion Markup Language 2.0*) on XML-il põhinev turvalise autentimis- ja autoriseerimisandmete vahetamise protokoll [8]. Kõik liiklus läbi TAATi vastab SAMLi standaritele.

SimpleSAMLphp

TAATi keskne teenus kasutab andmete vahendamiseks SimpleSAMLphp-d ja lähtub sellest ka juhendite koostamisel. SimpleSAMLphp on vabavaraline soovituslik lahendus Identiteedi- ja teenusepakkujatele [9]. Tarkvara on välja arendatud Norra akadeemilise andmesidevõrgu UNINETT poolt ja see on ühilduv paljude teiste autentimisprotokollidega, sh Shibboleth 1.3, OpenID ja OAuth [10], mis on kasutusel ka Eestis.

Metaandmed

Autentimise osapooled vahetavad metaandmeid, sh sertifikaadiinfot, et tõendada oma autentsust. SAML metadata on sisaldab rolle, protokolle ja profiile, mida süsteem toetab [11]. Kõik metaandmed fikseeritakse asutuse liitumisel TAATiga haldusvahendis JANUS, kust need jõuavad TAATi jaoturitesse. Enamus andmetest esitatakse eesti ja inglise keeles, mis tähendab, et neid pole vajalik muuta rahvusvahelise liidestamise võimaldamiseks.

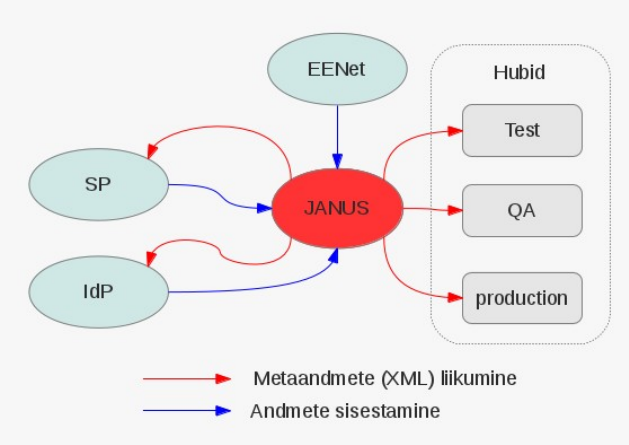
Jaoturid ja JANUS

JANUS on SimplaSAMLphp peale ehitatud metadata rehistri administreerimismoodul, mis on fokusseeritud SAMLi ühenduste registreerimisele iseteeninduse vormis. [12]

JANUSes võib ühendusel olla viis staatust [13].

1. **Test**, mis on vaikimisi staatus
2. **Kvaliteeditagamise ootel**, mis tähendab, et asutus soovib oma ühenduse ülevaatamist TAATi haldaja poolt
3. **Kvaliteeditagamine**, kus ülevaatamine teostatakse.
4. **Produktsiooni ootel** ühendustele, kes on kontrolli läbinud.
5. **Produktsioon** tööd olevatele ühendustele.

Vastavalt ühenduse staatusele jõuavad metaandmed erinevatesse TAAT jaoturitesse. Jaoturid on üksteisest eraldatud ja nende vahel ühendust ei ole. Testjaoturit võib kasutada igaüks, EENetti selleks teavitama ei pea.



Joonis 3: Metaandmete liikumine TAATis [13]

2.2 Seotud osapooled ja neile kehtivad nõuded

EENet

EENet on TAAT teenuse haldaja ja keskne osapool. EENet kontrollib Föderatsiooni liikmete ja liituda soovivate asutuste kvalifitseerumist Föderatsiooni liikmeks ning avalikustab Föderatsiooni Liikmete ja Partnerite nimekirja TAATi veebilehel [5].

EENet ei ole andmete omanik ega ei vastuta nende sisu eest. EENeti hallatava teenuse poolt ei talletata ega logita isikute andmeid.

Identiteedipakkuja

Identiteedipakkuja on asutus, kelle kasutajate andmebaas on TAATiga ühendatud ja kelle lõppkasutaja saab seeläbi TAATiga seotud teenuseid kasutada.

Identiteedipakkujaks võivad saada asutused, mis kvalifitseeruvad EENeti kliendiks vastavalt EENeti põhimäärusele. TAAT teenuse kasutamiseks peab identiteedipakkuja olema sõlminud EENetiga vastava teenuslepingu.

Identiteedipakkuja on kohustatud teavitama endaga seotud Lõppkasutajat TAATi kasutamise korrast

ning vajadusel pakkuma kasutajatuge [5].

Teenusepakkuja

Teenusepakkuja on asutus, kelle teenuseid on TAATi vahendusel võimalik kasutada.

Teenusepakkujateks võivad saada asutused, mis pakuvad haridus- ja teadusalaseid teenuseid Föderatsiooni Lõppkasutajatele [5].

Lõppkasutaja

Föderatsiooni lõppkasutaja on isik, kellel on kasutajakonto mõne TAATiga liitunud identiteedipakkuja juures. Lõppkasutajaks võib olla (üli)õpilane, õpetaja, õppejõud, haridus- või teadusasutuse töötaja või mõni muu asutusega seotud isik.

2.3 Äriprotsess: Födereeritud sisselogimine

Asutustevaheline sisselogimine on TAATi peamine eemärk ja seega kõige olulisem protsess.

Protsess saab alguse lõppkasutaja soovist teenust kasutada. Teenuse veebilehel kuvatakse TAAT sisselogimisnuppu kas ainsa või ühenda sisselogimise meetoditest või suunatakse sisselogimislink („logi sisse”) otse TAAT jaoturisse. Teenus lisab päringule oma metaandmed.

TAAT jaotur kontrollib teenuse metaandmete vastavust JANUSes fikseeritud tingimustele ning väljastab veateate, kui vastavust ei tuvastata. See võib juhtuda juhul, kui teenus on oma tingimusi muutnud TAAT haldajale teada andmata või kolmas osapool püüab esineda teenusena.

Kui vastavus tuvastatakse, kuvab TAAT jaotur kasutajale nimekirja kõigist liitunud identiteedipakkujatest, mille seast kasutaja valib selle, mille juures tal on konto. Kui kasutaja oma koduasutust nimekirjast ei leia, pole TAATiga sisselogimine võimalik ja protsess katkestatakse.

Pärast asutuse valimist suunatakse kasutaja oma koduasutuse sisselogimislehele. Koduasutus ehk identiteedipakkuja tuvastab kasutaja vastavalt TAAT Föderatsioonipoliitikaga määratud nõuetele, kasutades selleks ID-kaarti, Mobiil-ID või kasutajanime ja parooli [14].

