Kotiorganisaation käyttäjähallinnon kuvaus

Versio	Tekijä	Päiväys	Muutos
0.1	tp@puv.fi	2006-03-28	CSC-pohja
0.2	tp@puv.fi	2006-03-30	VAMK:n muutokset
0.3	timo.pitkaranta@puv.fi	2007-01-31	WINHA primääriksi henkilöstön osalta
0.4	timo.pitkaranta@puv.fi	2008-03-03	MOSS-frontend henkilöstölle
0.5	timo.pitkaranta@puv.fi	2008-03-04	Attribuuttitiedot päivitetty
0.6	timo.pitkaranta@puv.fi	2008-03-04	WINHA estää henkilökunnan duplikaatit
0.7	jval@puv.fi	2009-11-09	Attribuuttitiedot päivitetty

Tässä dokumentissa ollaan kiinnostuneita käyttäjätietokannan ja sen tietojen ajantasaisuuden toteutuksen yleisistä periaatteista sellaisella tasolla, joka antaa riittävät tiedot käyttäjätietojen laadun ja ajantasaisuuden arvioimiseksi.

Kotiorganisaatio asettaa tämän dokumentin www:hen kaikkien saataville ja päivittää sitä oma-aloitteisesti, kun muutoksia tulee. Dokumentti linkitetään Haka-infrastruktuurin kotisivulta.

Tässä dokumentissa käyttäjätietokannalla tarkoitetaan sitä loppukäyttäjien attribuuttien joukkoa, johon organisaation Identity Provider-palvelin tukeutuu. Käyttäjätietokannan tekninen toteutus voi olla esim. LDAP-hakemisto tai relaatiotietokanta, tai niiden yhdistelmä niin, että Identity Provider -palvelin noutaa osan attribuuteista LDAP-hakemistosta ja osan JDBC:n yli opiskelijarekisteristä.

1. Käyttäjätietokannan ja perusrekistereiden kytkentä

1.1. Opiskelijarekisteri

Lähtöoletuksena on, että opiskelijarekisterin henkilötiedot ovat ajantasalla.

Opintosihteerit suorittavat WINHA-kannan päivityksen virkatyönä. ja päivittävät opiskelijoiden läsnäolokoodit WINHA-kantaan.

Miten käyttäjätietokanta on kytketty opiskelijarekisteriin?

LDAP (Open LDAP) - ja Microsoft AD- hakemistot päivitetään koneellisesti ajamalla cronista joka yö perl-päivityskripti, joka lukee WINHA-kannasta opiskelijoiden läsnäolokoodit ja päivittää LDAP:iin attribuutit WINHA_kannan läsnöolokoodia vastaavasti

1.1.1. Uusi opiskelija

Miten uuden opiskelijan tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?
LDAP (Open LDAP) - ja Microsoft AD- hakemistot päivitetään koneellisesti ajamalla cronista joka yö perl-päivityskripti, joka lukee WINHA-kannasta uudet opiskelijat, luo niille käyttäjätunnukset sekä kotihakemistot. Opintosihteerit voivat tulostaa opiskelijoille ryhmittäin tai yksittäin uudet käyttäjätunnukset ja salasanat.

Koska uusi opiskelija saa käyttäjätunnuksen/opiskelijaroolin?
Opiskelijoille jaetaan käyttäjätunnuksen opiskelun alkaessa ja heiltä tarkistetaan henkiöllisyys ja pyydetään kirjallinen kuittaus tunnuksen vastaanottamisesta.

Mitä tunnukselle tapahtuu, jos uusi opiskelija ei ota opiskelupaikkaa vastaan, tai ottaa paikan vastaan mutta ilmoittautuu poissaolevaksi?
Opiskelijalle ei anneta uutta tunnusta/salasanaa ja tunnus poistuu sitten kun WINHA:n päivittyy vastaava tilanne (opiskelija poistetaan tai merkitään poissaolevaksi). Poissaoleville, jos ovat ilmoittautuneet ja kuitanneet tunnuksen/salasanan jää tunnus käyttöön poissaolon ajaksi.

