

SHAMAN-PROJEKTI

Marko Andersson

Mika Rinkinen

Matti Törmä

Timo Valonen

Vaatimusmäärittely

16.5.2005

Versio 1.0

Jyväskylän yliopisto

Tietotekniikan laitos

Tietoja projektista ja dokumentista

Tekijät:	Marko Andersson (maenande@cc.jyu.fi) Mika Rinkinen (mikarin@cc.jyu.fi) Matti Törmä (matorma@cc.jyu.fi) Timo Valonen (tijovallo@cc.jyu.fi)
Yhteystiedot:	Agora, huone Ag C223.3. Puhelin (014) 260 4965. Postilista shaman@korppi.jyu.fi. Postilistan arkisto https://korppi.it.jyu.fi/list-archive/shaman/ .
WWW-sivu:	http://sovellusprojektit.it.jyu.fi/shaman .
Työn nimi:	SHAMAN-projekti, vaatimusmäärittely
Työ:	Vaatimusmäärittely tietotekniikan sovellusprojektiin
Sivumäärä:	36
Tilaja:	Jyväskylän yliopisto, ATK-keskus
Tiivistelmä:	SHAMAN-projekti suunnittelee keskitetystä käyttäjähallinnasta vastaavan AMAN-järjestelmän seuraajan. Projekti toteuttaa järjestelmän prototyypiasteelle. Dokumentti kuvaa sovelluksen vaatimukset.
Avainsanat:	AMAN, tietokanta, käyttäjätunnus, salasana, käyttäjähallinta, hallinta.

Versiohistoria

Versio	Pvm	Tekijä	Kommentti
0.225	25.2.2005	Marko Andersson	Dokumentin laatiminen.
0.228	28.2.2005	Timo Valonen	Dokumentin muokkaus.
0.228.2	28.2.2005	Marko Andersson	Dokumentin kirjoitus.
0.301	1.3.2005	Timo Valonen	Dokumentin kirjoitus.
0.302	2.3.2005	Timo Valonen	Dokumentin kirjoitus.
0.308	8.3.2005	Marko Andersson	Dokumentin kirjoitus.
0.309	9.3.2005	Mika Rinkinen	Käyttötapauksien lisäys.
0.314	14.3.2005	Matti Törmä	Käyttötapauksien parannus.
0.314.2	14.3.2005	Mika Rinkinen	Käyttötapauksien parannus.
0.323	23.3.2005	Mika Rinkinen	Dokumentin kirjoitusasun parannus.
0.330	30.3.2005	Mika Rinkinen	Dokumentin korjailu.
0.408	8.4.2005	Mika Rinkinen	Dokumentin korjailu ja parannus.
0.412	12.04.2005	Mika Rinkinen	Prioriteettien lisäys toiminnallisiin vaatimuksiin.
0.425	25.4.2005	Mika Rinkinen	Dokumentin kirjoitusasun parannus, käyttötapauksien tarkennus sekä vaatimusten lisääminen ja tarkennus.
0.501	1.5.2005	Mika Rinkinen	Kirjoitusasun viimeistely ja prioriteettien ja käyttötapauksien hienosäätö.
0.510	10.5.2005	Mika Rinkinen	Pienten muotoilu- ja asiavirheiden korjaus.
0.513	13.5.2005	Mika Rinkinen	Kirjoitusvirheen korjaus.
1.0	16.5.2005	Mika Rinkinen	Julkaistu versio.

Termiluettelo

Projektin aiheeseen ja toteutustekniikoihin liittyviä termejä ja käsitteitä ovat seuraavat:

Acta	on Jyväskylän avoimessa yliopistossa käytössä oleva opintosuoritusrekisteri.
Alaryhmät	ovat ryhmiä, jotka ovat tietyn ryhmän jäseniä.
Apache	on ilmainen HTTP-palvelinohjelmisto.
SHELL-skripti	on UNIX- ja Linux-koneissa ajettava komentorivitiedosto.
CSS	(Cascade Style Sheets) on WWW-sivujen ulkoasun määrittelyyn käytetty kieli, jolla voidaan erottaa sivujen sisältö ja esitysasu toisistaan.
Fortime	on rekisteri, jossa säilytetään tietoja henkilökunnasta ja muista Jyväskylän yliopistolta palkkioita saavista.
FunetEduPerson	on skeema, joka määrittelee henkilön attribuutit korkeakoulujen välisessä viestinnässä.
HAKA	on Suomen yliopistojen ja ammattikorkeakoulujen yhteinen käyttäjätunnistusjärjestelmä. Siihen liittyneen korkeakoulun käyttäjät pääsevät yhdellä kirjautumisella korkeakoulusektorin palveluihin riippumatta, siitä kuka palvelun tuottaa.
Henkilö	kuvaava henkilöä ja hänen tietojaan.
HTML-template	on Perlin moduuli, joka mahdollistaa skriptien erottamisen HTML-sivusta.
JORE	on Jyväskylän yliopistossa kehitetty ja käytössä oleva opintosuoritusrekisteri.
Kohdejärjestelmät	ovat järjestelmiä, joihin käyttäjähallintajärjestelmä vie tietoa. Kohdejärjestelmiä käytetään rajapintojen kautta, ja niitä ovat mm. Kerberos, LDAP ja CGI.
Korppi	on Jyväskylän yliopiston opintotietojärjestelmä.
Lähdejärjestelmät	ovat järjestelmiä, joista käyttäjähallintajärjestelmä saa tietonsa henkilöistä. Järjestelmät ovat Fortime, Jore, Acta ja Korppi sekä salasana.jyu.fi.
Perl	on ilmainen skriptikieli, jolla voidaan toteuttaa myös ajettavia ohjelmia.

PostgreSQL	on ilmainen tietokannanhallintajärjestelmä.
Ryhmä	muodostaa toisten ryhmien kanssa ryhmähierarkian. Ryhmiin voidaan liittää käyttäjätunnuksia, resursseja ja toisia ryhmiä. Ryhmä voi myös kuvata erilaisia rooleja. Tunnuskohtaiseen ryhmään voi liittyä vain yksi tunnus.
Shibboleth	on organisaatorajat ylittävä käyttäjien hallintaprotokolla, joka tarjoaa autentikointi-, autorisointi- ja pääsynvalvontapalveluja.
Siirtotiedosto	Lähdejärjestelmästä tuleva tiedosto, joka sisältää henkilötietoja.
Tunnukset	ovat henkilöiden käyttäjätunnuksia. Henkilöllä voi olla useampia tunnuksia.
Yläryhmät	ovat tietyn ryhmän yläpuolella olevia ryhmiä, joiden jäsenenä ryhmä on.

Sisältö

1 JOHDANTO.....	1
2 NYKYINEN KÄYTTÄJÄTUNNUSTEN HALLINTAPROSESSI.....	2
2.1 HENKILÖTIETOJEN TUOMINEN LÄHDEJÄRJESTELMISTÄ.....	2
2.2 TIETOJEN VIEMINEN KOHDEJÄRJESTELMIIN.....	4
2.3 KÄYTTÄJÄN KÄYTTÖLIITTYMÄ.....	5
2.4 PÄÄKÄYTTÄJÄN KÄYTTÖLIITTYMÄ.....	5
3 TOIMINNALLISET VAATIMUKSET.....	6
3.1 RAJAPINTOJEN ASETTAMAT VAATIMUKSET.....	6
3.2 TILAT JA TILASHIIRTUMÄT.....	7
3.3 RESURSSIT.....	7
3.4 RYHMÄJÄSENYUDET.....	8
3.5 HISTORIA- JA LOKITIEDOT.....	9
3.6 KÄYTTÖLIITTYMÄT.....	9
3.7 LAITOSTEN JA TIEDEKUNTIEN KÄYTTÖLIITTYMÄ.....	10
3.8 JÄRJESTELMÄN PÄÄKÄYTTÄJÄN KÄYTTÖLIITTYMÄ.....	11
3.9 KÄYTTÄJÄN KÄYTTÖLIITTYMÄ.....	12
3.10 TIETOTURVA.....	13
4 TEKNISET VAATIMUKSET.....	14
5 KÄYTTÖTAPAUKSET.....	15
5.1 FORTIMEN KÄYTTÖTAPAUKSET.....	15
5.1.1 HENKILÖN LUONTI.....	15
5.1.2 HENKILÖN TIETOJEN MUUTTAMINEN.....	17
5.1.3 HENKILÖN HENKILÖKUNTASTATUKSEN POISTO.....	18
5.2 JOREN KÄYTTÖTAPAUKSET.....	19
5.2.1 HENKILÖN LUONTI.....	19
5.2.2 HENKILÖN OPISKELIJASTATUKSEN POISTO.....	20
5.2.3 HENKILÖN TIETOJEN MUUTTAMINEN.....	21
5.3 KORPIN KÄYTTÖTAPAUKSET.....	23
5.3.1 RYHMÄN LUOMINEN.....	23
5.3.2 RYHMÄN POISTO.....	24
5.3.3 RYHMÄN OIKEUKSIEN MUUTTAMINEN.....	26
5.3.4 KÄYTTÄJÄTUNNUKSIEN LISÄÄMINEN RYHMÄÄN.....	27
5.3.5 KÄYTTÄJÄTUNNUKSIEN POISTAMINEN RYHMÄSTÄ.....	28
5.3.6 HENKILÖIDEN LUONTI.....	29
5.4 SALASANA.JYU.FI:N KÄYTTÖTAPAUKSET.....	30
5.4.1 KIRJAUTUMINEN.....	30
5.4.2 HENKILÖN YHTEYSTIETOJEN KATSELU.....	31
5.4.3 HENKILÖN YHTEYSTIETOJEN MUOKKAUS.....	32
5.4.4 KÄYTTÄJÄTUNNUKSEN SALASANOJEN MUUTOS.....	33
5.4.5 KÄYTTÄJÄTUNNUKSEN OIKEUSTIETOJEN KATSELU.....	35
6 YHTEENVETO.....	36
LÄHTEET.....	37

1 Johdanto

SHAMAN-niminen tietotekniikan sovellusprojekti suunnittelee ja toteuttaa käyttäjätunnusten ja salasanojen sekä käyttöoikeuksien hallinnointiin käytettävän järjestelmän. Järjestelmä kehitetään AMAN-nimisen järjestelmän korvaajaksi, joka ei enää vastaa sille asetettuja uusia vaatimuksia.