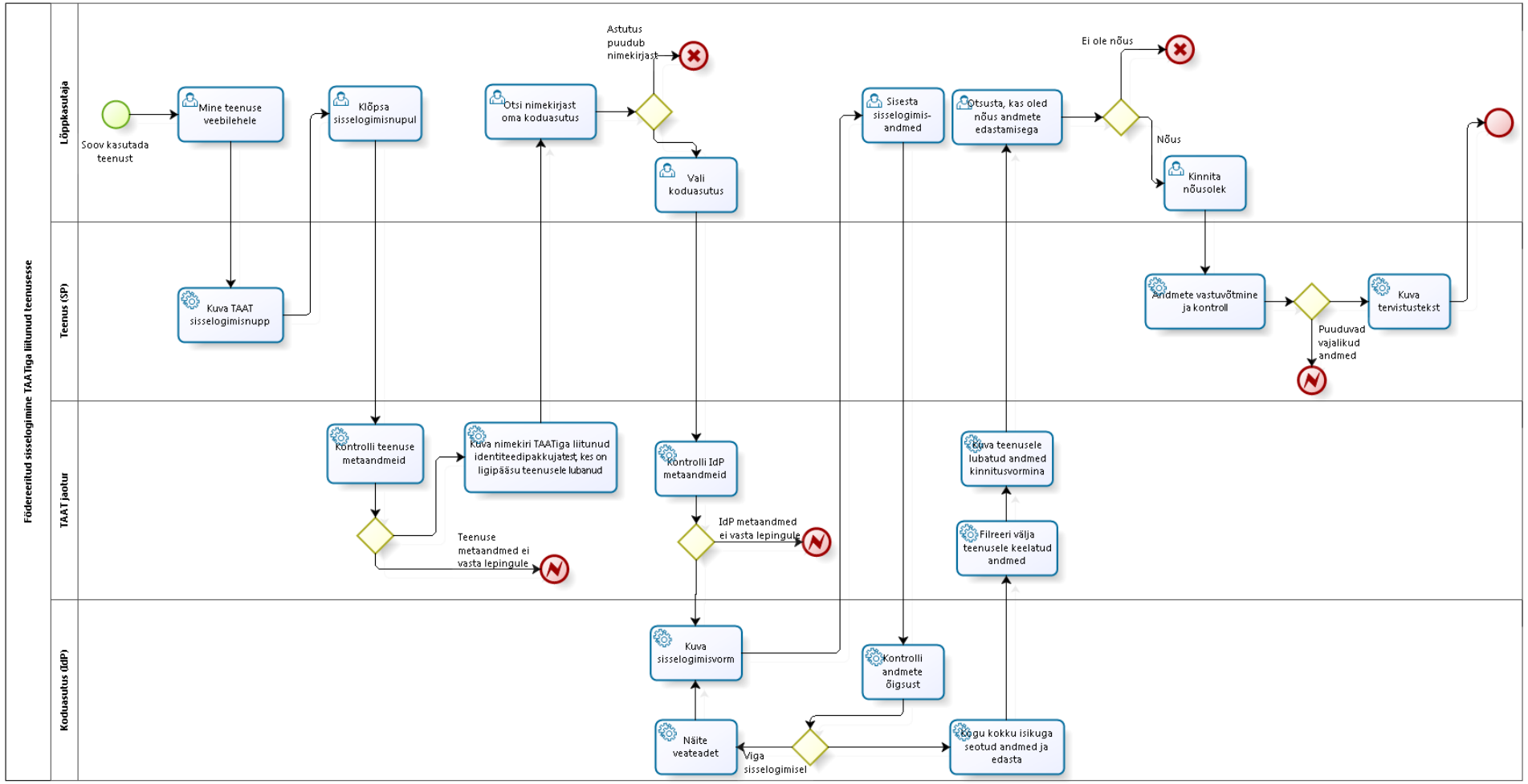
Kui isik on tuvastatud edastab identiteedipakkuja kinnituse isiku tuvastusest koos isikuga seotud

andmetega TAAT jaoturile.

Jaotur filtreerib andmetest välja teenusele keelatud väljad ja kuvab kasutajale kinnitusvormi andmete edastamiseks vajaliku nõusoleku küsimiseks. Ilma nõusolekuta pole võimalik sisselogimist jätkata ja protsess katkestatakse.

Kasutaja nõusoleku saamisel edastatakse andmed teenusele. Juhul kui andmevälju pole piisavalt, võib teenus väljastada veateate. See juhtub juhul, kui identiteedipakkuja ei väljasta teenuse jaoks vajalikus koguses andmeid. Hetkel puudub selline kontroll TAATi poolt keskselt.

Kui vajalikud andmed on olemas, loetakse sisselogimise protsess teostatuks.



Joonis 4: Sisselogimise hetkeolukord Bizagi diagrammina

2.4 Äriprotsess: IdP liitumine TAATiga

Identiteedipakkuja liitumine saab alguse huvist TAATiga liitumise vastu. Kuna TAATi testimine on avatud kõigile, siis saab esimesed sammud ära teha ilma TAATi haldajat teavitamata.

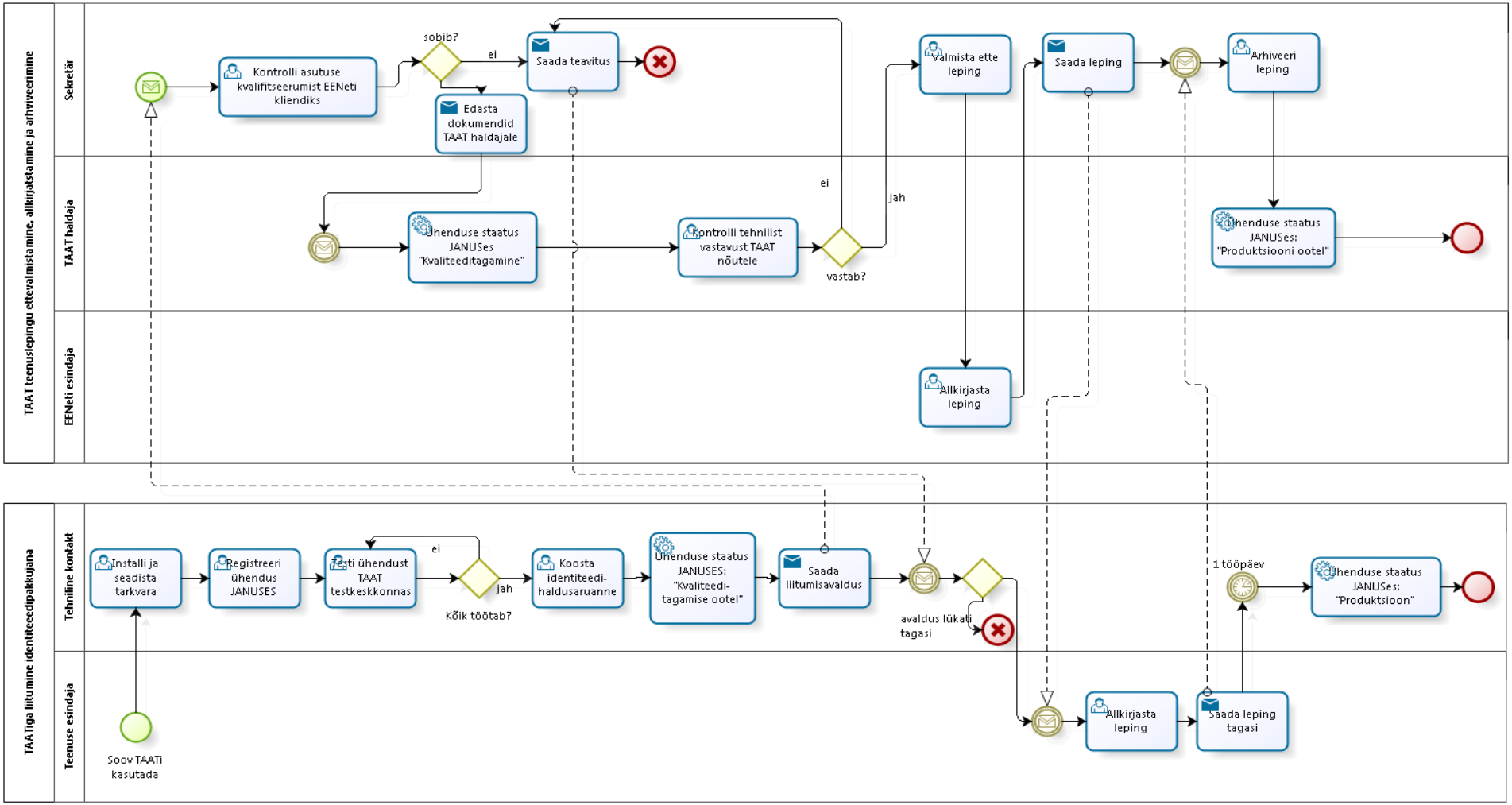
IdP tehniline isik seadistab tarkvara, ühendab selle külge oma kasutajate andmebaasi ning seejärel registreerib ühenduse haldusvahendis JANUS (staatus: „Test”). Kui ühendus töötab TAAT testteenuses, on see valmis TAATiga liitumiseks. IdP määrab JANUSes ühenduse staatuseks „Kvaliteeditagamise ootel” ja saadab EENetile kirjaliku liitumisavalduse, millele on lisatud identiteedihalduse aruanne, kus kirjeldatakse isikute ja kasutajakontode haldamise vastavust TAATi standarditele [5].