1.1.2. Opiskelijan tiedoissa tapahtuu muutos

Miten opiskelijan muuttuneet tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?
Tiedot päivitetään kerran yössä ajattavalla perl-skriptillä WINHA-kannasta

1.1.3. Opiskelija lakkaa olemasta opiskelija

Koska organisaatio (esim. opintoasiainhallinto) katsoo, että opiskelija lakkaa olemasta opiskelija
a) sen jälkeen kun opiskelija valmistuu
Kyllä.
b) sen jälkeen kun lukukausi vaihtuu, ja opiskelija ei ole ilmoittautunut läsnäolevaksi?
Ei – vasta sitten kun hän eroaa. Opintohallinto merkitsee eronneiksi ne opiskelijat, jotka eivät ole ilmoittautuneet joko läsnä- tai poissaoleviksi määräaikaan mennessä.

c) sen jälkeen kun opiskelija ilmoittaa keskeyttävänsä opinnot?
Kyllä

Kuinka kauan ylläolevien tapahtumien jälkeen kestää, että organisaatio (esim. tietohallinto) sulkee opiskelijan käyttäjätunnuksen tai poistaa opiskelijaroolin?
Opiskelijan rooli deaktivoidaan (ei voi kirjautua sisään) 7 päivän kuluttua, kun tieto on saatu WINHA:sta. Kotihakemistojen ja käyttäjätunnuksen sisäinen (lopullinen) poisto tapahtuu 400 päivän kuluttua.

1.2. Henkilökuntarekisteri

1.2.1. Uusi työntekijä

Se henkilö, joka palkkaa uuden työntekijän, täyttää MOSS-lomakkeen, joka lähtee Workflow-prosessin mukaisesti ensin WINHA-pääkäyttäjälle, joka vie henkilön WINHA-kantaan, jolloin hänelle muodostuu uniikki henkilökunnan tunnus (n. 3 merkkinen UID). Sen jälkeen kun WINHA-tunnus on luotu, workflow jatkuu siten, että ao.tiedot toimitetaan seuraaville organisaation toimijoille (sähköpostilistoja) : Opintorekisterin pääkäyttäjä (WINHA), IT-ylläpitäjä, Taloushallinto (palkkajärjestelmä), Vahtimestari, Puhelinvaihde. Jos työsuhde on määräaikainen, loppupäivä viedään jo tässä vaiheessa opintohallinnon rekisteriin.

Kun uuden työntekijän tiedot on viety WINHA-kantaan ja hänelle on annettu WINHA:an käyttäjätunnus, IT-ylläpitäjä luo hänelle samansisältöisen käyttäjätunnuksen cron-ajona LDAP:iin ja AD:hen sekä hänelle tehdään kotihakemisto ja tietohallinto tekee manuaalisesti **etunimi.sukunimi@puv.fi** alias-sähköpostiosoitteen.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Työntekijä ilmoittaa itse muuttuneista tiedoista WINHA-pääkyttäjälle, joka päivittää tiedot WINHA:an tai osoitteenmuutosten tapauksessa työntekijä voi päivittää tietonsa myös WINHA-WIIVI www-käyttöliittymän kautta. Cronista joka yö ajettava synkronointiajo päivittää muutuneet tiedot WINHA:sta AD:hen ja LDAP:iin. Esimiehille on myös tehty mahdollisuus päivittää henkilön työsuhdetietoja samalla tavalla MOSS-workflow-lomakkeella kuin 1.2.1-kohdassakin.

1.2.3. Työntekijä lakkaa olemasta työntekijä

Esimies ilmoittaa MOSS-workflow-lomakkeella muuttuneista työsuhteen tiedoista/päättymisesistä ja opintorekisterin pääkäyttäjä saa tiedon muuttuneista tiedosta sekä päivittää tiedot WINHA:an. MOSS workflow lähettää postia kuten 1.2.1.ssä on kuvattu seuraaville toimijoille (sähköpostilistoja) : Opintorekisterin pääkäyttäjä (WINHA), IT-ylläpitäjä, Taloushallinto (palkkajärjestelmä), Vahtimestari, Puhelinvaihde.