AMAN-järjestelmällä hallitaan Jyväskylän yliopiston opiskelijoiden, henkilökunnan ja muiden tahojen käyttäjätunnuksia ja salasanoja eri kohdejärjestelmissä. AMAN välittää käyttäjätunnukset ja salasanat eri autentikointipalvelimille, joista eri järjestelmät voivat autentikoida käyttäjän. AMAN saa tietonsa automaattisesti lähdejärjestelmistä, joita ovat mm. JORE, Fortime, Acta ja Korppi.

AMAN-järjestelmän heikkoutena on tietokannan puutteellinen suunnittelu, joten tietokanta ei enää suoriudu uusista vaatimuksista. Käyttöliittymän HTML-kieli on Perl-lähdekoodiin seassa, joten käyttöliittymän muokkaaminen vaatii ohjelmointitietämystä ja on hankalaa.

Dokumentissa esitellään projektissa toteutettavalle sovellukselle asetetut vaatimukset ja käyttötapaukset. Sovelluksen suunnitteluun ja toteutukseen tarvittavan vaatimusten määrittelyn ovat suorittaneet tilaaja ja SHAMAN-projektiryhmä yhdessä.

Projektisuunnitelma käsittelee tarkemmin projektin tavoitteet, aikataulutuksen sekä riskit. Sovellusraportti esittelee tarkemmin järjestelmän käyttöliittymien ja moduulien rakenteet. Projektin lopussa laadittavassa projektiraportissa esitellään mm. tavoitteiden ja aikataulun toteutuminen, sekä kuvataan alkuperäisten tavoitteiden ja aikataulun muutoksia ja niiden syitä. Raportissa tarkastellaan myös riskien toteutuminen, ennakointi ja vaikutus projektin kulkuun.

Luvussa 2 kuvataan nykyisen AMAN-järjestelmän toimintaa. Luvussa 3 esitetään uudelle järjestelmälle asetettavat toiminnalliset vaatimukset ja käyttöliittymien tarjoamat toiminnot. Luku 4 käsittelee teknisiä vaatimuksia. Luvussa 5 esitetään käyttötapaukset.

2 Nykyinen käyttäjätunnusten hallintaprosessi

Nykyisen käyttäjätunnusten hallintaprosessin päätehtäviä ovat tietojen päivittäminen lähdejärjestelmien muodostamien siirtotiedostojen sekä käyttöliittymien kautta, käyttäjien lisääminen sekä tietojen vieminen kohdejärjestelmiin. AMAN-järjestelmä saa tietonsa lähdejärjestelmiltä, joita ovat JORE, Fortime ja Korppi. Tietoja voidaan viedä ulospäin kohdejärjestelmille, mm. Kerberosin ja LDAPin kautta. Tietoja voidaan viedä ulospäin myös suoraan, tiedoston kautta tai CGI-rajapinnan kautta.

2.1 Henkilötietojen tuominen lähdejärjestelmistä

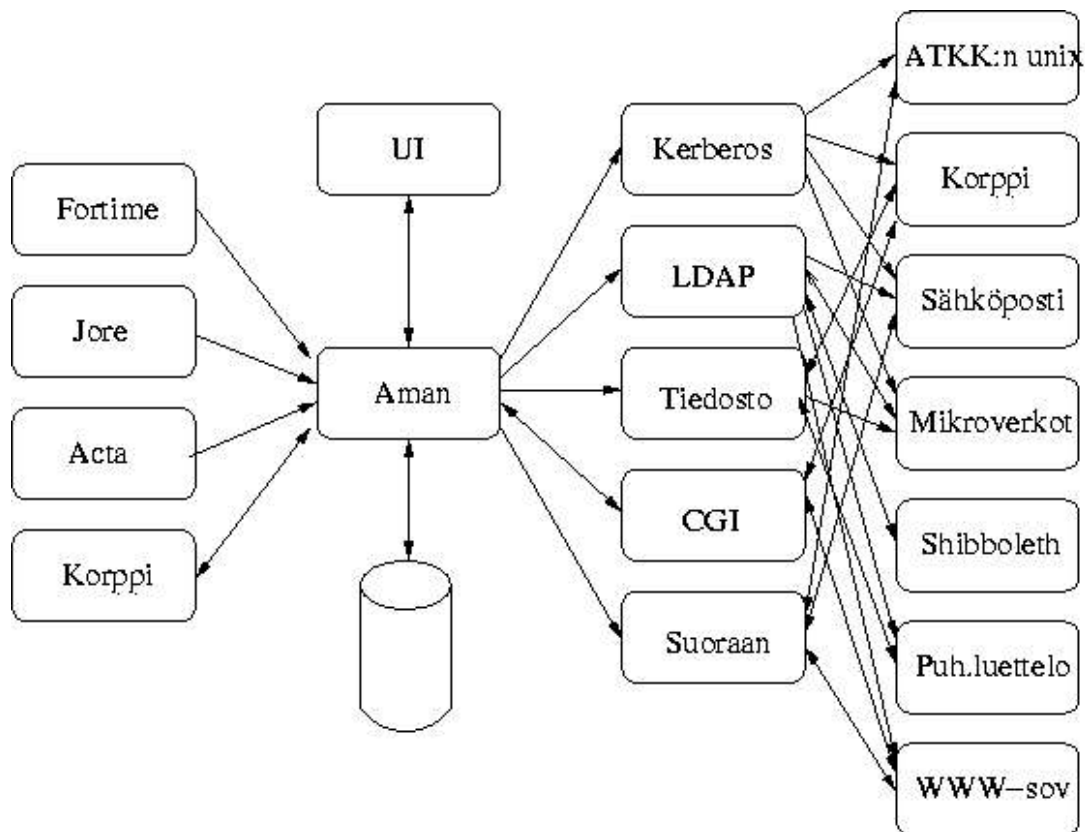
Jyväskylän yliopistoon tulee opiskelemaan joka vuosi noin 2000 uutta opiskelijaa. Kaikille uusille opiskelijoille on luotava tunnukset yliopiston atk-järjestelmiin, sekä sähköpostilaatikat ja kotisivuhakemistot.

Henkilöt saavat tunnusten kautta perusoikeudet tiettyihin kohdejärjestelmiin (kuten sähköpostiin) riippuen siitä, mihin ryhmään (esim. opiskelijat, henkilökunta) he kuuluvat. Tunnuksille voidaan myöntää myös erityisoikeuksia, joita ovat mm. oikeudet rinnakkaislaskentakursilla käytetylle koneelle. Erityisoikeudet joudutaan AMAN-järjestelmässä antamaan ylläpidon käyttöliittymän kautta. Eräajoina tuotavien siirtotiedostojen tietojen päivitys vaatii pääkäyttäjän toimintaa virheellisen, ristiriitaisen tai puutteellisen tiedon tapauksessa.

Jyväskylän yliopiston AMAN-järjestelmä saa tietonsa siirtotiedostoina eri lähdejärjestelmiltä, joita ovat mm. JORE, Fortime, Acta ja Korppi. Lähdejärjestelmät generoivat ajastetusti siirtotiedostot, jotka lähetetään AMAN-järjestelmälle. JOREsta tiedot tulevat CSV-tiedostona, jossa kentät on eroteltu pilkulla toisistaan. Fortimelta tulevien siirtotiedostojen kentät ovat samanpituisia riippumatta kentän sisällöstä. AMAN-järjestelmä vertaa oman tietokannan sisältöä siirtotiedostoihin sekä lisää tietokantaansa uudet henkilöt ja käyttäjätunnukset sekä päivittää muuttuneet tiedot riippuen siitä, mistä lähdejärjestelmästä tieto välitetään AMANiin. Muutokset henkilön tunnuksen ryhmiin kuulumisessa tulee välittää kohdejärjestelmiin oikeuksien muutoksena.

Tietoa välittävien järjestelmien kesken ei ole määritelty mitään yhtenäisiä tietojoukkoja, josta johtuen esimerkiksi laitos-tieto saattaa poiketa järjestelmien välillä. Suurin syy tähän on ollut tietojen vapaa muokattavuus, joten sama tieto on voitu ilmaista usealla eri tavalla, kuten lyhennettynä tai kokonaan kirjoitettuna.

Kuva 1 esittää AMANille tietoja toimittavat lähdejärjestelmät sekä kohdejärjestelmät, joille AMAN välittää käyttöoikeustietoja.