Liitumisavalduse võtab vastu sekretär ja kontrollib liituda sooviva asutuse kvalifitseerumist EENeti kliendiks. Kui asutus on juba klient, siis pole kontroll vajalik. Seejärel saadab sekretär IdP andmed koos identiteedihalduse aruandega TAAT operaatorile.

TAAT operaator määrab ühenduse staatuseks JANUSes „Kvaliteeditagamine”, kontrollib identiteedihalduse aruande vastavust TAAT identiteeditagamisprofiilile ning JANUSesse sisestatud metaandmete vastavust TAAT tehnoloogilisele profiilile. Vastavuse tuvastamisel teavitab operaator sekretäri, kes valmistab ette TAAT lepingu, laseb EENeti esindajal selle allkirjastada ja saadab selle IdP esindajale allkirjastamiseks.

Kui allkirjastatud leping tagasi jõuab arhiveerib sekretär selle ning teavitab TAAT operaatorit, kes määrab ühenduse staatuseks JANUSes „Produktsiooni ootel”. Sellekohast teavitust IdP-le ei saadeta.

Viimane samm liitumises on IdP poolt, kes muudavad ühenduse staatuseks JANUSes „Produktsioon”, mida reeglina on võimalik teha ühe tööpäeva möödudes pärast allkirjastatud lepingu saatmist EENetile.



Joonis 5: IdP liitumine, hetkeolukord Bizagi diagrammina

2.5 Äriprotsess: SP liitumine TAATiga

Sarnaselt identiteedipakkujaga saab teenusepakkuja liitumine alguse huvist TAATiga liitumise vastu. Kuna TAATi testimine on avatud kõigile, siis saab esimesed sammud ära teha ilma TAATi haldajat teavitamata.

SP tehniline isik seadistab tarkvara, ühendab selle külge oma kasutajate andmebaasi ning seejärel registreerib ühenduse haldusvahendis JANUS (staatus: „Test”). SP peab enne liitumisavalduse esitamist defineerima andmed, mida ta soovib kasutada luues JANUSes enda asutuse nimelise atribuutide väljastamise poliitika (ARP). Selles lähtutakse minimaalsuse põhimõttest ehk isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks [7].

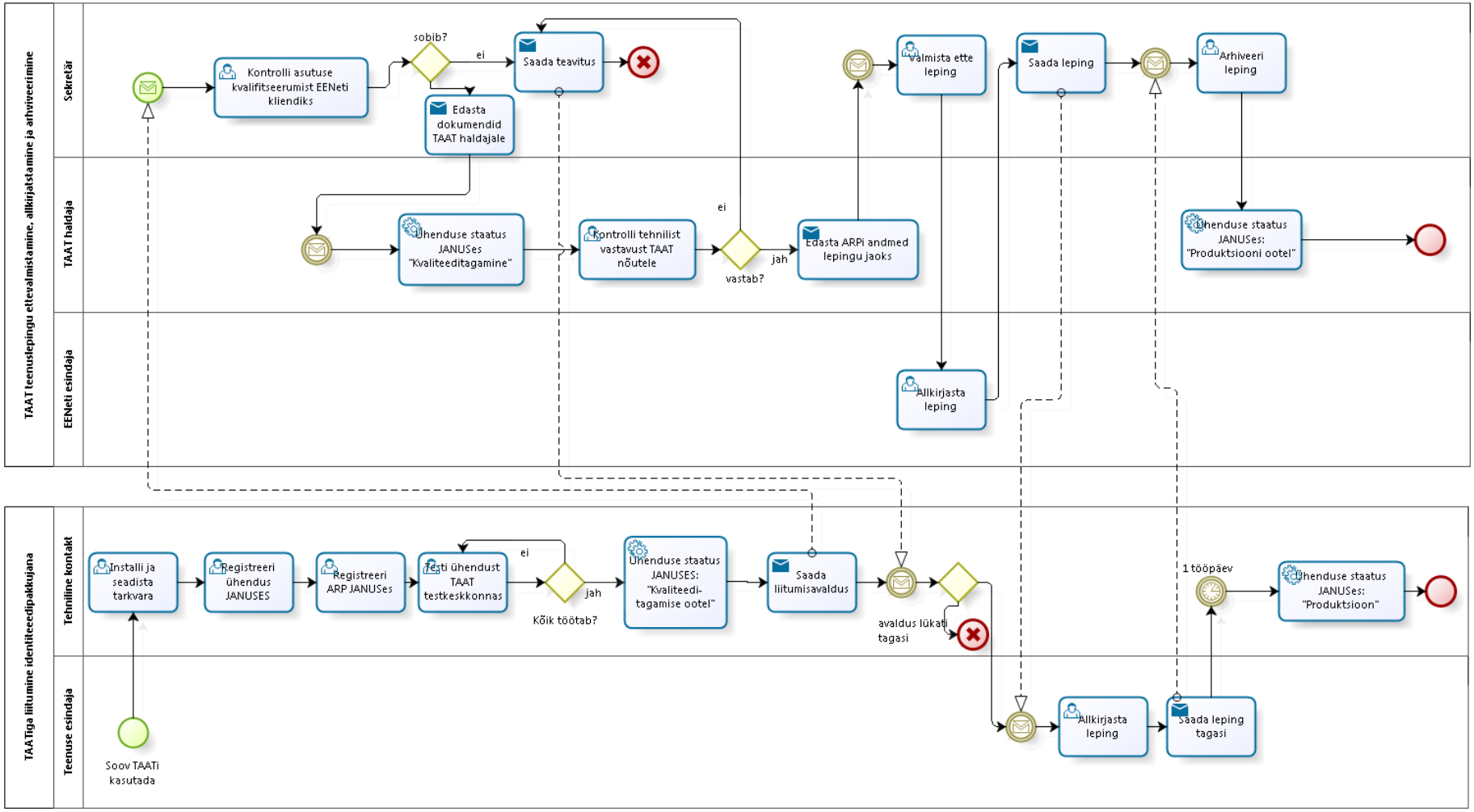
Kui ühendus töötab TAAT test-IdP-ga ning ARP on lisatud, on teenus valmis TAATiga liitumiseks. SP saadab EENetile liitumisavalduse.

Liitumisavalduse võtab vastu sekretär ja kontrollib liituda sooviva asutuse kvalifitseerumist EENeti kliendiks. Kui asutus on juba klient, siis pole kontroll vajalik. Seejärel saadab sekretär SP andmed TAAT operaatorile.

TAAT operaator määrab ühenduse staatuseks JANUSes „Kvaliteeditagamine”, kontrollib JANUSesse sisestatud metaandmete ja ARP-i vastavst TAAT poliitikaga. Vastavuse tuvastamisel teavitab operaator sekretäri, kes valmistab ette TAAT lepingu, ning edastab talle ARP andmed, mis lisatakse lepingusse. Sekretär laseb EENeti esindajal lepingu allkirjastada ja saadab selle SP esindajale allkirjastamiseks.

Kui allkirjastatud leping tagasi jõuab arhiveerib sekretär selle ning teavitab TAAT operaatorit, kes määrab ühenduse staatuseks JANUSes „Produktsiooni ootel”. Sellekohast teavitust SP-le ei saadeta.

Viimane samm liitumises on SP poolt, kes muudavad ühenduse staatuseks JANUSes „Produktsioon”, mida reeglina on võimalik teha ühe tööpäeva möödudes pärast allkirjastatud lepingu saatmist EENetile.



