Haaga-Helia
ammattikorkeakoulu Oy

Identiteetin- ja käyttövaltuuksienhallinta – ensimmäisen tason kyberpuolustus: käyttäjä

Sara Koivunen

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2019

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Sara Koivunen

Koulutusohjelma
Tietojenkäsittely

Opinnäytetyön ohjaaja
Raine Kauppinen

Raportin/Opinnäytetyön nimi
Identiteetin- ja käyttövaltuuksienhallinta – ensimmäisen tason kyberpuolustus: käyttäjä

Sivu- ja liitesivumäärä
57 + 45

Identiteetin- ja pääsynhallinta yleistyy käsitteenä (engl. Identity and Access Management – IAM). Identiteetin- ja pääsynhallintaa on aina tehty tietojärjestelmissä, mutta kyseisten toimintojen kehittämisen ja tuotteistamisen tarve on tunnistettu laajalti. Toiminnallisessa opinnäytetyössä suunnitellaan palanen IAM-järjestelmän käyttöliittymään, sekä laaditaan sähköpostiviestinä lähetettävä ohje käyttöliittymän käyttöön. Käyttöliittymätyökalun käyttötarkoitus on käyttäjätunnuksen siirtäminen vanhasta identiteetin- ja käyttövaltuuksienhallintajärjestelmästä uuteen järjestelmään.

Aikakehys opinnäytetyöprojektille on 2019 kevät. Toimeksiantajalla Helsingin yliopistolla on opinnäytetyön tekemisen hetkellä käynnissä monivaiheisentunnistuksen pilottiprojekti, jotta löydetään sopiva vahvan tunnistuksen ratkaisu yliopiston tarpeisiin, tätä näkökulmaa avataan loppukäyttäjän kannalta.

Opinnäytetyössä tutkitaan sekä käyttöliittymän käytettävyyttä, että viestintää ja monivaiheista tunnistamista tietoturvan näkökulmasta käyttäjälähtöisesti. Helsingin yliopistolla on ollut käynnissä laaja tietojenkalastelukampanja, jota hyödynnetään tässä työssä käyttäjän turvallisuuden näkökulman avaamiseen.

Alkuun valaistaan kybersäätä, minkä jälkeen siirrytään aiheisiin identiteetin- ja pääsynhallinta, monivaiheinen tunnistaminen, käyttöliittymän suunnittelu, käyttöliittymän prototyypin testaus, tietojenkalastelu sekä viestintä, jota seuraa muutaman suboptimaalisen diskurssin konsolidointi.

Asiasanat
Käyttövaltuuksienhallinta, Identiteetinhallinta, Tietojenkalastelu, Kyberturvallisuus, Käyttöliittymän suunnittelu

Sisällys

1 Johdanto

Identiteetin- ja pääsynhallinta (Identity and Access Management – *IAM*) on tämän opinnäytetyön keskeisimpiä käsitteitä. Sillä tarkoitetaan niitä prosesseja ja periaatteita, joiden mukaan käyttäjien *digitaalisia identiteettejä* eli käyttäjätunnuksia hallitaan, valtuutetaan ja tunnistetaan eri tietojärjestelmissä. Yhteistä noille periaatteille on se, että *käyttövaltuushallinta* pyritään keskittämään ja automatisoimaan mahdollisimman pitkälle. Niin ikään saman henkilön eri identiteettien määrä pyritään minimoimaan. Tämä on seurausta ilmiöstä vuosituhannen vaihteen tienoilta, missä havaittiin, että eri henkilöiden lukuisien käyttäjätunnusten hallitseminen työllisti IT-tukea kuin monipäinen mytologinen hirviö. Uuden henkilön tullessa töihin organisaatioon hänelle luotiin tunnukset esimerkiksi kymmeneen tietojärjestelmään ja tehtiin kaikki tunnusten valtuutukseen liittyvät toimet. Tämän jälkeen joka toinen päivä palautettiin jokin uuden työntekijän kymmenen eri tunnuksen unohtuneista salasanoista. Paljon resursseja vaativat tilanteet, joissa käyttäjätunnuksia luodaan massoittain. (Linden 2017, 4.)

Edelleen havaittiin käyttäjätunnusten elinkaareen liittyvät tietoturvariskit. Henkilöiden vaihtaessa tehtävää tai organisaatiota käyttövaltuuksien ja tunnusten *deprovisiointi-* tai *revokointiprosessi* voi tiedonkulun puutteiden vuoksi jäädä käynnistymättä. (Linden 2017, 4, 18, 48.) Tällöin käyttäjälle jää tarpeettomia valtuuksia tai järjestelmiin jää haamukäyttäjätunnuksia, jotka aiheuttavat organisaatiolle mm. lisäkustannuksia lisenssimaksujen muodossa.

Lainsäädännön noudattaminen ohjaa myös identiteetin- ja pääsynhallinnan järjestelmien suunnittelua. (Linden 2017, 66.) Yleinen tietosuoja-asetus, GDPR (General Data Protection Regulation eli Euroopan parlamentin ja neuvoston asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta) annettiin EU:sta 2016 ja astui voimaan toukokuussa 2018. Se määrittelee miten luonnollisten henkilöiden tietoja on käsiteltävä. Määräysten laiminlyönnistä voi pahimmillaan koitua organisaatiolle sanktio, jonka suuruus on 20 miljoonaa euroa tai 4% yrityksen vuotuisesta liikevaihdosta.

Suomen kyberturvallisuusstrategian mukaisesti *kyberympäristön* turvallisuus on oleellinen tekijä elintärkeiden toimintojen suojaamisessa, ” Suojaamisen ensimmäinen askel on organisaation toiminnan kannalta kriittisen kyberympäristön tunnistaminen: mitkä tiedot ja tietojen järjestelmät ovat keskeisiä organisaation toiminnan kannalta?” (Wirman 2014, 127). Mikä seuraus organisaatiolle on siitä, jos identiteetin- ja pääsynhallintajärjestelmä ei toimi?

Monessa paikassa se voi merkitä työpäivän päättymistä siihen. Lisäksi suomalaisessa yhteiskunnassa asioiminen vaikeutuu tai syrjäseuduilla käy lähes mahdottomaksi, mikäli sähköinen tunnistaminen ei onnistu. Maksuliikenne puolestaan ei kuulu IAM-käsitteen alle, mutta verkkopankin käyttäjätunnukset sen sijaan kuuluvat. Mäntylä arvelee kandissaan, 2014 seuraavaa:

> ”Kriittinen infrastruktuuri on kaikkiaan 80-prosenttisesti yksityisessä omistuksessa, ja osa siitä on hyvin vanhanaikaisilla menetelmillä suojattua tai pahimmassa tapauksessa suojausta ei ole huomioitu lainkaan, koska laitos ei ole kiinni yleisessä verkossa. Tällä hetkellä toteutetulla laajalla kyberoperaatiolla kyettäisiin hyvin todennäköisesti lamauttamaan suurin osa yhteiskuntamme informaatioinfrastruktuurista. -- vain harvat tiedostavat, että yksittäinen krakkeri kykenee tuottamaan muutamassa minuutissa kyberaseilla enemmän vahinkoa yhteiskunnan elintärkeisiin toimintoihin kuin kokonainen armeija kykenee tuottamaan päivässä tai jopa viikoissa.”

IAM-järjestelmän joutuessa tällaisen hyökkäyksen kohteeksi *kybernetiikan* termein kyseessä voisi olla TY-V / TO-I / KT-Info, eli virtuaalisessa toimintaympäristössä ihmisen tietojärjestelmään kohdistama hyökkäys (Ahvenainen 2014, 31-33). Minkälainen hyökkäys kyseisiin järjestelmiin voisi olla ihmiskuntaa uhkaava? Kybernetiikan termein TY-V / TO-T / KT-C-T eli simuloitu tietokoneen *kyberfyysisten* rakenteiden manipulointi tietokoneen toimesta.

Helsingin yliopisto on ollut laajan kyberhyökkäyksen kohteena vuoden 2018 elokuusta lähtien. Hyökkäyksen välineenä ovat kalastelusähköpostit ja jo elokuun aikana kalastelukampanjalla oli noin 300 uhria. Helsingin yliopiston tietohallintojohtajan Siissalon Helsingin Sanomille antamien tietojen perusteella hyökkäyksestä epäillään ammattimaista rikollisjoukkiota. Hyökkäyksen jälkien sanotaan johtavan Etelä-Afrikkaan (HS 2018). Yleensä maa, josta viestit lähtevät on kauttakulkuvaltio, jota käytetään jälkien peittämiseen. Hewlett Packardin teettämän tutkimuksen mukaan 68% yritysten sisäisistä tietoturvahyökkäyksistä tehdään oman henkilökunnan toimesta (Andreasson & Koivisto 2013, 107).

Ammattirikolliset arvioivat rikoksen kannattavuutta sen perustella, minkälainen tuomio rikoksesta seuraa kiinni jäätäessä ja miten se vaikuttaa tuottoihin. Kuten muussakin liiketoiminnassa, ammattirikollinen arvioi kannattaako toiminta. Miten siinä tapauksessa, että ennakkotapauksia ei ole? Hyökkääjän arvioidessa kiinnijäämisen todennäköisyyttä ja toimiessa sillä perusteella, kyseessä on luultavimmin uhkapeluri. Siinä tapauksessa, että hyökkääjä ei ole arvioinut kumpaakaan seikkaa motiivi voi olla poliittinen tai hyökkääjä on robotti.

Hyökkäyksen ollessa laaja ja nopea todennäköistä on, että robotteja on käytetty. Huomion arvoinen asia on se, minne kalasteluviestejä lähetetään. Löytyvätkö osoitetiedot julkisesta osoitekirjasta, joka on ladattu robotille, johonkin muuhun henkilötietorekisteriin, vai perustuvatko lähetetyt viestit kaapatun käyttäjätilin yhteystietoihin.

Arvioitaessa Helsingin yliopistoa kohteena kyseessä voi olla raha, vakoilu tai poliittinen vaikuttaminen. Summat joita valtio myöntää yliopiston toimintaan sekä tutkimukseen ovat julkisia. Helsingin yliopisto on akateemisesti ja tieteellisesti merkittävä laitos ja nämä ovat perusteita poliittiselle tai vakoilumotiiville. Huomioidaan että vakoilu on toissijainen motiivi, sen takana on oltava jotakin muuta esimerkiksi raha. Poliittisia motiiveja voivat olla esimerkiksi maine, jokin seikka tai arvo.

Edellisen kaltainen lähestymistapa ongelmanratkaisuun on verrattavissa, kriminologiassa, Cornishin ja Clarken rationaalisen valinnan teoriaan, joka koostuu rikokseen johtavasta päätöksentekoprosessista, jota seuraa kohteen valinta (Valtioneuvosto 2019, 15-16). Toinen lähestymistapa voisi olla Cohenin ja Felsonin rutiinitoimintojen teoria, joka keskittyy motiivien sijasta ympäristötekijöihin. Niitä ovat: motivoituneiden rikoksentekijöiden läsnäolo, sopivien kohteiden läsnäolo ja kykenevien puolustajien määrä jonakin ajan hetkenä. (Valtioneuvosto 2019, 16; Leukfeldt 2016, 11.) Käyttäjien koulutus vähentää otollisten kohteiden määrää, sekä kasvattaa kykenevien puolustajien määrää. Tässä suhteessa opinnäytetyön ratkaisumalli soveltaa jälkimmäistä teoriaa.

Jokainen kyberhyökkäys tarvitsee fyysisen tai virtuaalisen pääsyn tietoverkkoon, -järjestelmään tai kohteeseen: ihmisen kyberfyysiset osat ja, tai tieto. Identiteetin- ja pääsynhallintajärjestelmät valvovat omalta osaltaan tietojärjestelmien *tulokohtia,* kun on kyse digitaalisista identiteeteistä. Se on osa organisaatioiden kyberpuolustusta.

1.1 Tausta ja organisaatio

Helsingin yliopisto, joka on opinnäytetyön toimeksiantaja, käynnisti IAM-projektin vuonna 2013. Hankkeen tavoitteet ovat käyttäjäkokemuksen parantaminen toteuttamalla käyttövaltuuksiin liittyviä toimenpiteitä mahdollisimman pitkälle automatisoituina prosesseina ja samalla parantaa arkkitehtuuria ja tietoturvaa uusimalla käytössä olevia prosesseja ja teknisiä ratkaisuita (Helsingin yliopisto 2013). Tavoitteena on ollut ajaa pitkään käytössä ollut vanha käyttövaltuuksien- ja identiteetinhallintajärjestelmä alas. Tavoitetilassa on todettu myös, että järjestelmää on tarkoituksenmukaista kehittää siten, että valtionhallinnon Virtu-luottamusverkostoon liittyminen on mahdollista (Pääkkö & Tenhunen 2011, 21). Täl-

löin edellytetään korotettua tietoturvan tasoa. Tietoturvan tasot on kuvailtu ICT-varautumisen vaatimukset -ohjeessa VAHTI 2/2012, poikkeustilanteisiin varautumisen osalta (VM 2012).

1.2 Opinnäytetyöprojektin tavoite ja rajaus

Opinnäytetyöprojektin tavoite on suunnitella selkeää, helposti ymmärrettävää ja tietoturvan huomioivaa viestintää IAM-järjestelmän migraatiotoimintoon liittyen sekä tehdä käyttöliittymäsuunnitelma migraatiotyökalulle. *Migraatiossa* käyttäjätunnukset siirretään vanhasta järjestelmästä uuteen käyttövaltuuksien- ja identiteetinhallintajärjestelmään. Siirtoa ei tehdä automaattisena massasiirtona, vaan jokaisen käyttäjän on hyväksyttävä tunnuksen siirtäminen. Tässä yhteydessä voidaan suorittaa tarkistus henkilötietojen ajantasaisuudesta, johon GDPR velvoittaa *rekisterinpitäjää*. Käyttöliittymän ja viestinnän suunnittelussa pyritään huomioimaan käyttäjää. Lisäksi laaditaan käyttäjille lähetettävälle sähköpostiviestille pohja.

Helsingin yliopistolla on samaan aikaan käynnissä kaksivaiheisentunnistuksen mobiilisovelluksen pilottikokeilu, jonka yhdistämistä projektin aihealueeseen toivottiin. Kaksivaiheista tunnistusta päätettiin pohtia loppukäyttäjän näkökulmasta sen tuoman lisäsuojan kannalta. Opinnäytetyöhön kuuluu lisäksi läpikäytävien työprosessien kuvaus.

Projekteille on usein määritelty omistaja, jota voidaan pitää vastuullisena, mutta käytännössä esimerkiksi ohjelmistoprojektissa voi olla niin paljon eri toimijoita ja ulkopuolelta lainattua koodia, että kokonaisuuden hallitseminen on hankalaa. Heikoin lenkki vastuuketjussa on kuitenkin loppukäyttäjä. Lisäksi henkilöiden korotettu yksityisyydensuoja vaikeuttaa luottamussuhteita. Ihmiset haluavat luonnostaan tietää, keiden kanssa ovat tekemisissä, mutta tietoverkkojen ja niiden käyttäjien kypsymättömyys sekä markkinoiden aggressiivinen datanjano on johtanut tarpeeseen varjella henkilöiden yksityisyyttä kovemmin ottein.

Vastuun edistämiseksi tarvitaan koulutusta, vastuun jakamista ja toimivaa kommunikaatiota. Edelliset toimet edistävät luottamusta ja siten yhteistyökykyä, millä voidaan edesauttaa turvallisten ja yhteen toimivien ympäristöjen muodostumista. IAM-projektin yhteydessä on mahdollisuus tehdä loppukäyttäjien koulutusta ja viestiä vastuun antamisesta.

Helsingin yliopistolla käytetään Scrum-viitekehystä ohjelmistoprojekteissa ja sitä voidaan soveltaa projektinhallintaan yleisestikin. Ydinajatuksena on, että projektin elämänkaareen ja vaiheisiin sisältyy aina jonkin verran epävarmuutta ja muutosta (Tapio 2010, 54). Tähän

opinnäytetyöhön Scrumia päätettiin soveltaa löyhästi siten, että saadaan ajankäyttöön ja riskeihin sopiva määrä hallintaa aikataulun ollessa todella tiivis ja emoprojektin koostuessa monenlaisista haasteista ja epävarmuudesta. Työlistaa päivitetään projektin edetessä.

1.3 Käsitteitä

Deprovisiointi	Tarkoitetaan käyttäjätunnuksen sulkemista tai poistamista kokonaan kohdejärjestelmistä.
Digitaalinen identiteetti	Joukko attribuutteja, jotka henkilöivät tietojärjestelmässä tosielämän henkilön. Samalla henkilöllä voi olla lukuisia digitaalisia identiteettejä.
Diskurssijärjestys	on instituutiossa vallitseva genrejärjestelmä. Diskurssijärjestys rakentuu diskurssityypeistä. Genre on tyylilaji; tiettyyn käytäntöön pohjautuvaa kielenkäyttöä.
Diskurssityyppi	Diskurssityyppi koostuu diskursseista ja genreistä. Diskurssi tarkoittaa lausetta laajempaa kielellistä ilmausta, joka on spatiotemporaalisesti tietoinen.
Herätin	Engl. trigger. Tietokannoissa (myös ohjelmoinnissa) proseduurinen erikoistapaus, joka käynnistyy automaattisesti muutoksia tekevien lauseiden yhteydessä.
Hybridisota	Hybridisodassa voidaan pyrkiä esimerkiksi heikentämään vastustajan käsitystä tosiasioista. Sodankäynnissä yhdistetään perinteisiä voimakeinoja, epätavanomaisia menetelmiä ja rikollisia keinoja. Sotaa voivat käydä valtiolliset ja ei-valtiolliset toimijat.
IAM	Engl. identity and access management, identiteetin- ja pääsynhallinnan periaatteet. Toimintamallit, säännöt, prosessit ja teknologiat jotka mahdollistavat pääsynhallinnan sekä identiteetin hallinnan.
Julkinen toimialue	Engl. public domain, monikossa: julkinen internet.
Kyberfyysinen	Rakenne joka voi olla yhteydessä sekä tietoverkkoon, että fyysiseen maailmaan, esimerkiksi silmä tai peltipoliisi.
Kybernetiikka	Tiede joka tutkii ”systeemejä”, jotka ovat kykeneviä vastaanottamaan, säilömään ja käsittelemään informaatiota kontrollin tarkoituksessa.
Kyberympäristö	Sähköiset tietojärjestelmät, niiden muodostama toimintaympäristö.
Käyttövaltuushallinta	pääsynhallinta
LDAP	Engl. lightweight directory access protocol on hakemistopalveluiden käyttöön tarkoitettu ohjelmakerroksen protokolla.
Legacy-järjestelmä	Legacy-järjestelmillä tarkoitetaan tässä vanhentuneita teknologioita ja järjestelmiä, joiden jatkokehittämisestä on luovuttu.

Metahakemisto	Tässä yhteydessä tarkoitetaan IAM-moottorin ydintietoa.
MFA	Engl. multi factor authentication ali monivaiheinen tunnistaminen. Termiä on käytetty synonyyminä kaksivaiheiselle tunnistukselle.
Migraatio	Migraatio on tietojoukon siirtäminen yhdestä tietomallista toiseen.
Palveluväylä	Engl. ESB, enterprise service bus. Palvelukeskeisen arkkitehtuurin osa, joka toteuttaa järjestelmien väliset liitokset - kääntää ja välittää viestit eri järjestelmien välillä.
Provisiointi	Käyttäjätunnuksien perustaminen.
Rekisterinpitäjä	Organisaatio on rekisterinpitäjä, jos se päättää millä tavoin ja minkä vuoksi henkilötietoja käsitellään.
Revokointi	Revokointi tarkoittaa yksilöivän tunnisteen ja identiteetin välisen kytköksen katkaisua, peruuttamista. Kyseinen tunniste ei enää viittaa identiteettiin.
SAML2	Engl. Security Assertion Markup Language 2.0 on XML-pohjainen protokolla käyttäjien tunnistamiseen ja valtuuttamiseen eri toimijoiden (engl. security domain) välillä.
SSO	Engl. single sign-on teknologialla toteutetaan pääsy useampaan järjestelmään yhdellä kirjautumisella toimialueen sisällä. Monesti ratkaisu perustuu aktiivihakemistoon tallennettuun LDAP-kantaan.
Tulokohta	Engl. entry point ohjelmoinnissa ja tietojärjestelmissä termi, joka tarkoittaa ohjelman kohtaa, mikä suorittaa syötteeseen perustuvia toimintoja.
Ydintietovaranto	Engl. master data storage on tietokanta, joka sisältää organisaation toiminnan kannalta välttämättömät tiedot.

2 Identiteetin- ja pääsynhallinnasta

2.1 Identiteetti ja käyttövaltuus

Digitaalisella identiteetillä tarkoitetaan tietojärjestelmään tallennettua, kohteen kuvaamiseen käytettyä attribuuttijoukkoa, jonka avulla kohde tunnistetaan. IAM:in yhteydessä käsitellään luonnollisten henkilöiden identiteettejä, mutta myös yrityksellä, laitteella tai palvelulla on identiteettejä, jotka koostuvat näille tyypillisistä attribuuteista. Linden tähdentää, että tyypillisesti käytetään RFC-standardien mukaisia olioluokkia, joissa attribuutit on määritelty, mutta organisaatio voi myös kehittää oman skeemansa ja edelleen: ”käyttötilanteesta riippuu, mitä attribuutteja identiteettiin kulloinkin tarvitsee liittää; itse asiassa muiden kuin tarpeellisten attribuuttien kerääminen ja tallettaminen henkilöstä kielletään tietosuojalainsäädännössä”. (Linden 2017, 10.)

Kuuluvatko muunlaiset identiteetit kuin henkilöiden, käyttövaltuuksien- ja identiteetinhallintajärjestelmään on väittelyn arvoinen kysymys. Mitä enemmän toiminnot, prosessit ja liikenne voidaan yhdistää luonnolliseen henkilöön sen parempi, mutta emme voi kuitenkaan määritellä, että järjestelmä on arkkitehti, palvelin on ylläpitäjä tai että pilvi on lakimies. Lisäksi ihmisten yksityisyydensuojaa on kunnioitettava auditointitarpeen rinnalla. Käyttövaltuusjärjestelmän onkin tarkoitus mahdollistaa hienojakoinen ja yhtenäinen valvontamalli, mikä ehkäisee tiedon väärinkäytöksiä, tietovuotoja sekä vaarallisten työyhdistelmien muodostumista.

VAHTI -ohjeissa kerrotaan, että tietojärjestelmässä on oltava luotettava käyttäjähallinta, mikä tarkoittaa, että ainoastaan auktorisoidut henkilöt pääsevät luomaan, lisäämään, muuttamaan tai poistamaan tietojärjestelmään tai arkistonmuodostussuunnitelmaan sisältyviä tietoja tai tietojen luokitteluperusteita (VM 2006a).

Käyttövaltuuksilla tarkoitetaan tietojärjestelmien käyttäjille myönnettyjä yksilöityjä oikeuksia tietojärjestelmän käyttöön tai tietojen saantiin. Käyttövaltuuksien tulee vastata työtehtäviä ja ne on pidettävä ajan tasalla. Käyttövaltuuksien antaminen, muuttaminen ja poistaminen on dokumentoitava ja niiden hallinnasta on tallennuttava tietojärjestelmään valvontalokitietoa. (VM 2006a.)

Monissa organisaatioissa tilanne on se, että käyttäjillä on enemmän käyttövaltuuksia, kuin olisi tarpeen. Organisaation tietoturvaan voidaan lisätä kerros yhdenmukaistamalla ja au-

tomatisoimalla käyttövaltuuksia koskevat prosessit. Samalla kevennetään IT-tuen työkuormaa. Keskitetyllä identiteetin- ja pääsynhallintajärjestelmällä pyritään toteuttamaan kyseisiä tavoitteita ja huolehtimaan siitä, että organisaatio kykenee vastaamaan annettujen säädösten noudattamisesta. Oikeaoppisesti tavoitteet säätää strategia.

2.2 Autentikointi ja kaksivaiheinen tunnistaminen

Identiteetin todentaminen - autentikointi eli käyttäjän tunnistaminen on yksi IAM-järjestelmän tehtävistä. Tunnistustapoja on vahvoja ja heikkoja; katso taulukko B. Yksinkertainen salasana-autentikointi on heikko tunnistus. Vahvana tunnistusta pidetään, jos vähintään kaksi eri ryhmiin kuuluvaa turvatekijää ovat läsnä eli kyseessä on kaksivaiheinen tunnistaminen. Eri tekijöinä pidetään käyttäjän tietoa, käyttäjän biometrisia ominaisuuksia tai jotakin, mitä käyttäjällä on. (Linden 2017, 16-17.)

Useat web-palvelut tekevät ensitunnistuksen lähettämällä käyttäjälle sähköpostin jolla varmennetaan vain, että kyseinen sähköposti kuuluu kyseiselle henkilölle. Monet heikolla tunnistuksella käytettävät palvelut tarjoavat autentikointia palveluna toisille web-palveluille. Ensitunnistus on vahva, kun käyttäjän identiteetti varmistetaan kasvotusten henkilökortista. Sähköinen tunnistaminen jatkossa on vahva, jos tunnistus on kaksivaiheinen. (Linden 2017, 16-19.)

Taulukko B. Ensitunnistuksen ja sähköisen tunnistuksen nelikenttä (mukaillen Linden 2017, 19).

Ensitunnistus/ Sähköinen tunnistus	**Heikko: rekisteröityminen itsepalveluna**	**Vahva: reaalimaailmassa kasvotusten**
Heikko: salasana	- ilmaispalvelut	- operaattoripalvelut - monet organisaation sisäiset palvelut
Vahva: kaksivaiheinen	- ilmaispalvelut voivat tarjota, lisäksi - pseudonyymiä vaativat palvelut	- asiointipalvelut - organisaation sisäiset palvelut tarvittaessa

Kaksivaiheisen tunnistuksen menetelmissä on eroja. Esimerkiksi pankkien tarjoama kaksivaiheinen tunnistus, joka perustuu salasanaan ja kertakäyttösalasanaan voidaan huijata käyttäjältä monella tavalla. Pankkitunnisteiden käyttö jättää aina rahajäljen, koska palvelu on maksullinen. Käyttäjää se ei auta huijauksen havaitsemisen suhteen. Kun huijaukses-

sa onnistutaan viemään pankkitunnistuksessa käytettävät tiedot ja useampi kertakäyttökoodi, olisi vielä havaittava, että tunnisteita on käytetty jossakin palvelussa. Tunnisteita käytetään yleensä heti, ellei olla saatu käyttäjän koko koodilistaa haltuun. Koodilistan vaihtoehto on avaingeneraattori, jonka vohkiminen on myös mahdollista, mutta laitteen valokuvaaminen ei olisi yhtä tuottoisaa kuin koodilistan.

Puhelimeen lähetettävä varmennekoodi on astetta varmempi varomenetelmä ja sen väärentämisestäkin jää toivottavasti kiinni. Aukoton menetelmä tuskin on ja sitä käytettäessä joutuu luovuttamaan puhelinnumeronsa palvelulle. Puhelimessa oleva kertakäyttöisiä koodeja generoiva sovellus on tekstiviestiä yksityisempi ja varmempi, jos luottaa puhelimensa turvallisuuteen. Lisäksi puhelimessa voi olla varmenneviesteillä toimiva sovellus, mikä eriyttää menetelmää hiukan inhimillisten virheiden osalta. Asiaa selvennetään edempänä.

Sovellukseen perustuvat menetelmät tarvitsevat varokeinon siltä varalta, että puhelimelle tapahtuisi jotain, mikä voi edellyttää jälleen puhelinnumeron käyttöä. Käyttäjän huolimattomuus voi heikentää joitakin sovellukseen perustuvia menetelmiä. Tästä näkökulmasta on merkitystä sillä, käytetäänkö tekstiviestivarmennetta vai varmennesovellusta ja ero on rahajäljessä sekä operaattorin lokitiedoissa. Varjopuoli on, että ennakkoon maksettujen liittymien hankkijoille ei tehdä minkäänlaista tunnistusta, mikä mahdollistaa varmenneviestiväärennösten lähettämisen. Asian tila voi muuttua tulevaisuudessa.

Puhelimen käyttäminen kaksivaiheeseen tunnistukseen on kyseenalaista siinä tilanteessa, että samaa puhelinta käytetään sekä palveluun kirjautumiseen, että toisen vaiheen tunnistusvälineenä, kyse ei silloin ole enää kaksivaiheisesta jakamattomasta tunnistamisesta. Tarkoittaen sitä, että puhelin tietää sen, minkä käyttäjänsä ja puhelin on se, mitä käyttäjällään on. Teknisesti tällä tasolla tapahtuvat väärinkäytökset vaativat kuitenkin juuritason haavoittuvuuksia tai epävirallisen järjestelmän ajamista. Kuitenkin jos pidämme puhelinta älyllisenä toimijana, sen kohdalla toteutuu vaarallinen työyhdistelmä. Se sekä käskee palvelussa sijaitsevia resursseja, että myöntää pääsyn niihin.

Ei ole kaukaa haettua pitää mobiililaitetta älyllisenä ilman laitteen murtamistakaan, joidenkin mobiililaitevalmistajien puhelimet sisältävät erillisen piirin koneoppimisalgoritmien ajamiseen (Lawler 2017; Owen 2018). Lisäksi ihmisillä on taipumusta terveeseen resurssitietoisuuteen - jos laite vaikuttaa toimivan normaalisti ja se on fyysisesti ehjä, niin se on palvelukelpoinen. Käyttäjät voivat päättää näin tietoisena tai tietämättään siitä, kun laite lakkaa saamasta päivityksiä.