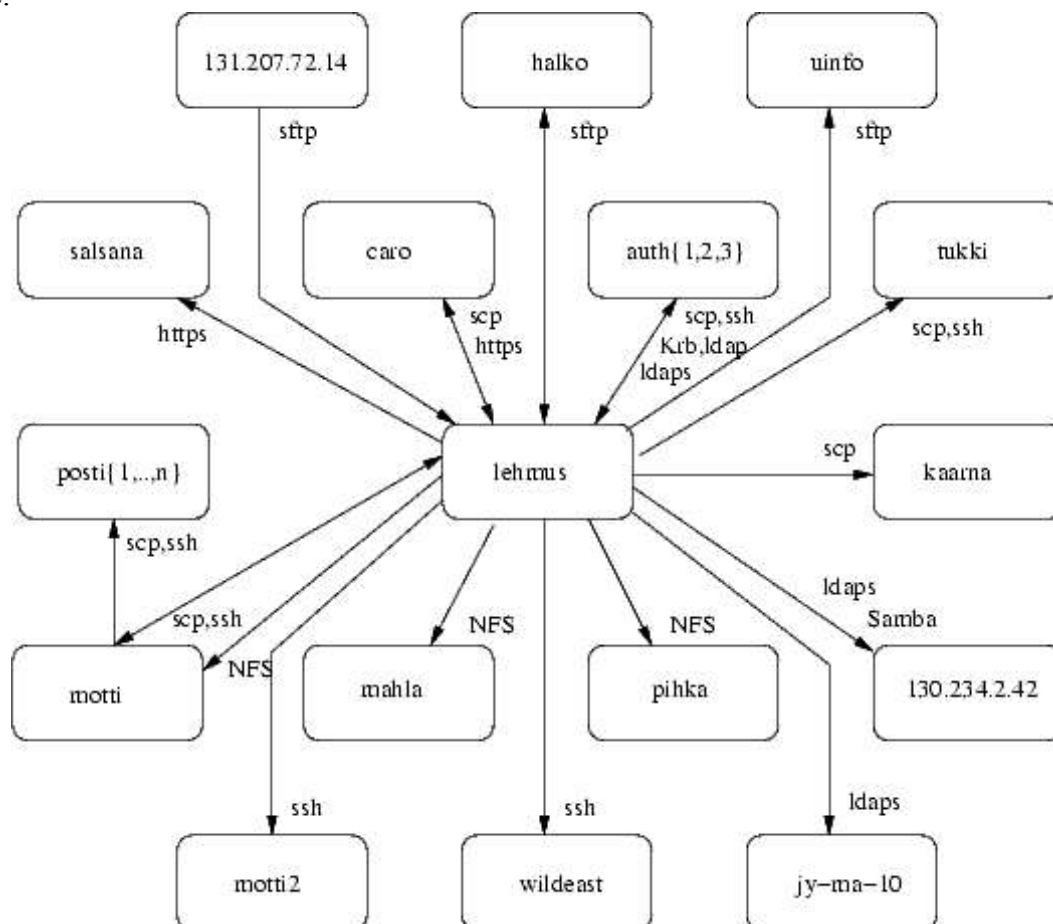


Kuva 1. AMAN-järjestelmän yhteydet muihin järjestelmiin [Toivonen].

2.2 Tietojen vieminen kohdejärjestelmiin

AMAN generoi tietoja käyttäjätunnuksien käyttöoikeuksista eri autentikointipalveluille, kuten Kerberosille ja LDAP-hakemistoihin. Kohdejärjestelmät autentikoivat käyttäjät näiden palveluiden kautta, eikä suoraan AMAN-järjestelmästä. Tiedot generoidaan eräajoina, jolloin AMAN-järjestelmä siirtää tiedot käyttäjien oikeuksista autentikointipalvelimille. Kriittisissä toimenpiteissä (kuten tunnusten lukituksissa) oikeuksien muutokset tulee välittyä reaaliajassa. Myös ylläpidon käyttöliittymästä suoritettujen muutosten tulee näkyä järjestelmissä reaaliajassa.

Kuvassa 2 on Jyväskylän yliopiston palvelimet, joiden kanssa AMAN-järjestelmä keskustelee.



Kuva 2. AMAN-järjestelmä (lehmus) on yhteydessä useisiin palvelimiin [Toivonen].

2.3 Käyttäjän käyttöliittymä

Käyttäjät voivat tarkastella ja muuttaa joitakin tietojaan CGI-pohjaisen salasana.jyu.fi-käyttöliittymän kautta. Käyttöliittymän kautta voi muuttaa esimerkiksi salasanaa ja postin uudelleenohjausta.

2.4 Pääkäyttäjän käyttöliittymä

Pääkäyttäjän käyttöliittymästä voidaan hallita kaikkia tietoja AMAN-järjestelmässä. Pääkäyttäjä voi mm. muokata henkilön oikeuksia, lukita tunnuksia ja muuttaa henkilötietoja. Käyttöliittymässä on muutamassa kohdassa vapaat tekstikentät esimerkiksi laitoksen nimelle, joka mahdollistaa erilaisten nimien käyttämisen samaa laitosta kuvattaessa.

Käyttäjille voidaan myöntää erityisoikeuksia esimerkiksi johonkin kurssiin liittyen, mutta nämä joudutaan tekemään käsin. Opiskelijoilta vaaditaan hakemus, jolla he hakevat lisäoikeuksia kurssin ajaksi. Kurssin loputtua oikeudet poistetaan käsin.

3 Toiminnalliset vaatimukset

AMAN-järjestelmän korvaavan järjestelmän olennaisena vaatimuksena on nykyaikaistaa olemassaoleva järjestelmä. AMAN-järjestelmä on hankala ylläpidettävä, mukautuvuus uusille kohdejärjestelmille on huono ja järjestelmän toiminallisuudessa on puutteita. Järjestelmän toteutus jakaantuu karkeasti viiteen osaan: dynaamiseen käyttöliittymään, lähde- ja kohdejärjestelmien rajapintoihin, tietokantaan sekä tietokannan hallintamoduuleihin.

Toiminnalliset vaatimukset kuvaavat toiminnot, joita järjestelmältä odotetaan. Vaatimukset on numeroitu ja niiden prioriteetit on jaoteltu tasoihin välttämätön, tärkeä, toteutetaan ajan salliessa ja ei toteuteta projektissa.

3.1 Rajapintojen asettamat vaatimukset

Rajapintojen vaatimukset kuvaavat seuraavia lähde- ja kohdejärjestelmien asettamia vaatimuksia:

- 1.1. Lähdejärjestelmiltä tulevat siirtotiedostot käsitellään määräajoin ja muuttunut tieto päivitetään tietokantaan. Prioriteetti on ajan salliessa.
- 1.2. Lisättäessä uutta henkilöä järjestelmään voidaan valita, luodaanko samalla henkilölle myös käyttäjätunnus, kotihakemisto ja sähköpostilaatikko. Prioriteetti on ajan salliessa.
- 1.3. Lisättäessä uutta henkilöä järjestelmään voidaan henkilön käyttäjätunnus liittää organisaation ja roolin mukaisten ryhmien jäseneksi. Tällöin tietyn käyttäjätunnuksen omaava henkilö saa oikeuksia tiettyihin järjestelmiin (kuten Korppi, mikroverkot ja UNIX). Prioriteetti on ajan salliessa.
- 1.4. Henkilöllä voi olla useita käyttäjätunnuksia, joista yksi voidaan valita ensisijaiseksi. Prioriteetti on tärkeä.

- 1.5. Järjestelmän on mahdollistettava tiettyjen oikeuksien siirtäminen toiselle henkilölle. Esimerkiksi lomien yhteydessä tai laitoksen amanuenssin vaihtuessa uudelle amanuenssille on pystyttävä antamaan helposti ko. roolille kuuluvat oikeudet. Prioriteetti on tärkeä.
- 1.6. Tietyn lähdejärjestelmän kautta luotu henkilö ja käyttäjätunnus täytyy pystyä merkitsemään kyseisen järjestelmän luomaksi. Prioriteetti on ajan salliessa.

3.2 Tilat ja tilasiirtymät

Seuraavat vaatimukset liittyvät tiloihin ja tilasiirtymiin:

- 2.1 Tilasiirtymä voidaan määritellä henkilölle, käyttäjätunnukselle, käyttäjätunnuksen ryhmäjäsennyksille, ryhmille ja ryhmien ryhmäjäsennyksille. Prioriteetti on tärkeä.
- 2.2 Järjestelmä suorittaa automaattisesti määritetyt tilasiirtymät niille määritettyinä ajanhetkinä. Prioriteetti on tärkeä.
- 2.3 Tilasiirtymässä voidaan suorittaa ennalta määriteltyjä järjestelmän sisäisiä tai ulkoisia toimintoja. Prioriteetti on tärkeä.

3.3 Resurssit

Resurssien vaatimukset kuvaavat seuraavia tietojen käsittelyyn liittyviä vaatimuksia:

- 3.1. Järjestelmän täytyy pystyä tallentamaan erityyppistä resurssitietoa käyttäjätunnuksista, ryhmistä ja rajapinnan järjestelmistä (esim. sähköpostialiaksia, sekä levy- ja tulostuskiintiöitä). Prioriteetti on tärkeä.
- 3.2. Tiedon tallennukseen tarkoitettuja tietotyyppisiä täytyy pystyä muokkaamaan, lisäämään ja poistamaan. Prioriteetti on ajan salliessa.

- 3.3. Järjestelmän tulee toimia henkilötietorekisterinä, josta voidaan helposti hakea ja ylläpitää henkilöiden tietoja. Prioriteetti on välttämätön.
- 3.4. Järjestelmän tulee toteuttaa FunetEduPerson-yhteensopivuus. Prioriteetti on välttämätön.
- 3.5. Tietojen muuttuessa täytyy kohdejärjestelmille viedä muuttunut tieto. Prioriteetti on tärkeä.
- 3.6. Vietäessä tietoa kohdejärjestelmille täytyy paluutieto käsitellä, virheet havaita ja yrittää tietojen viemistä myöhemmin uudelleen. Prioriteetti on tärkeä.

3.4 Ryhmäjäsennydet

Ryhmäjäsennyden vaatimukset kuvaavat seuraavia ryhmähierarkian vaatimuksia:

- 4.1 Henkilön käyttäjätunnus voi liittyä moneen ryhmään. Prioriteetti on välttämätön.
- 4.2 Ryhmä voi liittyä moneen ryhmään. Prioriteetti on välttämätön.
- 4.3 Ryhmät muodostavat ryhmähierarkian, jossa oikeudet periytyvät ylärhymiltä alaryhmille. Prioriteetti on välttämätön.
- 4.4 Henkilö saa oikeudet ryhmistä, joihin hänen käyttäjätunnuksensa kuuluu. Henkilön käyttäjätunnus voi kuulua moneen ryhmään (esim. opiskelijoihin ja työntekijöihin) saaden kaikki niille kuuluvat oikeudet. Prioriteetti on välttämätön.