Joonis 6: SP liitumine, hetkeolukord Bizagi diagrammina

3. Soovitav tulemus

Soovitud tulemus on täielik tehniline liidetus eduGAINiga, mis tähendab, et realiseeritud on nii födereeritud sisselogimine väljaspool Eestit paiknevasse teenusesse, kasutades selleks TAATiga liitunud IdP-d, kui ka TAATi teenusesse väljaspool Eestit paikneva IdP kontoga sisselogimine.

3.1 Nõuded

Implementeeritud peavad olema järgmised kasutusjuhud ja nõuded:

1. Kasutajaliides, kus TAATi haldajal on võimalik määrata, milliste IdP metaandmeid eduGAINis avaldatakse, ja millistel SP-del on lubatud ligipääs eduGAINi kuuluvate IdP-de avastamise teenusele.

2. Kasutajaliides, kus SP või IdP esindajal on võimalik vastavalt IdP-sid või SP-sid *whitelist*i lisada. Paljud rahvusvahelised teenused, näiteks CLARIN nõuavad, et SP-le ligipääsuks peab seda olema soovinud mõni föderatsiooni kuuluv IdP [15].

3. Eesti IdP-de nimekirja kuvamine eduGAINi kuuluva teenuste juures.

4. eduGAINi IdPde nimekirja kuvamine TAAT teenuse juures.

5. Võimalus kontrollida, mis mahus andmeid eduGAINi edastatakse, lähtudes seejuures minimaalsete andmete põhimõttest.

6. Kasutaja nõusoleku küsimine andmete edastamiseks ka piiriülese autentimise puhul.

7. Keskselt ei toimu isikuandmete talletamist ega logimist.

Seejuures peab olema TAAT mugavalt kasutatav ka kõigi hetkeolukorras kirjeldatud protsesside puhul, st hoiduma peab lisavaadetest ja pikkadest nimekirjadest, mis vähendavad kasutatavust eestisisese autentimise puhul.

3.2 Äriprotsess: Födereeritud sisselogimine eduGAIN teenusesse TAAT IdP-ga

eduGAIN kasutab *hub-and-spoke* mudeli asemel *mesh*i ehk iga teenus hoiab ise kõikide võimalike IdP-de metaandmeid. Kõikvõimalike IdP-de avastamiseks pöördutakse on vajalik teenuse metaandmete registreerimine eduGAINis ning avastamisteenust (*discovery service)*. See tähendab, et sisselogimisel kuvatavat asutuste nimekirja on võimalik kuvada ka teenuse enda juures, mitte TAAT keskses jaoturis. Kasutajamugavuse suurendamiseks võimaldatakse mõlemat varianti.

IdP-de nimekirja täiendamiseks pöördub teenus eduGAINi poole, kus on avaldatud riiklikesse föderatsioonidesse (sh TAAT) kuuluvate IdP-de metaandmed. TAAT avaldab eduGAINile ainult nende IdP-de andmed, kes on eduGAINi lubatud.

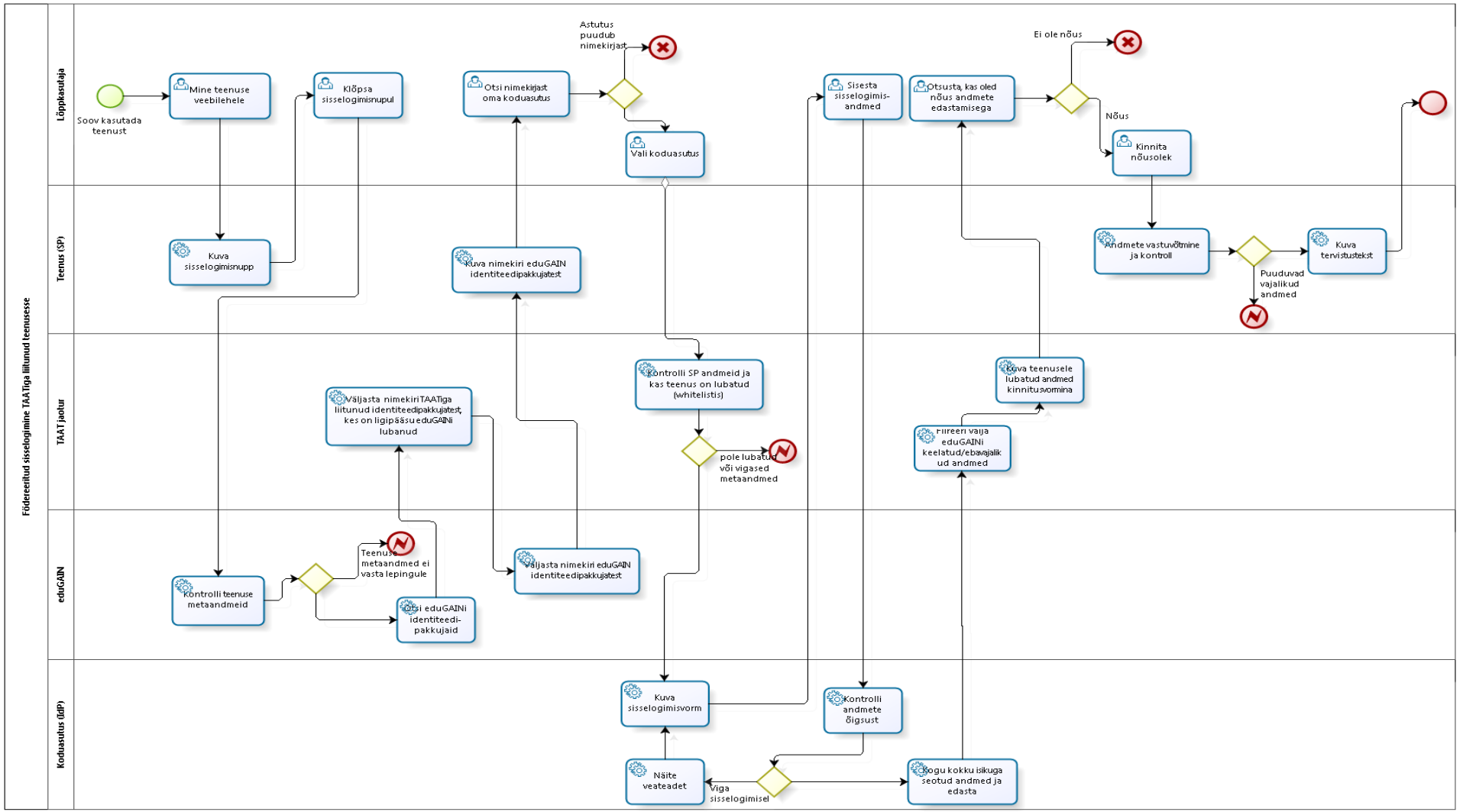
Kasutaja sisselogimisel kontrollib SP metaandmeid TAAT. Implementeeritud on *whitelist*, mille alusel teenustele ligipääsu lubatakse. Samuti filtreerib TAAT välja andmed, mida pole lubatud eduGAINi saata.

Igas muus osas toimub sisselogimise protsess sama moodi nagu hetkeolukorras kirjeldatud.

Probleemid

1. Kuidas ja mis tingimustel implementeerida *whitelist*? Ligipääsu lubamine teenustele vaid nimekirja alusel võib piirata Eesti kasutajate ligipääsu vajaminevatele teenustele, kuid kõik IdP ei pruugi soovida oma kasutajate ligipääsu samadele teenustele. Teenuste filtreerimine iga IdP kohta erinevalt eeldab väga mahukat ja raskesti hallatavat õiguste andmebaasi ning lisatööd IdP poolt.

2. Kuidas määrata, mis andmeid on õigus eduGAINi teenustel kasutada? Võimalikud variandid on teatud grupi andmete edastamine kõigile eduGAINi kuuluvatele teenustele või iga teenusele vajalike andmete määramine. Esimene variant võib olla takistuseks mõne teenuse kasutamisel, teine tähendaks taaskord väga mahuka andmebaasi haldamist [6] ning tõuseb küsimus, milline osapool seda baasi haldama peaks?