Biometrisia tunnisteita kokeillaan aina uusissa käyttökohteissa, kuitenkin niihin liittyy pelote tunnisteiden varkaudesta. Sormenjälki voidaan valmistaa synteettisesti (Mythbusters 2006). Yhteinen heikko kohta monille biometrisille tunnisteille on se, että niitä voidaan joissain tilanteissa käyttää vastoin kantajansa suostumusta. Esimerkiksi kasvojen tunnistuksessa on hyvä, jos positiivinen tunnistaminen edellyttää silmien aukioloa. Iirisskannauksessa edellytetään silmän aukioloa, mutta tekniikan käytettävyyttä rajoittaa se, että katseen on pysyttävä kohdistettuna skanneriin. Mobiililaitteita ei pitäisi käyttää liikenteessä ajettaessa.

Kasvotunnistuksen käytettävyyttä rajoittavat lisäksi valaistusolosuhteet. Eri maiden viranomaiset käyttävät kasvojentunnistusta monenlaisiin tarkoituksiin (The Washington Post 2018). Useamman mobiililaitevalmistajan puhelimissa on tai tullaan ottamaan käyttöön infrapuna-tunnistus, joka perustuu ihonalaiseen verisuonistoon ja on todella tarkka (patentlyapple 2019). Kasvojen lisäksi tunnistus voidaan tehdä vaikka kämmenestä (Business Insider Nordic 2019). On kuitenkin oltava jokin tapa kiertää myös kasvojentunnistus, jotta laitteen saa auki poikkeustapauksessa, mikä heikentää menetelmää ja aina jää kysymys siitä, miten turvallisessa säilössä tunniste on. Voiko tunnistejälki vuotaa ja pystytäänkö vuotanutta tunnistetta hyödyntämään; onko tunniste laitekohtainen, avaako tunniste myös sovelluksia?

DNA on luultavasti biometrisistä tunnisteista yksilöivin. Tärkeintä ei kuitenkaan ole tunnisteen jakamattomuus eli atomaarisuus vaan se, miten luotettavasti ainoastaan valtuutettu henkilö voi tunnistetta käyttää. Kerran digitaalisiksi muunnetut tunnisteet ovat lopulta vain määrämuotoisia ykkösten ja nollien oktetteja. Sormenjäljet voidaan jo lukea RFID-skannerilla passista muiden tietojen muassa, samoin kuin pankkikortit voidaan skannata, mistä syystä markkinoilla on erilaisia RFID-suojatuotteita, kuten lompakoita.

Salasanankokeiluhyökkäykset pitäisi olla teknisesti estetty organisaation palveluissa. Riittävällä laskentateholla monimutkaisetkin salasanat ovat nopeasti laskettavissa, joten enää ei pitäisi olla huolissaan hyökkääjistä, jotka saavat salasanat hallintaansa nopeammin kuin brute force -hyökkäyksessä, vaan hyökkääjistä, jotka ylipäätään voivat saada salasanat haltuunsa muilla keinoilla. Puhelimienkin pitäisi olla suojattuja kokeiluhyökkäystä vastaan. Turvallisuuden kannalta oleellista on, että käytetty tunniste ei välity minnekään puhelimesta ulkoisesti tai sisäisesti, puhelinta ei ole murrettu ja koodin tapauksessa se ei ole intuitiivisesti arvattavissa. Kasvot eivät tässä tapauksessa ole riippuvaiset käyttäjän muistista. Käyttäjä itse voi asettaa jotakin vaatimuksia tunnistusteknologialle.

Käyttäjän tulee aina huomioida, että keksityt tai generoidut salasanat eivät ole lähelläkään todellista satunnaista ja siitäkin syystä puhtaasti entropiaan perustuva suositus on huono, koska käyttäjän pitäisi pystyä arvioimaan asia tai muistaa laskukaava ulkoa (useita kirjoittajia, toim. Wikimedia Foundation, Inc 2019). Erilaisen näppäimistön käyttäminen voi olla mahdotonta, jos käyttäjä ei edes verbaalisesti tiedä omaa salasanaansa, mutta tämä auttaa kiinnittämään huomiota siihen, mistä minnekin kirjaudutaan. Vaikeasti murrettavan salasanan käyttämisestä ei ole apua, jos hyökkääjä on saanut käsiinsä tietokannan, jossa salasanat ovat selväkielisinä.

Suositeltavaa olisi käyttää pitkiä salasanoja, jotka on mahdollista muistaa. Kirjoitusvirheilläkin on käyttötarkoitus - ne sopivat salasanoihin. Käytettävyyskin on huomioitava, kirjautumiseen ei pitäisi kulua liikaa aikaa. Mobiililaitteelle kannattaa valita toisenlainen autentikointimenetelmä käytettävyyden vuoksi. Salasanojen suositusten mukaiset vahvuusvaatimukset on huomioitava, jos ei ole varmaa tietoa siitä, miten salasanoja palvelussa käsitellään, kuinka ne on suojattu. Esimerkkinä Facebook (STT:n mukaan, HS 2019). Palveluntarjoaja ilmoittaa omat vaatimuksensa.

Olkoonkin että on huolimatonta käyttää lemmikkinsä nimeä salasanana, jättää laitteensa lukitsematta tai asettaa turvakysymyksiä joihin, joku muu henkilö tietää vastauksen; käyttäjän tulisi kiinnittää enemmän huomiota siihen, miten ja minne hän tunnistautuu. Salasanan lähettäminen suojaamattoman yhteyden yli voi tapahtua huomaamatta ja tuolloin salasana voidaan lukea matkanvarrella monessa kohdassa, mutta kyseessä voi silloin hyvinkin olla väärennetty sivusto, jos se sallii tunnistuksen suojaamattoman yhteyden yli.

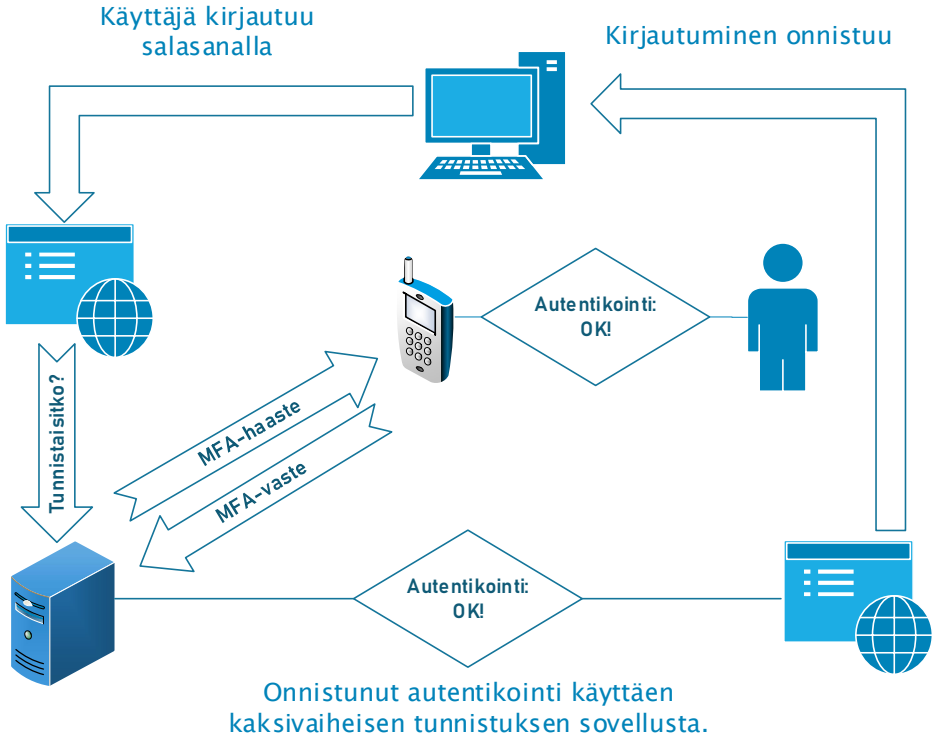
Monivaiheisen tunnistuksen käyttötapaukset puhelimella

Tämä luku on tarkoitettu pohdinnan tueksi kaksivaiheisen tunnistuksen käyttöönotossa. Aiheen ollessa entuudestaan tuttu, luvun voi ohittaa. Puhelimeen perustuvien kaksivaiheisten tunnistusmenetelmien skenaarioita mallinnetaan käyttäjän näkökulmasta, sekä esitetään käyttäjän muodostama hyökkäysvektori. Kuvat on pelkistetty palvelun päästä, koska käyttäjälle näkyvä prosessi halutaan esittää yksinkertaisesti. Väärinymmärrysten välttämiseksi, tarkennuksena: palvelu johon käyttäjä pyrkii, ei ole sama kuin palvelu, jota käytetään kaksivaiheiseen tunnistukseen. Palveluntarjoaja voi olla sama. Tämäkin on asia, johon tulee kiinnittää huomiota. Mille taholle käyttäjä luovuttaa tietonsa, ja mitkä tiedot kaksivaiheisen tunnistuksen tarjoamiseksi. Kuvat eivät koske mitään tiettyä tuotetta, vaan yleistävät toimintamallin.

Kyseiset käyttötapaukset perustuvat ajatusmalleihin, sillä tämän tapaista tutkimusta ei pidä teettää ihmisillä eettisistä syistä. Erilaiset analytiikankeruukomentosarjat ovat hyvin tavallisia nettisivustoilla ja tietosuojalaki edellyttää, että tiettyjä tietoja kerättäessä käyttäjää on informoitava siitä.

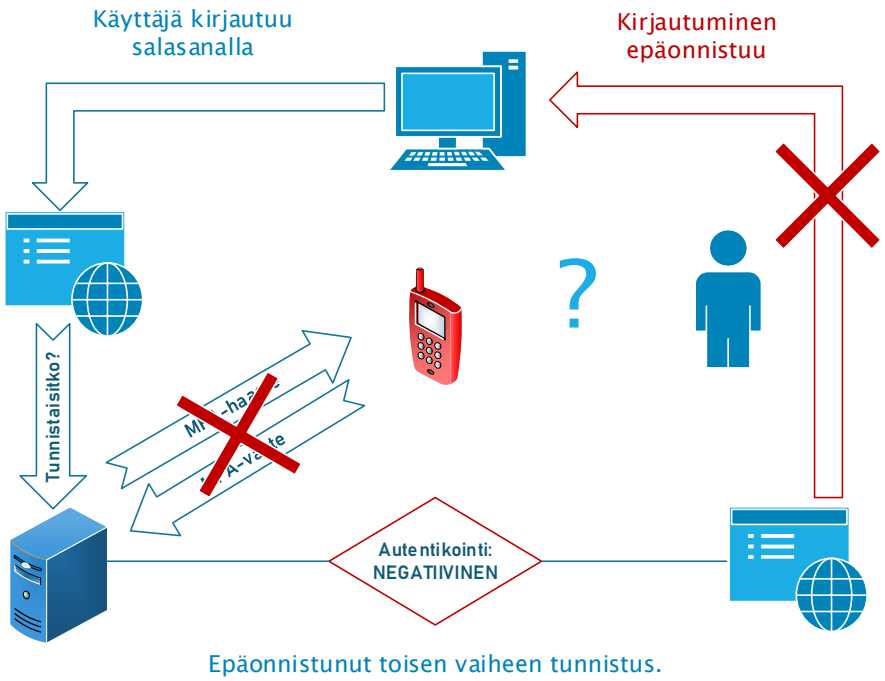
Työkaluna on käytetty Microsoft Visiota.

Kuvassa 1 käyttäjä on kirjautumassa aitoon palveluun ja palvelussa on käytössä kaksivaiheinen tunnistus. *MFA* eli *multi factor authentication* on toteutettu mobiilisovelluksella johon lähetetään push-viestejä ja sovellus vastaa kuhunkin viestiin käyttäjän kuitattua viestin.



Kuva 1. Tapahtuma on positiivinen: tunnistus onnistuu MFA-sovelluksella.

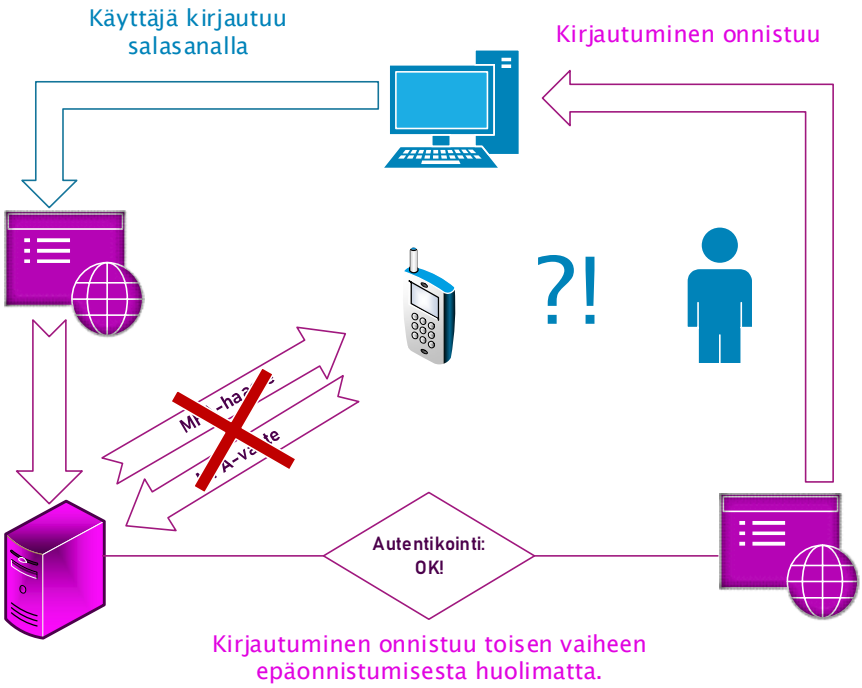
Kuvassa 2 käyttäjä on kirjautumassa aitoon palveluun ja palvelussa on käytössä kaksivaiheinen tunnistus mobiilisovelluksella, mikä toimii viesti ja kuittaus periaatteella. Käyttäjän puhelimessa on ongelma esimerkiksi tietoliikenneyhteyksissä tai sovelluksessa. Puhelin ei joko saa push-viestejä, ei kykene lähettämään vahvistusviestejä tai kykene näyttämään saapunutta vahvistuskyselyä. Hyökkääjän onnistuessa manipuloimaan puhelinta tässä tilanteessa lopputulos on palvelun estyminen. Käyttäjällä on kuitenkin mahdollisuus selvitellä ongelmaa.



Kuva 2. Tapahtuma on negatiivinen: autentikointi epäonnistuu toisessa vaiheessa.

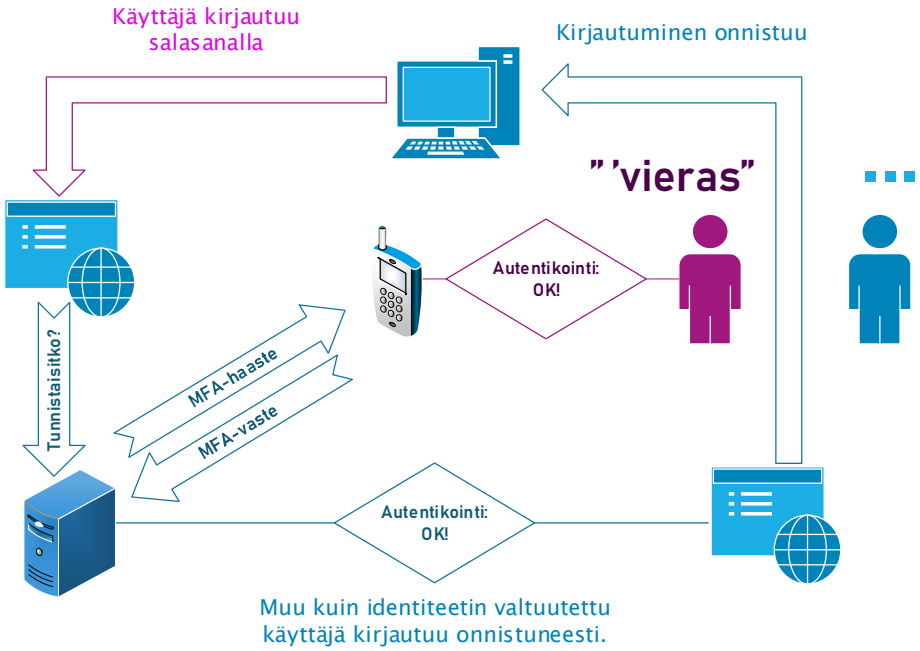
Kuvassa 3 käyttäjä on kirjautumassa väärennetylle sivustolle. Hänellä on käytössään kaksivaiheinen tunnistus, mikä toimii mobiilisovelluksella, joka käyttää push-viestejä. Sivusto ei voi lähettää MFA-sovellukselle aitoa viestiä, jos puhelin on rikkumaton. Väärä sivusto voi päästää tai olla päästämättä käyttäjää ’palveluunsa’ riippuen siitä, onko kaksivaiheisen tunnistuksen käytöstä ennakkotietoa. Hyvin valmistellussa huijauksessa voidaan myös esittää epäonnistunut toisen vaiheen tunnistus, jolloin käyttäjän epäilyksiä ohjataan muualle, eikä hän ehkä epäile mitään. Tällöin kirjautuminen epäonnistuu, mutta hyökkääjä saa saaliiksi käyttäjän käyttäjätunnuksen ja salasanan.

Käyttäjän epäluulojen pitäisi viimeistään herätä, kun kaksivaiheinen tunnistus ohitetaan. Kaikki sovellukset eivät kuitenkaan vaadi monivaiheisen tunnistuksen tekemistä joka kirjautumisella. Käyttäjä joko huomaa tai ei huomaa, että jokin meni vikaan, jollei monivaiheista tunnistusta tehdä joka kerralla. Ohjelmassa voi toisaalta olla joitakin sääntöjä sen suhteen, milloin monivaiheinen tunnistus tehdään, mikä tuo käyttäjälle lisäsuojaa.



Kuva 3. Tapahtuma on väärä positiivinen ja voi sisältää rikoksia. Käyttäjä onnistuu tunnistautumaan väärennettyyn palveluun, toisen vaiheen epäonnistumisesta huolimatta.

Kuvassa 4 muu kuin valtuutettu henkilö tunnistetaan jälkimmäisen identiteetillä tämän kirjautuessa esimerkiksi fyysisesti toisen henkilön laitteilta. Tilanne on rikos, kun muulla henkilöllä ei ole aidon henkilön lupaa toimia näin riippumatta siitä, miten hän on saanut kahden laitteen salasanat haltuunsa. Tähän sovelletaan lakia tietomurrosta 10.4.2015/368 (Rikoslaki, 38 luku, 8 §). Salasanojen puuttuessa kyseessä on rikos, jos muu henkilö näkee jotakin yksityistä tai muuten salaista. Salasanojen tai muiden tunnistusmenetelmien puuttuessa kyseessä ei ole kirjautuminen tai tunnistaminen eli, jos laitteita ei ole lukittu tai tunnistusmenetelmää asetettu ylipäätään.

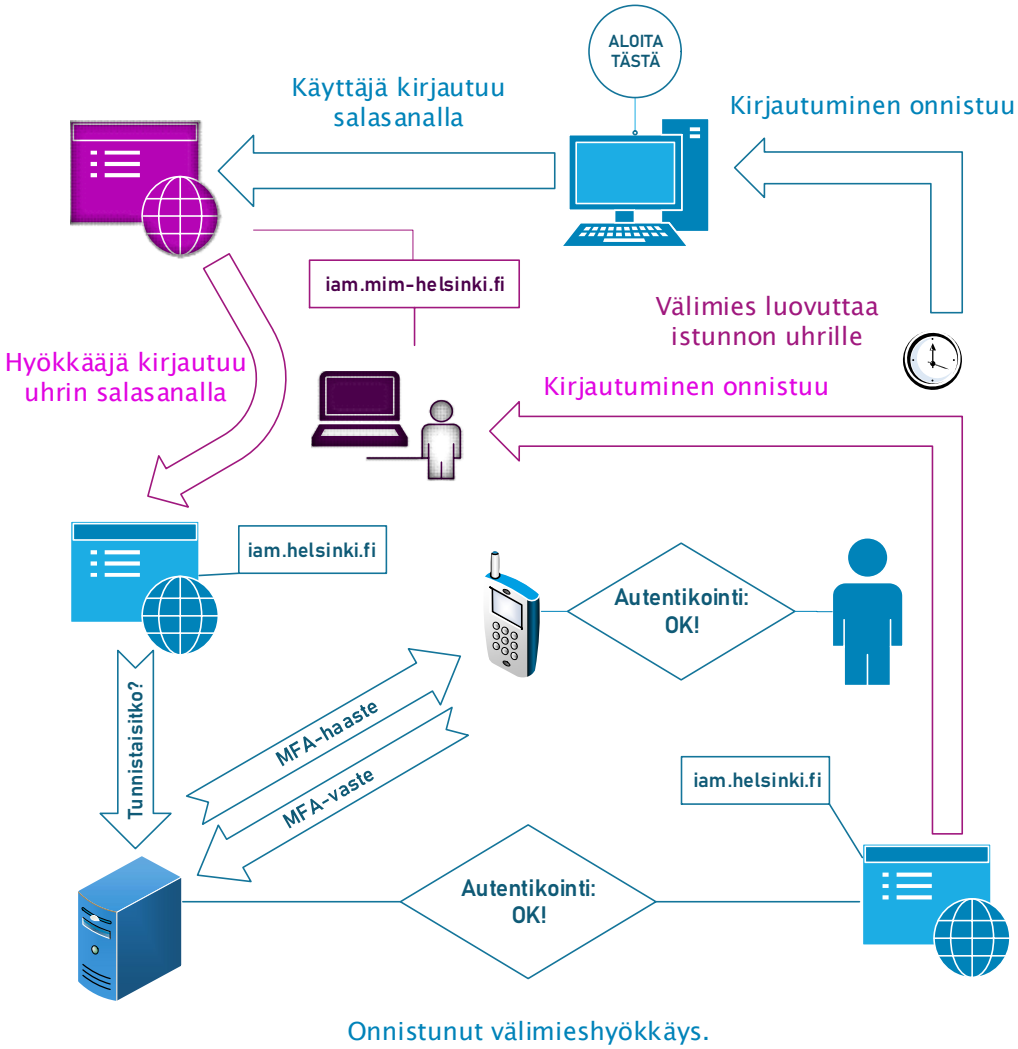


Kuva 4. Tapahtuma on käyttäjän näkökulmasta väärä positiivinen ja voi sisältää rikoksen. Kirjautuminen onnistuu.

Kuvassa 5 tapahtuu välimieshyökkäys. Hyökkäyksen voi toteuttaa monella tavalla. Tässä kuvassa välimies on välityspalvelimena (engl. proxy server) uhrin ja aidon palvelun välissä, hyökkääjä on aktiivinen. Hyökkääjä on voinut kaapata kohteensa kotireitittimen, jolloin hän voi myös tarjota omaa nimipalveluaan, käytännössä selvittää uskottavilta näyttäviä osoitteita. Hyökkäys voi esimerkiksi tapahtua myös paikassa, jossa on avoin Wi-Fi.

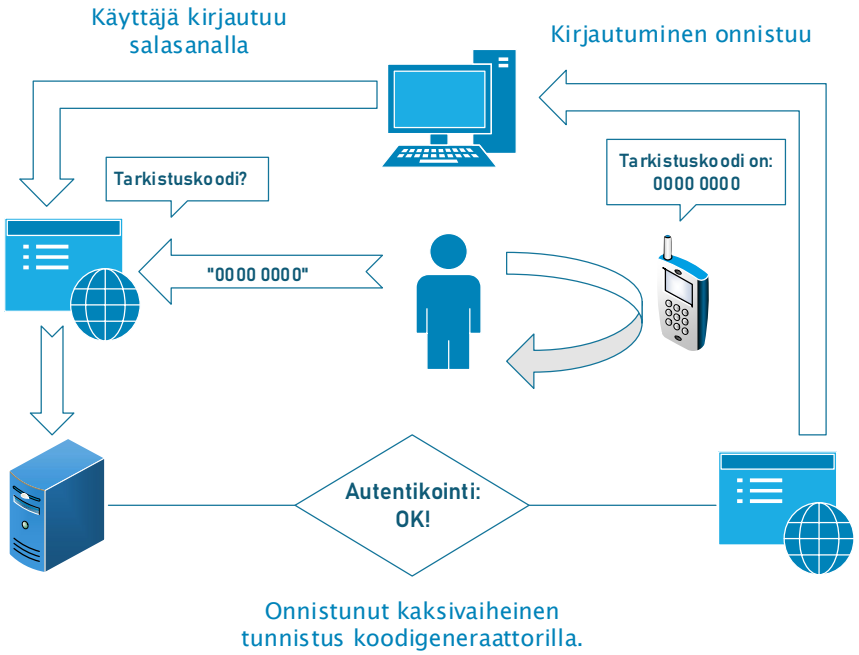
Internetissä olevaa sivustoa, jonka toimialuepääte on ”.fi” voidaan pitää siinä mielessä luotettavana, että se todennäköisesti voidaan jäljittää johonkuhun. On kuitenkin mahdollista, että nimen omistaja on jälleenmyynyt sen. Osoitteen on oltava aito, eli varmenteiden on oltava kunnossa.

Tässä tapauksessa kaksivaiheinen tunnistus ei tuo lisäsuojaa tai helpota hyökkäyksen havaitsemista muuten kuin viiveen muodossa. Tilanne ei kuitenkaan ole se, ettei kaksivaiheisesta tunnistuksesta olisi hyötyä. Kaksivaiheinen tunnistus auttaa suojautumaan useammilta hyökkäyksiltä ja välimieshyökkäys voi olla passiivinen, mikä onkin todennäköisempää. Hyökkääjä kerää tuolloin kirjautumistietoja myöhemmin käytettäväksi, eikä uhrin kirjautumisessa esiinny merkittävää viivettä. Aidon henkilön saadessa haasteviestin sovellukselta, kun hän ei itse ole kirjautumassa palveluun ei hän luultavasti hyväksy todentamishaastetta. Toisaalta ammattimainen tai kohteensa valinnut krakkeri kerää uhristaan riittävästi tietoa, jotta kykenee tekemään myös aktiivisen hyökkäyksen oikeana hetkenä.



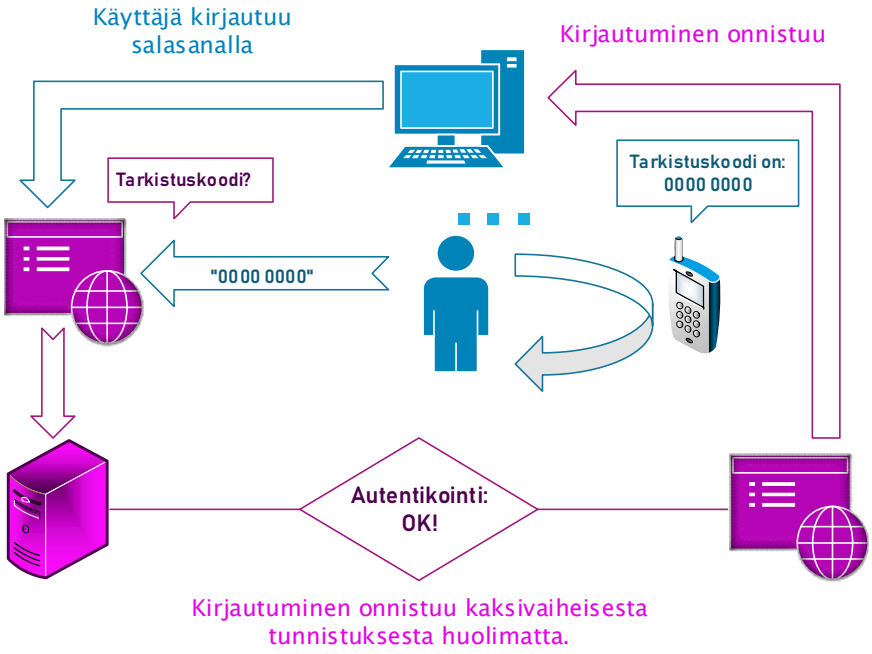
Kuva 5. Tapahtuma on väärä positiivinen ja sisältää rikosvyyhdin. Kirjautuminen onnistuu viiveellä.

Kuvassa 6 käytetään kaksivaiheisen tunnistuksen menetelmänä koodigeneraattorisovellusta puhelimella. Koodigeneraattorit perustuvat jaettuun salaisuuteen. Käyttäjä syöttää sovelluksen sen hetkisen koodin palveluun, jossa se pystytään vahvistamaan jaetun salaisuuden perusteella. Autentikointi onnistuu.