3.5 Historia- ja lokitiedot

Historiatietojen vaatimukset kuvaavat järjestelmän tietojen vanhoja arvoja ja niiden jäljitettävyyttä. Lokitietojen vaatimukset liittyvät järjestelmän sisäiseen toimintaan. Vaatimuksia ovat seuraavat:

- 5.1 Järjestelmä kirjoittaa historiatietoja tietojen muutoksien yhteydessä. Prioriteetti on tärkeä.
- 5.2 Historiatiedoista voidaan hakea entisiä arvoja ainakin henkilöiden, käyttätunnuksien ja ryhmien tiedoille. Prioriteetti on ajan salliessa.
- 5.3 Lokitietoihin kirjoitetaan tietoja järjestelmän toiminnasta sisältäen mm. käyttäjien ja pääkäyttäjien suorittamat toimenpiteet, eräajossa tapahtuvat tiedon päivitykset ja tilasiirtymien aiheuttamat muutokset. Prioriteetti on ajan salliessa.
- 5.4 Lokitietoihin kirjoitetaan tietoja virhetilanteista. Tiedoissa tulisi olla tarkka kuvaus siitä, mikä toiminto virheen aiheutti ja mikä oli virheen edeltävä tilanne. Prioriteetti on ajan salliessa.

3.6 Käyttöliittymät

Sovellusta käytetään WWW-käyttöliittymien kautta. Käyttöliittymästä toteutetaan dynaaminen, jolloin se mukautuu eri tarpeisiin käyttäjien oikeuksien perusteella. Koko järjestelmän pääkäyttäjille näytetään kaikki toteutetut toiminnot. Laitosten ja tiedekuntien pääkäyttäjien oikeuksilla käyttöliittymä on hieman suppeampi. Käyttöliittymää tarvitsevat myös mm. tavalliset käyttäjät, kansainvälisten asioiden hoitajat sekä ATK-keskuksen palvelupiste. Heidän näkymät mukautetaan tarvittavien oikeuksien mukaan.

Yleisiä vaatimuksia käyttöliittymille ovat seuraavat:

- 6.1 Käyttöliittymän tulee olla helppokäyttöinen ja helposti muutettavissa ilman Perl-ohjelmointikielen tuntemusta. Prioriteetti on tärkeä.
- 6.2 Ensisijainen käyttökieli on suomi, mutta myös muiden kielivaihtoehtojen lisäykseen on varauduttava. Prioriteetti on tärkeä.
- 6.3 Käyttöliittymästä tehdyt muutokset tulee viedä kohdejärjestelmille reaaliajassa. Prioriteetti on välttämätön.

Muita yleisiä vaatimuksia käyttöliittymän käytettävyyttä koskien ovat seuraavat:

- 6.4 Usein käytettävät toiminnot on oltava selkeästi esillä. Prioriteetti on tärkeä.
- 6.5 Tietokannasta voidaan hakea tietoja henkilöistä ja käyttäjätunnuksista monen eri hakuehdon mukaan. Hakuehtoina ovat mm. nimi, henkilötunnus, käyttäjätunnus, oikeustiedot ja ryhmiin kuuluminen. Prioriteetti on välttämätön.

3.7 Laitosten ja tiedekuntien käyttöliittymä

Laitosten ja tiedekuntien pääkäyttäjien käyttöliittymien vaatimukset ovat seuraavat:

- 7.1 Ryhmien tietoja ja oikeuksia voidaan hakea ja muuttaa. Prioriteetti on ajan salliessa.
- 7.2 Henkilöitä ja heidän tietoja voidaan lisätä ja poistaa. Prioriteetti on ajan salliessa.
- 7.3 Henkilöitä ja heidän tietoja voidaan hakea ja muuttaa. Prioriteetti on ajan salliessa.

- 7.4 Käyttäjätunnuksia ja niiden tietoja voidaan lisätä, hakea ja muuttaa sekä salasanaa voidaan vaihtaa. Prioriteetti on ajan salliessa.
- 7.5 Käyttäjätunnuksien ja henkilöiden tilaa voidaan muuttaa. Prioriteetti on ajan salliessa.
- 7.6 Käyttäjätunnuksia voidaan sijoittaa ryhmään ja poistaa ryhmästä oman organisaation ryhmiin liittyen. Prioriteetti on ajan salliessa.
- 7.7 Ylläpitäjien oikeudet määritellään erikseen omassa taulussaan erotettuna järjestelmän muista oikeuksista parantaen tietoturvaa. Prioriteetti on ajan salliessa.
- 7.8 Pääkäyttäjän oikeus tiettyyn ryhmään tarkoittaa oikeutta kyseiseen ryhmään sekä kaikkiin sen alaryhmiin. Prioriteetti on välttämätön.

3.8 Järjestelmän pääkäyttäjän käyttöliittymä

Koko järjestelmän pääkäyttäjän käyttöliittymän vaatimukset sisältävät laitosten ja tiedekuntien pääkäyttäjien käyttöliittymien vaatimukset (katso luku 3.7) sekä lisäksi seuraavat:

- 8.1 Pääkäyttäjällä on oikeus käyttää kaikkia järjestelmään liittyviä toimintoja. Prioriteetti on välttämätön.
- 8.2 Siirtotiedostoa läpikäydessä järjestelmä ilmoittaa virheellisistä, puutteellisista tai ristiriitaisista tiedoista antaen pääkäyttäjälle mahdollisuuden korjata tiedot. Prioriteetti on ajan salliessa.
- 8.3 Ryhmiä voidaan luoda ja poistaa. Prioriteetti on välttämätön.
- 8.4 Ryhmien tietoja voidaan hakea ja muuttaa. Prioriteetti on välttämätön.

- 8.5 Ryhmä voidaan liittää toisen ryhmän jäseneksi ja poistaa toisen ryhmän jäsenyydestä. Prioriteetti on välttämätön.
- 8.6 Ryhmä voidaan kopioida uudeksi ryhmäksi. Prioriteetti on ajan salliessa.
- 8.7 Useampia ryhmiä voidaan yhdistää yhdeksi ryhmäksi. Prioriteetti on ajan salliessa.
- 8.8 Ennaltamääritellyjä valikkovaihtoehtoja voidaan muuttaa. Tällaisia ovat esim. laistosten ja tiedekuntien nimet. Prioriteetti on ajan salliessa.
- 8.9 Pääkäyttäjä voi vaihtaa ryhmien, käyttäjätunnuksen ryhmäjäsennyksien ja ryhmien ryhmäjäsennyksien tilaa. Prioriteetti on tärkeä.

3.9 Käyttäjän käyttöliittymä

Käyttäjän käyttöliittymän vaatimukset ovat seuraavat:

- 9.1 Henkilö voi katsella itsestään järjestelmään tallennettuja tietoja. Prioriteetti on ajan salliessa.
- 9.2 Henkilö voi muuttaa omia yhteystietoja. Prioriteetti on ajan salliessa.
- 9.3 Henkilö voi vaihtaa käyttäjätunnuksen salasanaa. Prioriteetti on ajan salliessa.
- 9.4 Henkilö voi asettaa sähköpostin uudelleenohjauksen haluamaansa osoitteeseen. Prioriteetti on toteutetaan ajan salliessa.
- 9.5 Henkilö voi kieltää itseään koskevien tietojen esittämisen esimerkiksi sähköposti- ja kotisivulistauksissa. Prioriteetti on ajan salliessa.

3.10 Tietoturva

Tietoturva on keskeisessä roolissa järjestelmän suunnittelussa ja toteutuksessa. Järjestelmä sisältää tietoa henkilöistä ja heidän käyttäjätunnuksista, joten tietoa ei saa vuotaa kolmansille osapuolille. Tietoturvaa koskien on määritelty seuraavat vaatimukset:

- 10.1 Muutoksia järjestelmän tietoihin saa tehdä vain autentikoituneet käyttäjät, joilla on tarvittavat oikeudet. Prioriteetti on välttämätön.
- 10.2 Järjestelmään sekä tietokantapalvelimeen saa ottaa yhteyden vain tietyistä ip-osoitteista. Prioriteetti on välttämätön.
- 10.3 Salasanoja säilytetään tietokannassa kryptatussa muodossa, eikä niitä voi palauttaa selväkieliseksi. Prioriteetti on välttämätön.
- 10.4 Pääkäyttäjille voidaan määritellä eritasoisia oikeuksia järjestelmän tietojen muokkaamiseksi. Prioriteetti on ajan salliessa.
- 10.5 Pääkäyttäjien oikeudet määritellään omassa tietokannan taulussa. Prioriteetti on välttämätön.
- 10.6 Käyttöliittymän tulee käyttää HTTPS-protokollaa. Prioriteetti on välttämätön.

4 Tekniset vaatimukset

Järjestelmän toimimiseksi palvelinympäristöltä edellytetään seuraavat tekniset vaatimukset:

- 11.1 Järjestelmä toimii Internetiin kytketyllä Linux-palvelimella, jolloin sitä voidaan käyttää verkkoon kytketystä tietokoneesta. Prioriteetti on välttämätön.
- 11.2 Järjestelmän asennus ja käyttöönotto on oltava helppoa. Prioriteetti on tärkeä.
- 11.3 Järjestelmä on oltava helposti monistettavissa toiseen hakemistoon tai toiselle koneelle. Prioriteetti on tärkeä.
- 11.4 Järjestelmä tulee toteuttaa mahdollisimman versioriippumattomaksi, jotta toiminen muilla versioilla on mahdollista. Prioriteetti on tärkeä.
- 11.5 Palvelimelle tulee olla asennettuna Apache-palvelinohjelmiston versio 2.0.51 sekä Perl-tulkkin versio 5.8.3. Uudemmat ja osa vanhemmista versioista saattavat olla yhteensopivia. Prioriteetti on välttämätön.
- 11.6 Järjestelmä tarvitsee PostgreSQL-tietokantahallintajärjestelmästä version 7.4.7. Se voi olla asennettuna samalle tai ulkoiselle palvelimelle kuin itse järjestelmä. Uudemmat ja osa vanhemmista versioista saattavat olla yhteensopivia. Prioriteetti on välttämätön.
- 11.7 Järjestelmän palvelimelle tulee olla asennettuna Perl-ohjelmointikielen tuki tietokantayhteyksille. Prioriteetti on välttämätön.