Joonis 7: Soovitud sisselogimine eduGAINi teenusesse Bizagi diagrammina

3.3 Äriprotsess: Födereeritud sisselogimine eduGAINi kaudu TAAT teenusesse

Identiteedipakkujate nimekirja kuvamiseks pöördutakse eduGAINi metaandmete repositooriumi poole, kus kontrollitakse päringu autentsus TAAT metaandmete alusel ning seejärel väljastatakse eduGAINiga liidestatud identiteedipakkujate metaandmed.

TAATi poolt peab olema võimalik rakendada *whitelist*i ehk nimekirja identiteedipakkujatest, kellele on ligipääs TAATi lubatud. Nimekirja lubatud asutustest kuvatakse lõppkasutajale.

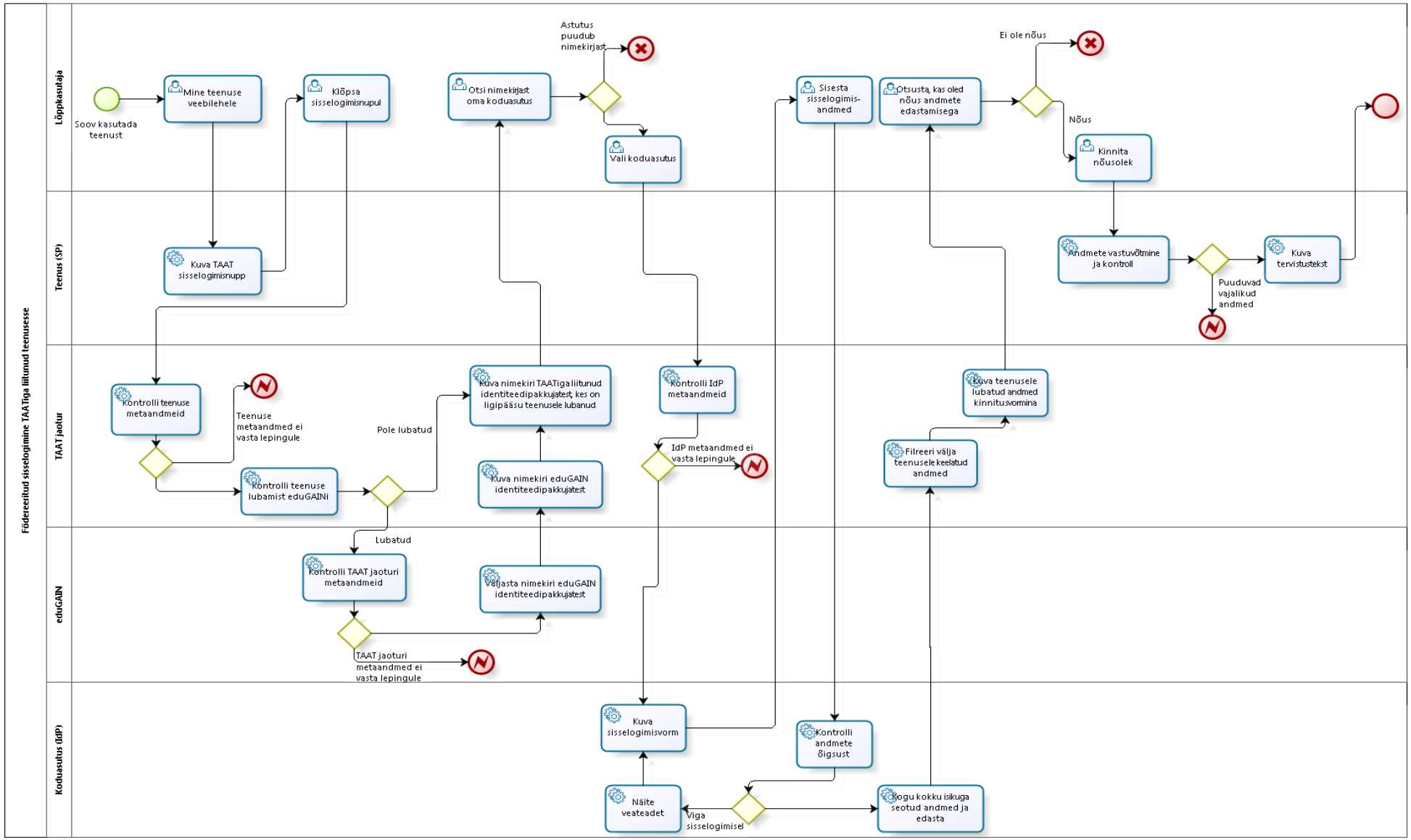
Igas muus osas toimub sisselogimise protsess sama moodi nagu hetkeolukorras kirjeldatud.

Probleemid

eduGAINi vahendusel sisselogimisega tekib kaks suuremat probleemi.

3. Kuidas ja mis tingimustel implementeerida *whitelist*? Asutuste filtreerimine ei tohi piirata teenuse poolt soovitud rahvusvaheliste identeedipakkujate ligipääsu, kuid ühe asutuse poolt soovitud identiteedipakkuja ei pruugi olla teise teenuse jaoks vajalik või soovitud. Asutuste filtreerimine iga teenuse kohta erinevalt eeldab väga mahukat ja raskesti hallatavat õiguste andmebaasi ning lisatööd teenusepakkujate poolt.

4. Kuidas sorteerida pikka asutuste nimekirja, et kasutajal oleks mugav oma asutust leida? Kui kasutajale kuvatakse kõik eduGAINiga liitunud identiteedipakkujad, võib nimekiri ulatuda sadadesse kirjetesse. Sealt sobiva leidmine on keeruline ning Eesti kasutajal ei ole vajadust rahvusvaheliste identiteedipakkujate nägemiseks.



Joonis 8: Soovitud sisselogimine eduGAINi kaudu Bizagi diagrammina

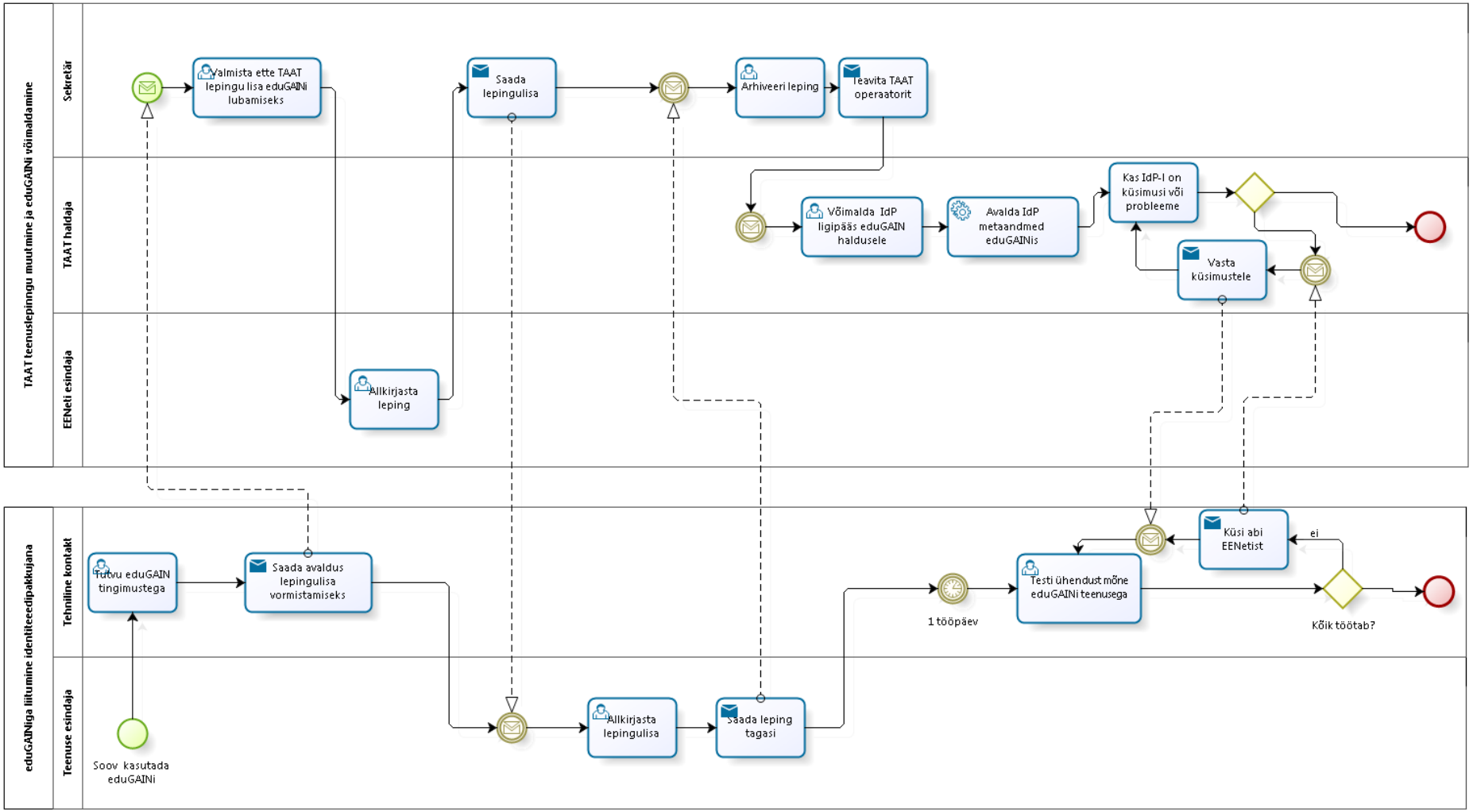
3.4 Äriprotsess: IdP liitumine eduGAINiga