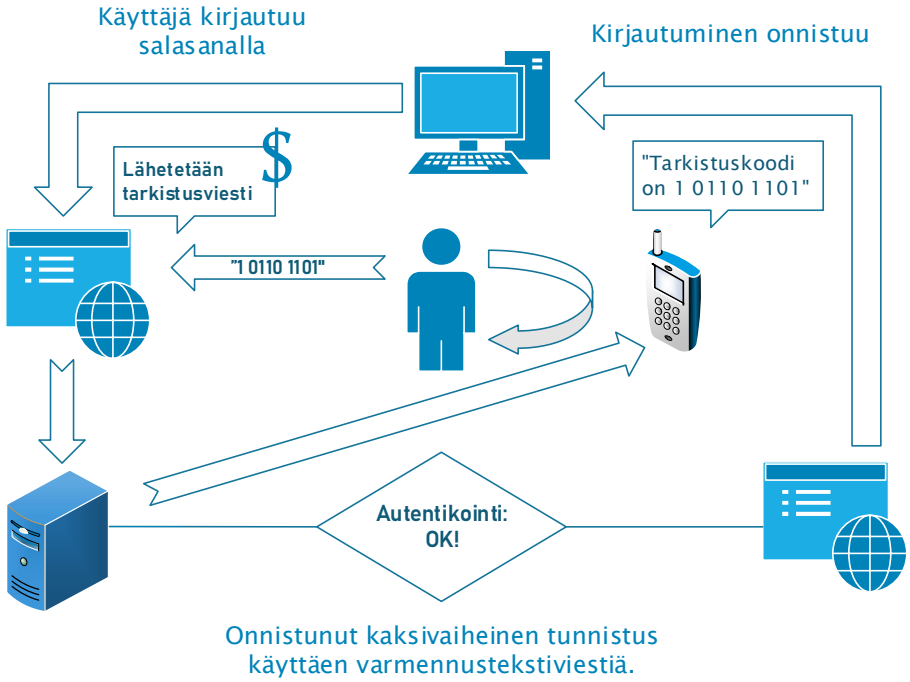
Kuva 6. Tapahtuma on positiivinen: kaksivaiheinen tunnistus koodigeneraattorilla.

Kuvassa 7 käytetään koodigeneraattorisovellusta kaksivaiheisen tunnistuksen menetelmänä. Käyttäjä kirjautuu väärennetylle sivustolle, joka olettaa käyttäjän käyttävän kyseistä MFA-menetelmää. Sivusto pyytää tarkistuskoodia, mutta hyväksyy minkä tahansa oikeanmuotoisen koodin. Tässä tapauksessa kaksivaiheinen tunnistus ei auta käyttäjää suojautumaan huijaukselta, tai toteamaan sitä.



Kuva 7. Tapahtuma on käyttäjän kannalta väärä positiivinen. Käyttäjä kirjautuu väärennettyyn palveluun ja kaksivaiheinen tunnistus onnistuu näennäisesti.

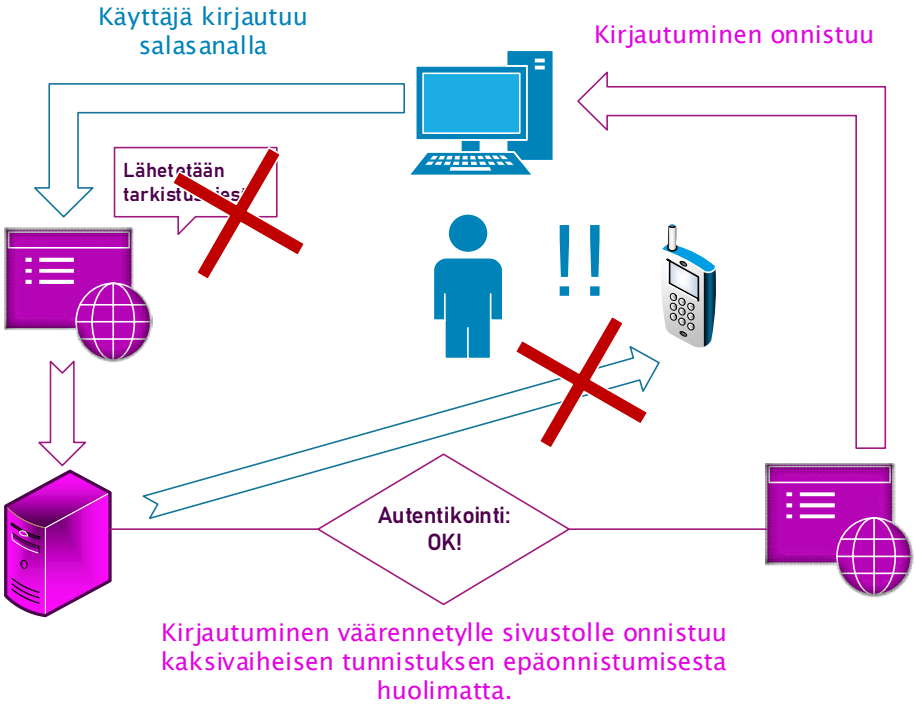
Kuvassa 8 käytetään toisen vaiheen tunnistuksessa tekstiviestivarmistusta. Palvelu on ostettu verkko-operaattorilta. Palvelu, jossa menetelmää käytetään kaksivaiheiseen tunnistamiseen, tarvitsee käyttäjän puhelinnumeron, jotta operaattori voi lähettää varmistustekstiviestin (Linden 2017, 26).



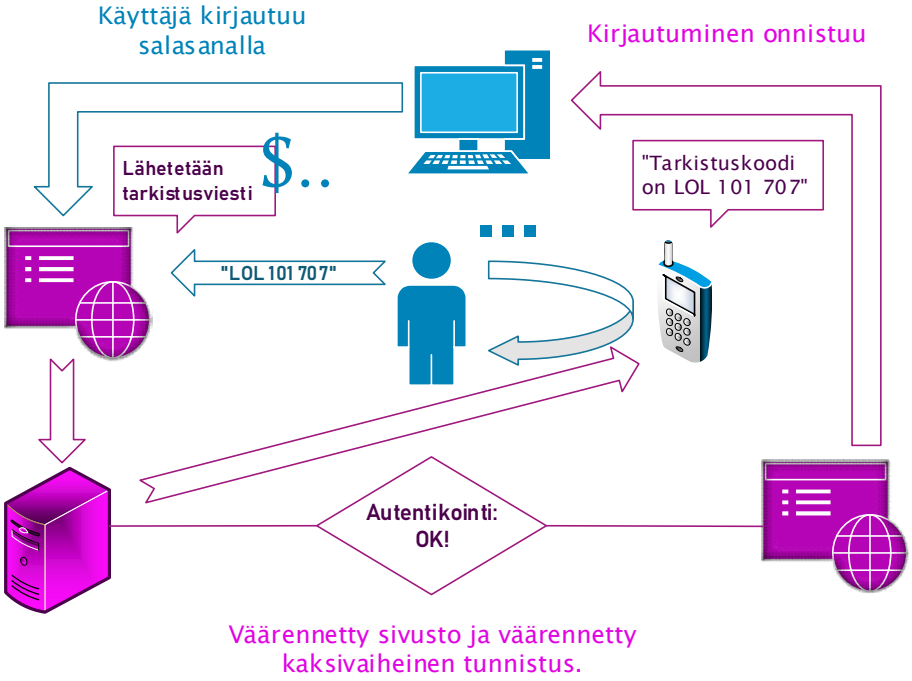
Kuva 8. Tapahtuma on aito positiivinen. Käyttäjä kirjautuu palveluun, toisen vaiheen varmenteena käytetään tekstiviestiä.

Kuvassa 9 käyttäjä on kirjautumassa väärennetylle sivustolle. Sivusto ei tiedä kaksivaiheisesta tunnistuksesta ja päästää käyttäjän sisään heikolla tunnistuksella. Tämän pitäisi herättää käyttäjän huomio.

Kuvassa 10 myös kaksivaiheinen tunnistus on väärennetty. Tällöin edellytetään, että hyökkääjä tietää mitä kaksivaiheista tunnistusta käytetään sekä käyttäjän puhelinnumero on saatu tietoon. Siten käyttäjälle voidaan lähettää halutunlainen varmennusviesti. Epätodennäköistä on, että viestin muoto olisi epäilyksiä herättävä kuten kuvassa. Tietojenkalastelussa yleisesti käytetty keino on jonkin halun herättäminen ja se voi toimia, vaikka teoreettisella tasolla käyttäjä uskoisi olevansa sellaisen yläpuolella. Käytännöntilanteessa toimintaan ja päätöksiin vaikuttavat tekijät, joita ei teoreettisella tasolla ehkä oteta huomioon. Sellaisia ovat esimerkiksi kiire, uteliaisuus, kiihtymys, pelko, yksinäisyys tai temperamentti. Nigerialaiskirjeisiin vastaaminen on kuitenkin väärä toimintamalli. Asian ilmoittaminen tietoturvalle helpdeskin kautta on suositeltavaa. Käyttäjän kannattaa kiinnittää huomiota siihen tulevatko varmennusviestit aina samasta numerosta kyseisessä palvelussa.



Kuva 9. Tapahtuma on käyttäjän kannalta väärä positiivinen. Kaksivaiheinen tunnistus epäonnistuu, mutta kirjautuminen väärennetylle sivustolle onnistuu.



Kuva 10. Tapahtuma on käyttäjän kannalta väärä positiivinen. Tilanne voi olla välimieshyökkäys. Onnistuakseen hyökkääjällä on oltava uhrin puhelinnumero.

Kuvasarjan kiteyttäen - monia epätoivottuja asioita voi tapahtua kaksivaiheisesta tunnistuksesta huolimatta tietämättömän tai huolimattoman käyttäjän avustuksella. Tarkastellaan esimerkiksi tilannetta, jossa kloonattu kirjautumissivu varastaa käyttäjätunnuksen ja

salasanan, minkä jälkeen botti syöttää ne aitoon palveluun ja käyttäjä ohjataan perässä ilman, että tämä huomaa mitään tavallisuudesta poikkeavaa. Kaksivaiheista tunnistusta käytettäessä, jos palvelu vaatii tunnistuksen joka kerta, tällainen kirjautuminen epäonnistuu aina siinä tapauksessa, että väärennetty kirjautuminen ei osaa ennakoida kaksivaiheista tunnistusta sekä väärentää sitäkin uskottavasti tai luovuttaa istuntoa aidolle käyttäjälle kaksivaiheisen tunnistuksen alkaessa. Jälkimmäisessä tapauksessa hyökkääjä – ihminen tai tietokone ei pääsisi palveluluun, mutta saisi riittävät tiedot onnistuakseen seuraavalla kerralla, jos muuttaa hyökkäystään.

Kaksivaiheista tunnistusta käytettäessä vaaditaan oikean käyttäjän aktiivisuutta ja osallisuutta tietomurto- ja identiteettivarkaustilanteessa, kun taas ilman sitä hyökkääjä voi kerran käyttäjän tunnukset varastettuaan toimia oman aikataulunsa ja mielensä mukaan käyttäjän tunnuksilla tämän sitä huomaamatta ehkä pitkään aikaan. MFA-autentikoinnin käyttäminen suojaa matalan tason hyökkäyksiltä ja hidastaa sekä hankaloittaa korkeatasoisempia hyökkäyksiä antaen valppaalle käyttäjälle ideaalisesti myös vihjeitä hyökkäysyrityksistä.

Kaksivaiheisen tunnistuksen palvelut ovat väärinkäytöksiä ehkäisevässä mielessä toteutettuja. Viestivarmistuksen tapauksessa esimerkiksi, tarkistusviestiä ei yleensä lähetetä automaattisesti, vaan erillisestä kehotteesta käyttäjän itse käynnistämänä. Käyttäjälle ei siis välity tietoa siitä, että käyttäjätilille on yritetty murtautua, koska hyökkäys keskeytyy kaksivaiheisen tunnistuksen alkaessa, kun sitä ei ole ennakoitu. Palvelu voi muulla tavalla pitää kirjaa kirjautumisyrityksistä, mutta tiedot eivät välttämättä ole kattavasti käyttäjän käytettävissä. Tarkistusviestipalvelunkin voi toteuttaa niin, että viesti lähetetään automaattisesti.

Suomi.fi-palvelu tarjoaa myös mobiilivarmennetta, eli operaattorin Sim-kortille myöntämää varmennetta autentikointimenetelmänä. Sim-kortissa on oltava tuki mobiilivarmenteelle. Varmenne voidaan aktivoida vahvan tunnistuksen jälkeen. Tunnistusprosessi mobiilivarmenteella etenee niin, että käyttäjä antaa palvelulle kirjautuessaan puhelinnumeronsa ja operaattorin mobiilivarmennepalvelu lähettää loppukäyttäjän puhelimeen tapahtumatunnisteen, jonka myös varmennepalvelu selaimessa ilmoittaa. Käyttäjä tarkistaa että tapahtumatunnisteet ovat samat ja hyväksyy tapahtuman puhelimessa, minkä jälkeen puhelin kysyy mobiilivarmenteen PIN-koodia, jonka käyttäjä tietää. Koodin syötettyään puhelin lähettää varmennepalvelulle tekstiviestin, minkä jälkeen kirjautuminen etenee. (Linden 2017, 26.)

2.3 Pääsynhallinta

Auktorisoinnissa tehdään nk. pääsynvalvontapäätös, mikä määrittää, onko tunnistetulla henkilöllä oikeus kyseiseen resurssiin. Auktorisointi on pääsynvalvonnan ydinprosessi. Pääsynhallinta pitää sisällään käyttövaltuushallinnan sekä pääsynvalvonnan. (Linden 2017, 31.)

Pääsynvalvonnassa on kyse funktiosta $f(S, O, A, e)$. Funktiossa S (subject) on tunnistettu käyttäjä, O (object) on suojattava kohderesurssi, A (action) on toiminto kuten lue, kirjoita tai suorita ja e (environment) ympäristömuuttujat, kuten kellonaika tai verkko, josta käyttäjä tulee. (Linden 2017, 31.)

Pääsynvalvontamenetelmä voi perustua käyttäjän rooliin, jolloin puhutaan roolipohjaisesta pääsynhallinnasta. Tällöin käyttäjät pyritään luokittelemaan esimerkiksi työtehtävän perusteella, jolloin erilaisille käyttäjäryhmille määritellään valmis malli halutuista käyttöoikeuksista ja kaikki saman roolin saavat henkilöt saavat yhtenevät käyttöoikeudet kyseisen roolin osalta. Roolipohjainen malli voidaan toteuttaa hierarkkisesti, jolloin käyttöoikeudet voivat periytyä roolista toiseen. Roolit jaetaan vielä työrooleihin, ylempi taso ja järjestelmärooleihin alempi taso. (VM 2006b, 17-18; Linden 2017, 32-34.) Helsingin yliopistolla pääsynvalvonta on toteutettu näin.

Muita pääsynvalvonnan menetelmiä ovat attribuutteihin perustuva pääsynvalvonta ABAC (engl. attribute-based access control), mikä on roolipohjaista valvontaa joustavampi menetelmä. Pakotettu pääsynvalvonta MAC (engl. mandatory access control) on kehitetty Yhdysvaltain armeijan tarpeisiin. Menetelmä on yksinkertainen ja kankea. Ylempi taso ei voi kirjoittaa alemman turvallisuusluokituksen materiaalia ja alempi taso ei voi lukea korkeamman turvaluokituksen materiaalia. Näiden lisäksi puhutaan jäljitettävyyteen perustuvasta mallista (engl. accountability based access control), mikä ei varsinaisesti ole pääsynhallintamenetelmä. Sekä ylläpitotunnusten hallinnoinnista PAM (engl. privileged account management), mikä on IAM-järjestelmään rakennettu osa ylläpitotunnusten valvomiseen. (Linden 2017, 34-35; Marjomaa 2018, 20-21.)

2.4 Helsingin yliopiston IAM-projekti

IAM-hankkeiden onnistumisen kannalta, huolelliset valmistelut ja yhteistyö eri osastojen välillä on tärkeää. Organisaatiolla on oltava yhtenäinen identiteetinhallintastrategia, selkeät tavoitteet, sidosryhmien tuki ja määritellyt toimintaprosessit, jotta hankkeeseen voidaan turvallisesti lähteä. (Martin & Waters 2004.)

Yliopistolla on noin 70 000 käyttäjää ja noin 20 000 työasemaa. Keskitettyä käyttäjäntunnistusta käyttäviä sovelluksia on noin nelisen sataa ja keskitetyn tunnistuksen ulkopuolelle jää puolet edellisestä määrästä.

Esiselvitys hanketta varten teetettiin vuonna 2011. Kaupallisia ja avoimen lähdekoodin ratkaisuita vertailtiin ja toteutuksessa päädyttiin avoimen lähdekoodin tuotteeseen Syncopeen osittain siksi, että kaupalliset ratkaisut ovat hintavia ja toisaalta yliopistolla on vahvat perinteet omavaraiseen toteutukseen. Projekti toteutettiin pääosin sisäisin resurssein käyttäen jonkin verran ulkoista asiantuntemusta. (Pääkkö 22.3.2019.)

Projektin hallintaan yliopistolla käytetään Scrum-viitekehystä. Hankkeen suurimpia haasteita on ollut vanhojen järjestelmien monimutkaisuus ja yhteen sovittaminen uuden järjestelmän kanssa. Paljon resursseja on vaatinut myös se, että on haluttu laajasti ominaisuuksia järjestelmältä sen sijaan, että oltaisi tyydytty prioriteetiltaan välttämättömiin ominaisuuksiin. (Pääkkö 22.3.2019.)

Projektilla on budjettia satatuhatta euroa. Projektin hyödyt näkyvät käyttäjille nopeampina tunnusten toimitus- ja hallintaprosesseina, helpdeskin työkuorma vähenee useita henkilötyövuosia ja yliopiston hallinnollinen työkuorma kevenee, Pääkkö arvioi.

Infrastruktuuri on yksi IAM-projektien suurimpia haasteita. *Legacy*-järjestelmiä voi olla miltei mahdoton integroida uusien teknologioiden kanssa.

2.5 Arkkitehtuuri

Helsingin yliopistolla on käytössä palvelukeskeinen arkkitehtuuri. Identiteetinhallintajärjestelmässä on *laskentamoottorina* Apache Syncope, joka laskee käyttäjien identiteettejä ja *provisioi* niitä eri järjestelmien kesken. Laskentamoottori lähettää viestejä mm. Active Directoryyn ja *LDAP:lle* tunnuksiin liittyvistä muutoksista, kuten työsuhteen päättyminen tai nimenvaihdos. Laskentamoottori toimii identiteettien ja käyttövaltuuksien *ydintietovarantona*. Se sisältää *metahakemiston*, jota se ylläpitää ja joka saa sopimustietosyötteensä henkilöstöresurssijärjestelmästä ja opintotietojärjestelmästä, joiden kanssa se keskustelee *palveluväylän* kautta. Tulevaisuudessa lähdejärjestelmiin voi kuulua myös kumppanien rekisteri. (Pääkkö & Tenhunen 2011.) Laajemman pääsyn tarjoaminen ulkopuolisille sidosryhmille voi tuoda organisaatiolle hyötyjä yhteistyö-, tutkimus- ja kehittämisetuina sekä työtyytyväisyyden lisääntymisenä (Martin & Waters 2004). Saavutettavat hyödyt ovat kuitenkin vain yksi näkökulma.

Kerrospuolustukseen vedoten erilaiset vahvat ja palvelutunnukset voisi pitää erillään IAM-järjestelmästä. Kyseisten tunnusten eheys ja tiedon täsmäytettävyys halutaan varmistaa samalla tai korkeammalla tasolla, kuin muunkin tiedon. Onko yhteinen ydintietovaranto paras ratkaisu ottaen huomioon, että mainitut tunnukset käyttäytyvät hyvin eri tavoin? Yksi tähän vaikuttava tekijä on se, miten metahakemistoa voidaan kirjoittaa tai lukea noilla tunnuksilla. Yliopiston uuden IAM:in kautta ei voida kirjoittaa metahakemistoa ja tavalliset tunnukset voivat lukea vain oman käyttäjänsä perustietoja. Helpdesk -henkilöstö voi tehdä hakuja metahakemistoon, mutta luettavissa ovat vain luonnollisten henkilöiden tiedot. IAM:n käsittelemiin tietoihin sovelletaan, mitä valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa 9 § mukaan määritetään sovellettavaksi (TTA 9 §).

Ydintieto lasketaan uudelleen määräajoin tiedon eheyden varmistamiseksi. Laskentamoottori käskyttää itse itseään ajastimien ja ulkoisten *herättimien* avulla. Se kirjoittaa ja lukee aktiivihakemistoa sekä LDAP-verkkohakemistoa suoraan ja palveluväylän kautta esimerkiksi NAS-verkkotallennusjärjestelmää, sekä henkilöstöresurssijärjestelmää roolien osalta. Kohdejärjestelmiä lisätään tarpeen mukaan.

Käyttäjän tunnistus on mahdollista tehdä yliopiston omalla kirjautumisella, aktiivihakemiston (engl. Active Directory), LDAP:n tai Shibboletin välityksellä, missä käytetään *SAML2:ta* kuten Suomi.fi:ssä, Suomi.fi -palvelulla tai ID Point -tunnistuksella, jossa käyttäjälle tehdään vahva tunnistus ja annetaan kertakäyttöinen kirjautumiskoodi.

Voidaanko IAM:in kanssa ottaa käyttöön kertakirjautumisteknologia? Yleensä kertakirjautuminen parantaa käytettävyyttä huomattavasti, jos se toimii. Siihen liittyy kuitenkin aina tietoturvariskejä, koska se avaa ovet moniin järjestelmiin yhdellä kertaa. Ongelmia aiheutuu silloin, kun käyttäjä tallentaa salasanan sovelluksen muistiin. Pahimmassa tapauksessa salasana tallentuu jonnekin selväkielisenä. Ongelmia voi tuottaa myös useammalla työasemalla kirjautuneena oleminen, se voi johtaa tunnuksien lukittumiseen. Toimiessaan *Single Sign-On* -ratkaisu on hyvä, jos kaksivaiheista tunnistamista edellytetään lisäksi. Toteutuksessa käytetään SAML2:ta.

Helsingin yliopistolla on monivaiheisen tunnistuksen pilotissa käytössä Duo Mobile sovellus, jossa voidaan käyttää tunnistamiseen push-viestejä, mikä on käyttäjälle vaivattomin tapa, myös koodit ja soitto ovat vaihtoehtoina. Järjestelmään on annettava varmistuspuhelinnumero, joka voi olla sama, kuin laitteessa tai eri puhelinnumero siltä varalta, että sovelluksen sisältävä laite hajoaa. (Helsingin yliopisto 2019.) Tuolloin voidaan käyttää tekstiviestiä tai soittoa autentikoinnin toisena vaiheena. Sim-kortin kadotessa esimerkiksi puhelimen mukana, on oltava yhteydessä operaattoriin.

Käyttöliittymän funktiot ja loppukäyttäjän vastuut

Helsingin yliopistolla ei ole käytöntukipalvelupisteitä, joten loppukäyttäjien tunnuksen hallintaa halutaan helpottaa tarjoamalla itsepalvelutyökaluja, kuten salasanan palauttaminen, nimitietojen päivittäminen ja sähköpostiosoitteen vaihdos on mahdollinen ainakin käyttäjille, joiden nimi on muuttunut. Sähköpostiosoitteen vaihtamiseksi tulisi edellyttää vahvaa tunnistusta. Käyttäjä ei itse voi määrittää uutta sähköpostia, vaan valitsee muutamasta algoritmin laskemasta vaihtoehdosta mieleisensä.

Asiakkaasta talletetaan myös kutsumasukunimitieto, jota ei ole aiemmin kerätty. Kutsumanimien vaihtaminen on käyttäjälle mahdollista. Kutsumanimi on käyttäjän näyttönimi järjestelmissä virallisen kokonimen sijaan. Käyttäjätunnuksen aktivoiminen itse on ollut aiemmin mahdollista opiskelijoille, IAM:n myötä myös yliopiston työntekijöillä on mahdollisuus tehdä tämä itse.

Käyttäjälle voidaan antaa vain vähän mahdollisuuksia muokata omia tietojaan tietojen eheyden säilyttämiseksi. Käytännössä sellaisia tietoja, jotka käyttäjät voivat itse järjestelmään syöttää ovat yliopiston ulkopuolinen sähköpostiosoite ja puhelinnumero. Yleinen tietoturvallisuus vaikuttaa myös siihen, millaista vastuuta käyttäjälle voidaan antaa. Vuoden 2018 kesällä oletettavasti kaikkiin yliopiston sähköpostiosoitteisiin lähetettiin tietojenkalasteluviestejä joihin osa käyttäjistä ”haksahti” (HS 2018). Kalastelijat lähettivät roskapostia kaapatuilla tunnuksilla, jolloin kaapatut tunnukset lukittiin.

Kaapatulla käyttäjätunnuksella voi tehdä edelleen identiteettivarkauksia toisen henkilön nimissä. Ellei käyttäjän oikeuksia muokata omia tietojaan ole rajoitettu, kaappaaja voi tehdä esimerkiksi sukupuolenvaihdoksen ja nimenmuutoksen käyttäjälle - virtuaalisesti. Asiointikielen vaihtaminen on myös tihutyö, joka voi aiheuttaa hetkellistä harmia. Hyökkääjä saattaa vaihtaa käyttäjän salasanan, tällöin käyttäjä voi vielä palauttaa salasanansa. Kuitenkin jos käyttäjällä ei ole kaksivaiheinen tunnistus käytössä ja hyökkääjä tallentaa käyttäjän tietoihin väärän puhelinnumeron sekä ottaa kaksivaiheisen tunnistuksen käyttöön omalle laitteelleen ei uhri enää pääse tililleen. Näin toimivan hyökkääjän on täytynyt harkita kiinnijäämisen mahdollisuutta. Yliopiston henkilökunnan puhelinnumeroita ei käyttäjä voi itse muokata.

Edellisen kaltaisia hyökkääjän toimia yhdistää se, että ne huomataan helposti ja ollessaan ammattimaisia ne voivat kohdistua esimerkiksi maineeseen. Huomaamatta jäävien hyökkäysten tarkoitusta on kuitenkin mahdoton selvittää ja niitä voidaan ainoastaan ehkäistä.

Helsingin yliopiston käyttäjätunnuksia koskevat käyttösäännöt muuttuvat. Käyttäjän käydessä siirtämässä tunnuksensa uuteen identiteetinhallintaan nuo säännöt luetutetaan hänellä. Palvelua ei tarvitse tarjota, jos käyttäjä ei tätä tee. Käyttösitoumuksen voi ajastaa aktivoitumaan uudelleen määräajoin, jolloin tunnusta jatketaan vasta, kun käyttösitoumus on kuitattu (Andreasson & Koivisto 2013, 111.) Yliopistolla tästä käytännöstä on luovuttu. Näin loppukäyttäjältä jää ylimääräinen työvaihe pois. Käyttäjätunnukset sulkeutuvat kuitenkin, mikäli opiskelija ei maksa HYY:n jäsenmaksua tai kun työntekijän työsopimus umpeutuu. Opiskelijan tapauksessa tieto opiskelijan aktiivisuudesta IAM:iin tulee opintotietojärjestelmästä.

3 Käyttöliittymän suunnittelu

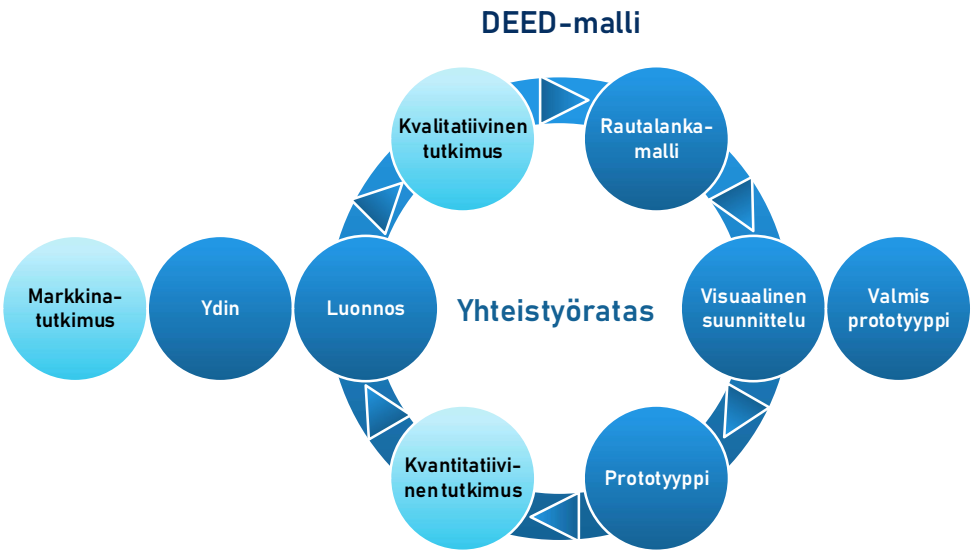
3.1 Toimeksianto ja ongelman määrittely

Asiakkaan kannalta tärkeintä on, että kaikki käyttäjät saadaan itse siirtämään tunnuksensa järjestelmästä toiseen, eikä tunnuksia siirretä automaattisesti. Tässä yhteydessä halutaan, että käyttäjät tarkistavat nimitietonsa sekä hyväksyvät tunnuksen uudistetun käyttösitoumuksen. Helppokäyttöisyys, vaivattomuus, selkeys, esteettömyys ja alustariippumattomuus ovat siis tärkeitä tekijöitä siirtotyökalun käyttöliittymässä. Henkilötietojen käsittelyä koskevat määräykset on huomioitava ja yliopiston tietojen eheydestä ja ajantasaisuudesta on huolehdittava. Suunnitteluvirheet ovat oma riskinsä tähän tarkoitukseen suunnitellussa käyttöliittymässä, esimerkiksi sensitiivisen henkilödatan joutuminen vääriin käsiin heikon tunnistamismenetelmän vuoksi. Riskit pyritään tunnistamaan hahmottamalla erilaiset käyttötapaukset.

Käyttäjälähtöisyys pyritään huomioimaan käyttöliittymäsuunnitelman ideointi-, suunnittelu- ja toteutusvaiheissa. Käyttöliittymän testauksen aikana saadaan eniten todellista käyttökokemusinformaatiota.

3.2 Menetelmät

Käyttöliittymän suunnittelussa ei noudatettu orjallisesti mitään tiettyä menetelmää. Aikataulullisesti työvaiheet oli jaettu karkeasti Scrum-sprintteihin. Toteutunutta toimintasuunnitelmaa voidaan verrata DEED- mallissa (engl. design-based evidence collection and evidence-based design thinking) käytettyyn prosessimalliin (McColeman, Barrett, Blair, Fraser 2017, 136). Tutkimusosioita ei toteutettu, mutta kutakin osaa pohjustettiin joltakin osin.