Cronista ajettava skripti lähettää mailia ja tekstarin ao. henkilölle ja deaktivoi käyttäjätunnuksen 7 pv kuluttua WINHA:ssa olevan läsnäolokoodin perusteella.

1.3. Muut käyttäjät ja heidän henkilötietojensa ajantasaisuus

Mille muille käyttäjille organisaatio antaa käyttäjätunnuksia (Suomen Akatemian tutkijat? Ravintolahenkilökunta? Siviilipalvelusmiehet? Dosentit? Alumnit? Emeritukset? Kirjaston asiakkaat?). Minkälainen hyväksymismenettely näihin tunnuksiin liittyy?
Muuta käyttäjäkuntaa käsitellään samalla tavalla kuin henkilökuntaakin.

(Suunnitelma alumneille – ei vielä toteutettu): Alumneilla säilyy sähköpostiosoite ja siihen voidaan laittaa haluttu e-mailin forwardointipalvelu päälle. Lisäksi alumnit voivat kirjautua tunnuksellaan mahdollisesti tehtävään alumniportaaliin, mutta eivät saa muuta palvelua.

Miten heidän käyttäjätietojensa ajantasaisuus ja sulkeutuminen/roolitiedon päivittyminen on varmistettu?
Sivarit ja ruorakaloiden henkilöstö käsitellään vastaavasti kuin muu henkilöstö.

Sellaiset käyttäjät, jotka eivät ole luonnollisia henkilöitä (esim. ainejärjestöt), eivät ole myöskään Haka-infrastruktuurin tarkoittamia loppukäyttäjiä, eikä heidän kirjautumistaan Identity Provider-palvelimen kautta palveluihin tule sallia.

Meillä ainejärjestöillä on oma nettilittymä ja omat palvelut. Tunnuksia annetaan vain luonnollisille henkilöille ja muut kuin luonnolliset henkilöt erotellaan omaksi haarakseen eikä niitä tarjota Shibboleth-palvelussa ulospäin.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

Millä tavalla uuden käyttäjän henkilöllisyys todennetaan, kun hänelle annetaan käyttäjätunnus?
Ajokortti tai muu virallinen henkilötodistus

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksen avulla

Salasanatodennukseen liittyvät laatuvaatimukset.
Vähintään kahdeksanmerkkinen salasana, jossa pitää olla vähintään yksi iso kirjasin ja vähintään yksi numero. Salasanan uusimista määräajoin ei vaadita, mutta siihen on varauduttu tarvittaessa tai jos ilmenee syytä tai herää epäilyksiä salasanojen ”vuotamisesta” asiaankuulumattomille tahoille. Suosimme yhtä kunnollista salasanaa kuin jatkuvaa salasanan vaihtamispakkoa, joka johtaa usein salasanojen kirjaamiseen erilisille lappusille jne.

Mahdolliset käytettävissä olevat salasanaa tukevammat autentikointimenetelmät.
Ei käytetä.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Rasti kohtaan "Saatavuus", jos kyseinen henkilötieto on ajantasalla ja siten saatavilla Identity Provider -palvelimen yli.
Kohtaan "Miten ajantasaisuus turvataan" esimerkiksi viittaus luvun 1. järjestelmiin.

Jos organisaatiolla on omia (ei siis funetEduPersonin mukaisia) attribuutteja, jotka näkyvät ulospäin Identity Provider-palvelimesta, lisää ne taulukon loppuun. Tarvittaessa linkki dokumenttiin, joka tarkemmin kuvailee omien attribuuttien skeeman.