5 Käyttötapaukset

Luvussa on kuvattu Fortimen, JOREn, Korpin sekä salasana.jyu.fi-palvelun käyttötapaukset. Osa käyttötapauksista on ajastettuja eräajoluontoisia ja toiset voivat tapahtua minä hetkenä hyvänsä.

5.1 Fortimen käyttötapaukset

Fortimesta tulevien siirtotiedostojen tietokentät ovat henkilötunnus, työntekijänumero, nimi, työnimikkeen ID-numero, työnimi sekä työsopimuksen päättymispäivämäärä. Tietokentät ovat vakiopituisia. Erotinmerkkiä ei ole. Rivinvaihto erottaa tietueet.

5.1.1 Henkilön luonti

Versio: 0.5

Nimi: Henkilön luonti (Fortime)

Edellytykset: Yhteys tietokantaan on toiminnassa ja siirtotiedosto on olemassa.

Alkutilanne: Käyttötapaus alkaa, kun huomataan uusi henkilö verratessa uutta Fortimen siirtotiedostoa tietokannan tietoon.

Tapahtumat: Järjestelmä etsii Fortimen siirtotiedoston perusteella tietokannasta henkilöitä ja huomaa uuden henkilön. Uuden henkilön löytäminen tarkoittaa, ettei tietokannasta löydy siirtotiedoston sisältämää henkilötunnusta. Lisätään henkilö tietokantaan Fortimesta tulevilla tiedoilla ja asetetaan henkilön elinkaari alkuarvoonsa [Poikkeus 1: Henkilötunnus on virheellinen.] [Poikkeus 2: Tietokantakysely ei onnistu.]. Tämän jälkeen luodaan uudelle henkilölle käyttäjätunnus sekä liitetään se Fortimen henkilökuntaryhmään ja vastuualuekoodin mukaisesti organisaatioita vastaaviin ryhmiin [Poikkeus 3: Käyttäjätunnus on jo olemassa.]. Samalla alustetaan myös henkilön, käyttäjätunnuksen ja sen ryhmäjäsenyyksien elinkaaret. Käyttäjätunnus generoidaan nimestä ja salasana jollain muulla generaattorilla. Salasana tal-

lennetaan väliaikaisesti selväkielisenä, jotta se voidaan saada selville, kun henkilölle annetaan henkilökohtaisesti hänen käyttäjätunnus ja salasana. Loki- ja historiatietoihin kirjoitetaan tieto henkilön luomisesta.

Jälkitilanne: Järjestelmän tietokannassa on uuden henkilön osalta päivitetty tiedot Fortimesta. Tietokantaan on myös mahdollisesti muodostettu henkilön ensisijaiselle tunnukselle uusia ryhmäjäsennyksiä. Muutokset kirjataan loki- ja historiatietoihin.

Poikkeukset: [Poikkeus 1: Henkilötunnus on virheellinen.] Jos henkilötunnus on virheellinen, ei henkilöä lisätä. Tapaus ilmoitetaan pääkäyttäjälle sekä kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Tietokantakysely ei onnistu.] Henkilöä ei voida luoda tietokantaan. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 3: Käyttäjätunnus on jo olemassa.] Henkilölle täytyy generoida uusi yksilöllinen käyttäjätunnus.

Huomioitavaa: Henkilön elinkaari alustetaan aktiiviseen tilaan määräaikaiseksi. Käyttäjätunnuksen ja sen ryhmäjäsennyksien elinkaaret asetetaan aktiiviseksi toistaiseksi. Ryhmäjäsennys Fortimeen asetetaan työsuhteen päättymispäivän mukaisesti.

Luotujen käyttäjätunnuksien tiedot tulisi olla haettavissa myöhemmin kun sopimuksia tulostetaan henkilön allekirjoitusta varten.

5.1.2 Henkilön tietojen muuttaminen

Versio: 0.5

Nimi: Henkilön tietojen muuttaminen (Fortime)

Edellytykset: Yhteys tietokantaan toiminnassa ja siirtotiedosto on olemassa.

Alkutilanne: Käyttötapaus alkaa, kun huomataan henkilön tietojen muuttuneen verrattuna Fortimen siirtotiedostoa tietokannan tietoon.

Tapahtumat: Järjestelmä etsii Fortimen siirtotiedoston perusteella tietokannasta henkilöitä ja huomaa henkilön tietojen muuttuneen. Henkilön tietojen muuttuminen tarkoittaa, että tietokantaa tutkittaessa löydetään sama henkilötunnus ja työntekijännumero kuin siirtotiedostossa, mutta muut tiedot eriävät. Henkilön tiedot päivitetään tietokantaan muuttuneiden tietojen osalta käyttäen henkilötunnusta yksilöivänä tietona [Poikkeus 1: Kaikki tiedot eriävät.] [Poikkeus 2: Henkilötunnus on virheellinen.] [Poikkeus 3: Tietokantakysely ei onnistu.]. Kirjoitetaan tietojen muutos loki- ja historiatietoihin.

Jälkitilanne: Henkilön tiedot on muutettu. Muutokset on kirjattu loki- ja historiatietoihin.

Poikkeukset: [Poikkeus 1: Kaikki tiedot eriävät.] Jos kaikki muut tiedot kuin henkilötunnus ja työntekijännumero eriävät, ilmoitetaan ristiriidasta pääkäyttäjälle ja kirjoitetaan virhe loki-tietoihin.

[Poikkeus 2: Henkilötunnus on virheellinen.] Jos Fortimesta tuleva henkilötunnus on väärää muotoa, esim. ulkomaalaisille luotu väliaikaishetu, niin käytetään nimeä ja syntymäaikaa yksilöivänä tietona. Jos nimi tai syntymäaika puuttuu, niin laitetaan henkilö ylläpitäjän jonoon käsiteltäväksi.

[Poikkeus 3: Tietokantakysely ei onnistu.] Kirjoitetaan virhe lokitietoihin.

Huomioitavaa: Henkilö saattaa löytyä tietokannasta, mutta hänen ensisijainen käyttäjätunnus ei välttämättä kuulu työntekijäryhmiin. Täten ryhmiinkuulumiset täytyy myös tarkistaa ja sijoittaa henkilön ensisijainen käyttäjätunnus kuulumaan oikeisiin ryhmiin.

Tietojen samankaltaisuuden tarkistamisen yhteydessä kasvatetaan henkilökuntaryhmän ryhmäjäsenyyden tilasiirtymäpäivämäärää. Toisin sanoen ilmoitetaan, että henkilö on vielä Fortimen listoilla.

5.1.3 Henkilön henkilökuntastatuksen poisto

Versio: 0.6

Nimi: Henkilön henkilökuntastatuksen poisto (Fortime)

Edellytykset: Yhteys tietokantaan toiminnassa ja siirtotiedosto on olemassa.

Alkutilanne: Käyttötapaus alkaa, kun huomataan henkilön poistuneen verratessa uutta Fortimen siirtotiedostoa tietokannan tietoon.

Tapahtumat: Järjestelmä etsii Fortimen siirtotiedoston perusteella tietokannasta henkilöitä ja huomaa henkilön poistuneen. Henkilön poistuminen tarkoittaa, ettei siirtotiedostosta löydy samanlaista henkilötunnusta ja työntekijänumeroa kuin on tietokannassa. Asetetaan henkilön tunnusten jäsenyys henkilökunta- ja muissa organisaatioon liittyvissä ryhmissä määräaikaisesti tilaan aktiivinen (poistumassa) [Poikkeus 1: Tietokantakysely ei onnistu.]. Jos henkilön tunnukset eivät ole jäsenenä opiskelijoiden, avoimen yliopiston tai muissa käyttöoikeuden antavissa ryhmissä, asetetaan myös henkilö ja käyttäjätunnus määräaikaisesti tilaan aktiivinen (poistumassa). Lähetetään sähköpostivaroitus henkilölle. Kirjataan tilanmuutos loki- ja historiatietoihin.

Jälkitilanne: Henkilökunnasta Fortimen mukaan poistuneen henkilön tunnusten jäsenyys henkilökunta- ja muissa organisaatioon liittyvissä ryhmissä on asetettu tilaan poistumassa. Henkilö ja siihen liittyvät tunnukset asetettu tilaan poistumassa, jos henkilö ei enää kuulu opiskelijoihin, henkilökuntaan tai muihin käyttöoikeutettuihin ryhmiin. Tilanmuutos kirjaetaan loki- ja historiatietoihin.

Poikkeukset: [Poikkeus 1: Tietokantakysely ei onnistu.] Kirjoitetaan virhe loki- ja historiatietoihin.

5.2 JOREn käyttötapaukset

JOREn siirtotiedoston tietokentät ovat sukunimi, etunimet, henkilötunnus, tiedekunta, laitos, opiskelijanumero, opiskelijastatus, läsnäolotieto. Kentät ovat mainitussa järjestyksessä pilkulla erotettuna. Rivinvaihto erottaa tietueet.

5.2.1 Henkilön luonti

Versio: 0.6

Nimi: Henkilön luonti (JORE)

Edellytykset: Tietokantayhteys toiminnassa ja siirtotiedosto on olemassa.

Alkutilanne: Käyttötapaus alkaa, kun huomataan uusi henkilö verratessa uutta JOREn siirtotiedostoa tietokannan tietoon.