Kuva 11. DEED model (mukaillen McColeman, Barrett, Blair 2017, 136).

Käyttöliittymän suunnittelu alkaa ideoinnista. Työkaluiksi valittiin paperi, HTML, CSS ja JavaScript. Aluksi käyttöliittymän tehtävää hahmoteltiin paperikanvaasilla, seuraavaksi kuvattiin eri käyttötapauksia paperille prosessikaavioina. Kolmannessa vaiheessa liittymän prototyyppi koodattiin HTML:lla ja yliopiston CSS -tyyliohjetta käyttäen, mikä havaittiin hyväksi prototyypittelytyökaluksi (Idean). Tarkoitus oli tehdä prototyyppi mahdollisimman pitkälle HTML:lla, kuitenkin jo ensimmäisessä versiossa havaittiin, että ei ole järkevää tehdä prototyyppiä ilman JavaScriptiä. Huomioitavaa on, että koodaus on vielä hitaampaa, kuin visuaalisten prototyypittelytyökalujen käyttäminen.

Liittymästä tehtiin kaksi harjoitusversiota yhdellä käyttötapauksella. Kolmannesta versiosta lähetettiin asiakkaalle kuvakaappauksia ohjaavan palautteen saamiseksi. Ensimmäisen harjoitusversion suunnittelun jälkeen hahmoteltiin taulukoiksi useampia käyttötapauksia ja kehiteltiin niiden pohjalta riskimatriisi, joka koskee palvelun saatavuutta taulukko E, liitteessä 13.

Prototyypittelyn vaiheet etenevät sen mukaan, minkälaista tietoa suunnitteluun kulloinkin tarvitaan. Karkeasti vaiheet olivat:

1. Keskeisimmän ongelman hahmottaminen paperikanvaasilla ”value proposition canvas” ali arvolupaus-kanvaasi (Wiley 2014), toimeksiannon ja omien näkemysten perusteella.
2. Kahdeksan erilaista käyttötapausta listattiin paperille.
3. Kahdeksan käyttötapausta piirrettiin prosessikaaviona paperille.

4. Prototyypin kuvaa ei piirretty, sillä tarkasteltavana oli kuvia Yliopiston IAM-projektin demon eri käyttöliittymistä, jotka antoivat riittävästi suuntaa. Paperidemot ovat melko staattisia ja visuaalisten suunnittelutyökalujen toiminnallisuus on rajallinen, joten prototyyppi tehtiin koodaamalla. Tyhjästä aloitettaessa kuvien piirtäminen on tarpeellista.

5. Tehtiin ensimmäiset digitaaliset prototyypit, joista sai käsityksen käyttäjävuosta (engl. user flow). Kolmannella digitaalisella prototyypillä tehtiin ensimmäiset käyttäjätestaukset.

6. Edellisen vaiheen havainnot johtivat erilaisten käyttötapauksien kuvaamiseen taulukossa. Aluksi kaksitoista tapausta, minkä jälkeen laajennettiin kuuteentoista.

7. Käyttöliittymän kolmannesta prototyypistä pyydettiin asiakaspalautetta kuvien perusteella.

8. Prototyypin toiminnallisuutta laajennettiin kattamaan useampia käyttötapauksia.

9. Teetettiin käyttäjätestaus, jossa oli kaksi eri käyttötehtävää.

10. Suunniteltiin prototyyppiä edellisten testien perusteella ja tehtiin lisää testausta. Asiakaspalautteessa mainittuun käyttötapaukseen, jossa käsiteltiin käyttäjän ”taiteilijanimeä”, mikä on muu kuin virallinen nimi ei ehditty syventymään.

11. Raportoitiin tuloksista asiakkaille ja jatkettiin prototyypin kehitystä palautteen perusteella. Prototyypin testausta jatkettiin.

12. Käyttöliittymäsuunnitelman versio 8 esiteltiin asiakkaalle.

13. Käyttöliittymäsuunnitelman versioon 9 toteutettiin muutoksia palautteen perusteella.

14. Tähän mennessä on testattu vain kahta käyttötehtävää. Katsotaan tarpeelliseksi palata alkuun ja tehdä käyttäjäkuvaukset taulukoksi sekä harkita käyttöliittymään uutta käyttötapausta ”taiteilijanimi”, mikä jää opinnäytetyöprosessin ulkopuolelle.

3.3 Käyttötapaukset

Käyttötapauksesta käytetään termiä Case (lyh. engl. use case). Käyttötapauksista on kartoitettava vähemmän suotuisat tilanteet ja huomioitava ne käyttöliittymän toteutuksessa. Kuten jo luvussa 2.2 on käyty lävitse käyttäjälle epäepäedullisia tilanteita, luvussa 3.3 kartoitetaan erilaiset tapaukset ja kirjautumistapaukset taulukoiksi.

Käyttötapauksia hahmoteltiin aluksi useita tunnistamismetodin mukaan, sekä sen mukaan onko käyttäjän henkilötiedoissa tapahtunut muutoksia, sekä arvioiden sitä, mihin kaikkiin tietoihin halutaan ottaa kantaa käyttäjätunnuksen siirron yhteydessä. Taulukkoon C, liitteessä 12 on listattu mahdollisia käyttötapauksia.

Taulukointi selvitti, että ei ole syytä näyttää käyttäjälle tämän henkilötunnusta, vaikka se useimmiten järjestelmästä löytyy. Ei voida kuitenkaan olla varmoja, että kirjautuja on käyt-

täjä itse, koska käytettävissä on muitakin kuin vahvan tunnistuksen menetelmiä: yliopiston tavallinen kirjautuminen. Samasta syystä puhelinnumeroiden näyttäminen on tarpeetonta.

Asiakkaan toiveesta käyttäjälle annetaan mahdollisuus vaihtaa kutsumanimeään tai sähköpostiosoitettaan. Sähköpostiosoitteen muuttaminen on mahdollista vasta vahvan tunnistuksen jälkeen, sillä käyttäjälle voisi aiheutua harmia siitä, jos joku muu, kuin käyttäjä itse vaihtaisi hänen sähköpostiosoitteensa. Lisäksi sähköpostin vaihtamismahdollisuus aukeaa vasta, kun käyttäjä on valinnut nimitietojensa päivityksen väestörekisterikeskuksesta. Tuolloin hänellä voi olla oikea tarve vaihtaa sähköpostiosoitettaan nimen muuttumisen johdosta. Kutsumanimen vaihtamisessa ei edellytetä vahvaa tunnistusta. Käyttäjän näyttönimi muuttuu, kun kutsumanimeä vaihdetaan, sekin voi hämmentää ihmisiä. Lisäksi käyttäjän asiointia helpottaa, jos hänen ei tarvitse kirjautua useita kertoja.

Tietojenkalastelijalle asiointikieli on hyödyllinen tieto. Loppukäyttäjillä on mahdollisuus vaihtaa oma asiointikielensä omien tietojen kautta. Olisi hyvä jos tällöin edellytettäisiin vahvaa tunnistusta. Migraatiotyökalun yhteyteen muuttamismahdollisuutta ei tarvitse sisällyttää. Helpdesk-henkilöstölle asiointikieli on myös hyödyllinen tieto.

Taulukko D selittää eri kirjautumisvaihtoehdot. Tapauksissa 3A kirjautuminen Suomi.fi-palvelulla päättyy käytännössä virheeseen, koska järjestelmässä ei ole vielä kyseistä henkilötunnusta, eikä se näin ollen tunnista vanhaa käyttäjää samaksi. Yliopiston tunnuksilla kirjautuminen onnistuu edelleen tapauksissa 3A ja 3B, mutta henkilötiedot eivät tuolloin ole ajan tasalla ja tästä aiheutuu tietosisällön eheysvirhe. Käyttöliittymä ei kuitenkaan ota kantaa kirjautumistilanteessa tapahtuneeseen virheeseen, vaan kirjautumispalvelu ilmoittaa virheestä.

Taulukko D. Käyttötapausten kirjautumistilanteet.

Kirjautumistapa/ Käyttötapaus	Suomi.fi	Käyttäjätunnus ja salasana	ID Point - tunnistaminen
Case 1A	OK	toissijainen	toissijainen
Case 1B	määrittämätön	OK	toissijainen
Case 1C	määrittämätön	virhe	OK
Case 1D	määrittämätön	virhe	määrittämätön
Case 2A	OK	toissijainen	toissijainen
Case 2B	määrittämätön	OK	toissijainen
Case 2C	määrittämätön	virhe	OK
Case 2D	määrittämätön	virhe	määrittämätön
Case 3A	eheysvirhe	eheysvirhe	OK
Case 3B	määrittämätön	eheysvirhe	OK
Case 3C	määrittämätön	virhe	OK
Case 3D	määrittämätön	virhe	määrittämätön
Case 4A	määrittämätön	OK	toissijainen
Case 4B	määrittämätön	OK	toissijainen
Case 4C	määrittämätön	virhe	OK
Case 4D	määrittämätön	virhe	määrittämätön

Käyttötapausten ja tunnistamisen riskimatriisit

Edellisissä taulukoissa on selitetty kuusitoista erilaista käyttötapausta. Seuraavassa riskimatriisissa on esitetty nuo kuusitoista tapausta erotellen käyttäjästä ja palvelusta aiheutuvat riskiattribuutit. Taulukon E, liitteessä 13, vasemmanpuoleisessa sarakkeessa on annettu arvo riskille, joka aiheutuu kuvatun käyttötapauksen käyttäjän tilasta, läsnä olevat riskitekijät katsotaan tässä käyttäjästä johtuviksi. Tapauksissa 4B, 4C ja 4D voidaan yhden riskitekijän olettaa olevan seuraus toisesta, joten niitä ei pidetä kahtena erillisenä riskitekijänä. Tästä huolimatta Helsingin yliopiston on tarjottava palvelua samalla tasolla kaikille käyttäjilleen. Vaikka riskitekijöitä ei pidetä erillisinä, niin palvelun saatavuudesta on huolehdittava. Kolmessa seuraavassa sarakkeessa lisätään riskiä yhdellä, jokaista palvelua kohden kuvaamaan tilannetta, jossa palvelu on estynyt käyttäjästä aiheutumattomasta syystä esim. palvelunestohyökkäys. Arvoa ei kuitenkaan kasvateta, jos käyttäjällä ei käyttäjästä johtuvasta syystä ole mahdollisuutta käyttää palvelua. Oikeanpuoleisessa sarak-

keessa on toteutuneiden riskitekijöiden yhteenlaskettu summa. Ideaalisessa tilanteessa käyttäjällä on vähintään kaksi tunnistamisvaihtoehtoa käytettävissä.

Riskitekijöiden arvot selitetään seuraavasti:

- 0 – 1, värikoodi vihreä, tilanne OK
- 2, värikoodi keltainen, kohonnut riski
- 3, värikoodi oranssi, korkea riski tai palvelu estynyt
- 4, värikoodi musta, palvelu estynyt

Liitteen 13, taulukon E matriisi kuvaa pääasiassa erilaisia poikkeustapauksia ottamatta kantaa niiden todennäköisyyteen. Taulukon avulla voidaan havainnollistaa 48 tapausta ja kolmatta ulottuvuutta käyttäen vielä useampia tapauksia, kun kaikilla palveluilla on kaksi tilaa, joko palvelu on käytettävissä tai alhaalla. Kaikki tapaukset eivät kuitenkaan ole relevantteja, koska käyttäjän kannalta on samantekevää, jos palvelu on alhaalla sikäli, kun hän ei muutoinkaan voi sitä käyttää. Mahdollisia palveluiden tilojen yhdistelmiä on 2^3 eli 8. Käyttäjätiloja on määritelty neljä a) ei muutoksia, b) nimimuutos, c) henkilötunnusmuutos ja d) ei henkilötunnusta. Ei ole merkityksellistä, jos jotkin ehdot esiintyvät yhtä aikaa, kuten nimen ja henkilötunnuksen muutos. Lisäksi käyttäjästä johtuvasta syystä hän voi tai ei voi käyttää kutakin tunnistusmenetelmää jälleen 2^3. Ei kuitenkaan ole merkitystä johtuuko tunnistuksen epäonnistuminen käyttäjästä vai palvelusta, lisäksi käyttäjätilojen C ja D kannalta Suomi.fi -palvelu ei ole käytettävissä ensikirjautumisessa tai ollenkaan. Näin ollen erilaisia tapauksia on $2^3 \times 2 + 2^2 \times 2$ eli 24. Liitteen 14, taulukon F matriisi kuvaa noita tapauksia.

3.4 Käytettävyys ja käyttäjäkokemus premissit

Kirjoittajan omakohtaisen kokemuksen tuottamat hypoteesit selainpohjaisista käyttöliittymistä on listattu alla.

1. Tyylit vaikuttavat ihmisaivojen prosessointitehoon ja nopeuteen:

    A. Tiedon älyllinen käsittely tapahtuu nopeammin, jos visuaalista meteliä on vähän.

    B. Listat ovat helpompia lukea, kuin polveileva tyyli, jossa on mm. nostoja.

    C. Raaka teksti on helpompaa lukea, kuin pitkälle tyylitelty. Tässä raakatekstillä viitataan perinteiseen tekstityyliin, joka sisältää kappalejakoja ja otsikoita.

    D. Puuhakemistot ja listat kertovat paljon nopeammin ja kokonaisvaltaisemmin, mistä tietojoukossa on kysymys, kuin yksittäiset tyylitellyt representaatiot, jotka eivät paljasta paljoa logiikasta.

E. Motorisen tehtävän suorittaminen voi tapahtua nopeammin visuaalisten johtolankojen avustuksella.

F. Alituiseen vaihtuva tyyli hidastaa toimenpiteiden suorittamista ja voi jopa aiheuttaa turhautumia.

G. Paperisten kirjojen, kaavioiden ja karttojen käyttöliittymä on nykyisessä muodossaankin satoja vuosia vanha. Formaattia ei ole järkevää rikkoa pelkän taiteellisuuden nimessä.

H. Konventioiden noudattaminen helpottaa käyttöliittymien käyttöä.

I. Konventioita ei pitäisi rikkoa muuten kuin opetustarkoituksessa.

2. Tyyleillä voidaan ohjata käyttäjää ja tuottaa disinformaatiota:

J. Tyyleillä ja visuaalisilla vihjeillä voidaan johdatella käyttäjää.

K. Tyyleillä ja visuaalisilla vihjeillä voidaan myös mahdollistaa prosessin läpivieminen ilman, että käyttäjä ymmärtää tekemästään paljoakaan.

L. Konventioiden noudattaminen helpottaa käyttöliittymien käyttöä.

M. Konventioiden rikkominen voi johtaa arvaamattomiin lopputuloksiin.

N. Alituiseen vaihtuva tyyli voi harhauttaa ja hämmentää käyttäjää.

O. Vaihtuvalla tyylillä voidaan ohjata käyttäjä ajattelemaan aktiivisesti.

Käytettävyyden ja käyttöliittymäsuunnittelun pioneerit puoltavat osaa väitteistä ja saattavat olla eri mieltä toisista. Käyttöliittymän testauksessa ei pyritä todistamaan esitettyjä väittämiä, eikä kaikkia väittämiä hyödynnetä. Tavoite on optimoida käyttöliittymän käytettävyyttä siten, että annettujen tehtävien suorittaminen onnistuisi kaikilta käyttäjiltä mahdollisimman vaivattomasti.

Esimerkiksi Ben Shneidermanin kahdeksasta heuristiikasta viimeinen (S8) tukee väittämän 1 kohtaa A, heuristiikka koskee työmuistin kuormituksen keventämistä yksinkertaisilla ja yhtenäisillä rakenteilla. Shneiderman ja Jacob Nielsen listaavat konventioiden noudattamisen tärkeyden omissa heuristiikoissaan (S1, N4, N2). Väitteiden kohdat E-O liittyvät kaikki jotenkin konventioihin. Nielsenin tutkimustulosten mukaan paperisen median, kirjan, lukunopeus on edelleen 10,7% korkeampi, kuin tekstin luettuna tabletilta (Reading Today 2010). Tämä puoltaa väitettä 1, erityisesti kohtia G ja A, mutta myös C. (Shneiderman, 1998, 74-75; Nielsen 1994.)

Kohtia B, C ja D voidaan tarkentaa siten, että erityisesti informaation haussa mahdollisimman pelkistetty tyyli tai ei tyyliä lainkaan voi olla parempi, kuin vaikkapa tiettyyn tyyli-

kaavaan upotettu hakemisto. Raskaat tyylielementit, vaikka ne olisivat vain fontteja, reunuksia, värejä ja hehkuja ovat raskaita lukea ja kuormittavat työmuistia. Tyylejä ja visuaalisia elementtejä käyttämällä voidaan helposti piilottaa oleellista informaatiota, jopa aivan näkyville.

Tyylin on vaikea kilpailla raakatekstin kanssa, koska tyyli on kaikkialla erilaista, jokaisella sivustolla on oma visuaalinen murteensa. Visuaalinen kieli on karkeasti sama, jos vakiintuneita konventioita noudatetaan. Tyylittelemättömiä sivustoja ei juuri enää näe. Kannattaa kuitenkin harkita sitä, miltä käyttöliittymä näyttää, kun sen riisuu ja toimiiko se edelleen (havainnollistettu liitteessä 10). Lopputulos esimerkissä voisi olla parempi visuaalisen esteettömyyden näkökulmasta, mutta liittymä toimii. Liitteessä 11 on esitetty mobiiliversio käyttöliittymästä, vaikka yliopiston tyyli on mukautuva ero riisutun ja tyylitellyn version selkeydessä on suuri.

4 Käyttöliittymän prototyypin testaus

4.1 Testiasetelma

Ensimmäisellä testikierroksella testattiin kahta käyttötapausta, joista ensimmäisessä käyttäjää pyydettiin siirtämään käyttäjätunnuksensa migraatiotyökalulla vanhasta käyttövaltuusjärjestelmästä uuteen järjestelmään. Käyttäjälle kerrottiin hänen olevan testitapauksessa nimetty henkilö, että hänellä oli tunnukset Helsingin yliopistolla ja viestin mukaan hänen tuli siirtää käyttäjätunnuksensa vanhasta IAM-järjestelmästä uuteen IAM-järjestelmään. Lisäksi kerrottiin, että käyttäjä oli ohjattu sivulle, josta käyttöliittymän testaus alkaa. HTML-sivu oli avattu valmiiksi selaimeen.

Käyttäjälle annettiin lähtötilanteessa kaikki oikeat nimet sekä käyttäjätunnus erillisessä tekstitiedostossa, josta niitä oli mahdollisuus verrata käyttöliittymän tietoihin. Tehtävä olisi luonnollisesti helpompi käyttäjän omilla tiedoilla. Käyttäjän omia tietoja ei käytetty monesta syystä. Oleellisin syy on se, että käyttäjä ei voi kirjoittaa järjestelmään henkilötietojaan todellisuudessa, joten tiedot olisi pitänyt kerätä erikseen ja syöttää demoon valmiiksi. Testaajien henkilötietoja ei ole mielekästä kerätä tai säilöä tässä tarkoituksessa ylimääräisen työn ja ennen kaikkea tietosuojamääräysten vuoksi.

Käyttäjän hypoteettinen eteneminen on kuvattu liitteessä 4. Kaikki testattavat eivät tehneet testiä käyttöliittymäsuunnitelman versiolla 6, josta liitteen 4 kuvat ovat. Ensimmäiset testit tehtiin versiolla 3. Käyttöliittymään tehtiin suhteellisen pieniä muutoksia testien myötä ja asiakkaalta saadun palautteen perusteella. Toisessa käyttötapauksessa käyttäjälle kerrottiin, että hänen nimitietonsa ovat muuttuneet etunimien ja kutsumanimen osalta ja että yliopistolla on vanhat nimitiedot järjestelmissään. Käyttäjää kehotettiin päivittämään tietonsa. Odotettu toimintavuo on kuvattu liitteessä 5. Käyttäjille ilmaistiin, että testilaitteistossa ei ole tallentavia elimiä - ainoastaan valvoja tarkkailee käyttäjän tekemisiä ja katsoo toisinaan muualle. Tallentamisella ei kuitenkaan tarkoiteta järjestelmän ja sovellusten muisteja.

Näiden testien tarkoituksena oli varmistaa, että liittymän visuaaliset elementit ovat riittävän selkeät toimintavuon läpiviemiseksi. Jälkimmäisissä versioissa kiinnitettiin huomiota tekstiin ja sanamuotoihin.

4.2 Riskit ja mahdollisuudet

Käyttöliittymätestauksessa on tärkeä tavoittaa käyttäjiä, joilla on erilaiset taustat tietotekniikan käytössä sekä tulevan kohderyhmän käyttäjiä. Tieteellisen tutkimuksen periaatteita ei kannata soveltaa loppuun asti, sillä testijärjestelyjen tekeminen veisi liikaa aikaa ja resursseja. Hyödyllisempää on muuttaa käyttöliittymää useammin havaintojen pohjalta ja jatkaa testausta päivitetyillä versioilla. Testaajajoukon ei myöskään tarvitse olla käyttöliittymätestauksessa kovin suuri. Muutamilla tapauksilla voidaan haarukoida yleisimmät ongelmat, eikä käyttöliittymätesteillä tarvitse todistaa mitään. Suuremmassa tuotannossa tieteellisen käytännön soveltaminen pidemmälle olisi suotavaa.

Käyttöliittymätestauksessa ei kerätä henkilödataa. Tietyn roolin asettaminen testaajalle on ongelmallinen kohta. Käyttötapaukset perustuvat tavallisesti käyttäjäkuvauksiin, jossa kerrotaan käyttäjästä eräänlainen käyttäjätarina. Käyttäjäkuvaus voi sisältää kuvitteellisia henkilötietoja kuten sukupuolen, iän, etnisen taustan, elämäntilanteen kuvauksen ja käyttötarpeen. Käyttäjäkuvauksiin voidaan perustaa käyttötapaukset, joita halutaan testata.

Siirryttäessä testaamaan käyttöliittymää aidoilla testaajilla ei ole tarkoitus, että testaajan täytyy kyetä näyttelemään jokin rooli. Testaajia pyydetään viemään läpi halutut käyttötapaukset ja tämä voi vaatia testattavilta eläytymistä, vaikka toimenpide ei olisi henkilötietojen tarkistamista monimutkaisempi. Testaajan omia henkilötietoja ei voida käyttää, joten sellaiset on keksittävä. Luonnollisten henkilöiden tietoja ei voida käyttää, ettei rikota yleistä tietosuoja-asetusta. Nimi ei ole arkaluonteinen henkilötieto, mutta siihen voidaan yhdistää paljon arkaluonteisina pidettyjä henkilötietoja. Identiteettivarkaus ei ole riski, jos henkilö on kuollut, eikä yksityisyydensuojakaan päde, mutta kuolleen rooli on testaajille ehkä vaikeampi. Miten testataan käyttöliittymä johon ei voi syöttää tietoja, mutta josta on tarkistettava henkilötietoja, eivätkä tiedot voi olla henkilön omat tiedot.

Testitiedoiksi voi antaa Nimi Nimisen tai Testi Testaajan, minkä jälkeen henkilötiedot voidaan päivittää Nimi Testaajaksi, mutta tällainenkaan asettelu ei ole roolipuhdas ja voi olla entistä hankalampi testaajalle suoritettavan tehtävän kannalta. Testi Agentti ei tässä tapauksessa ole paljoa parempi, koska sitä on edelleen vaikea pitää nimenä ja agenttiroolinkin voi tarkoittaa useampaa asiaa. Käyttötapausesimerkeissä käytetään usein vakiintuneita nimiä, kuten Alice ja Bob tai Matti ja Maija tai Essi Esimerkki, mutta jos on päästävä eroon vielä sukupuolioletuksista, olisi valittava sukupuolineutraaleita nimiä. Sellaisia ei ole kovin helppo keksiä ja koska ne ovat vakiintumattomia esimerkkejä, yhdistyvät ne helpommin luonnollisiin henkilöihin.

Todellisuudessa voidaan käyttää vain yhtä nimeä ja toisen nimen on oltava ei-nimi tai muu attribuutti, jonka johonkin henkilöön voi yhdistää. Pohdinnan jälkeen Lex Neutraali, Talvi Anonyymi, Kesä Anonyymi ovat mahdollisia esimerkkivariaatioita, kun vielä käy läpi minkälainen käyttäjätunnus nimistä muodostuu. Sittenkin nimien vakiintumattomuus tekee niistä muuta, kuin neutraaleita Neutraalia lukuun ottamatta. Joskus nimistä muodostuu loukkaavaksi koettu yhdistelmä käyttäjätunnusta muodostettaessa ja tästäkin syystä hyvä suositus olisi, että käyttäjätunnuksia ei muodostettaisi käyttäjien nimistä. Turvallisuus on toinen syy. Ongelmaan ei ole mitään selkeitä vastauksia testitilanteessa ja käyttöliittymää suunniteltaessa tähän ei kulutettu aikaa.

Hyvän käytännön mukaista olisi pitää testidemot organisaation verkossa. Pääsyä voidaan haluta rajoittaa sisäverkon sisälläkin. Käytettävyystestaukseen tarkoitettujen demoprojektien ei pitäisi sijaita kenenkään henkilökohtaisella toimialueella, vaan mahdollisimman virallisessa osoitteessa, jossa joku muukin voi tarkastaa koodin. Sopimukset antavat luottamussuhteelle pohjan ja siihen perustuen toimeksiantaja voi luottaa siihen, että koodi ei sisällä mitään haitallista.

4.3 Tulokset – käytettävyys ja käyttäjäkokemus

Käyttöliittymäsuunnitelman ensimmäistä versiota ei testattu, sillä siinä ei noudatettu toimeksiantoa riittävästi, eikä liittymä ollut lainkaan mukautuva. Suunnitelman versio 2 korjasi mukautuvuutta. Testit aloitettiin versiolla 3.

Käyttäjien ohjeistus

Käyttöliittymän versio 3 huomioi toimeksiantoa paremmin. Version 3 varhaisesta muodosta pyydettiin asiakaspalautetta kuvien perusteella. Viimeistellympää versiota testattiin useammalla testihenkilöllä.

Ensimmäisessä käyttötapauksessa suurin osa käyttäjistä kirjautui mutkitta, joko Suomi.fi -tunnistuksella tai yliopiston tunnuksella ja salasanalla. Haasteelliseksi osoittautui kuitenkin näkymä kirjautumisen jälkeen: liite 1, kuva 14. Jotkut testaajat harhailivat navigaatiossa, sen johdosta visuaalisia ärsykkeitä vähennettiin seuraavissa versioissa. Kaikki eivät ymmärtäneet heti, mitä käyttäjältä odotettiin tässä näkymässä. Mielenkiintoa herätti erityisesti ylänavigaation välilehtipainikkeista ”Omat tiedot” -painike. Testaajista osa nojasi verbaaliseen tukeen tähdentämällä vielä kuvitteellisen sähköpostiviestin sisältöä, joka oli johdattanut heidät sivustolle. Tietoa kaivattiin myös siitä, minkä järjestelmien välillä tietoja siirtyy. Kyselyihin vastattiin joko ”en tiedä”, ”tämä on keskitettyä tunnustenhallintaa”, ”se ei kuulu

käyttöliittymään” tai ”tiedot siirtyvät vanhasta järjestelmästä uuteen” suhteellisen pehmeään sävyyn.

Edellisen kaltaiset kysymykset on hyvä ennakoida ja noudattaa vastauksessa ennalta määrättyä kaavaa. Mitä systemaattisemmin testaajalle vastataan eri tilanteissa, sitä paremmin hygieenisyys säilytetään testissä – testattavilla on samat lähtötiedot, jotka tässä tapauksessa rajoittuisivat kuvitteelliseen sähköpostiviestiin ja muistioon, josta henkilö voi tarkistaa tietonsa. Harjoiteltu vastaus edesauttaa testaajan viihtymistä tilanteessa ja tavallisesti testaajan halutaan rentoutuvan testitilanteessa. Sosiaalisen krakkeroinnin välineisiin kuuluu käyttäjän tunnetilojen manipulointi. Kalasteluviestit voivat käyttää taktiikkanaan käyttäjän stressaamista huonoilla uutisilla kuten esimerkiksi: ”Käyttäjätililläsi on havaittu poikkeavia tapahtumia. Tarkista toiminta ja vaihda salasanasi, mikäli et tunnista tapahtumia.” Asianmukainen huijauslinkki on liitetty viestiin. Kalastelija toimii sillä premissillä, että osa ihmisistä tekee huonoja päätöksiä peloteltuina.

Käyttöliittymää testattaessa ei tyypillisesti haluta, että tilanne muistuttaa sosiaalisen krakkerin johdattelua. Tämän näkökulman voi huomioida vastausta laatiessa. ”Kyllä” ja ”ei” vastauksia kannattaa välttää, koska ne ovat johdattelevia, ja lisäksi sisältävät potentiaalisesti paljon informaatiota, jonka laatu riippuu kysymyksestä. Tällä tarkoitetaan, että sanojen luonne on ehdoton, mutta niillä ei voida kuvailla asioita sen tarkemmin. Vastaaja ei välttämättä tiedä, mitä kysyjä on tarkalleen tarkoittanut, vaikka ymmärtääkin kysymyksen ja toisin päin. Tämän tasoinen pohdinta on järkevää, kun huomioidaan, että käyttäjien taso tietoteknisissä asioissa voi olla hyvin vaihteleva. Alan sanastossa on lisäksi paljon monimerkityksisiä sanoja sekä sanoja, jotka muistuttavat läheisesti toisiaan, nämä voivat aiheuttaa sekaannusta. Tässä tilanteessa kielteinen vastaus muotoiltaisiin: ”eivät siirry”.