Kuna IdP saab eduGAINiga liituda nii samaaegselt kui ka pärast TAATiga liitumist, siis kirjeldatakse järgnevalt ainult eduGAINiga liitumise protsesse, jättes välja TAATiga liitumise. IdP võib saata sooviavalduse eduGAINi ka oma ühenduse testimisjärgus, kuid lepingulisa ei saa allkirjastada enne lepingu sõlmimist.

IdP saadab vabas vormis avalduse eduGAINi võimaldamiseks EENetti. Kui TAATi nõuded on täidetud, pole ühtegi lisakontrolli vajalik teostada ning EENeti esindaja allkirjastab lepingulisa. Lepingulisa saadetakse IdP esindajale allkirjastamiseks ning pärast seda arhiveerib sekretär lepingu ja teavitab TAAT operaatorit.

TAAT operaator võimaldab IdP ligipääsu eduGAINile haldusliideses, misjärel IdP metaandmed eduGAINis avaldatakse.

IdP testib ühendust mõne eduGAINis oleva avatud teenusega ja vajadusel küsib EENetist abi ühenduse seadistamisel.



Joonis 9: Soovitud IdP liitumine eduGAINiga Bizagi diagrammina

3.5 Äriprotsess: SP liitumine eduGAINiga

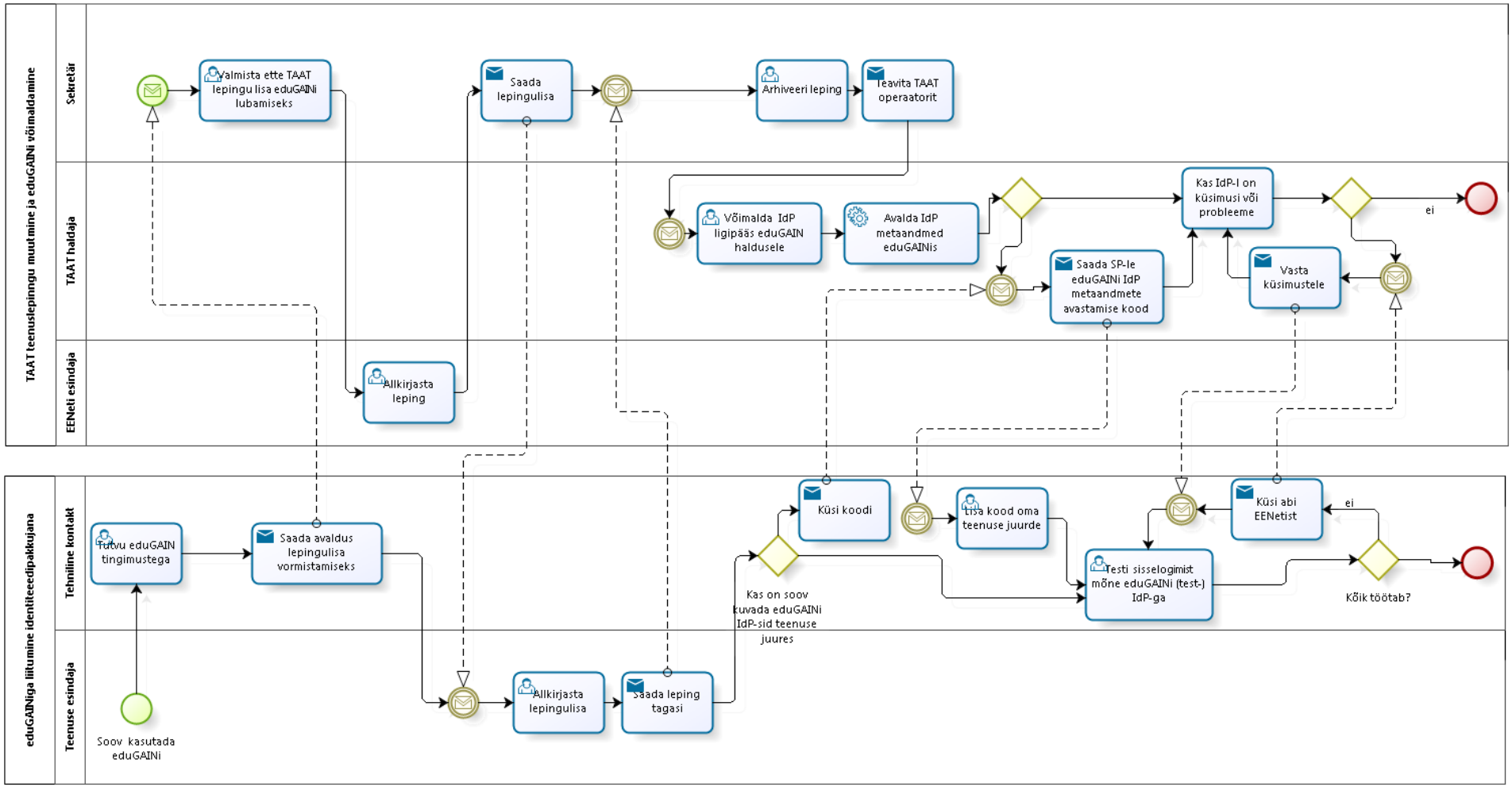
Kuna SP saab eduGAINiga liituda nii samaaegselt kui ka pärast TAATiga liitumist, siis kirjeldatakse järgnevalt ainult eduGAINiga liitumise protsesse, jättes välja TAATiga liitumise. SP võib saata sooviavalduse eduGAINi ka oma ühenduse testimisjärgus, kuid lepingulisa ei saa allkirjastada enne lepingu sõlmimist.

SP saadab vabas vormis avalduse eduGAINi võimaldamiseks EENetti. Kui TAATi nõuded on täidetud, pole ühtegi lisakontrolli vajalik teostada ning EENeti esindaja allkirjastab lepingulisa. Lepingulisa saadetakse SP esindajale allkirjastamiseks ning pärast seda arhiveerib sekretär lepingu ja teavitab TAAT operaatorit.

TAAT operaator võimaldab SP ligipääsu eduGAINile haldusliideses, misjärel SP metaandmed eduGAINis avaldatakse.

Kui SP soovib kasutada eduGAINi IdP-de nimekirja oma veebilehel, siis küsib SP tehniline kontakt TAAT haldajalt vajaminevat koodi ning lisab selle oma teenuse juurde.