Tapahtumat: Järjestelmä etsii JOREn siirtotiedoston perusteella tietokannasta henkilöitä ja huomaa uuden henkilön. Uuden henkilön löytäminen tarkoittaa, ettei tietokannasta löydy siirtotiedoston sisältämää henkilötunnusta [Poikkeus 1: Henkilötunnus virheellinen.]. Lisätään henkilö tietokantaan JOREsta tulevilla tiedoilla [Poikkeus 2: Tietokantakyselyä ei voida suorittaa.]. Tämän jälkeen luodaan uudelle henkilölle käyttäjätunnus ja liitetään se opiskelijaryhmään sekä mahdollisesti tiedekunta- sekä laitosryhmiin [Poikkeus 3: Käyttäjätunnus on jo

olemassa.]. Käyttäjätunnus generoidaan nimestä ja salasana jollain muulla generaattorilla. Salasana tallennetaan väliaikaisesti selväkielisenä, jotta se voidaan saada selville, kun henkilölle annetaan henkilökohtaisesti hänen käyttäjätunnus ja salasana. Loki- ja historiatietoihin kirjoitetaan tieto henkilön luomisesta.

Jälkitilanne: Järjestelmän tietokannassa on uuden henkilön osalta päivitetty tiedot JOREsta. Tietokantaan on myös mahdollisesti muodostettu henkilön ensisijaiselle tunnukselle uusia ryhmäjäsenyyksiä. Muutokset on kirjattu loki- ja historiatietoihin.

Poikkeukset: [Poikkeus 1: Henkilötunnus on virheellinen.] Jos henkilötunnus on virheellinen, ei henkilöä lisätä. Tapaus ilmoitetaan pääkäyttäjälle sekä kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Tietokantakysely ei onnistu.] Henkilöä ei voida luoda tietokantaan. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 3: Käyttäjätunnus on jo olemassa.] Henkilölle täytyy generoida uusi yksilöllinen käyttäjätunnus.

Huomioitavaa: Henkilön elinkaari alustetaan aktiiviseen tilaan määräaikaiseksi. Käyttäjätunnuksen ja sen ryhmäjäsenyyksien elinkaaret asetetaan aktiiviseksi toistaiseksi. Ryhmäjäsenyys JOREen asetetaan aktiiviseksi toistaiseksi.

Luotujen käyttäjätunnuksien tiedot tulisi olla haettavissa myöhemmin, kun sopimuksia tuostetaan henkilön allekirjoitusta varten.

5.2.2 Henkilön opiskelijastatuksen poisto

Versio: 0.5

Nimi: Henkilön opiskelijastatuksen poisto (JORE)

Edellytykset: Tietokantayhteys toiminnassa ja siirtotiedosto on olemassa.

Alkutilanne: Käyttötapaus alkaa, kun huomataan henkilön poistuneen verratessa uutta JOREn siirtotiedostoa tietokannan tietoon.

Tapahtumat: Järjestelmä huomaa henkilön poistuneen JOREsta. Henkilön poistuminen tarkoittaa, ettei siirtotiedostosta löydy samanlaista henkilötunnusta ja opiskelijanumeroa kuin on tietokannassa. Asetetaan henkilön tunnusten jäsenyys opiskelijoiden ja muissa organisaatioon liittyvissä ryhmissä määräaikaisesti tilaan aktiivinen (poistumassa) [Poikkeus 1: Tietokantakyselyä ei voida suorittaa.]. Jos henkilön tunnukset eivät ole jäseninä henkilökunnan, avoimen yliopiston tai muissa käyttöoikeuden antavissa ryhmissä, asetetaan myös henkilö ja tunnus määräaikaisesti tilaan aktiivinen (poistumassa). Lähetetään sähköpostivaroitus henkilölle. Kirjataan tilanmuutos loki- ja historiatietoihin.

Jälkitilanne: JOREn mukaan opiskelijoihin kuulumattoman henkilön tunnusten jäsenyys opiskelijoiden ja muissa organisaatioon liittyvissä ryhmissä on asetettu tilaan aktiivinen (poistumassa). Henkilö ja siihen liittyvät tunnukset on asetettu tilaan aktiivinen (poistumassa), jos henkilö ei enää kuulu opiskelijoihin, henkilökuntaan tai muihin käyttöoikeutettuihin ryhmiin. Tilanmuutos on kirjattu loki- ja historiatietoihin.

Poikkeukset: [Poikkeus 1: Tietokantakyselyä ei voida suorittaa] Kirjoitetaan virhe lokitietoihin.

5.2.3 Henkilön tietojen muuttaminen

Versio: 0.6

Nimi: Henkilön tietojen muuttaminen (JORE)

Edellytykset: Tietokantayhteys toiminnassa ja siirtotiedosto on olemassa.

Alkutilanne: Käyttötapaus alkaa, kun huomataan henkilön tietojen muuttuneen verrattuna uutta JOREn siirtotiedostoa tietokannan tietoon.

Tapahtumat: Järjestelmä etsii JOREn siirtotiedoston perusteella tietokannasta henkilöitä ja huomaa henkilön tietojen muuttuneen. Henkilön tietojen muuttuminen tarkoittaa, että tietokantaa tutkittaessa löydetään sama henkilötunnus ja opiskelijanumero kuin siirtotiedostossa, mutta muut tiedot eriävät. Henkilön tiedot päivitetään tietokantaan muuttuneiden tietojen osalta käyttäen henkilötunnusta yksilöivänä tietona [Poikkeus 1: Kaikki tiedot eriävät.] [Poikkeus 2: Henkilötunnus on virheellinen.] [Poikkeus 3: Tietokantakysely ei onnistu.]. Kirjoitetaan tietojen muutos loki- ja historiatietoihin.

Henkilö saattaa löytyä tietokannasta, mutta hänen ensisijainen käyttäjätunnus ei välttämättä kuulu opiskelijaryhmiin. Täten ryhmiin kuulumiset täytyy myös tarkistaa ja sijoittaa henkilön henkilökohtainen ryhmä kuulumaan oikeisiin ryhmiin. Muutokset kirjataan loki- ja historiatietoihin.

Jälkitilanne: Henkilön tiedot on muutettu. Muutokset on kirjattu loki- ja historiatietoihin.

Poikkeukset: [Poikkeus 1: Kaikki tiedot eriävät.] Jos kaikki muut tiedot kuin henkilötunnus ja opiskelijanumero eriävät, ilmoitetaan ristiriidasta pääkäyttäjälle ja kirjoitetaan virhe loki-tietoihin.

[Poikkeus 2: Henkilötunnus on virheellinen.] Jos JOREsta tuleva henkilötunnus on väärää muotoa (esim. ulkomaalaisille luotu väliaikaishetu) niin käytetään nimeä ja syntymäaikaa yksilöivänä tietona. Jos nimi tai syntymäaika puuttuu, niin sijoitetaan henkilö ylläpitäjän jonoon käsiteltäväksi.

Huomioitavaa: Tietojen samankaltaisuuden tarkistamisen yhteydessä siirretään opiskelija-ryhmän ryhmäjäsenyyden tilasiirtymäpäivämäärää. Toisin sanoen ilmoitetaan, että henkilö on vielä JOREn listoilla.

[Poikkeus 3: Tietokantakysely ei onnistu.] Kirjoitetaan virhe lokitietoihin.

5.3 Korpin käyttötapaukset

Korppi lähettää pyynnöt suoraan verkon yli ilman siirtotiedostoja ja niihin vastataan välittömästi. Korppi voi myös käyttää siirtotiedostoja.

5.3.1 Ryhmän luominen

Versio: 0.6

Nimi: Ryhmän luominen (Korppi)

Suorittajat: Korppi

Edellytykset: Yhteydet tietokantaan ja Korppiin toimivat.

Alkutilanne: Korppi lähettää pyynnön ryhmän luomisesta.

Tapahtumat: Järjestelmä vastaanottaa pyynnön Korpilta ryhmän luomiseksi. Tietona saadaan Korpin valitsema, yksilöivä ryhmän nimi ja ryhmän tilasiirtymän päivämäärä. Luodaan ryhmä ja ryhmäjäsenyys Korpin ylärhyhmään, asetetaan ryhmän nimi ja tilasiirtymän päivämäärä sekä lisätään ryhmä Korpin pyynnöstä luotuihin ryhmiin Korpin luomien ryh-

mien yläryhmään. [Poikkeus 1: Ryhmä on jo olemassa.] [Poikkeus 2: Tietokantakyselyä ei voida suorittaa.]. Lähetetään Korpille tieto onnistumisesta. Kirjoitetaan tapahtuma loki- ja historiatietoihin.

Jälkitilanne: Järjestelmän tietokannassa on Korpin pyytämä ryhmä luotuna.

Poikkeukset: [Poikkeus 1: Ryhmä on jo olemassa.] Jos pyydetty ryhmä on jo olemassa, niin lähetetään tieto ryhmän olemassaolosta Korpille. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Tietokantakyselyä ei voida suorittaa.] Lähetetään Korpille tieto epäonnistumisesta. Kirjoitetaan virhe lokitietoihin.

Huomioitavaa: Käyttötapauksen vaatimia toimintoja ei toteuteta tämän projektin puitteissa.

5.3.2 Ryhmän poisto

Versio: 0.6

Nimi: Ryhmän poisto (Korppi)

Suorittajat: Korppi

Edellytykset: Yhteydet tietokantaan ja Korppiin toimivat.

Alkutilanne: Korppi lähettää pyynnön ryhmän poistamisesta.

Tapahtumat: Järjestelmä vastaanottaa pyynnön Korpilta ryhmän poistamisesta. Tietona saadaan ryhmän Korpin generoima, yksilöivä nimi. Järjestelmä etsii Korpin pyynnöstä luo-
duista ryhmistä vastaavasti nimetyn ryhmän ja asettaa ryhmän sekä siihen liittyvien ryhmä-
jäsenyyksien tilat poistetuksi ja tilasiirtymäpäivämäärän sopivan ajan päähän sekä lähettää
tiedon onnistumisesta takaisin Korpille [Poikkeus 1: Ryhmää ei ole olemassa.] [Poikkeus 2:

Tietokantakyselyä ei voida suorittaa.]. Ryhmän varsinainen poisto tapahtuu tulevassa tilasiirtymässä. Lähetetään Korpille tieto onnistumisesta. Kirjoitetaan tapahtuma loki- ja historiatietoihin.