Tilannetta kannattaa paremmin kuvailla yleisistä lähtökohdista. ”En tiedä” ei ole paras tapa ilmaista testaajalle, että asiaa ei tässä yhteydessä haluta tuoda esille, vaikka kiusaus olisi suuri vastata näin. Kaavamainen vastaus jota voi tilanteessa käyttää kuuluu: ”Tiedot siirtyvät järjestelmästä A järjestelmään B.” Testitilanteessa ei pitäisi olla syytä vastata testin asetelmaa koskeviin kysymyksiin tarkemmin. Tilanne halutaan säilyttää samanlaisena testikierroksen ajan, jos kiinnitetään huomiota testitulosten yleisyyteen. Liiallinen jutustelu voisi myös johtaa sellaisten asioiden paljastumiseen, mitkä on tarkoitettu salassa pidettäviksi. Jatkokysymyksiin kannattaa varautua, jos esittää tietosisällöltään kovin täsmällisiä oletusvastauksia. Sanoja kuten tietovaranto, hakemisto tai rekisteri on parempi käyttää harkiten. Yleiskielessä pysyminen on suositeltavaa.

Enemmistö testaajista tarkasti annetut henkilötiedot, on kuitenkin epäselvää, kuinka moni huomasi niiden puutteellisuuden tai virheellisyyden. Tästä syystä käyttäjän kaikki viralliset nimet olisi tullut näyttää heti kutsumanimien lisäksi, jotta käyttäjien olisi ollut helpompi suorittaa tarkistus.

Yksikään testihenkilö ei yrittänyt päivittää tietojaan tässä käyttötapauksessa. Suurin osa ohitti käyttösääntöjen kokonaisen version syystä tai useammasta. Mainittakoon että testilaite oli kytketty vain sähköverkkoon ja käyttösäännöt aukenivat *julkisen toimialueen* sivustolle. Harvaa testaajaa häiritsi liikaa, että käyttöliittymän ensimmäisellä sivulla olevan ohjeen ”Aloita tarkistamalla henkilötietosi ja etene käyttösääntöjen kautta hyväksymään tunnuksen siirto IAM-järjestelmään.” noudattaminen oli monessa suhteessa mahdoton tehtävä. Tämä oli kuitenkin yksi kohta, jota voitiin pitää testin päättävänä virhemahdollisuutena. Pieni osa testaajista pyrki noudattamaan ohjetta sanatarkasti.

Toinen käyttötapaus oli testaajille helpompi. Odotettu toimintavuo on kuvattu liitteessä 5, se on käyttöliittymäsuunnitelman versiosta 6.

Tilatiedot graafisesti

Versioon 4 tuotiin modaalisuutta parantamaan toiminnan tilan käsitystä. Nielsenin ensimmäinen heuristiikka (N1) koskee järjestelmän tilatietoa (Nielsen 1994). Versiota testattiin. Liitteessä 2, kuva 17 taustalle jäävät objektit sumennetaan. Jotkut testaajat vieroksuivat toteutusta, mutta haittaakaan siitä ei havaittu olevan. Taustan sumentamisella redusoidaan visuaalista meteliä, kuitenkin on huomioitava, että se on itsessään visuaalinen efekti.

Version 3 ja 4 testaajat kaipasivat palaa takaisin tai peruuta toimintoja käyttöliittymään ja lisää värejä, kuten punaista. Palaa takaisin -näppäimiä ei sovellettu seuraavissa versioissa, sillä toimeksiannossa määriteltiin, että kaikkien käyttäjien halutaan tekevän migraatio. Palaa takaisin -näppäimen lisääminen on suositeltava vaihtoehto, jos pääsivun elementit jaetaan useammalle sivulle, mikä on yksi mahdollisuus. Värejä ei lisätty, sillä visuaalinen esteettömyys on pyritty huomioimaan yliopiston tyylioppaassa.

Käyttöliittymäsuunnitelman versio 5 on version 6 modaalinen versio, tätäkin testattiin. Koko käyttöliittymää ei viety kyseisellä idealla pidemmälle, koska suurempia etuja ei tehdyissä testeissä havaittu. Modaalisia elementtejä käytettäessä voi olla parempi, jos elementti suljetaan klikkaamalla elementin ulkopuolelle sen sijaan, että klikataan jotakin tiettyä elementtiä.

Pikanäppäimet

Testeissä havaittiin, että jotkut käyttäjät kaipasivat pikanäppäimiä, kuten *palautusnäppäin*. Pikanäppäimistä on sanottua hyötyä tottuneemmille käyttäjille GOMS näppäilymoodin (engl. Goals, Operators, Methods and Selectors keystroke mode) kehittäjä, Raskin, on esittänyt mallissaan aika-arvoja käyttäjän eri toimintojen suorittamiselle: taulukko G (Huai & Qi 2017, 5).

Taulukko G. GOMS keystroke mode (mukaillen Huai & Qi 2017).

Nimi	**Näppäily** (Keying, *K*)	**Osoitus** (Pointing, *P*)	**Palauttaminen** (Homeing, *H*)	**Käsittely** (Mentally preparing, *M*)	**Vaste** (Responding, *R*)
Aika keskimäärin *(S)*	0,2 *s*	1,1 *s*	0,4 *s*	1,35 *s*	
Merkitys	Näppäimen tai hiirennäppäimen painallukseen kuluva aika	Hiirellä kohdistamiseen kuluva aika	Käden palauttaminen hiirelle tai näppäimistölle näppäimistöltä tai hiireltä	Seuraavaan toimintoon siirtymiseen kuluva aika	Tietokoneen vasteaika

Shneidermanin heuristiikoista toinen (S2) koskee pikatoimintoja, myös Nielsen kehottaa huomioimaan edistyneempien käyttäjien toiminnot (N7) (Shneiderman, 1998, 74-75; Nielsen 1994). Hän kehottaa mahdollistamaan käyttäjille oikopolkujen käyttämisen ja GOMS-moodi osoittaa myös, että tämä säästää käyttäjälle aikaa. Palautusnäppäimen tuki lisättiin myöhemmin joihinkin nappeihin tulevissa versioissa.

Kehotteet

Käyttöliittymäsuunnitelman versioon 7 muutettiin ohjetekstien tyylit vaaleansinisestä kursiivista tavalliseksi leipätekstiksi, koska testausten edetessä syntyi vaikutelma siitä, että testaajat ohittivat koristeellisen tekstin tai jotkut suorastaan eivät havainneet sitä suuremmasta pistekoosta huolimatta. Visuaalinen esteettömyys on hyvä pitää mielessä tässäkin kohtaa. Ohjeteksti on hyvä olla myös siltä varalta, että käyttäjä voi ainoastaan kuunnella sivun näytönlukijan lukemana. Taulukoiden osalta on mietittävä luetaanko ne rivi riviltä vai

sarake sarakkeelta ja valikoiden on myös oltava mahdollisimman selkeitä (da Silva Bastos & Muñoz 2017, 331).

Kehotteita ei lisätty aiempiin versioihin muuten, kuin tietojen päivittämisen osalta väestörekisterikeskuksesta. Kehotteita lisättiin kutsumanimen ja sähköpostin muokkaukseen. Käyttäjän poistuessa sivulta tekemättä muutoksia näytetään ilmoitus ”Muutoksia ei tehty” samalla korkeudella, josta toiminto käynnistettiin. Ilmoitukset näytetään vain, jos käyttäjä ei tee muutoksia, mutta voi olla perusteltua näyttää ilmoitus tai varmistuskysymys, jos käyttäjä on aikeissa muuttaa tietojaan. Käyttökokemusta ajatellen käyttäjältä vaaditaan ylimääräinen klikkaus, jos esitetään varmistuskysymys, mutta prosessi tuntuu luotettavammalta, kun muutos on vahvistettava.

Toinen vaihtoehto on vain näyttää ilmoitus kutsumanimitietojen päivittämisestä. Toisaalta ihmiset arvioivat muutossokeuden vaikutuksen vähäisemmäksi kuin, mikä se todellisuudessa on (McColeman & Barrett & Blair 2017, 139). Ihmisen kannalta olisi miellyttävää, jos kehotteessa kerrottaisiin, mikä uusi nimi tai sähköposti on sen lisäksi, että tiedot näkyvät niiden oletuspaikoilla, mutta rajapinnan ei ehkä haluta käsittelevän tietoja siten. Pelkistetyn ilmoituksen näyttäminen on kuitenkin parempi vaihtoehto kuin ei mitään.

Asiakasesittely

Edellisestä versiosta tehtiin vielä asiakasesittelyä varten seuraava versio, jossa käyttösäännöt avattiin modaaliseen ikkunaan uuden välilehden sijaan. Koodi siistittiin myös tähän versioon. Koodiin tehtävät muutokset tai siistimisoperaatiot ovat oma työsarkansa. Tämän prototyypin kohdalla työtä koituu siitä, että liittymän jokainen looginen vaihe kuvattiin aluksi omaksi sivukseen, minkä jälkeen jokaiselle sivulle rakennettiin halutut JavaScript blokit, jotka kutsuvat yleisiä JavaScript luokkia. Kertautuvaa koodia kirjoitettiin paljon. Mallissa jokaisen sivun toiminnallisuus on erilainen, vaikka lopputulos näyttää samalta. Sivuston olisi voinut toteuttaa yhtenä sivuna, jolloin JavaScriptiä olisi hyödynnetty enemmän ja koodia olisi vähemmän. Perinteisen ja koodikirjaston ero on se, että perinteinen kirjasto ei lataa itseään.

Käyttöliittymäsuunnitelman versio 8 esiteltiin asiakkaalle.

Käyttäjävuon seuraamiseksi sivuhistorian avulla ja myös versionhallinnallisista syistä prototyypissä säilytettiin monisivuinen rakenne. Lisäksi sivulta toiselle siirryttäessä käyttäjälle annetaan mahdollisuus testeissä kiinnittää huomiota viittausosoitteisiin eri elementeissä. Näppäin voi olla linkki ja minne linkki viittaa? Valpas testaaja kiinnitti viittausosoitteisiin

huomiota ja reagoi eri tavoin Suomi.fi-tunnistukselta näyttävälle sivulle tultaessa (liite 5, kuva 31). Käsittelyaika tuolla sivulla oli merkittävästi pidempi, kuin normaali tehtävästä toiseen siirtymään kuluva aika. Kaikki testaajat eivät pohtineet tuolla sivulla tunnistamisvaihtoehtoja, vaan jotkut odottivat valvojalta signaalia siitä, että testi voisi jatkua.

Korjaukset

Käyttöliittymäsuunnitelman versioon 9 lisättiin asiakkaan esittämät muutokset. Henkilötiedot sisältävä elementti avattiin valmiiksi pääsivulle, näin käyttäjältä säästetään yksi klikkaus sekä selkiytetään sitä, mitä käyttäjän on tarkoitus tehdä sivulle päästyään. Vastavaikutuksena mobiiliversion pääsivu vaatii vierittämistä, jotta kaikki sisältö nähdään, koska sisältöä on näkyvissä enemmän.

Henkilötietojen päivittämistarkoituksiin tehty nappi siirrettiin pystyakselilta vasemmasta reunasta oikealle ohjetekstin perään ja napin tyyliä muutettiin vähemmän kutsuvaksi – pienempikokoiseksi, harmaaksi.

Yhteenveto testituloksista

Helsingin yliopiston tyylioppaassa on runsaasti nuolia sisältäviä elementtejä ja etenkin ”haitari”-elementit ylös ja alas osoittavine nuolineen on hankala saada toimimaan loogisesti. Nuolet osoittavat aina muualle, kuin elementtiin itseensä ja käyttäjä voi jossain tapauksessa seurata nuolien muodostamaa polkua. Nuolia käytetään osoittamaan jonkinlaista toimintoa, mutta ne voivat hämmentää käyttäjää tarpeettomasti. On hyvä kyseenalaistaa, kannattaako kyseisiä elementtejä käyttää.

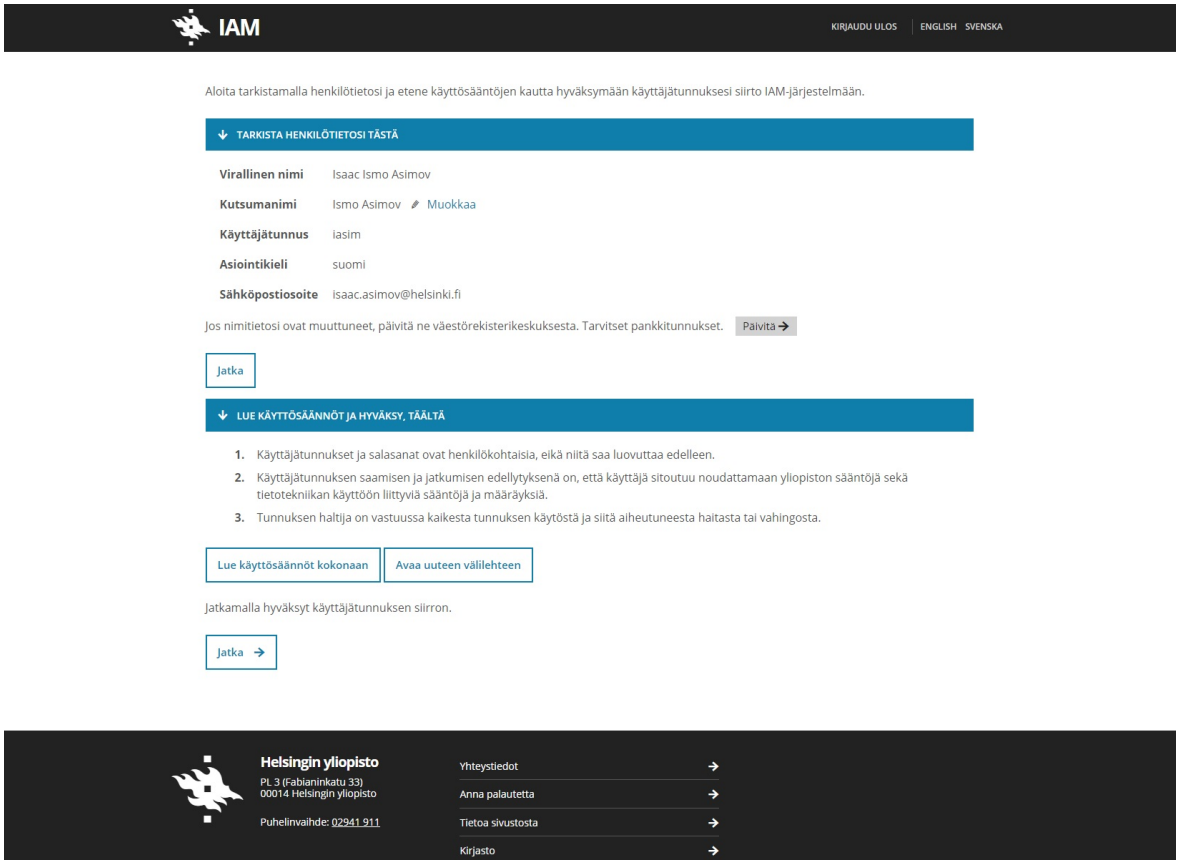
Tietojenmuokkaussivuilla lienee tarpeetonta näyttää toista haitarielementtiä, koska käyttäjä ei voi sitä avata kyseisellä sivulla. Vertaa kuvaa 12 ja liitteen 7 kuvaa 44, kyseisessä tapauksessa käyttöliittymäsuunnitelman koodaaminen aiheutti ylimääräisen objektin käyttöliittymään. Kyseistä virhettä ei olisi luultavasti syntynyt, jos käyttöliittymästä olisi aluksi piirretty kuvat. Näinkin pientä kokonaisuutta kirjoitettaessa liittymään jää kaikkea tarpeetonta. Ilmiö ei toki rajoitu ohjelmointiin vaan koskee myös kirjoittamista ja muita työskentelymuotoja, siksi työtapojen muuntelu: piirtäminen, kirjoittaminen, ohjelmointi, keskustelu ja mielellään ulkopuolinen arvioija ovat tarpeellisia elementtejä suunnitteluprosessissa.

Kuva 12. Sähköpostin muokkausnäkymä.

Toisessa käyttötapauksessa näytettiin ohjeteksti, jossa luki ”Tarvitset pankkitunnukset”. Aiemmista versioista ohje puuttui. Tapauksessa ei käytetty Suomi.fi -tunnistuksen näköistä sivua minkään todistamiseen tai tietojenkalasteluun. Kuitenkin havaittiin, että testitilanteessa sivun näyttäminen ei ole paras tapa toimia, vaikka valvoja katsoi muualle. Ei ole erityisen suositeltavaa pitää ainakaan julkisessa verkossa sivuja, jotka muistuttavat Suomi.fi -kirjautumispalvelua. Odotettu käyttäjävuo on kuvattu liitteessä 5.

Testattavista osalle esitettiin kysymys testien jälkeen, miten he erottavan tietojenkalastelun aidoista viesteistä. Moni vastasi kiinnittävänsä huomiota oikeinkirjoitukseen. Jotkut kiinnittävät huomioita viestin lähettäjään ja tahon virallisuuteen. Valvojan havaintojen mukaan testaajat huomioivat linkkien viittausosoitteita ainakin osan ajasta.

Kuvassa 13 esitellään käyttöliittymäsuunnitelman pääsivu.



Kuva 13. Käyttöliittymäsuunnitelman versio 9.

5 Viestintä

Ohjeteksteille on tyypillistä, että lukijalle välttämättömimmät asiat ilmaistaan heti alussa ytimekkäästi. Tekstissä voi olla ingressi, josta käy ilmi myös se, kenelle teksti on tarkoitettu ja mihin käyttöön. Toimintajärjestys on luonteva etenemisjärjestys kertaluonteiselle toimintaohjeelle. Tekstin voi jäsennellä niin, että olennainen erottuu helpolla silmäilyllä. Huomiota kannattaa kiinnittää sekä siihen, mikä on riittävä määrä ohjeistusta, että asianmukaiseen kieleen. Liian laaja ja yksityiskohtainen ohjeistus on luotaan työntävä ja suppeasanaisuus taas voi jättää asioita arvailun varaan. Lukijaa ei pidä aliarvioida, mutta eritaustaiset käyttäjät on kuitenkin huomioitava. Halutaan että koko kohderyhmä pystyy suorittamaan käyttäjätunnuksen siirron. Käyttäjää on huomioitava ohjeistuksen kielessä; ammattisanaston välttäminen on suotavaa, kun puhutaan asioista, jotka eivät ole kaikille arkipäivää. (Honkala & Kortetjärvi-Nurmi & Rosenström & Siira-Jokinen 2009, 28, 35-36.)

Peruskäyttäjän motivoiminen voi olla haasteellista. Käyttäjä tekee asioita, jos niistä on hänelle etua tai häntä käsketään sopimusten nojalla sekä sanktion uhalla tai hänellä on entuudestaan motivaatio kyseisen tehtävän suorittamiseen. Korulauseet ovat merkityksetön palkkio käyttäjälle ja aineellisten palkkioiden lupaaminen vaikuttaisi tietojenkalasteluyritykseltä. Käyttäjä voidaan velvoittaa siirtämään tunnuksensa palvelun jatkumisen edellytyksenä. Asia on kuitenkin ilmaistava selkeästi ja uskottavasti ja lisäksi on esitettävä aikakehykset tai mitään ei tapahdu. Käyttäjillä voidaan teetättää esimerkiksi jonkinlainen tyytyväisyyskysely tai tietoturvakysely. Henkilöt joilla on näihin sanottavaa voivat motivoitua tällä tavalla. Ei ole helppo keksiä aihetta, joka motivoisi kaikkia käyttäjiä.

5.1 Tietojenkalastelu

Tietojenkalasteluun (engl. phishing) kuuluu yleensä kaksi komponenttia: sähköpostiviesti, joka kehottaa käyttäjää tekemään jotain ja väärennetty sivusto, jonne käyttäjä ohjataan tekemään jotain, yleensä antamaan tunnistetietonsa. Huijaukseen voi myös kuulua esimerkiksi puhelinsoitto, jonka on tarkoitus vakuuttaa käyttäjä viestin aitoudesta ja saada tämä toimimaan (Hadnagy & Fincher 2015, 5).

Soittaminen on aggressiivisempi ja hyökkääjälle riskialttiimpi tapa tehdä tietojenkalastelua, mutta puhelinsoitot voivat vahvistaa kalasteluviestin uskottavuutta. On hyvä hallita tapa olla vastaamatta puhelimeen, jos soittajan numero ei ole tunnistettavissa. Ulkomaisten suuntanumeroiden kanssa on oltava aina varovainen, mutta kotimaisten operaattoreidenkin numerot voivat olla yhtä vaarallisia.

Tietojenkalastelukampanjat saatetaan ajoittaa jonkin tilanteen perusteella kuten luonnon katastrofit tai poliittinen äänestys (CISA 2009). Tarkoituksena voi olla tilanteesta hyötyminen tai tilanteeseen vaikuttaminen, kuten vaalihäirintä.

Kesällä 2018 tapahtuneen tietojenkalastelukampanjan jälkeen yliopiston käyttäjiä on ohjeistettu olemaan varovaisempia. Migraatioprosessissa, käyttäjälle lähetetään sähköpostia ja pyydetään tekemään tunnistamista vaativa toimenpide entuudestaan tuntemattomassa järjestelmässä, haasteena on saada käyttäjät tekemään kyseinen tehtävä, mikä voisi hyvin heidän näkökulmastaan olla tietojenkalastelua.

Tietojenkalasteluhuijauksissa käytettävät tekniikat alkavat olla käyttäjille tuttuja. Huijauksissa voidaan käyttää kloonattuja web-sivuja, jolloin ne ovat saman sisältöiset, kuin alkuperäisetkin sivut ja sisältävät myös aidoille sivuille viittaavia linkkejä (Hadnagy & Fincher 2015, 4).

Lähettäjän sähköpostiosoite voidaan väärentää suhteellisen helposti (Andreasson & Koivisto 2013, 137). Sähköpostin sisältämä hyperlinkki voidaan nimetä aidolla osoitteella ja osoittaa aitoa osoitetta muistuttavaan osoitteeseen esim. helsinki.fi hyperlinkki, joka viittaa osoitteeseen heIsinki.fi (pieni L-kirjain, korvattu isolla i-kirjaimella jälkimmäisessä). Viitattu osoite voi olla myös jotain aivan muuta ja viestikenttä ruudun alalaidassa, joka paljastaa murupolun voidaan pyrkiä peittämään, lisäksi selaimen osoiterivi voidaan väärentää.

Eräässä huijauksessa käytettiin tyhjältä näyttävää sähköpostiviestiä, mikä tosiasiassa suoritti koodia, joka muokkasi käyttäjän koneen hosts-tiedostoa. Kone konfiguroitiin ottamaan yhteyttä väärään IP-osoitteeseen käyttäjän kirjoittaessa pankin osoitteen selaimeensa (Silver Lake 2006, 185). Tämä toimisi edelleen, jos hyökkääjä pääsisi kirjoittamaan tiedostoon. Osoitteisiin ei voi siis luottaa varmenteita tarkistamatta. Huijari voi tekaista myös varmenteen, mutta tuolloin se ei ole myönnetty aidon sivun osoitteeseen. Harhautus voi kuitenkin toimia.

Kalasteluviestien tunnistamiseksi voi käyttää teknisistä asioista riippumatonta järkeilyä arvioimalla viestiä muutamien asioiden suhteen. Aluksi onko viesti tutulta lähettäjältä ja odotitko viestiä kyseiseltä taholta. Ovatko viestin oikeinkirjoitus ja *diskurssijärjestys* kohdillaan. Ovatko viestissä esitetyt asiat tai pyynnöt kohtuullisia. Pyrkiikö viesti vaikuttamaan emotionaalisella tasolla; herätetäänkö pelkoa, osoitetaanko uteliaisuutta, herätelläänkö ahneutta ja onko tarkoitus saada käyttäjä tekemään jotakin. (Hadnagy & Fincher 2015, 77.)

5.2 Tietojenkalastelusta erottuminen viestinnässä

Virallisena tahona, jonka tarkoitus on saada käyttäjä tekemään jotakin, mutta erottua kalasteluyrityksistä, on huomioitava luvussa 5.1 tarkoitetut asiat. Käyttäjien on hyvä saada tietoa etukäteen muita kanavia pitkin samasta asiasta, jolloin viestiä osataan odottaa tai sen sisältämä asiasisältö on varmistettavissa muualta; Helsingin yliopiston muilta virallisilta viestintäkanavilta. Oikeinkirjoitukseen on kiinnitettävä huomiota. IT-tuen käyttämä ohjeidenlaatimistyyli on soveltuva genre. Viestiin ei haluta sisällyttää tunnelatauksia, jopa korostettu kohteliaisuus voi olla enemmän epäilyttävää tai ärsyttävää kuin tarpeellista.

Kohteliaisuus on kulttuurisidonnaista. Suomessa käytetään hillitympää *diskurssijärjestystä* ja asiakkaaseen otetaan vähän etäisyyttä verrattuna esimerkiksi amerikkalaiseen tykö tuttavalliseen tyyliin. Etäinen kohteliaisuus ilmenee esimerkiksi passiivin käytössä ja ylimääräisten kohteliaisuusfraasien poisjättämisenä. Huomiota pitäisi herättää, jos jotakin ylimääräistä sanotaan: ”Arvoisa”, ”Hyvä”, ”Onnittelut”, ”Kuulemiin”, ”Teidän”, jopa ”Ystävällisin” tai ”Parhain terveisin” voi olla paljon sanottu viralliselta taholta. Se ei tarkoita, että jokin näistä olisi väärin. Vakiintuneeseen käytäntöön tulee kiinnittää huomiota.

Passiivin käytöstä voi seurata vastuullisen tahon hämärtyminen, kun asioihin ei haluta ottaa selvää kantaa (Fairclough 1997, 40-42). Tekijä on kuitenkin yleensä ihminen ja tekijän ilmaisee verbi, mikä on tyypillistä suomen kielelle. Kieliopilliset seikat voivat paljastaa huijausviestin. Tekijä voi esiintyä esimerkiksi tarpeettomasti adjektiivissa tai substantiivissa. Tuloksena syntyvän tekstin genre voi vaikuttaa esimerkiksi proosalliselta ja kielioppivirheiden tyyli voi paljastaa jotain kääntäjänsä äidinkielestä, myös koneet tekevät omanlaisiaan käännösvirheitä.

Oletettavasti Tietotekniikkakeskus on tarkoittanut, että asiakkaan vastuun tulisi välittyä viestistä, joten tekijän ilmaisemiseen on paikoin kiinnitettävä huomiota. Asioiden ehdottomuutta voidaan ilmaista kategorisin sanamuodoin (Fairclough 1997, 12), kuitenkin kohteliaisuussyistä ja viestiä pehmentämään voidaan käyttää konditionaalia niiltä osin, kun käyttäjältä edellytetään toimia. (Honkala & Kortetjärvi-Nurmi & Rosenström & Siira-Jokinen 2009, 28-29.) Uhkaavilta kuulostavat viestit ovat myös tyypillisiä tietojenkalastelulle, koska viestin aiheuttama tunnereaktio voi johtaa hyökkääjään toivomaan lopputulokseen. Ilmauksia, jotka sisältävät kehotteen toimia nopeasti tai jotakin lopullista tapahtuu, kannattaa varoa.

Vääränlainen suostuttelu on myös riski. Käyttäjää voi provosoida, jos tälle puhutaan kuin lapselle tai tämän merkitystä toimijana vähätellään. Yllättävän *diskurssityypin* lainaaminen on yksi hyökkääjän aseista. Tällöin kontekstista poikkeavaa kieltä käytetään tehokeinona. Vähättelevää olisi sanoa: ”Emme tarvitse sinulta muuta, kuin käyttäjätunnuksesi.” ja lapsekkuutta olettava olisi: ”Käyttäjätunnuksen aktivoiminen on ihan helppoa!” Töykeää olisi sanoa: ”Onko noin vaikeaa, vaan antaa se käyttäjätunnus.” Kaikki edelliset herättävät tunnereaktioita vastaanottajassa ja ovat manipulointiin sopivia keinoja.

Hyökkääjän voi hyödyntää ihmisille tarkoitetuissa hierarkioissa esiintyvää mallia, jossa auktoriteettia tai hallintovaltaa käyttävää tahoa pidetään luotettavana. Tällöin kiinnitetään huomiota samoihin seikkoihin, kuin muidenkin tietojenkalasteluyritysten kohdalla, jollei tiettyä tahoa ole implikoitu. Esimerkki tietojenkalasteluyrityksestä, voisi olla vaikkapa: ”Tarvitsemme käyttäjätunnuksenne työtehtävien hoitamiseen.” Luonnollisten henkilöiden välillä tämän ei pidä toimia. Monikon ensimmäinen persoona ei ole sama asia kuin passiivi, jota virallisessa viestinnässä voidaan odottaa. Toinen esimerkki: ”Käyttäjätunnustasi tarvitaan työtehtävien hoitamiseen.” Hyvä nyrkkisääntö on, että kukaan ei tarvitse toisen henkilön salasanaa. Käyttäjätunnuksien osalta asia on mutkikkaampi.