Seejärel teenust testitakse mõne eduGAINi kuuluva avatud IdP juures. Probleemide tekkimisel küsitakse abi EENetist.



Joonis 10: Soovitud SP liitumine eduGAINiga Bizagi diagrammina

4. Lahendus

Punktis 3 kirjeldatud olukorra saavutamiseks on vaja järgmisi komponente:

1. JANUSe lisamoodul, mis võimaldab märkida ära teenused ja IdP-d, kes on lubatud eduGAINi, ning kogub kokku ja avaldab nende metaandmed eduGAINis
2. JANUSe lisamoodul, mis võimaldab TAATiga liitunud asutustel märkida ära eduGAINi teenuseid või IdP-sid, kellel on lubatud ligipääs vastavalt nende IdP-le või teenusele (*whitelist*).
3. eduGAINi IdP-de avastusteenus (*discovery service*), mis on kasutuses TAAT jaoturis, kuid mida on võimalik jagada ka teenustele, kes soovivad kasutajale ühte liigutust vähem ehk kuvavad eduGAINi IdP-d ise
4. Filtreerimise süsteem IdP-de nimekirja näitamiseks lõppkasutaja mugavuseks.
5. Keskne filter, mis määrab IdP-de poolt eduGAINi saadetavad andmed, filtreerides välja ainult Eestis kasutatavad või ebavajalikult spetsiifilised andmed.

Kõigi komponentide puhul otsitakse kõigepealt olemasolevaid sobilikke lahendusi või tarkvara ning nende puudumisel või liiga keerulise kohandamise puhul arendatakse vajalik tarkvara majasiseselt.

4.1 Haldusliidese tarkvara

Autorile teadaolevalt ei ole ühtegi terviklikku tarkvaralahendust, mis võimaldaks hallata eduGAINi saadetavaid metaandmeid, vaid kõik *hub-and-spoke* mudelit kasutavad riiklikud föderatsioonid on selle ise välja arendanud. Seega on vajalik liidese arendus.

Komponendid

Haldusliides sisaldab järgmisi komponente:

1. Födereeritud sisselogimine – ei vaja realiseerimist, kuna on JANUSes olemas
2. Kõikide liitunud asutuste kuvamine – ei vaja realiseerimist, kuna on JANUSes olemas
3. Lisaväli liitunud asutuse seadistustes, mis tähistab eduGAIN lepingu olemasolu ja on

muudetav vaid TAAT haldaja poolt

4. Teenus, mis avaldab märgitud asutuste metaandmed eduGAINi

5. Avastusteenus, mille alusel on teenustel võimalik näidata nimekirja IdP-dest teenustele *whitelisti* lisamiseks.

6. Teenus, mis filtreerib välja keskselt paikneva avastusteenuse poolt esitatud nimekirjast keelatud IdP-d, kui autentimispäring tuleb teenuse juurest, kus need on keelatud.

   NB! Kui SP soovib avastusteenust kasutada oma enda teenuse juures, on vajalik ka filtreerimise rakendamist kohalikult.

7. Avastusteenus, mille alusel on teenustel võimalik näidata nimekirja SP-dest, keda IdP saab *whitelist*i lisamiseks.

   NB! Kuna sellist teenust pole võimalik TAATis realiseerida, tuleb pöörduda eduGAINi poole, kasutades selleks näiteks GÉANT TrustBrokerit, mis on metaandmete ja neile kehtivate reeglite repositoorium just sellise eesmärgi täitmiseks [16].

8. Teenus, mis piirab TAATi jaoturis ligipääsu IdP-le, kui päring tuleb keelatud teenuse aadressilt.

   NB! Probleemi, et eduGAINi teenustele kuvatakse IdP-d, kes on keelanud neile teenustele ligipääsu, ei ole võimalik lahendada, kuna filtreerimine sooritatakse keskselt.

Disain

Haldusliidese disain ei kuulu käesoleva töö skoopi.

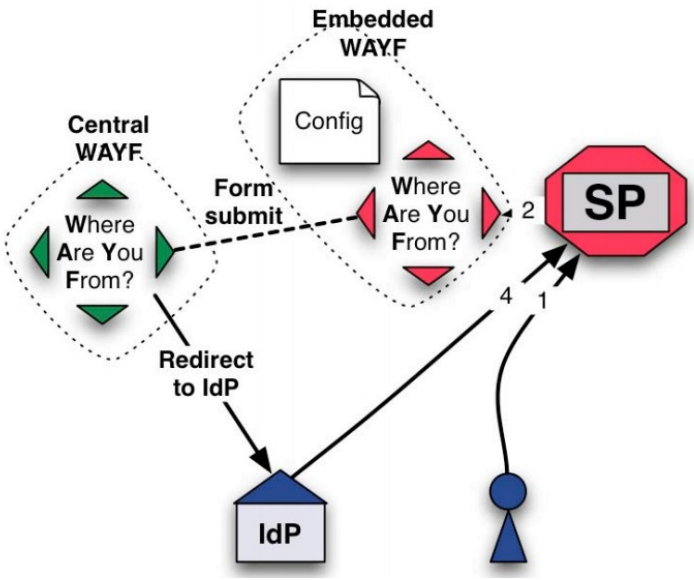
4.2 Avastusteenuse tarkvara

Avastusteenus ehk *discovery service* on teenus, mis võimaldab leida IdP-d mesh stiilis föderatsioonist. eduGAINi poolt soovitatakse ühte kolmest järgnevast tarkvarast, kuna need toetavad konföderatsioone [17].

Kuna kõik mainitud avastusteenused sisaldavad endas ka moodust IdP-de filtreerimiseks lõppkasutajale kuvatavas nimekirjas, puudub vajadus selle komponendi eraldi välja arendamiseks.

SWITCH Embedded Discovery Service/WAYF

Šveitsi akadeemiline AAI SWITCH on välja arendanud lihtsa avastusteenuse, mis kasutab ainult HTML-i ja JavaScripti ning on seega lihtsasti integreeritav nii teenuse juures kui keskselt [18]. Avastusteenus võimaldab *mesh* stiilis föderatsioonil käituda nagu *hub-and-spoke* föderatsioon, lisades keskse teenuse, kus IdP-de nimekirja koostamine toimub.



Joonis 11: SWITCH WAYF avastusteenuse tööpõhimõte [18]

Järeldus: SWITCH WAYF ei sobi soovitud tulemuses kirjeldatud tulemuse saavutamiseks, kuna nõuab nii tarkvara paigaldust iga teenuse juures kui keskselt, võttes teenuselt ära valikuvõimaluse.

DiscoJuice

DiscoJuice on lihtne Javascriptil põhinev avastusteenuse liides. DiscoJuice.org majutab ise keskset avastusteenust. Kui asutus on eduGAINi liikmete nimekirjas (k.a riikliku föderatsiooni kaudu), siis kuulub see DiscoJuice'i poolt usaldatud asutuste nimekirja [19].

DiscoJuice'i liidest on võimalik üles panna nii keskselt kui teenuse juures, kuid selle seadistamisel peab ära märkima vaid eduGAINi, et vältida DiscoJuice'iga otse või teiste konföderatsioonide kaudu ühenduvaid IdP-sid.

Kuna tarkvara tuleb kohandada ja seadistada nii keskseks kasutuseks kui teenuspakkujatele jagamiseks, et soovitud tulemus saavutada, on kasutuselevõtuks vajalik väikses mahus arendustöid.

Joonis 12: Kuvatõmmis DiscoJuice avastamisteenuse demokeskkonnast [19]

Järeldus: DiscoJuice sobib TAATis kasutamiseks, kuid vajab väikses mahus arendustöid. Samuti nõuab selle kasutuselevõttu DiscoJuice.org-i usaldamist.