Attribuutti	Saatavuus	Miten ajantasaisuus turvataan	Muuta (esim. tulkintaohje)
cn / commonName	x	cron WINHA 1/vrk	MUST
description			
displayName	x	cron WINHA 1/vrk	MUST
employeeNumber			
facsimileTelephoneNumber			
givenName	x		
homePhone			
homePostalAddress			

jpegPhoto			
l / localityName			
labeledURI			
mail	x	cron WINHA 1/vrk	
mobile		cron WINHA 1/vrk	voi puuttua (ruksi poistettu, koska ei IDP:ssä)
o / organizationName			
ou / organizationalUnitName			
postalAddress			
postalCode			
preferredLanguage			
seeAlso			
sn / surname	x	cron WINHA 1/vrk	MUST
street			
telephoneNumber		cron WINHA 1/vrk	vain staff (ruksi poistettu, koska ei IDP:ssä)
title			
uid	x		
userCertificate			
eduPersonAffiliation	x	cron WINHA 1/vrk	student, staff
eduPersonEntitlement			
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation			
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	x	cron WINHA 1/vrk	MUST
eduPersonScopedAddiliation			
eduPersonTargetedID	x		
schacMotherTongue			
schacGender			

schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization	x	cron WINHA 1/vrk	MUST. puv.fi
schacHomeOrganizationType	x	cron WINHA 1/vrk	MUST urn:mace:terena.org:schac:homeOrganizationType:fi:polytechnic
schacCountryOfResidence			
schacUserPresenceID			
schacPersonalUniqueCode	x	cron WINHA 1/vrk	urn:mace:terena.org:schac:personalUniqueCode:int:studentID:puv.fi:OPNRO (vain student)
schacPersonalUniqueID			
schacUserStatus			
funetEduPersonHomeOrganization			superseded
funetEduPersonStudentID			superseded
funetEduPersonIdentityCode			superseded
funetEduPersonDateOfBirth			superseded
funetEduPersonTargetDegreeUniversity			superseded
funetEduPersonTargetDegreePolytech			superseded
funetEduPersonTargetDegree	x		vain student
funetEduPersonEducationalProgramUniv			superseded
funetEduPersonEducationalProgramPolytech			superseded
funetEduPersonProgram	x		vain student
funetEduPersonMajorUniv			superseded
funetEduPersonOrientationAlternPolytech			superseded
funetEduPersonSpecialisation			
funetEduPersonStudyStart	x		vain student
funetEduPersonPrimaryStudyStart			
funetEduPersonStudyToEnd			
funetEduPersonPrimaryStudyToEnd			
funetEduPersonCreditUnits			

funetEduPersonECTS			
funetEduPersonStudentCategory			
funetEduPersonStudentStatus			
funetEduPersonStudentUnion			Mikä arvo on käytössä?
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp	x	cron WINHA 1/vrk	

4. Muuta

4.1. Kardinaliteetit

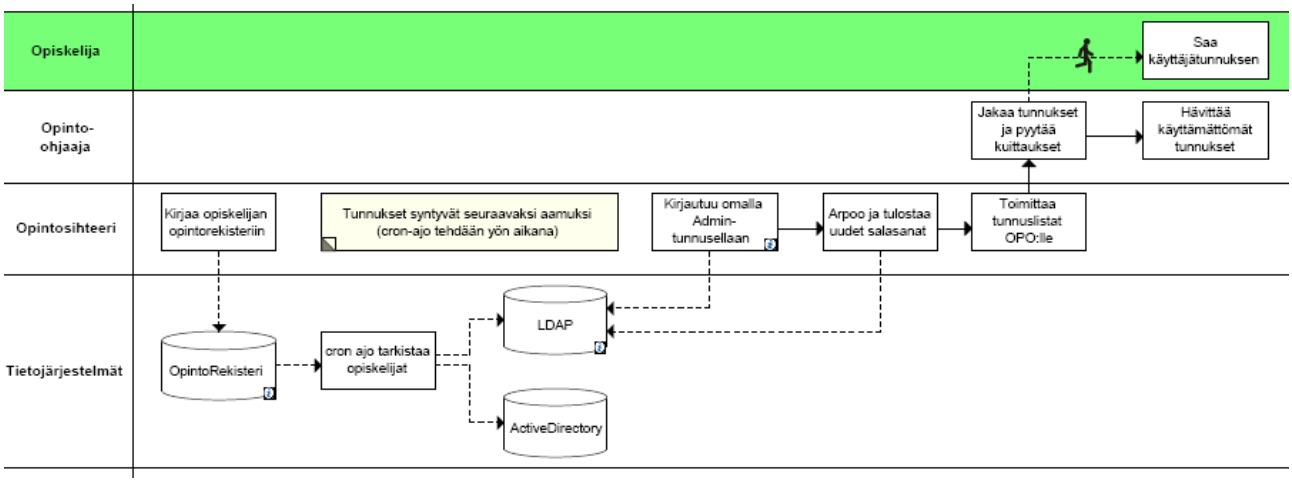
Yksi henkilöllisyys per tosielämän käyttäjä, vai
Yksi henkilöllisyys per rooli (esim. opiskelija-työntekijällä kaksi käyttäjätunnusta)?
Opiskelijalla voi olla useita rooleja ja useita käyttäjätunnuksia jos hän opiskelee useita koulutusohjelmia. Jos hän on samalla henkilökuntaa, hänellä voi olla lisäksi henkilökuntatunnus.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