Sanoja valitessa käyttäjälähtöisyys on pidettävä mielessä, kuitenkin sanavalinnat auttavat vielä erottumaan sarjatuotantohyökkäyksistä, joissa käytetään ilmaisia käännöspalveluita. Internetissä saatavilla oleville käännöspalveluille voivat tuottaa ongelmia esimerkiksi pitkät yhdyssanat kuten käyttövaltuuksienhallintajärjestelmä, joka kääntyy Google kääntäjä -palvelulla muotoon ”the use management powers” tai harvinaisemmat sanat kuten kolopesijä, joka on sama sana kaikilla kielillä kyseisen käännöspalvelun mukaan (Google Inc). Nämäkin palvelut kuitenkin kehittyvät nopeasti. Idiomit ovat myös kielelle tunnusomaisia, eivätkä monien kielien tapauksissa käänny, esimerkiksi Google kääntäjältä, mutta sellaiset tulevat harvoin kysymykseen virallisessa viestinnässä.

Hyökkäyksessä käytetyn suomenkielen ollessa epätäydellistä voidaan tutkia sitä, minkälaista käännöspalvelua on mahdollisesti käytetty. Tästä voi olla hyötyä kun yritetään määrittää, onko hyökkääjä suomenkielentaitoinen ja onko tämä silti käyttänyt robottia käännöspalveluna. Käännöksen on voinut myös tehdä ihminen. Hyökkääjällä on käytössään iso valikoima keinoja, kun hän haluaa peittää jälkensä. Jälkien johtaminen johonkin tiettyyn ihmisryhmään ei kuitenkaan olisi hyökkääjältä järkevää, koska se paljastaisi hyökkääjän tietojen tasosta paljon ja rajaisi mahdollisten syyllisten joukkoa. Se voi kuitenkin olla otettu riski tai virhe, minkä hyökkääjä on tehnyt. Helsingin yliopiston tapauksessa hyökkääjä tekee suurehkon oletuksen, jos hyökkäyksessä ei käytetä virallista suomea, englantia ja ruotsia, kun puhutaan virallisista viesteistä.

Kalasteluviestit sisältävät tyypillisesti hyperlinkkejä, jos selliasia ei ole viestissä ei käyttäjää voida niillä suoraan harhauttaa. Toimittaessa lähtöoletuksella, että käyttäjä jo tietää jotakin, voidaan viesteistä tarvittaessa jättää hyperlinkit pois ja antaa mieluummin navigointiohjeita. Vaihtoehtoinen ohjeistus tarkistaa, minne linkki viittaa viemällä kursori linkin päälle ei ole yleispätevä; se ei toimi kaikilla alustoilla, on virhealtis ja vaatii teknistä tietoutta.

Kalasteluviestit voivat olla myös asettelultaan suttuisia. Viesti on voitu esimerkiksi laatia jossakin toisessa ohjelmassa ja sisältää muotoiluja, jota sähköposti-klientti ei tue. Sähköposteissa kannattaisi välttää kaikkea, mikä muuttaa viestin html-viestiksi hymiöistä ja muotoiluista lähtien ja käyttää pelkkää tekstiä. Ainoastaan raakatekstiä sisältävään sähköpostiin ei voi upottaa haitallista koodia. Todella monet organisaatiot kuitenkin käyttävät viestinnässä organisaatiolle brändättyä tyyliä. Lähettäjä voidaan näennäisesti tunnistaa tyylistä, mutta myös huijari voi käyttää sitä hyväkseen.

Kohdistetummissa hyökkäyksissä, vaikka niiden alkuperä olisi ulkomailla, voidaan käyttää esimerkiksi verkkoliikenteestä kaapattuja aitoja viestejä tekaistujen sijaan. Sähköpostiviestintä on oletuksena salaamatonta. Organisaation sisällä lähetetyt viestit pysyvät talon sisällä, jos sähköpostipalvelu sijaitsee talon sisällä. Näin ei kuitenkaan enää monesti ole. Sähköpostin salaus ja sähköinen allekirjoitus ovat keinoja sekä viestin salaamiseen, että lähettäjän tunnistamiseen. Kyseiset teknologiat tulisi kuitenkin ensisijaisesti ottaa käyttöön organisaation tasolla. Helsingin yliopiston käyttäjillä on kuitenkin mahdollisuus käyttää sekä sähköpostin sähköistä allekirjoitusta, että viestin salaamista ja se on erittäin suositeltavaa. Ohjeet käyttöönottoon löytyvät helpdeskistä.

5.3 Viestintä Helsingin yliopistolla

Helsingin yliopiston virallisia viestintäkanavia ovat sähköpostin lisäksi Flamman uutiset, tapahtumakalenteri sekä Yhteisövirta Virtanen ja Yammer. Virallinen tieto pitäisi voida varmistaa sähköpostin lisäksi toisestakin virallisesta lähteestä. Viimeinen keino on soittaa tukipalveluun kysyä vahvistusta asiaan tai kulloisellekin taholle, joka on vastuussa viestistä ja varmistaa sen aitous. Tarkoituksen mukaista on, että varmistussoittoja ei tarvitse tehdä ja käyttäjät voivat omatoimisesti varmistua viestien aitoudesta.

Helsingin yliopistolla joukkotiedotteet lähetetään pääasiassa suomeksi, englanniksi ja ruotsiksi, saman viestin sisältäessä kaikki kieliversiot, jotka ovat myös saman sisältöiset. Kyseinen käytäntö olisi hyvä sääntö, silläkin nojalla, että Helsingin yliopiston kieliperiaat-

teiden mukaisesti tiedotteet tulisi tehdä kaikilla kolmella kielellä (Helsingin yliopisto 2014, 10). Kieliasun tutkiminen useammalla kielellä ei kuitenkaan auta kaikkia käyttäjiä vakuuttumaan virallisuudesta, koska käyttäjät voivat olla esimerkiksi vain englannin kielen taitoisia. Kääntäminen on ensisijaisesti käännöspalveluiden tehtävä, siten varmistutaan siitä, että linja pysyy yhdenmukaisena.

5.4 Tulokset

Viestin otsikoinnissa on hyvä huomioida Internet standardi RFC 2822. Otsikon pituus ei saa ylittää 998 merkkiä ja ei pitäisi mielellään ylittää 78 merkkiä (RFC 2822 kohta 2.1.1.) Näitä standardeja ei ole kuitenkaan tehty ihmisiä varten, joten on tasapainoiltava suositusten ja ymmärrettävyyden sekä uskottavuuden välillä. Viestihahmotelman otsikoista B on oikein, kun taas otsikko A on pitkähkö ja sisältää kehotteen, joka voi vaikuttaa negatiivisesti tai positiivisesti viestin tulkintaan. Otsikossa B käytetään terminologiaa yhdenmukaisesti viestiosan kanssa ja se on lyhyempi.

Pohdittavaksi jää vielä vaatiiko migraatiotyökaluun pääseminen uuden kirjautumisen, jos käyttäjä on jo kirjautunut Flammaan. Tässä ohjeessa sitä ei vaadita; se on yksi työvaihe lisää käyttäjälle. Viestintä tekee päätökset ohjeen soveltamisesta.

Viesti

Otsikko A:

Helsingin yliopiston käyttövaltuushallintajärjestelmä ja käyttösäännöt uudistuvat. Käy tutustumassa uuteen IAM-järjestelmään ja käyttöehtoihin

Otsikko B:

Helsingin yliopiston käyttövaltuuksienhallintajärjestelmä ja käyttösäännöt uudistuvat

Viesti:

Käyttövaltuuksien- ja identiteetinhallintajärjestelmä uudistuu. Uutta järjestelmää kutsutaan IAM-järjestelmäksi (engl. Identity and Access Management). Helsingin yliopiston käyttäjätunnuksia koskevat käyttösäännöt on päivitetty. Käythän hyväksymässä päivitetyt käyttösäännöt ja samalla käyttäjätunnuksesi siirron uuteen IAM-järjestelmään yx.yx.xxxx mennessä.

Ohje Flammaan:

1. Kirjaudu Flammaan yliopiston myöntämillä käyttäjätunnuksilla.
2. Valitse sivun ylänavigaatiosta, oikealta ”Työkalut” ja klikkaa sitä.
3. ”Työkalut”-listalta löytyy ”IAM-migraatiotyökalu”, klikkaa sitä.
4. Tarkista tältä sivulta, että henkilötietosi ovat ajan tasalla.
5. Paina ”Jatka” ja avaa uudet käyttösäännöt luettavaksi valitsemallasi tavalla.
6. Tutustuttuasi käyttösääntöihin paina vielä ”Jatka >”, jolloin hyväksyt käyttäjätunnuksen siirron uuteen järjestelmään.

   Käyttäjätunnuksen siirtäminen ei aiheuta käyttökatkoa. Saat uuden IAM-järjestelmän ominaisuudet käyttöön, kun kirjaudut järjestelmään uudelleen.

Huom! Kaikilla sivustoilla, joita tarvitset tässä ohjeessa on TERENA SSL CA 3:n myöntämä varmenne. Varmenteen voi tarkistaa klikkaamalla selaimen osoiterivin alussa olevaa lukko-ikonia.

6 Pohdinta

Opinnäytetyön monivaiheista tunnistusta käsittelevä osio on kevyt median tarkkailuun ja pohdintaan perustuva, perehdyttävä ajatusharjoitus. Tarkoitus on perustella, miksi monivaiheisen tunnistuksen käyttöä kannattaa harkita.

Käyttöliittymän suunnittelu toteutettiin rautalankamallilla, jota voidaan verrata DEED-malliin. Opinnäytetyön ensimmäisissä Sprinteissä suunniteltiin markkinatutkimusta, jota on myös hyödynnetty haastattelussa. Käyttöliittymän ydinsisältö on hahmoteltu arvolupauskanvaasilla. Luonnosta käyttöliittymästä ei piirretty, mikä osoittautui virheeksi. Ylimääräisiä työvaiheita pyrittiin välttämään. Kvalitatiivisen pohdinnan (mallissa tutkimuksen) kohteena oli palvelun saatavuus ja siihen perustuvan taulukoinnin avulla lähestyttiin käyttöliittymän vaatimuksia. Käyttöliittymän toimintavuosta muodostettiin rautalankamalli. Visuaalisessa suunnittelussa noudatettiin Helsingin yliopiston tyyliä. Käyttöliittymästä tehtiin prototyyppi, jota testattiin käyttäjillä ja paranneltiin; tätä prosessia toistettiin useampia kertoja.

Testitulokset taulukoitiin, mutta niitä ei analysoitu määrällisesti. Testaajista ei kerätty tietoja. Prosessin kulun aikana pyydettiin kommentteja ja palautetta asiakkaalta. Lopputulos hyväksyttiin, vaikka prototyyppi olisi voinut sisältää useampia käyttötehtäviä.

Oma pohdinnanaiheensa käyttöliittymän osalta ovat henkilötietojen käsittely, eri rajapintojen keskustelu keskenään ja inhimilliset testauskäytännöt. Kyseisiä seikkoja pohdittiin vasta käyttöliittymäsuunnitelman toteuttamisen jälkeen, sillä lopputuote on prioriteettina etusijalla. Käyttöliittymän kehotteiden suunnitteluun olisi syytä panostaa enemmän kuin tässä tehtiin. Käyttöliittymässä voi myös edelleen olla ylimääräisiä elementtejä.

Tietojenkalastelussa käytettyjen viestien sisältöä voidaan analysoida teknisten seikkojen lisäksi, jos materiaalia on riittävästi, ja selvittää onko Helsingin yliopiston tapauksessa kyseessä yksi vai useampi toimija ja eri rikollisryhmiä voidaan pyrkiä tunnistamaan. Huomiota voidaan kiinnittää sellaisiin seikkoihin, kuten ketkä ovat tietojenkalastelijan ennakoima kohderyhmä ja mitä ennakko-oletuksia hyökkääjä tekee heistä. Hyökkääjän ollessa hypoteettisesti robotti, ei tämä esimerkiksi tee ihmisille tyypillistä ennakko-oletusta, jonka mukaan kaikki hyökkäyksen todelliset kohteet ovat eläviä. Hyökkäyksen ollessa jotakin muuta, kuin luonnollisiin henkilöihin kohdistuvaa tietojenkalastelua tämän tyyppistä oletusta ei tehdä. Robotit kuitenkin toimivat niille annettujen käskyjen perusteella.

Visuaaliset keinot voivat parhaassa tapauksessa paljastaa hyökkääjän visuaalisen äidinkielen, kuten kielelliset paljastavat puhutun kielen. Useamman tutkimuksen aiheeksi soveltuu diskurssianalyyttinen näkemys tietojenkalasteluun sekä tietoturvalliseen viestintään. Kyberneettisen vaikuttamisen keinot visuaalisessa suunnittelussa sekä viestinnässä ovat myös omansa.

Toinen aihe-alue on markkinaselvityksen tekeminen siitä, onko maailmalla tahtotilaa globaalille IAM-järjestelmälle, johon autentikoidutaan julkiseen verkkoon siirryttäessä. Useat hajautettujen tietokantojen kehittäjät ovat lähestyneet aiheen mahdollisuutta erilaisilla käytännön toteutuksilla. Internetiä valvova globaali IAM on kuitenkin tulevaisuuden visio, joka vaatisi paljon infrastruktuurilta ja diplomatialta, liudan sopimuksia sekä nykytilassa voi olla mahdoton toteuttaa.

Opinnäytetyön keskeisin havainto on, että käyttäjiä ei voida suojella ainoastaan teknisin keinoin, vaan koulutusta, tasavertaisuutta, tietojärjestelmienpuolustuksen jatkuvaa kehitystä ja tutkimusta tarvitaan. Työ selvitti myös tekijälleen, että kyberrikollisuuden tutkinnassa tarvitaan monia sidosryhmiä ja laajaa kielien tutkimusta, tietotekniikan ja kulttuurien tuntemusta, teknisiä ja inhimillisiä näkökulmia.

Opinnäytetyöhän kuuluva viestinnän suunnittelu helpotti ennen kaikkea opinnäytetyön puhtaaksikirjoitusprosessia. Lisäksi verbaalinen pohdinta helpotti useamman asiakokonaisuuden yhteen sitomista.

Kiitän kaikkia, jotka edistivät opinnäytetyöni loppuunsaattamista.

Lähteet

Ahvenainen, Sakari. 2014. Teoksessa Kuusisto, Tuija (toim.) 2014. Kybertaistelu 2020 Maanpuolustuskorkeakoulu, Tak-tiikan laitos Julkaisusarja 2: Asiatietoa, No. 1/2014.

Andreasson, Ari & Koivisto, Juha. 2013. Tietoturvaa toteuttamassa. AS Packett. Tallinna.

Cybersecurity and Infrastructure Security Agency (CISA). 2009. Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks.
Luettavissa: https://www.us-cert.gov/ncas/tips/ST04-014
Luettu: 12.5.2019.

Denyer, Simon. 2018. The Washington Post. Beijing bets on facial recognition in a big drive for total surveillance.
Luettavissa:
https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.3f7c9331b5a1
Luettu: 11.4.2019.

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679,
annettu 27 päivänä huhtikuuta 2016,
luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679
Luettu: 1.3.2019.

Fairclough, Norman. 1997. Miten media puhuu. Vastapaino. Tampere.

Federley, Maija & Häkkinen, Tarja & Kekki, Tuula & Kyttä, Marketta & Mäkeläinen, Tarja & Nikkanen, Maija & Poutanen, Olli & Ratvio, Rami & Staffans, Aija & Välimäki, Suvi. 2019.
Turvalliseksi koetun lähiympäristön ohjauksen ja suunnittelun nykytila ja suosituksia. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 2019:31. Valtioneuvoston kanslia.
Luettavissa:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161592/31_Lahiymparisto_loppuraportti.pdf
Luettu: 10.5.2019.

Google Inc.
Luettavissa: https://translate.google.com/
Luettu: 15.5.2019.

Hadnagy, C. & Fincher, M. & Dreeke, R. 2015. Phishing dark waters: the offensive and defensive sides of malicious e-mails. John Wiley & Sons, Incorporated.

Hakkarainen, Jenni. 2018. Helsingin yliopistoa riivaa poikkeuksellisen suuri kalasteluviestien tulva – satoja ihmisiä on haksahtanut antamaan tietonsa rikollisille. Helsingin Sanomat.
Luettavissa: https://www.hs.fi/kaupunki/art-2000005805242.html
Luettu: 26.3.2019.

Helsingin Sanomat. 2019. Facebook säilytti miljoonia salasanoja salaamattomassa muodossa sisäisillä palvelimilla.
Luettavissa: https://www.hs.fi/teknologia/art-2000006043756.html
Luettu: 15.5.2019.

Helsingin yliopisto. 2014. HELSINGIN YLIOPISTON KIELIPERIAATTEET LINJAUKSISTA KÄYTÄNTÖÖN - KOHTI TOIMIVAA MONIKIELISYYTTÄ. Rehtorin päätös. Unigrafia. Helsinki.
Luettavissa:
https://blogs.helsinki.fi/centrumcampus/files/2015/04/kieliperiaatteet.pdf
Luettu: 10.5.2019.

Honkala, P. & Kortetjärvi-Nurmi, S. & Rosenström, A. & Siira-Jokinen, S. 2009. LINKKI Työyhteisön viestintä. Edita Publishing Oy. Helsinki.

Huai, Cao & Qi, Zhou. 2017. An Interactive Behavior-Based Hierarchical Design Method for Form Hints. Teoksessa Marcus, A. & Wang, W. (Eds.): DUXU 2017, Part III, LNCS 10290, s. 3–15. Springer International Publishing AG.

Idean. Styleguide.
Luettavissa: https://universityofhelsinki.github.io/Styleguide/
Luettu: 20.5.2019.

Laki tietomurrosta 10.4.2015/368.

Lawler, Richard. 2017. Engadget. Huawei's next mobile chipset is ready for our AI-powered future.
Luettavissa: https://www.engadget.com/2017/09/02/huaweis-next-mobile-chipset-is-ready-for-our-ai-powered-future/
Luettu: 12.12.2018.

Leukfeldt, Rutger. 2016. Cybercriminal Networks. Origin, Growth and Criminal Capabilities. Eleven international. Alankomaat.

Linden, Mikael. 2017. Identiteetin ja pääsynhallinta. Tampereen teknillinen yliopisto. Tietotekniikan laboratorio. Raportti 7.
Luettavissa:
https://tutcris.tut.fi/portal/files/11863886/linden_identiteetin_ja_paasynhallinta.pdf
Luettu: 11.1.2019.

Marjomaa, Tommi. 2018. Identiteetin- ja pääsynhallintapalvelun tuotteistaminen. Asiakastarpeiden selvittäminen ja tuotteiden soveltuvuuden varmistaminen. Opinnäytetyö. Metropolia Ammattikorkeakoulu.

Martin, J. & Waters, J. 2004. What is IAM? Identity and access management explained
Luettavissa: https://www.csoonline.com/article/2120384/identity-management/what-is-iam-identity-and-access-management-explained.html
Luettu: 7.2.2019.

McColeman, C. & Barrett, R. & Blair, M. 2017. Design-Based Evidence Collection and Evidence-Based Design (DEED) Model. Teoksessa Marcus, A. & Wang, W. (Eds.): DUXU 2017, Part I, LNCS 10288, s. 134–151. Springer International Publishing AG.

Mäntylä, Jose. 2014. KYBERASEIDEN VAIKUTUS KRIITTISEN INFRASTRUKTUURIN TIETOJÄRJESTELMIIN. Kandidaatintutkielma. Maanpuolustuskorkeakoulu.

Mythbusters. 2006. TV-ohjelma. Crimes and MythDemeanors II. Discovery.

Nielsen, Jackob. 1994. 10 Usability Heuristics for User Interface Design. Nielsen Norman Group.
Luettavissa: https://www.nngroup.com/articles/ten-usability-heuristics/
Luettu: 22.4.2019.

Owen, Malcom. 2018. Appleinsider. Apple considering offline mode for Siri that could process voice locally on an iPhone.
Luettavissa: https://appleinsider.com/articles/18/11/15/apple-considering-offline-mode-for-siri-that-could-process-voice-locally-on-an-iphone/
Luettu: 18.11.2018.

Patentlyapple. 2019. Apple Advances Face ID to be 'Twin Proof' using Machine Learning, Subepidermal Imaging and more.
Luettavissa: https://www.patentlyapple.com/patently-apple/2019/03/apple-advances-face-id-to-be-twin-proof-using-machine-learning-subepidermal-imaging-and-more.html
Luettu: 26.3.2019.

Pääkkö, Päivi & Tenhunen, Ville. 2011. Helsingin yliopiston identiteetin- ja pääsynhallinnan esiselvitys (julkinen versio). Helsingin yliopisto.

Pääkkö, Päivi. 2013. Helsingin yliopisto.
Luettavissa: https://wiki.helsinki.fi/pages/viewpage.action?pageId=122042358
Luettu: 7.2.2019.

Pääkkö, Päivi. 22.3.2019. Tietotekniikka-asiantuntija. Helsingin yliopisto. Haastattelu. Helsinki.

Pöyry, Anu. 2019. KAKSIVAIHEINEN TUNNISTUS YLIOPISTON PALVELUISSA. Helsingin yliopisto.
Luettavissa:
https://wiki.helsinki.fi/display/IAMasioita/Kaksivaiheinen+tunnistus+yliopiston+palveluissa
Luettu: 9.4.2019.

RFC 2822. 2001. QUALCOMM Incorporated. Internet Message Format. Line Length Limits.
Luettavissa: https://tools.ietf.org/html/rfc2822#section-2.1.1
Luettu: 26.4.2019.

Shneiderman, Ben. 1998. Designing the User Interface. Addison Wesley Longman, Inc. USA.

Da Silva Bastos, K. V. & Muñoz, I. K. 2017. The Challenges Found in the Access to Digital Information by People with Visual Impairment. Teoksessa Marcus, A. & Wang, W. (Eds.): DUXU 2017, Part III, LNCS 10290, s. 330–346. Springer International Publishing AG.

Silver Lake publishing. 2006. Scams & swindles: phishing, spoofing, ID theft, Nigerian advance schemes, investment frauds, false sweethearts: how to recognize and avoid financial rip-offs in the Internet age. Aberdeen.

Tapio, Tero. 2010. Riskienhallinta perinteisessä ja ketterässä ohjelmistonkehityksessä. Pro gradu -tutkielma. Tampereen yliopisto.

Tietotekniikka-asiantuntijat. Keskustelut tietotekniikka-asiantuntijoiden kanssa.

Wikimedia Foundation, Inc. 2019. Password strength.
Luettavissa: https://en.wikipedia.org/wiki/Password_strength
Luettu: 15.5.2019.

Wirman, Kari. 2014. Teoksessa Kuusisto, Tuija (toim.) 2014. Kybertaistelu 2020 Maanpuolustuskorkeakoulu, Tak-tiikan laitos Julkaisusarja 2: Asiatietoa, No. 1/2014.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010.
Annettu: 1.7.2010.

Valtiovarainministeriö. 2006a. VAHTI 7/2006. Käyttäjähallinta.
Luettavissa: https://www.vahtiohje.fi/web/guest/kayttajahallinta
Luettu: 18.3.2019.

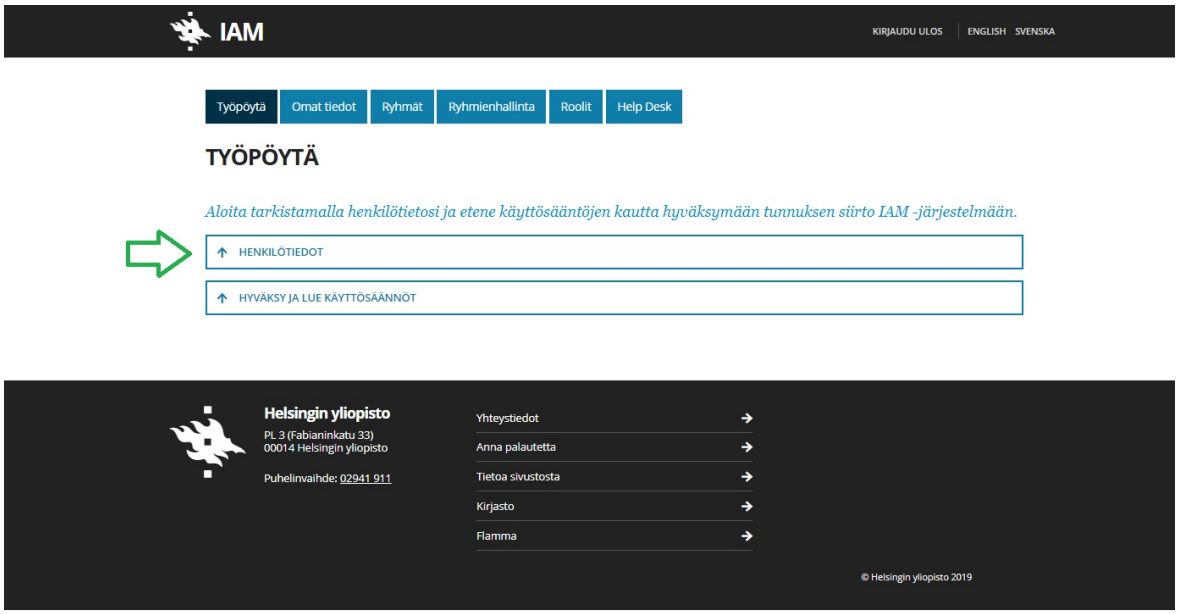
Valtiovarainministeriö. 2006b. VAHTI 9/2006. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Valtionhallinnon tietoturvallisuuden johtoryhmä. Helsinki.

Valtiovarainministeriö. 2012. VAHTI 2/2012. ICT-varautumisen vaatimukset. Helsinki.

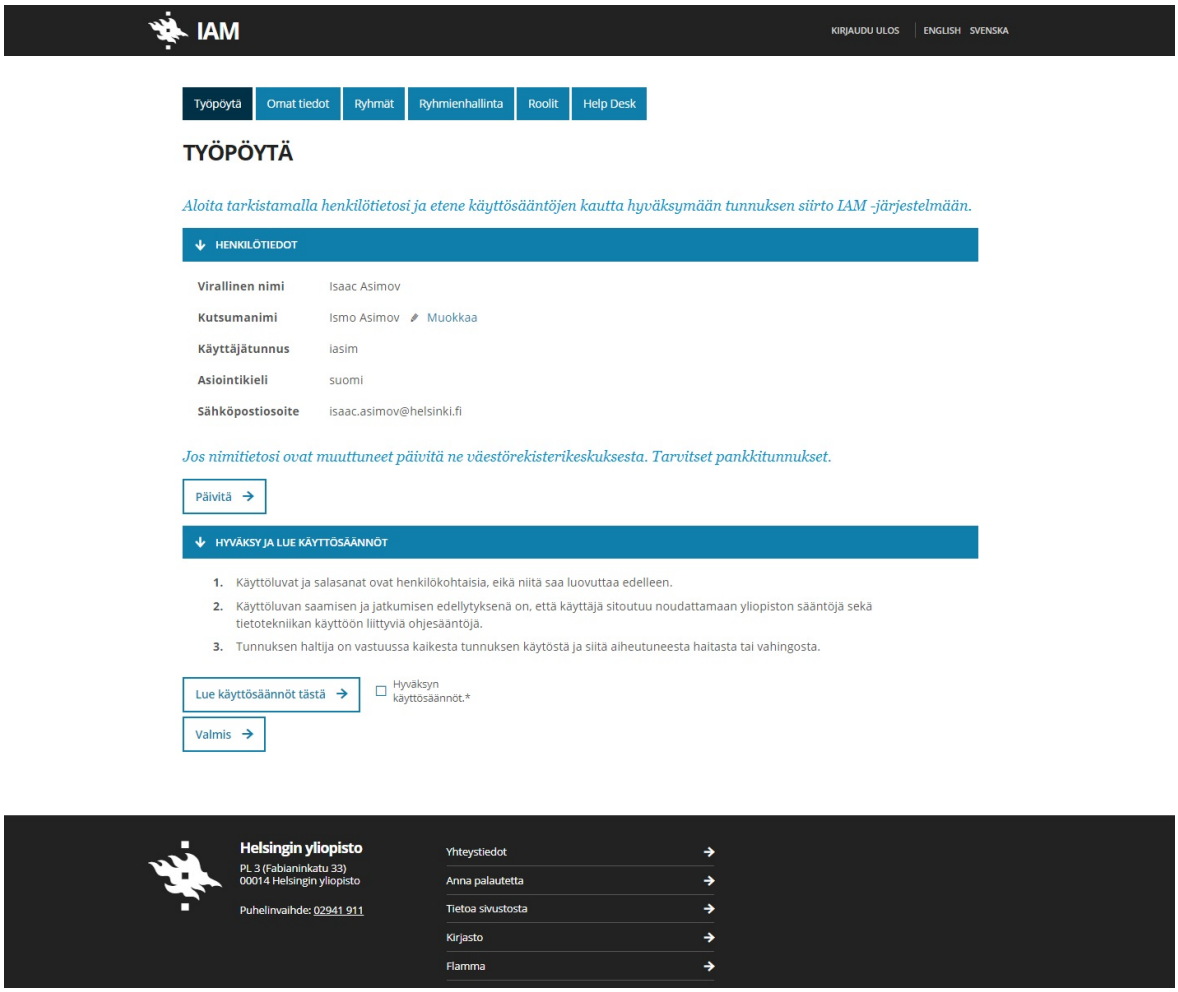
Villas-Boas, Antonio. 2019. Business Insider Nordic. LG's new smartphone unlocks by recognizing the veins in your palms — here's how it works.
Luettavissa: https://nordic.businessinsider.com/lg-g8-smartphone-unlocks-with-hand-id-vein-palm-recognition-2019-2
Luettu: 26.3.2019.

Liitteet

Liite 1. Käyttöliittymäsuunnitelman versio 3, pääsivu.