Shibboleth Discovery Service

Shibboleth on alternatiivne teenuspakkujatarkvara, mis lisaks SP funktsionaalsusele juba sisaldab avastusteenust [20]. Kuna TAATi keskne jaotur ja suur osa teenustest kasutavad aga SimpleSAMLphp-d ei ole see variant sobilik TAATis kasutamiseks.

4.3 Andmete filtreerimise realiseerimine

TAAT jaotur peab suutma filtreerida IdP väljastatud andmed, kui eduGAINi kaudu sisselogimine teostatakse. Kuna andmete filtreerimine teenuse kaupa on äärmiselt mahukas, on otstarbekas edastada igale teenusele kindel kogus andmeid isiku kohta, mis kehtib kõigile IdP-dele.

Sellise funktsionaalsuse realiseerimine on mahult väike lisaarendus, kuid vajalik on IdP-de teavitamine, kuna kasutavate teenuste filtreerimine on seega olulisem, vältimaks lõppkasutaja andmete sattumist ebausaldusväärsete kolmandate osapoolte kätte.

4.4 Arendus- ja halduskulud

Arenduskulude arvestamisel lähtutakse inimtöökuu maksumusest 2000 EUR.

Töö	**Maht (inimtöökuudes)**	**Maksumus (EUR)**
Haldusliidese arendamine JANUSe lisamoodulina	3	6000
DiscoJuice modifitseerimine ja teenustele jagatava tarkvarapaki loomine	0,5	1000
Andmete filtreerimise realiseerimine	0,5	1000
	4	**8000**

Ainus lisahalduskulu on teenuse või IdP eduGAINi lubamine TAAT haldaja poolt ning asutuste nõustamine eduGAINiga liitumisel, mis kokku teeb vähem kui 3h tööd kuus ja seega on juba arvastatud TAAT halduskulude hulka reservina.

Riistvara halduskulusid ei lisandu, kuna kõik lisanduvad teenused ja tarkvara on juba olemasoleva tarkvara lisamoodulid või paiknevad samas serveris.

Kokkuvõte

Töö eesmärk oli viia läbi analüüs TAATi hetkeolukorrast ja soovitud tulemusest pärast rahvusvahelise liidestamise võimaldamist. Seejärel esitada lahendus soovitud tulemuse saavutamiseks väljaarendamist või kasutuselevõttu vajava tarkvara nimistuna ning arendustööks vajalikud kulud.

Tulemused

1. Mõlemad analüüsid teostati nii tekstiliselt kui Bizagi diagrammidena ja neid kasutatakse edaspidi EENetis TAAT protsesside selgitamiseks teistele töötajatele.

2. Selgitati välja probleemid soovitud tulemuse saavutamisel.

3. Probleemide lahendamiseks koostati nimistu vajaminevatest keskkondadest ja teenustest.

4. Leiti sobivad tarkvaralahendused eelmainitud probleemide lahendamiseks kahe nõutud funktsionaalsuse puhul, kirjeldades ja võrreldes olemasolevaid tarkvaralahendusi.

5. Ülejäänud probleemide lahendamiseks vajaminevate arendustööde jaoks esitati arendus- ja halduskulud.

Järeldused

1. DiscoJuice on sobilik tarkvaralahendus TAATi liidestamiseks eduGAINiga ning katab vajaduse nii avastusteenuse kui IdP-de filtreerimise järgi, kuid vajab vähesel määral modifitseerimist TAATis kasutamiseks.

2. Täieliku liidestuse saavutamiseks eduGAINiga ei piisa olemasolevate tarkvaralahenduste kasutuselevõtust vaid on vajalik välja arendada ühenduste haldusliides JANUSe moodulina.

3. eduGAINi edastatavaid isikuandmeid pole otstarbekas filtreerida asutuseti erinevalt vaid kasutada ühtset malli.

4. Nõutud arendustööde eelarve on 8000 eur, võttes aega 4 inimtöökuud ehk kaks kuud tööd kahele arendajale, kusjuures teenuse edasised halduskulud ei suurene olulises mahus.

Käesolev töö on aluseks TAATi tehnilise liidestamise arenduse algatamiseks EENetis.

Summary

The goal of the thesis was to analyze the business processes of Estonian Academic Authentication and Authorization Infrastructure both in current situation and after enabling interfederating through eduGAIN and produce a list of necessary software or developments and their cost.

Results

1. Both analyses were conducted in both text and in form of Bizagi diagrams and they will be used to explain TAAT processes to EENet staff in the future.

2. The issues preventing achieving the goal were identified.

3. Introduced a list of interfaces and services to resolve the issues.

4. Suitable software solutions were found to solve the issues for two necessary functionalities by describing and comparing known solutions.

5. Rest of the problems are solved by developing necessary software, for which development and upkeep cost was presented.

Conclusions

1. DiscoJuice is suitable software for connecting TAAT to eduGAIN and covers the need for discovery service and IdP filtering as well. However, minor modifications are necessary.

2. Existing software solutions are not sufficient to achieve interfederating fully and it is necessary to develop additional JANUS modules.

3. Filtering personal data for every institution separately is not practical, therefore a single attribute release policy will be used.

4. The cost of development will be 8000 EUR, consisting of 4 man-months or two months work for two developers. Upkeep does not increase significantly.

Current thesis will be the basis for future developments in EENet for enabling interfederating through eduGAIN.

Kasutatud kirjandus

1. eduGAINi liikmete nimekiri [WWW] https://technical.edugain.org/status.php (15.05.2015)

2. Fryer, T. Research and education networks around the world and their use - Trabajos Conferencias TICAL [Online] RedCLARA (05.05.2014)

3. EENeti põhimäärus [WWW] http://www.eenet.ee/EENet/pohimaarus2013.html (15.05.2015)

4. TAAT veebileht [WWW] http://taat.edu.ee/ (15.05.2015)

5. TAAT Föderatsioonipoliitika [WWW] http://taat.edu.ee/main/dokumendid/ (15.05.2015)

6. Hörbe, R., A Model for Privacy-enhanced Federated Identity Management [Online] Cornell University (19.01.2014)

7. Isikuandmete kaitse seadus - Riigi Teataja I, 30.12.2010, 11

8. OASIS Security Services Technical Committee Wiki [WWW] https://wiki.oasis-open.org/security/ (15.05.2015)

9. TAAT tehnoloogiline profiil [WWW] http://taat.edu.ee/main/wp-content/uploads/Tehnoloogiline-profiil-v1.3.pdf (05.09.2012)

10. SimpleSAMLphp veebileht [WWW] https://simplesamlphp.org/ (15.05.2015)

11. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [WWW] http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf (15.05.2015)

12. JANUS wiki [WWW] https://github.com/janus-ssp/janus/wiki (15.05.2015)

13. TAAT wiki [WWW] http://taat.edu.ee/wiki/ (15.05.2015)

14. TAAT Identiteeditagamisprofiil http://taat.edu.ee/main/wp-content/uploads/Identiteeditagamisprofiil-v1.3.pdf (05.09.2012)

15. Broeder, D. CLARIN AAI Vision - DFN meeting June 7’th Berlin [Online] Max-Planck Institute for Psycholinguistics (07.06.2009)

16. Pöhn, D., Metzger, D., Hommel, W. A SAML Metadata Broker for Dynamic Federations and Inter-Federations - INFOCOMP 2014, The Fourth International Conference on Advanced Communications and Computation, July 20, 2014 to July 24, 2014, Paris, France [Online] IARIA (20.06.2014)

17. eduGAIN wiki: How to offer a service in eduGAIN [WWW]

https://wiki.edugain.org/How_to_offer_a_service_in_eduGAIN (15.05.2015)

18. Hämmerle, L. Embedded Discovery Service or how to save some clicks during AAI authentication - Zurich, 5. May 2009 [Online] ()

19. DiscoJuice veebileht [WWW] http://discojuice.org/demo/ (15.05.2015)

20. Shibboleth wiki [WWW] https://wiki.shibboleth.net/confluence/display/SHIB2/Installation (15.05.2015)