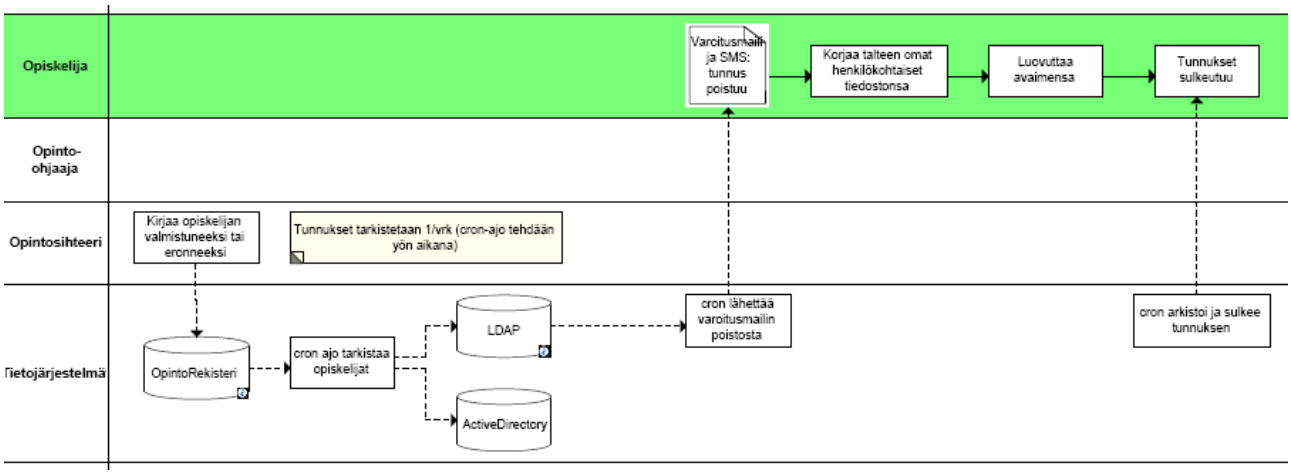
Voiko eduPersonPrincipalName vaihtua?
Ei.
Millä tavalla organisaatio kierrättää vapautuneita eduPersonPrincipalName-arvoja?
Uusiokäyttöä ei suosita eikä suositella, koska jotkut henkilöistä ovat halunneet sähköpostialiaksella tapahtuvaa postin forwardointiplavelua eläkkeelle siirtymisen jälkeenkin. WINHA-järjestelmässä henkilö arkistoidaan vähintään kahdeksi vuodeksi (24 kk), jolloin ei ole mahdollista tehdä duplikaattitunnusta tuona 24 kk aikana. Vasta kun henkilö poistetaan myös WINHA:n arkistosta, vapautuu henkilökunnan käyttäjätunnus uusiokäyttöön. Opiskelijoilla on luonnostaan juokseva opiskelijanumeroon perustuva nimi (esim e0612345), joka ei toistu. Henkilökunnan tunnusten leksikaalinen muoto on lyhyt n. kolmikirjaiminen (2…7) kirjaintunnus (esim. tp tai teu) ja lisäksi etunimi.sukunimi-muotoinen sähköpostialias.