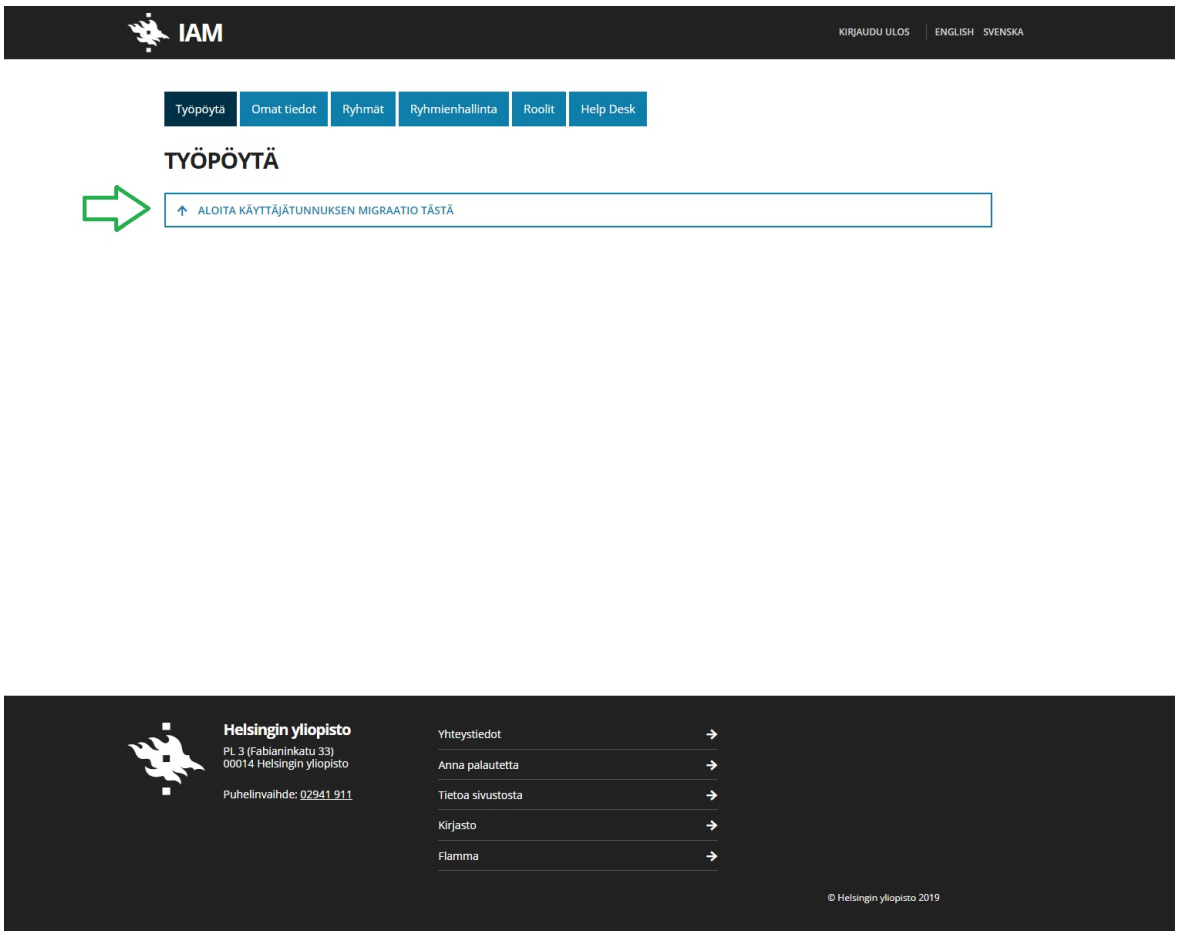


Kuva 14. Version 3 aloitussivu. Käyttäjän oletetaan valitsevan ”HENKILÖTIEDOT” -elementin.

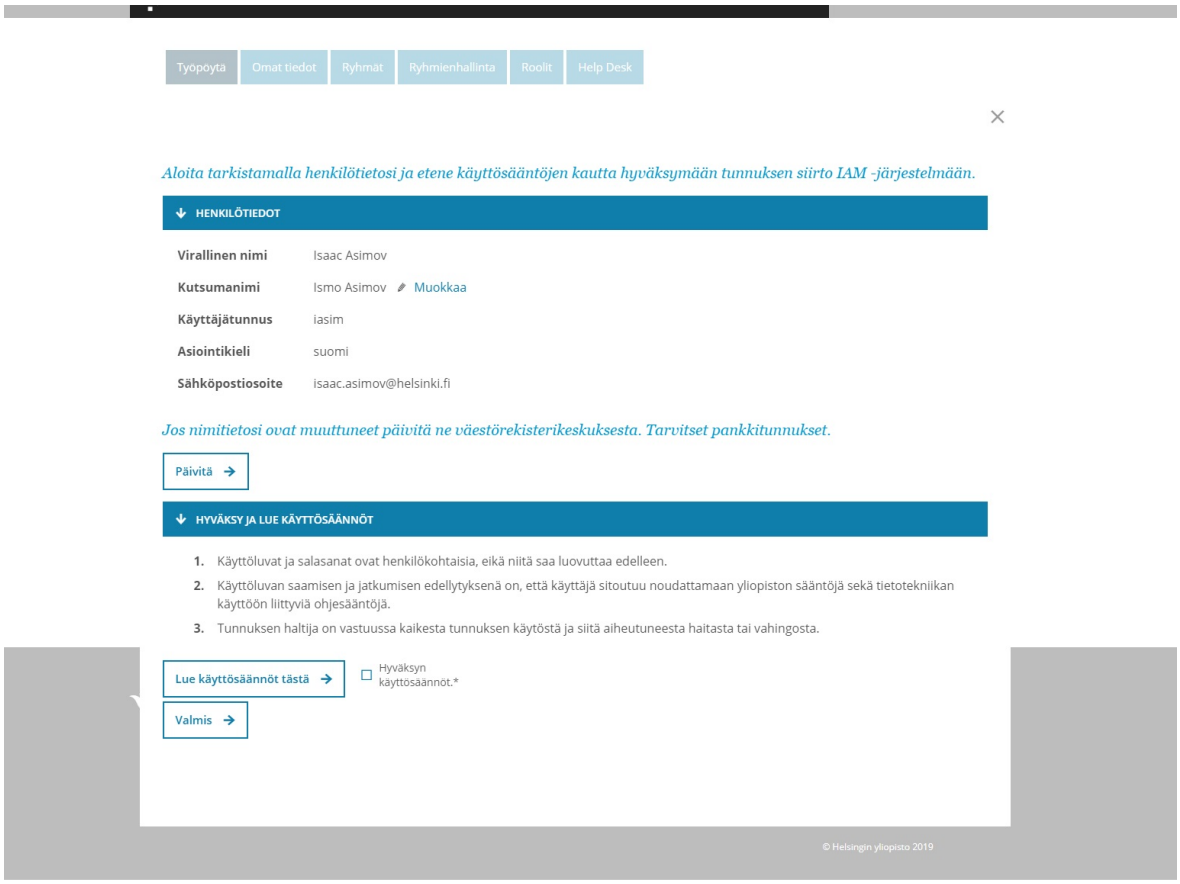


Kuva 15. Version 3 pääsivu molemmat haitari-elementit aukaistuina.

Liite 2. Käyttöliittymäsuunnitelman versio 4, pääsivu.

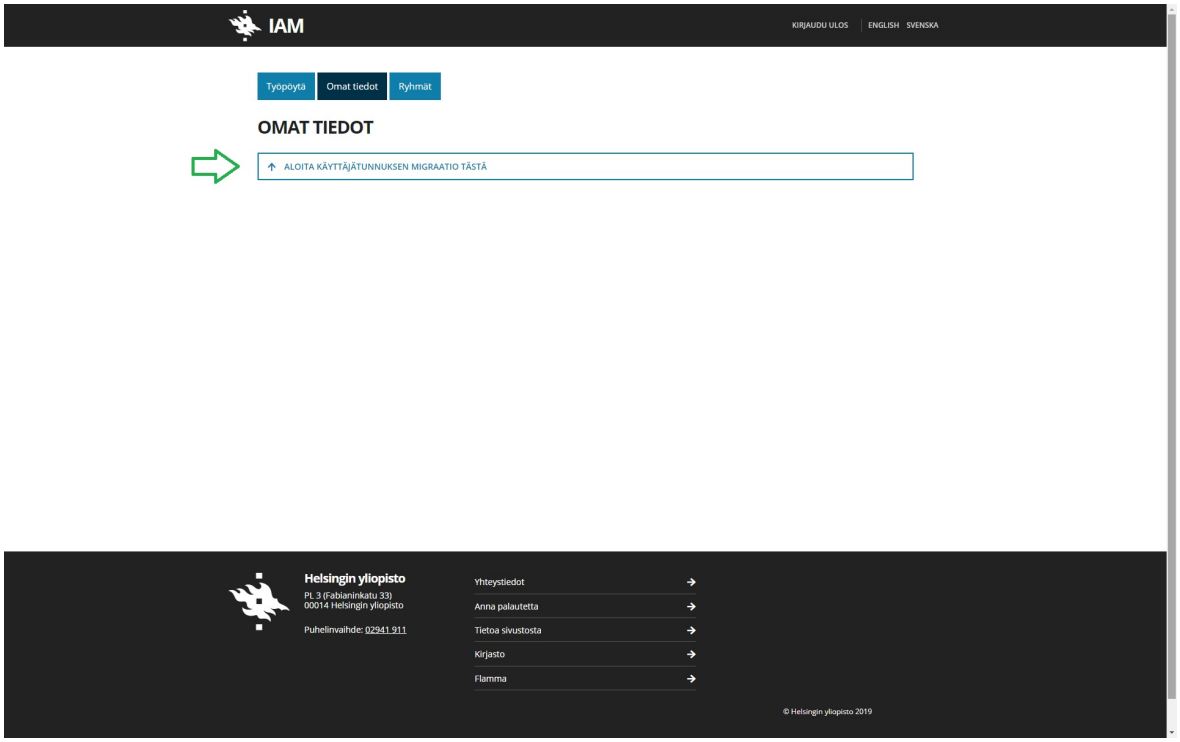


Kuva 16. Version 4 pääsivu on visuaalisesti kömpelö, mutta tarkoitus on ohjata käyttäjän toimia näyttämällä vain yksi haitarielementti.

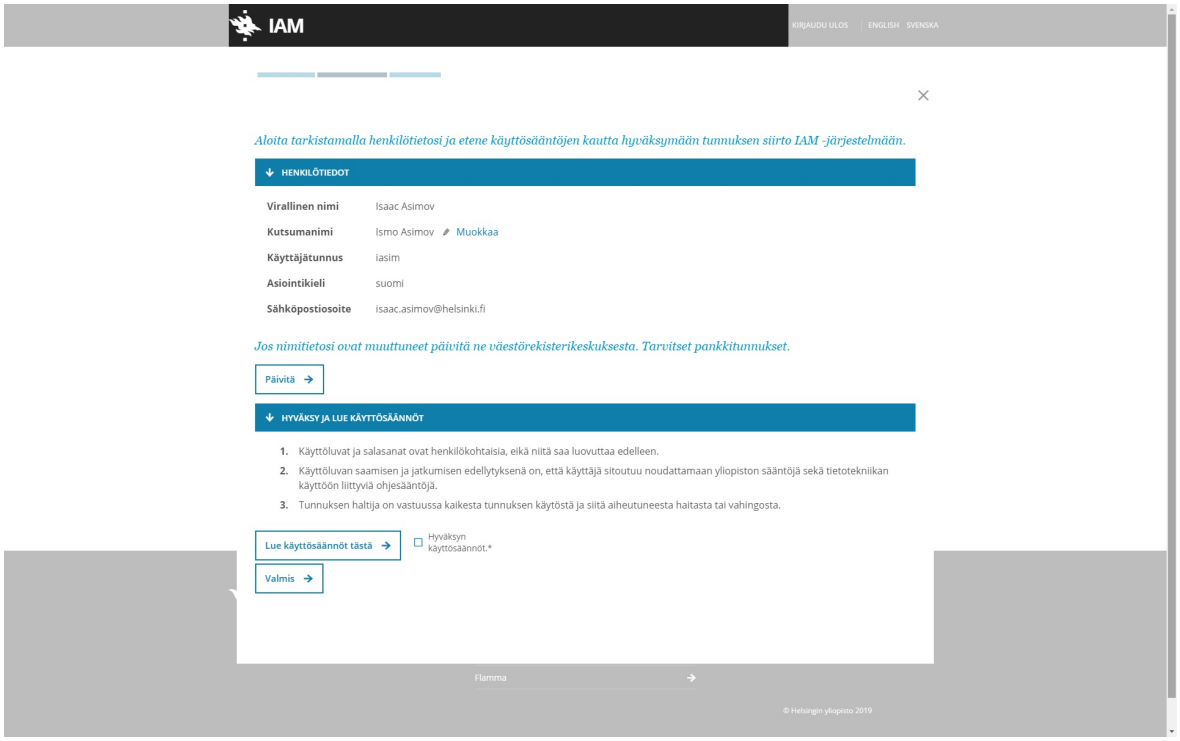


Kuva 17. Haitarista avataan modaali-ikkuna, jonka tarkoitus viestiä käyttäjälle toiminnan tilasta visuaalisesti.

Liite 3. Käyttöliittymäsuunnitelman versio 5, pääsivu.

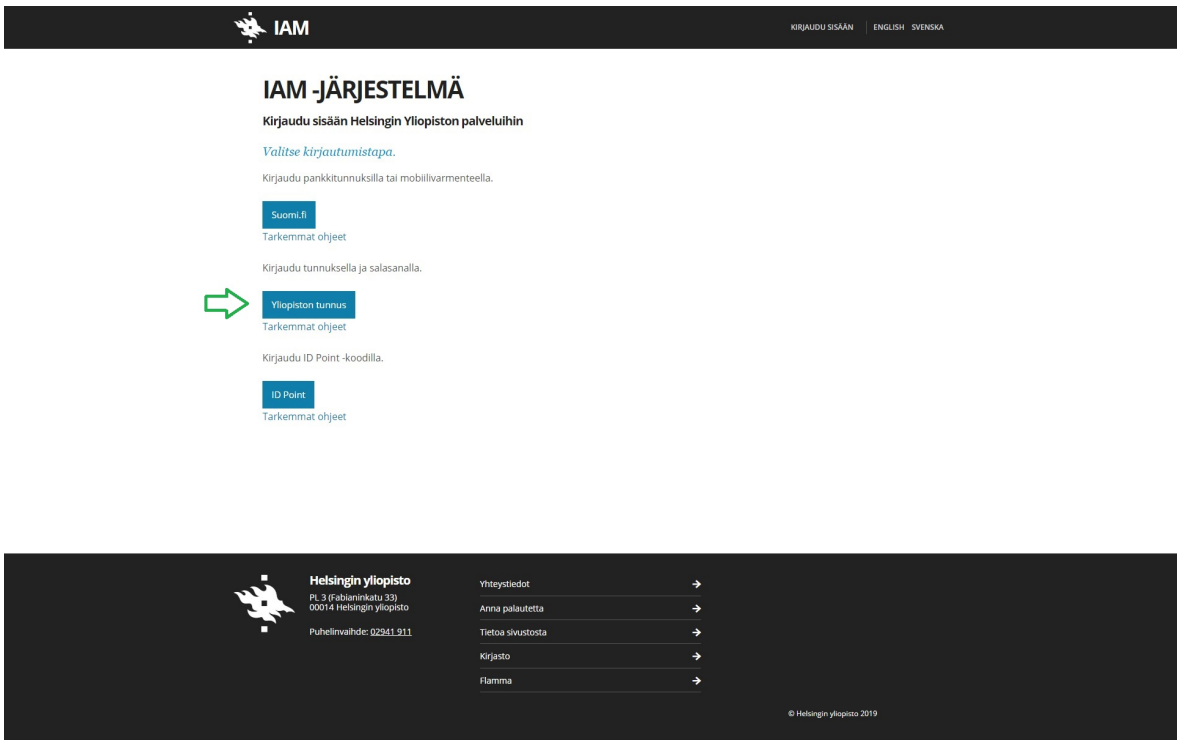


Kuva 18. Versiossa 5 ylärivin painikkeita karsittiin loppukäyttäjän näkymän mukaiseen suuntaan, visuaalisen metelin vähentämiseksi. Migraatiotyökalu on siirretty näkymään "Omat tiedot".

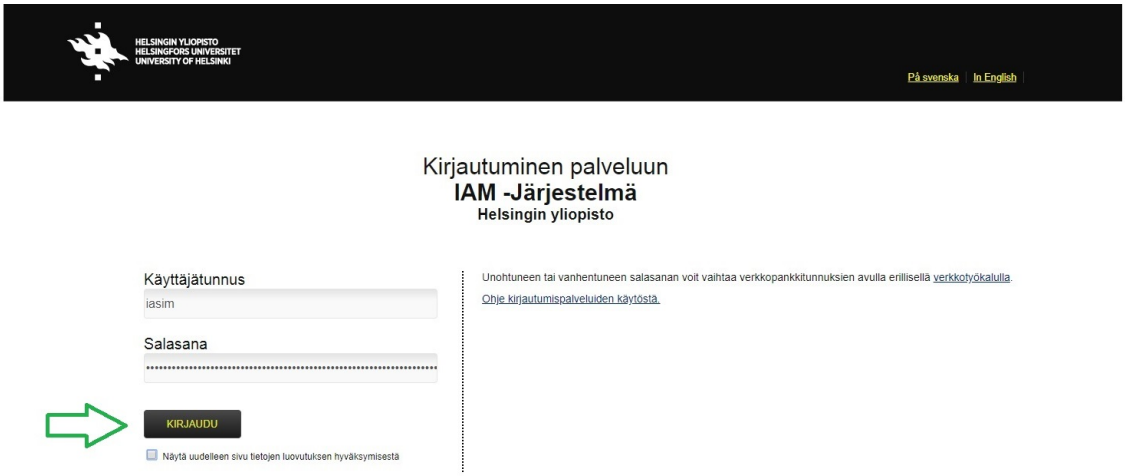


Kuva 19. Versiossa 5 käytetään myös modaali-ikkunaa.

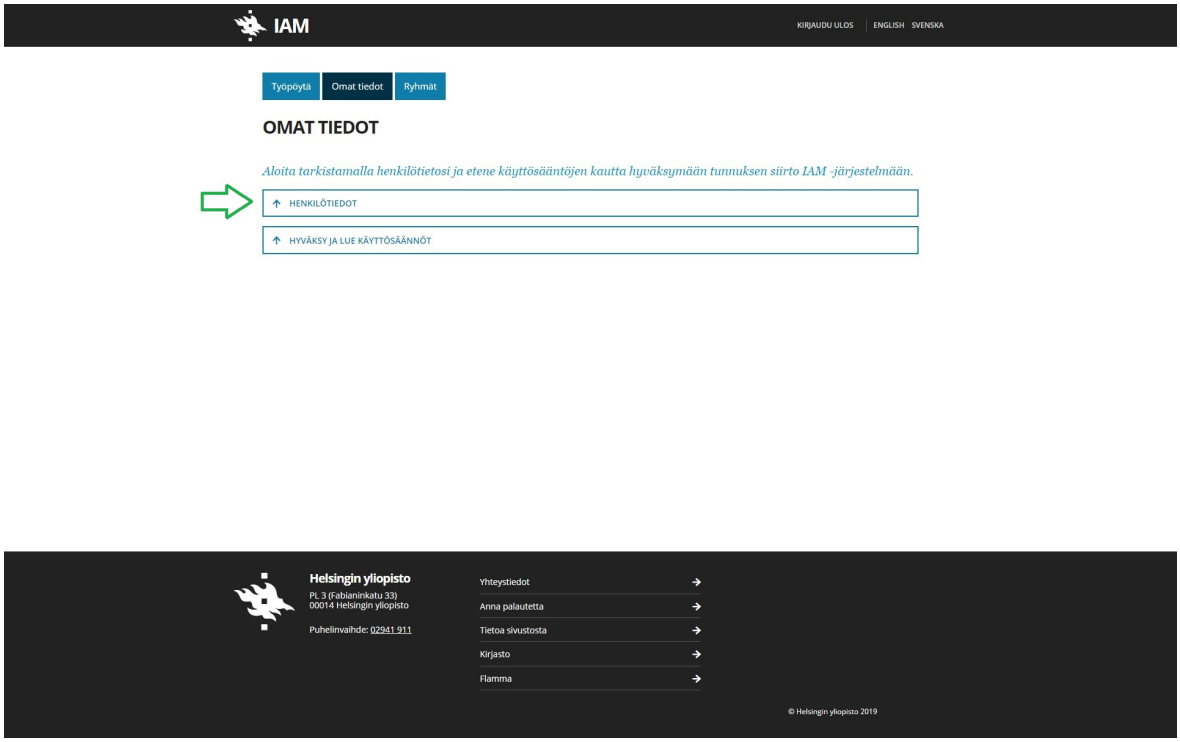
Liite 4. Käyttöliittymäsuunnitelman versio 6, tunnuksen siirto.



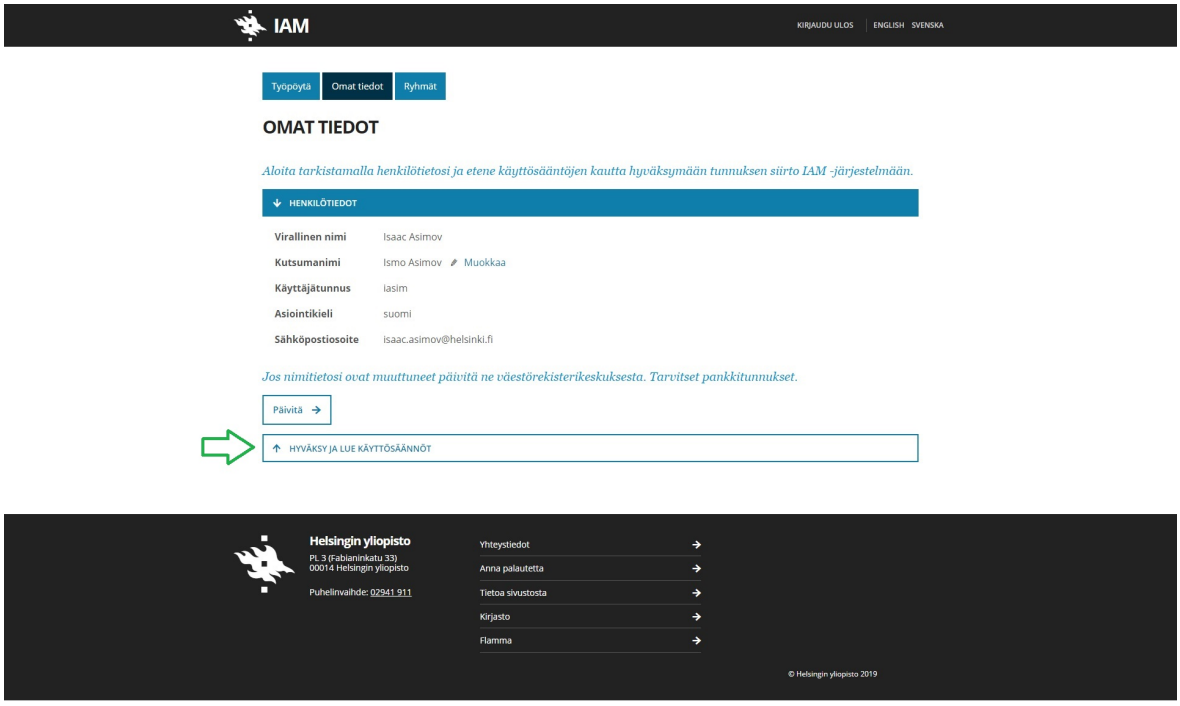
Kuva 20. Käyttötapauksen, jossa käyttäjä siirtää käyttäjätunnuksen oletettu toimintavuo.



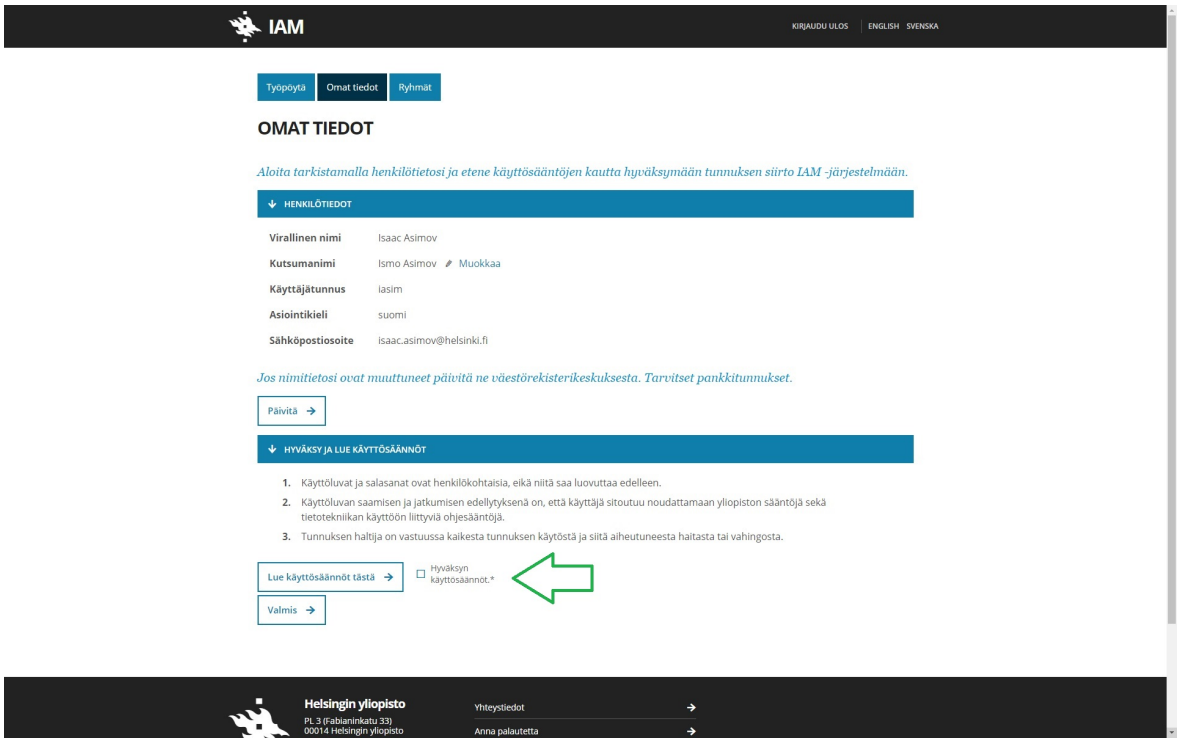
Kuva 21. Kirjautumissivu. Tiedot on valmiiksi syötetty. Käyttäjä klikkaa kuvaa.



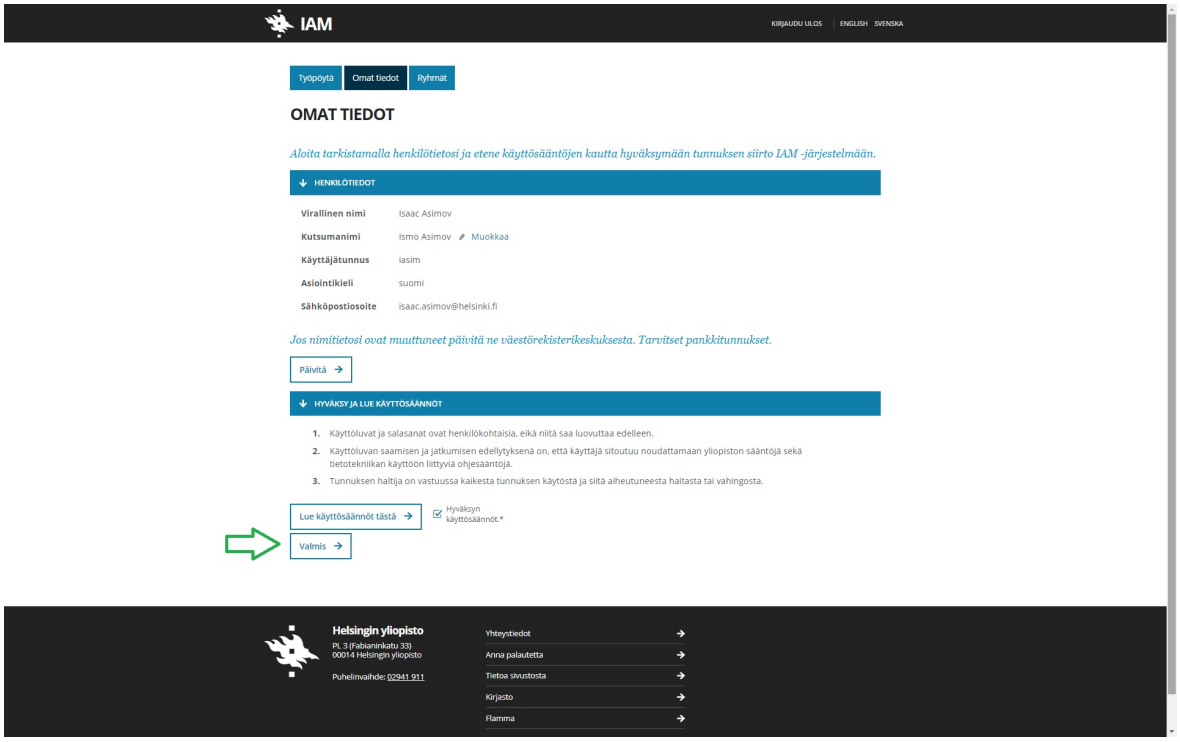
Kuva 22. Käyttäjä avaa ensimmäisen haitarielementin.