Jälkitilanne: Poistettavaksi pyydetty ryhmä on merkitty poistetuksi ja poistuu järjestelmästä seuraavassa tilasiirtymässään. Samalla poistetaan ryhmän ryhmäjäsenyydet muihin ryhmiin.

Poikkeukset: [Poikkeus 1: Ryhmää ei ole olemassa.] Lähetetään Korpille tieto, ettei ryhmää ole olemassa. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Tietokantakyselyä ei voida suorittaa.] Lähetetään Korpille tieto epäonnistumisesta. Kirjoitetaan virhe lokitietoihin.

Huomioitavaa: Käyttötapausten vaatimia toimintoja ei toteuteta tämän projektin puitteissa.

5.3.3 Ryhmän oikeuksien muuttaminen

Versio: 0.5

Nimi: Ryhmän oikeuksien muuttaminen (Korppi)

Suorittajat: Korppi

Edellytykset: Yhteydet tietokantaan ja Korppiin toimivat.

Alkutilanne: Korppi lähettää pyynnön ryhmän oikeuksien lisäämiseksi tai poistamiseksi.

Tapahtumat: Järjestelmä vastaanottaa pyynnön Korpilta tietyn ryhmän oikeuksien lisäämiseksi tai vähentämiseksi. Tietoina saadaan Korpin generoima, ryhmän yksilöivä ryhmän nimi, lista kolmikoista (kohdejärjestelmä-ID, oikeuskoodi, lisäys/poisto) [Poikkeus 1: Kohde-

järjestelmä-ID tai oikeuskoodi virheellinen.]. Järjestelmä etsii nimeä vastaavan ryhmän Korpin luomista ryhmistä ja muokkaa kyseisen ryhmän oikeuksia pyynnössä välitettyjen tietojen mukaisesti [Poikkeus 2: Ryhmää ei ole olemassa.] [Poikkeus 3: Parametrit ovat virheellisiä.] [Poikkeus 4: Tietokantakyselyä ei voida suorittaa.]. Lähetetään Korpille tieto onnistumisesta. Kirjoitetaan tapahtuma loki- ja historiatietoihin.

Jälkitilanne: Korpin ilmoittaman ryhmän oikeuksia on lisätty/poistettu Korpin pyyntöä vastaavasti.

Poikkeukset: [Poikkeus 1: Kohdejärjestelmä-ID tai oikeuskoodi virheellinen.] Lähetetään Korpille virhetieto. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Ryhmää ei ole olemassa.] Lähetetään Korpille tieto, ettei ryhmää ole olemassa. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Parametrit ovat virheellisiä.] Lähetetään Korpille tieto, että annettu pyyntö on virheellinen. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 3: Tietokantakyselyä ei voida suorittaa.] Lähetetään Korpille tieto epäonnistumisesta. Kirjoitetaan virhe lokitietoihin.

5.3.4 Käyttäjätunnuksien lisääminen ryhmään

Versio: 0.5

Nimi: Käyttäjätunnuksien lisääminen ryhmään (Korppi)

Suorittajat: Korppi

Edellytykset: Yhteydet tietokantaan ja Korppiin toimivat.

Alkutilanne: Korppi lähettää pyynnön käyttäjätunnuksien lisäämiseksi ryhmään.

Tapahtumat: Järjestelmä vastaanottaa pyynnön Korpilta tietyn käyttäjätunnuksien lisäämisestä tiettyyn ryhmään. Tietona saadaan lisättävät käyttäjätunnukset ja ryhmän nimi. Järjestelmä lisää tunnukset kuulumaan Korpin osoittaman ryhmän jäseneksi [Poikkeus 1: Ryhmää ei ole olemassa.] [Poikkeus 2: Käyttäjätunnusta ei ole olemassa.]. Lähetetään Korpille tieto jokaisen käyttäjätunnuksen lisäämisen onnistumisesta tai epäonnistumisesta. Kirjoitetaan tapahtuma loki- ja historiatietoihin.

Jälkitilanne: Käyttäjätunnus on liitetty Korpin osoittamaan ryhmän jäseneksi.

Poikkeukset: [Poikkeus 1: Ryhmää ei ole olemassa.] Lähetetään Korpille tieto, ettei ryhmää ole olemassa. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Käyttäjätunnusta ei ole olemassa.] Merkitään kyseisen käyttäjätunnuksen lisäys epäonnistuneeksi paluutietoon. Kirjoitetaan virhe lokitietoihin.

5.3.5 Käyttäjätunnuksien poistaminen ryhmästä

Versio: 0.5

Nimi: Käyttäjätunnuksien poistaminen ryhmästä (Korppi)

Suorittajat: Korppi

Edellytykset: Yhteydet tietokantaan ja Korppiin toimivat.

Alkutilanne: Korppi lähettää pyynnön tietyn käyttäjätunnuksien poistamiseksi ryhmästä.

Tapahtumat: Järjestelmä vastaanottaa pyynnön Korpilta käyttäjätunnuksien poistamiseksi ryhmästä. Tietona saadaan poistettavat käyttäjätunnukset ja ryhmän nimi. Järjestelmä pois-

taa Korpin osoittamat tunnukset Korpin osoittamasta ryhmästä [Poikkeus 1: Ryhmää ei ole olemassa.] [Poikkeus 2: Käyttäjätunnusta ei ole olemassa.]. Lähetetään Korpille tietoa jokaisen käyttäjätunnuksen lisäämisen onnistumisesta tai epäonnistumisesta. Kirjoitetaan tapahtuma loki- ja historiatietoihin.

Jälkitilanne: Käyttäjätunnukset on poistettu Korpin osoittamasta ryhmästä.

Poikkeukset: [Poikkeus 1: Ryhmää ei ole olemassa.] Lähetetään Korpille tieto, ettei ryhmää ole olemassa. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Käyttäjätunnusta ei ole olemassa.] Merkitään kyseisen käyttäjätunnuksen poisto epäonnistuneeksi paluutietoon. Kirjoitetaan virhe lokitietoihin.

5.3.6 Henkilöiden luonti

Versio: 0.6

Nimi: Henkilöiden luonti (Korppi)

Suorittajat: Korppi

Edellytykset: Yhteydet tietokantaan ja Korppiin toimivat.

Alkutilanne: Korppi lähettää pyynnön käyttäjien luomiseksi.

Tapahtumat: Järjestelmä vastaanottaa pyynnön Korpilta henkilöiden luomiseksi. Tietoina saadaan henkilöistä Korpin käyttäjä-ID, etunimet, sukunimi, henkilötunnus, haluttu tunnus ja salasana, sähköpostiosoite, titteli ja laitos/muu organisaatio. Luodaan henkilöt ja niille käyttäjätunnukset [Poikkeus 1: Laitosta tai organisaatiosta ei löydy.] [Poikkeus 2: Henkilö on jo järjestelmässä.] [Poikkeus 3: Käyttäjätunnus ei mahdollinen.]. Liitetään käyttäjätunnus

Korppi-käyttäjien ryhmään. Lähetetään Korpille tieto tunnuksen luonnin onnistumisesta. Kirjoitetaan tapahtuma loki- ja historiatietoihin.

Lopputilanne: Korpin pyytämät henkilöt ja käyttäjätunnukset on luotu ja virheet huomioitu.

Poikkeukset: [Poikkeus 1: Laitosta tai organisaatiosta ei löydy.] Palautetaan virhe Korpille. Kirjoitetaan virhe loki- ja historiatietoihin.

[Poikkeus 2: Henkilö on jo järjestelmässä.] Jos henkilö löytyy jo järjestelmästä ja henkilöön liittyy käyttäjätunnus, jolla on Korppi-oikeus, ei uutta käyttäjätunnusta luoda, vaan lähetetään Korpille tieto henkilön käyttäjätunnuksesta. Jos käyttäjätunnus on olemassa, muttei kuulu Korpin käyttöoikeuden antamaan ryhmään, liitetään se siihen. Jos henkilö löytyy jo järjestelmästä, mutta henkilöön ei liity käyttäjätunnusta, luodaan haluttu käyttäjätunnus ja liitetään se Korppi-käyttäjien ryhmään.

[Poikkeus 3: Käyttäjätunnus ei mahdollinen.] Jos haluttu käyttäjätunnus on jollain muulla tavoin kiellettyjen tai varattujen tunnusten listalla, niin lähetetään Korpille tieto, että tunnus on varattu.

5.4 Salasana.jyu.fi:n käyttötapaukset

Salasana.jyu.fi käyttötapaukset liittyvät tavallisen käyttäjän käyttöliittymästä suoritettuihin toimintoihin.

5.4.1 Kirjautuminen

Versio: 0.2

Nimi: Kirjautuminen (salasana.jyu.fi)

Suorittajat: Opiskelija, työntekijä tai muu henkilö.

Edellytykset: Yhteydet tietokantaan ja salasana.jyu.fi-palveluun toimivat.

Alkutilanne: Järjestelmä saa pyynnön salasana.jyu.fi-palveluun kirjautumiselle.

Tapahtumat: Järjestelmä saa pyynnön kirjautumiselle. Tietoina saadaan käyttäjätunnus ja salasana. Tällöin tarkistetaan, löytyykö kyseistä käyttäjätunnusta järjestelmän tietokannasta [Poikkeus 1: Tiedot puuttuvat.] [Poikkeus 2: Käyttäjätunnusta ei löydy.] Tämän jälkeen tarkistetaan, onko salasana oikea [Poikkeus 3: Salasana virheellinen.]. Lopuksi palautetaan tieto käyttäjän kirjautumisoikeudesta. Kirjoitetaan kirjautumisyrittäksen onnistuminen tai epäonnistuminen lokitietoihin.

Lopputilanne: Käyttäjä on autentikoitu ja palautettu tieto kirjautumisen onnistumisesta.