5. Prosessikuvaukset swimlane-kaavioina

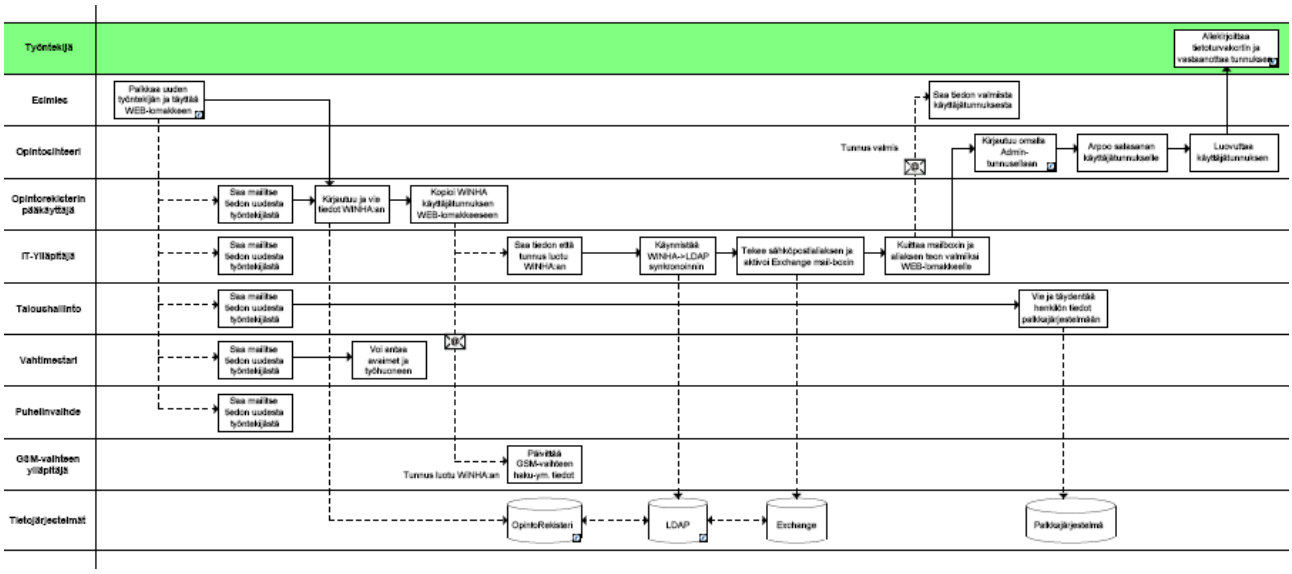
5.1. Opiskelijan käyttöoikeuksien aktivointi:



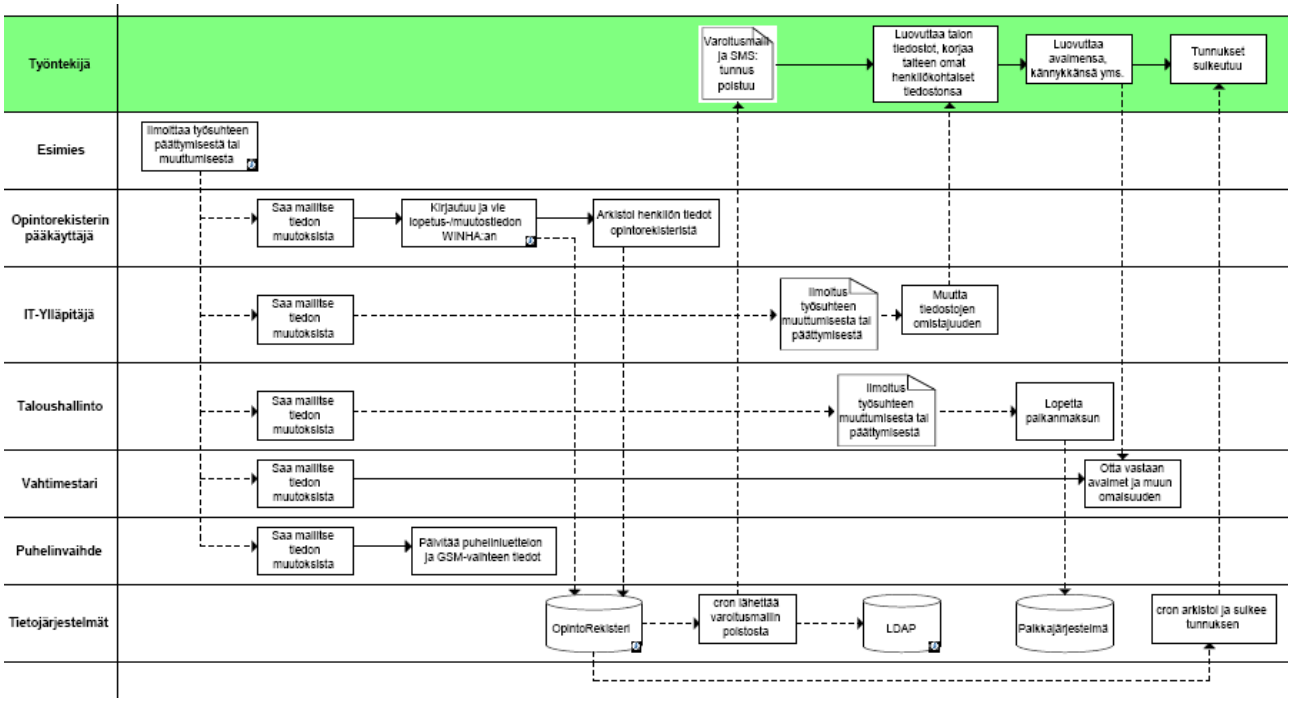
5.2. Opiskelijan käyttöoikeuksien poisto:



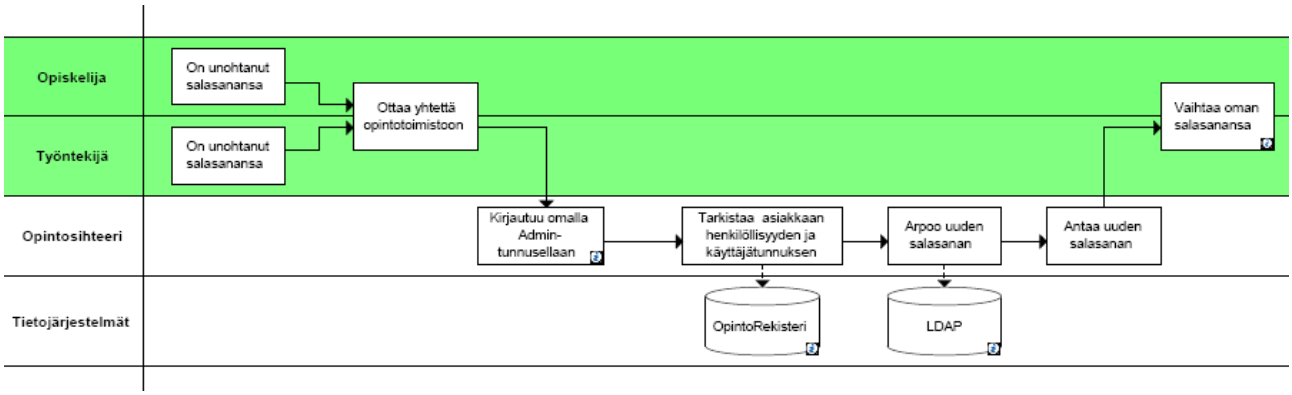
5.3. Henkilökunnan käyttöoikeuksien aktivoiminen:



5.4. Henkilökunnan käyttöoikeuksien poistaminen:



5.5. Unohtuneen salasanan palauttaminen:



Lisätietoja: timo.pitkaranta@puv.fi p. 040 5818832