Poikkeukset: [Poikkeus 1: Tiedot puuttuvat.] Lähetetty käyttäjätunnus tai salasana puuttuu. Tällöin palautetaan tieto kirjautumisen epäonnistumisesta ja tietojen puuttumisesta.

[Poikkeus 2: Käyttäjätunnusta ei löydy.] Käyttäjätunnusta ei löydy järjestelmän tietokannasta. Palautetaan tieto kirjautumisen epäonnistumisesta ja käyttäjätunnuksen puuttumisesta.

[Poikkeus 3: Salasana virheellinen.] Lähetetään paluutieto virheellisestä salasanasta.

5.4.2 Henkilön yhteystietojen katselu

Versio: 0.5

Nimi: Henkilön yhteystietojen katselu (salasana.jyu.fi)

Suorittajat: Opiskelija, työntekijä tai muu henkilö.

Edellytykset: Yhteydet tietokantaan ja salasana.jyu.fi-palveluun toimivat.

Alkutilanne: Järjestelmä saa pyynnön yhteystietojen katseluun.

Tapahtumat: Järjestelmä saa pyynnön henkilön tietojen katseluun tietyn käyttäjätunnuksen perusteella. Etsitään käyttäjätunnukseen liittyvät henkilön yhteystiedot ja lähetetään ne pyynnön kysyjälle. [Poikkeus 1: Käyttäjätunnusta ei löydy.] [Poikkeus 2: Ei oikeutta katseluun.] [Poikkeus 3: Tietokantakyselyä ei voida suorittaa.]

Lopputilanne: Pyyntöön vastattu tai virhe huomioitu.

Poikkeukset: [Poikkeus 1: Käyttäjätunnusta ei löydy] Lähetetään virhe tietojen kysyjälle. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Ei oikeutta katseluun.] Lähetetään tieto oikeuksien puuttumisesta. Kirjoitetaan katseluyritys lokiin.

[Poikkeus 3: Tietokantakyselyä ei voida suorittaa] Lähetetään virhe tietojen kysyjälle. Kirjoitetaan virhe lokitietoihin.

5.4.3 Henkilön yhteystietojen muokkaus

Versio: 0.5

Nimi: Henkilön yhteystietojen muokkaus (salasana.jyu.fi)

Suorittajat: Opiskelija, työntekijä tai muu henkilö.

Edellytykset: Yhteydet tietokantaan ja salasana.jyu.fi-palveluun toimivat.

Alkutilanne: Järjestelmä saa pyynnön yhteystietojen muokkaamiseen.

Tapahtumat: Järjestelmä saa pyynnön muuttaa henkilön yhteystietoja. Tietoina saadaan käyttäjätunnus sekä kaikki tiedot, mitä henkilöstä asetetaan muutokelpoisiksi. Etsitään henkilö tunnuksen mukaan ja muutetaan henkilön tiedot. [Poikkeus 1: Käyttäjätunnusta ei ole olemassa.] [Poikkeus 2: Ei oikeutta muutoksiin.] [Poikkeus 3: Tietokantakyselyä ei voida suorittaa.]. Henkilön tietojen muutokset kirjataan loki- ja historiatietoihin.

Lopputilanne: Yhteystiedot muutettu tai virhe huomioitu.

Poikkeukset: [Poikkeus 1: Käyttäjätunnusta ei olemassa.] Lähetetään virhe tietojen kysyjälle. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Ei oikeutta muutoksiin.] Lähetetään tieto oikeuksien puuttumisesta. Kirjoitetaan muutosyritys lokiin.

[Poikkeus 3: Tietokantakyselyä ei voida suorittaa.] Lähetetään virhe tietojen kysyjälle. Kirjoitetaan virhe lokitietoihin.

Huomioitavaa: Henkilön tietojen julkisuuden asettaminen hoidetaan mm. tällä käyttötapauksella.

5.4.4 Käyttäjätunnuksen salasanojen muutos

Versio: 0.6

Nimi: Käyttäjätunnuksen salasanojen muutos (salasana.jyu.fi)

Suorittajat: Opiskelija, työntekijä tai muu henkilö

Edellytykset: Yhteydet tietokantaan ja salasana.jyu.fi-palveluun toimivat.

Alkutilanne: Järjestelmä saa pyynnön salasanan muuttamiseksi.

Tapahtumat: Järjestelmä saa pyynnön muuttaa tietyn käyttäjätunnuksen salasanan. Tietoina saadaan käyttäjätunnus, kohdejärjestelmä, sekä uusi ja vanha salasana. Jos vanha salasana täsmää, voidaan muuttaa uusi salasana oikean kohdejärjestelmän kohdalle. [Poikkeus 1: Käyttäjätunnusta ei ole olemassa.] [Poikkeus 2: Kohdejärjestelmää ei ole olemassa.] [Poikkeus 3: Vanha salasana ei täsmää.] [Poikkeus 4: Uusi salasana on huono.] [Poikkeus 5: Tietokantakyselyä ei voida suorittaa.]. Lähetetään tieto onnistumisesta pyynnön lähettäjälle. Kirjoitetaan muutos loki- ja historiatietoihin.

Jälkitilanne: Salasana on muutettu tai virhetilanne käsitelty.

Poikkeukset: [Poikkeus 1: Käyttäjätunnusta ei ole olemassa.] Lähetetään tieto pyynnön suorittajalle. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Kohdejärjestelmää ei ole olemassa.] Lähetetään tieto pyynnön suorittajalle. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 3: Vanha salasana ei täsmää.] Jos vanhaa salasanaa ei ole olemassakaan, voidaan uusi salasana tallentaa suoraan jos se toteuttaa hyvän salasanan kriteerit. Muuten lähetetään virhe pyynnön suorittajalle ja kirjoitetaan virhe lokitietoihin.

[Poikkeus 4: Uusi salasana on huono.] Uusi salasana ei täytä hyvän salasanan kriteerejä. Lähetetään tieto pyynnön suorittajalle. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 5: Tietokantakyselyä ei voida suorittaa.] Lähetetään virhe tietojen kysyjälle. Kirjoitetaan virhe lokitietoihin.

5.4.5 Käyttäjätunnuksen oikeustietojen katselu

Versio: 0.5

Nimi: Käyttäjätunnuksen oikeustietojen katselu (salasana.jyu.fi).

Suorittajat: Opiskelija, työntekijä tai muu henkilö.

Edellytykset: Yhteydet tietokantaan ja salasana.jyu.fi-palveluun toimivat.

Alkutilanne: Järjestelmä saa pyynnön tietyn käyttäjätunnuksen oikeustietojen katseluun.

Tapahtumat: Järjestelmä saa pyynnön käyttäjätunnuksen oikeuksien katseluun. Tietoina saadaan käyttäjätunnus. Tämän perusteella haetaan ryhmähierarkiasta kaikki kyseiselle tunnuksesta liitetyt oikeudet, ottaen huomioon myös negatiiviset oikeudet. [Poikkeus 1: Käyttäjätunnusta ei löydy.] [Poikkeus 2: Tietokantakyselyä ei voida suorittaa.]. Negatiiviset oikeudet tarkoittavat tietyn oikeuden poistamista. Eteenpäin lähetettävät oikeudet muokataan senhetkisiä oikeuksia vastaaviksi poistamalla negatiivisiksi määritellyt oikeudet. Lähetetään oikeudet pyynnön lähettäjälle.

Jälkitilanne: Kyselyyn on vastattu tai virhe huomioitu.

Poikkeukset: [Poikkeus 1: Käyttäjätunnusta ei löydy] Lähetetään virhe kysyjälle. Kirjoitetaan virhe lokitietoihin.

[Poikkeus 2: Tietokantakyselyä ei voida suorittaa.] Lähetetään virhe tietojen kysyjälle. Kirjoitetaan virhe lokitietoihin.

6 Yhteenveto

Shaman-projekti määrittelee ja osaksi toteuttaa seuraajan olemassaolevalle käyttöoikeuksia hallitsevalle AMAN-järjestelmälle ottaen huomioon tämänhetkiset tarpeet ja tulevaisuuden vaatimukset. Sovellus toteutetaan edeltäjänsä tapaan Perl-kielellä PostgreSQL-tietokannan-hallintajärjestelmää käyttäen.

Järjestelmä koostuu erillisistä moduuleista. Ulkopuoliset järjestelmät käyttävät moduulien toimintoja rajapintojen kautta. Sovelluksen tulee olla mahdollisimman helposti laajennettavissa tulevaisuuden tarpeita varten ja se on otettu huomioon tietokannan ja moduulien suunnittelussa.

Järjestelmää käytetään monen eri käyttöliittymän kautta. Tuki eritasoisille käyttöliittymille on mahdollistettava. Pääkäyttäjien oikeudet on erotettu muista järjestelmässä olevista tavallisten käyttäjien oikeuksista tietoturvan vuoksi.

Järjestelmä kirjoittaa loki- ja historiatietoja toiminnastaan paremman seurattavuuden ja virhetilanteiden helpomman selvittämisen vuoksi. Tietoja voidaan palauttaa vanhoista tiedoista tarvittaessa.

Lähteet

Santanen Jukka-Pekka, ”Opinnäytteiden kirjoittaminen, lyhyt oppimäärä”, saatavilla HTML-muodossa osoitteesta <URL: <http://www.mit.jyu.fi/santanen/info/kirjoittamisesta.html>>, 23.8.2000, Jyväskylän yliopisto, tietotekniikan laitos.

Santanen Jukka-Pekka, ”Tietotekniikan Sovellusprojektien ohje”, saatavilla HTML-muodossa osoitteesta <URL: <http://www.mit.jyu.fi/palvelut/sovellusprojektit/projohje.html>>, 27.1.2005, Jyväskylän yliopisto, tietotekniikan laitos.

Toivonen Tero, ”AMAN-järjestelmän kaaviot”, saatavilla PNG-muodossa osoitteesta <URL: <http://www.cc.jyu.fi/~tptoivon/aman/>>, 2.3.2005, Jyväskylän yliopisto, ATK-keskus.