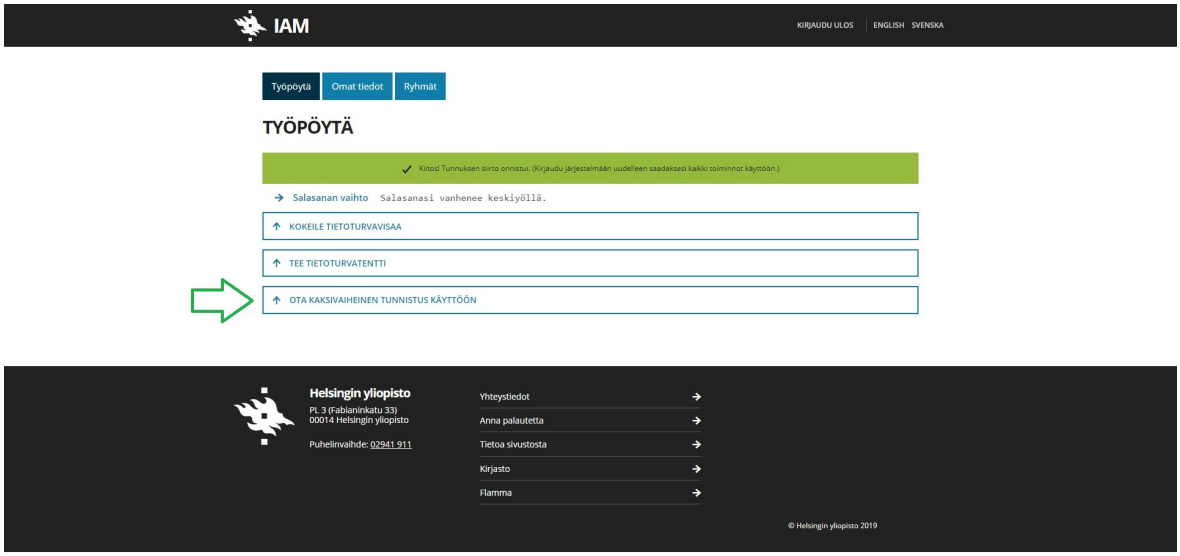
Kuva 23. Käyttäjä siirtyy toiseen haitarielementtiin.



Kuva 24. Käyttäjän oletetaan valitsevan "Hyväksyn käyttösäännöt." -ruutu.

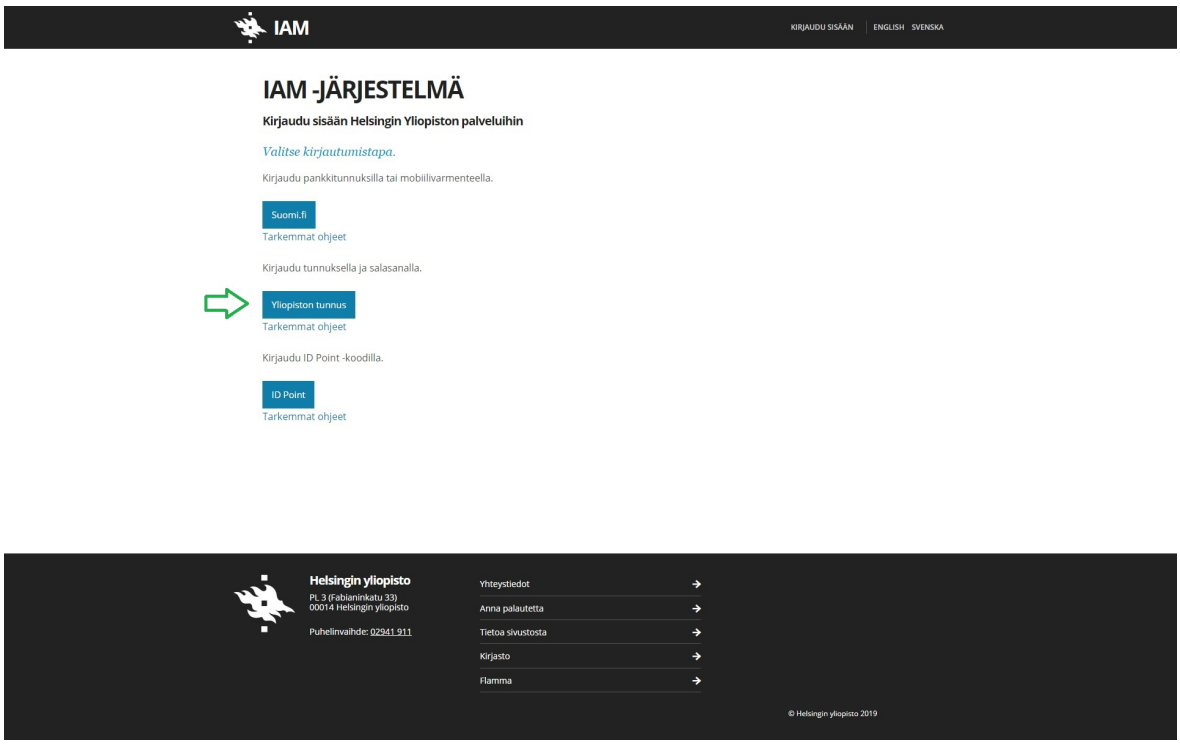


Kuva 25. Käyttäjä valitsee ”Valmis”-painikkeen.

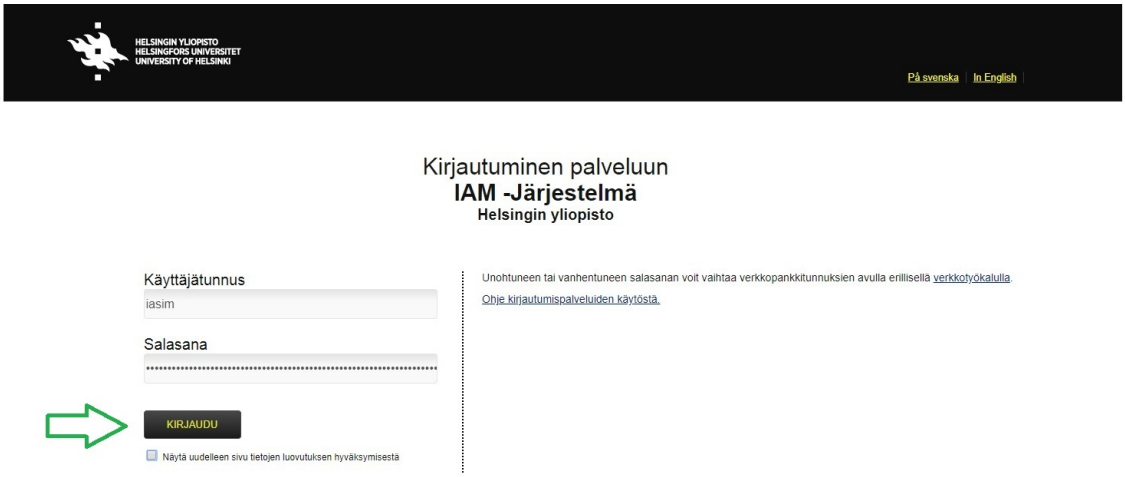


Kuva 26. Viimeinen sivu. Tunnuksen vienti onnistuu.

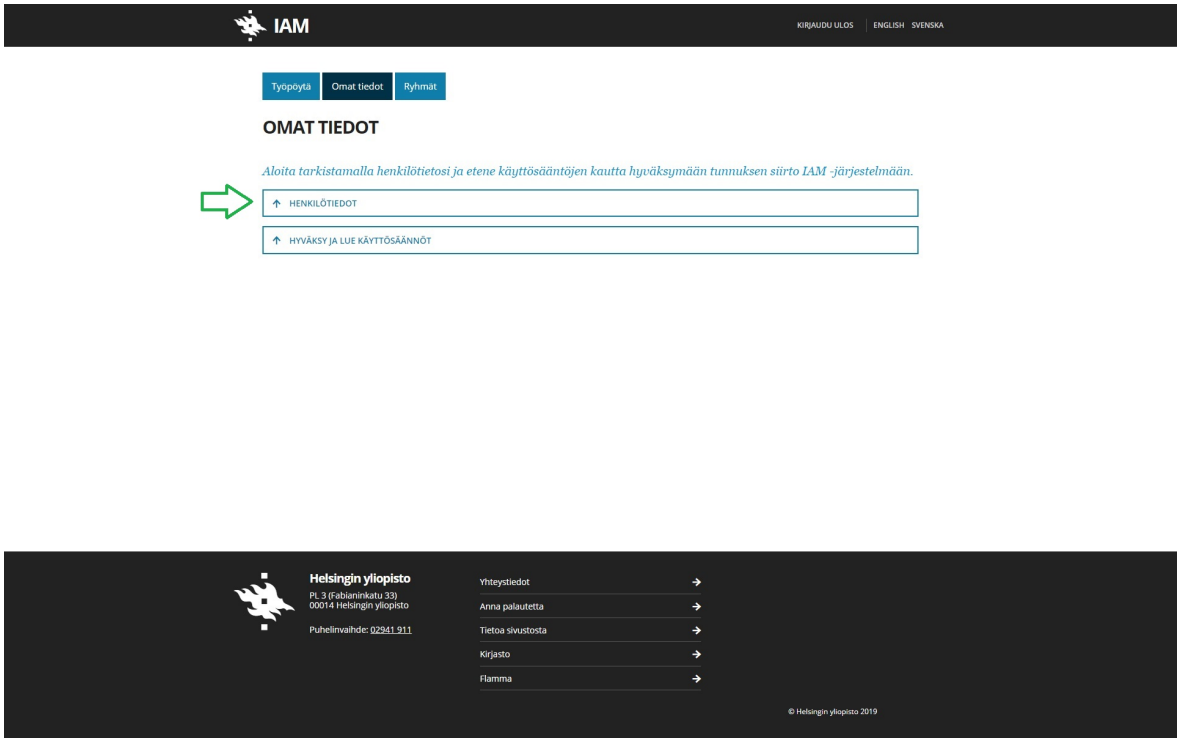
Liite 5. Käyttöliittymäsuunnitelman versio 6, tietojen päivittäminen.



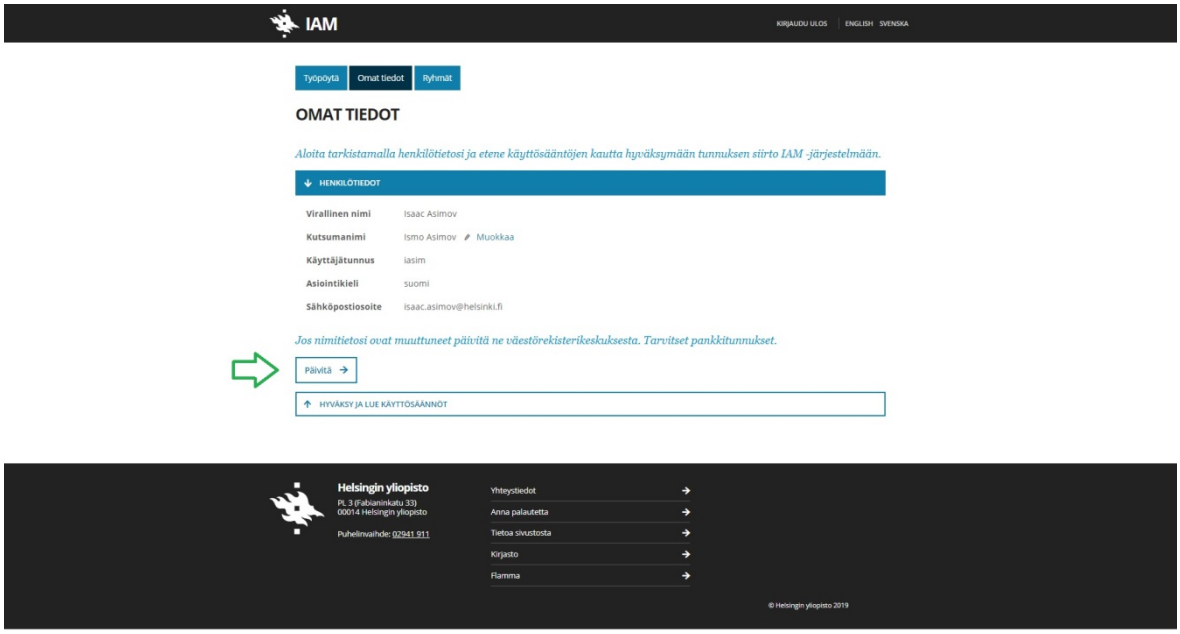
Kuva 27. Käyttötapaus, jossa käyttäjä päivittää tietonsa. Käyttäjä valitsee kirjautumistavan.



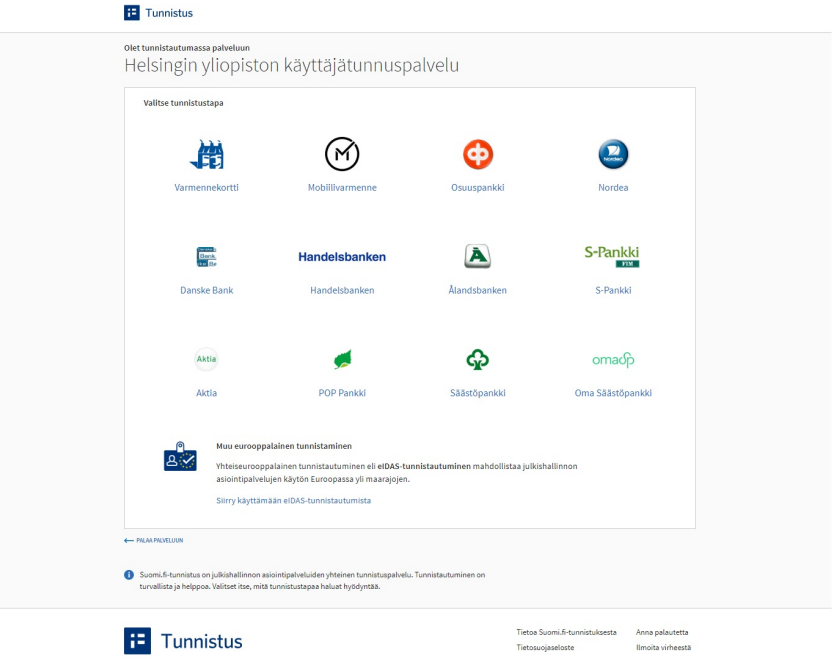
Kuva 28. Kirjautuminen yliopiston tunnuksilla.



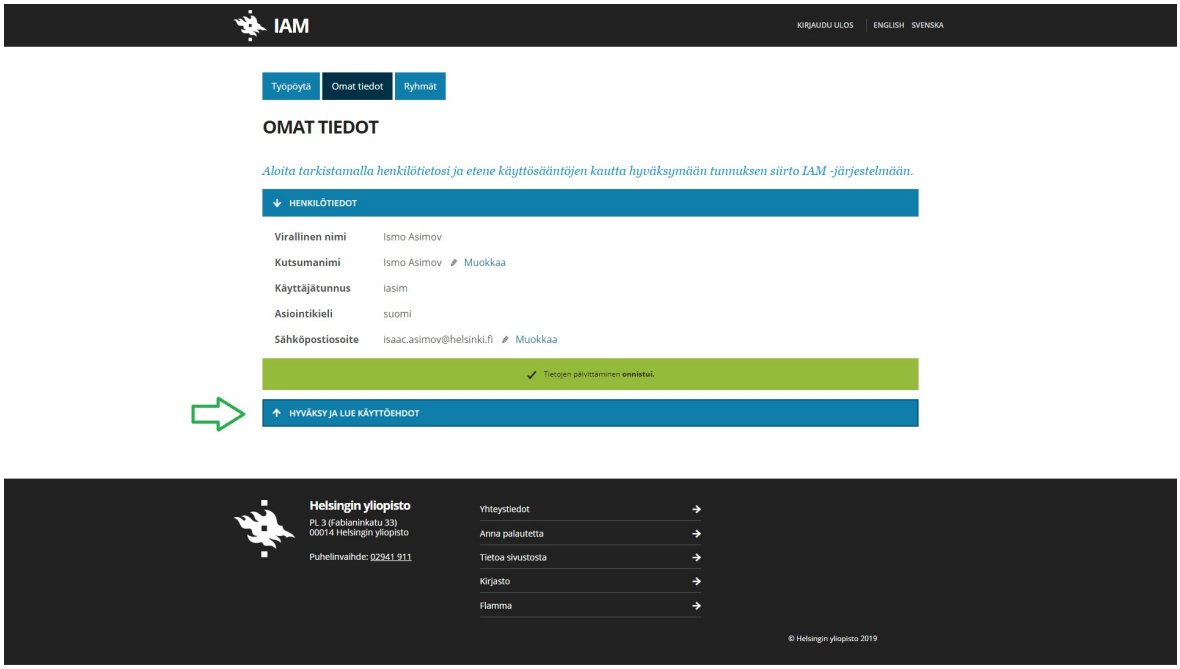
Kuva 29. Ensimmäinen haitarielementti.



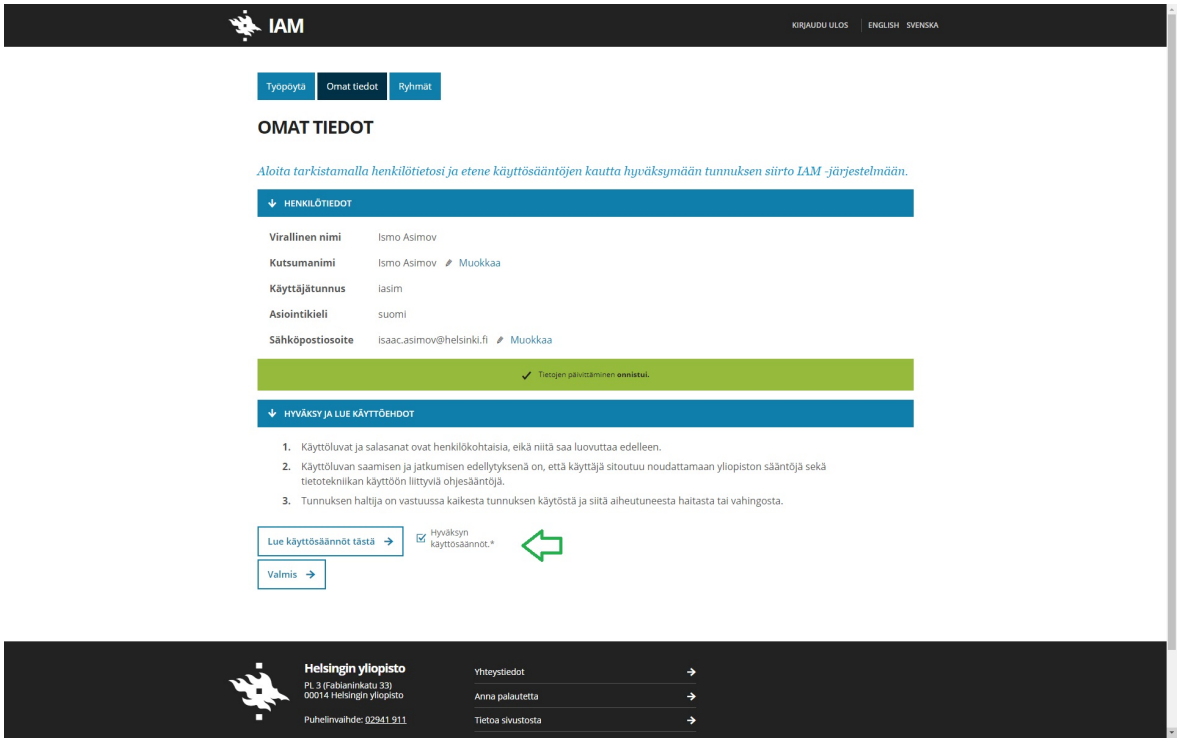
Kuva 30. Käyttäjä valitsee ”Päivitä”-painikkeen.



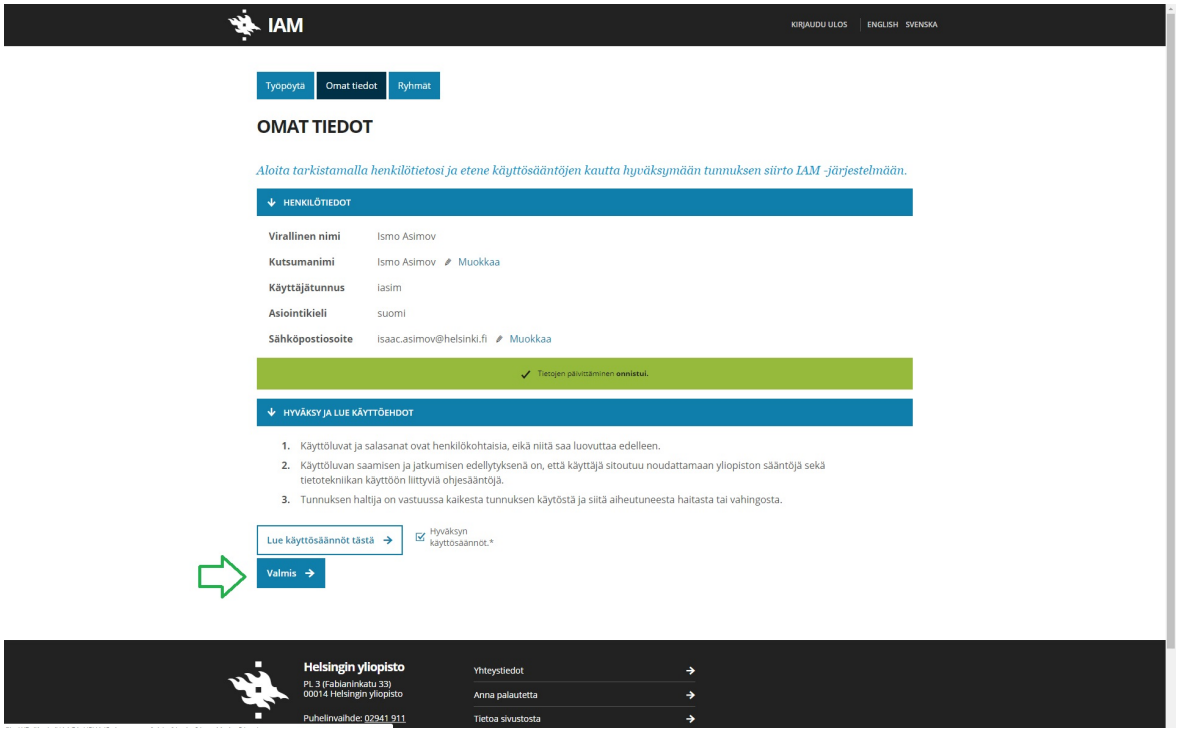
Kuva 31. Suomi.fi-kirjautumista läheisesti muistuttava kuva. Käyttäjä klikkaa mitä tahansa.



Kuva 32. Käyttäjä avaa toisen haitarielementin.

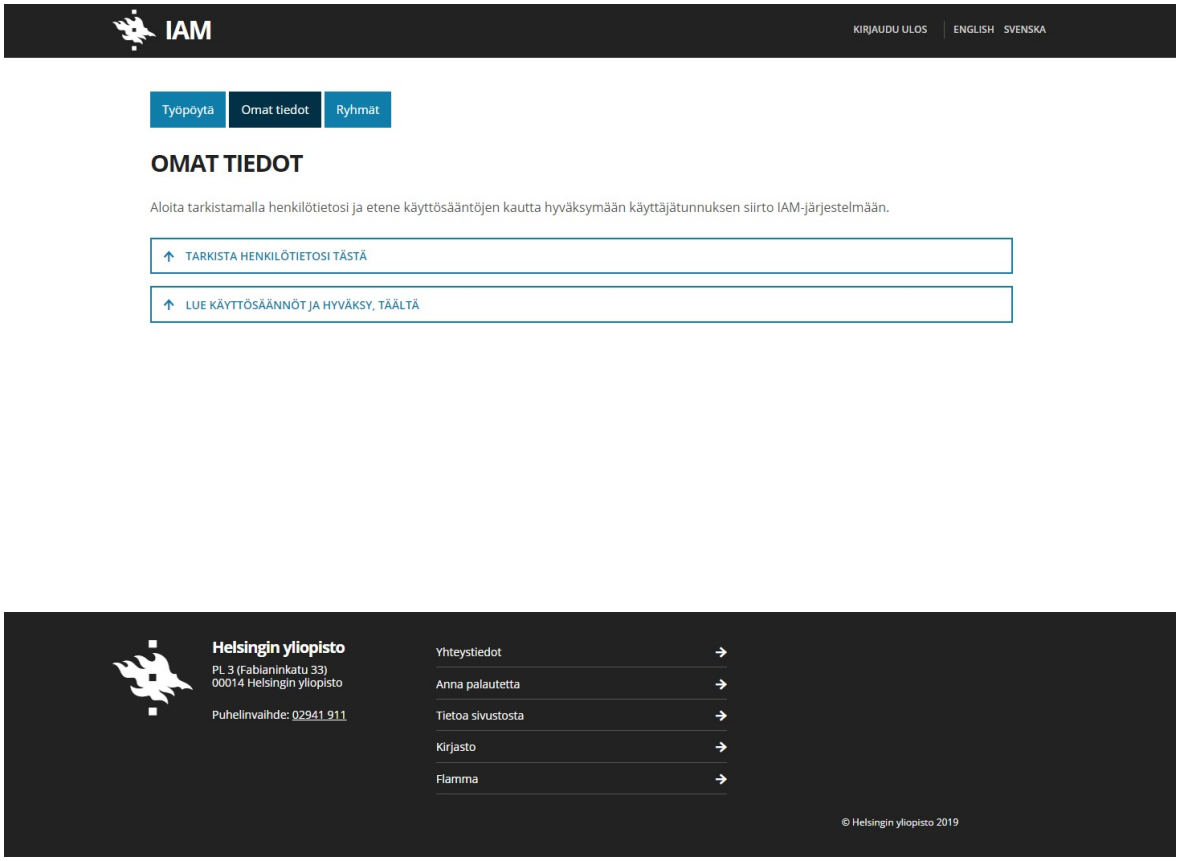


Kuva 33. Käyttäjä hyväksyy käyttösäännöt.

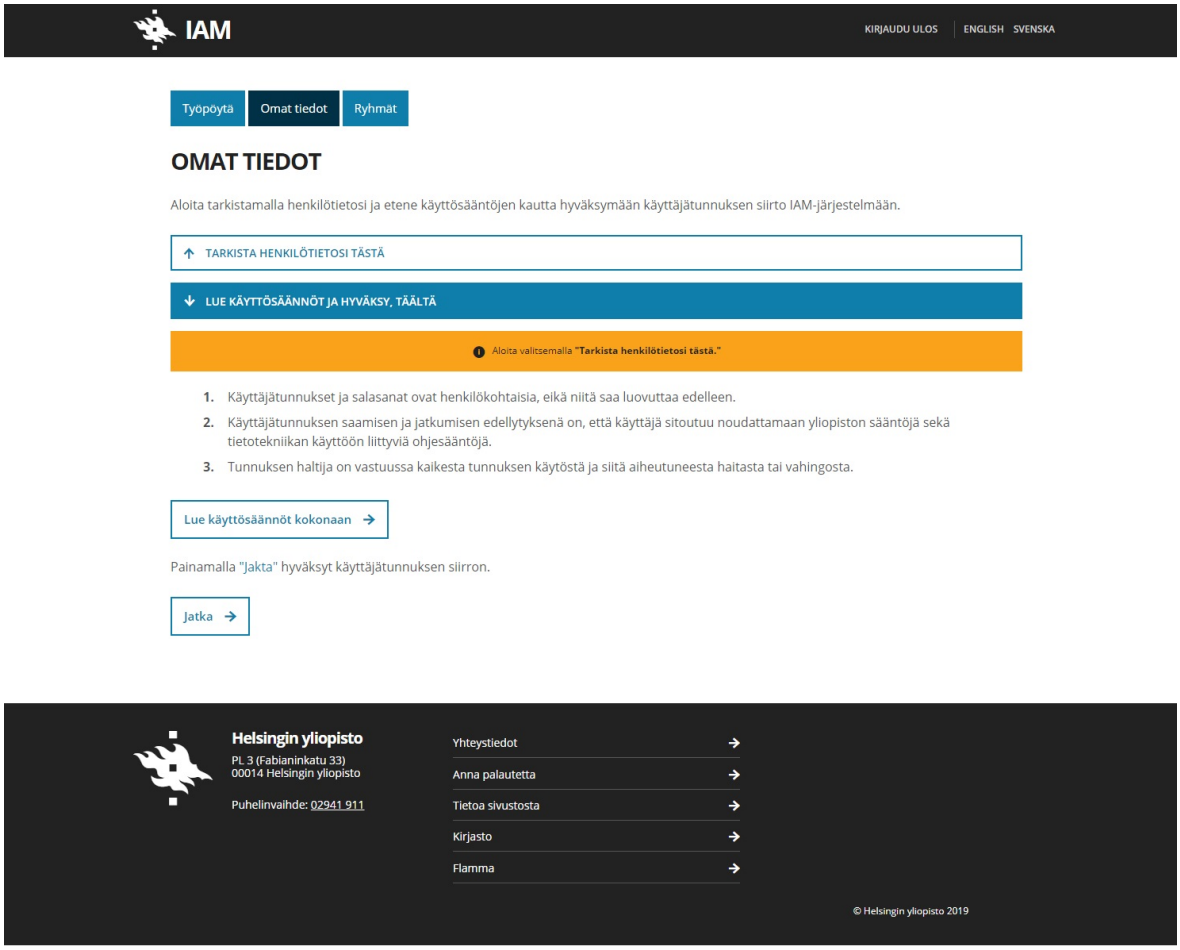


Kuva 34. Toiminto suoritetaan loppuun ”Valmis”-painikkeella.

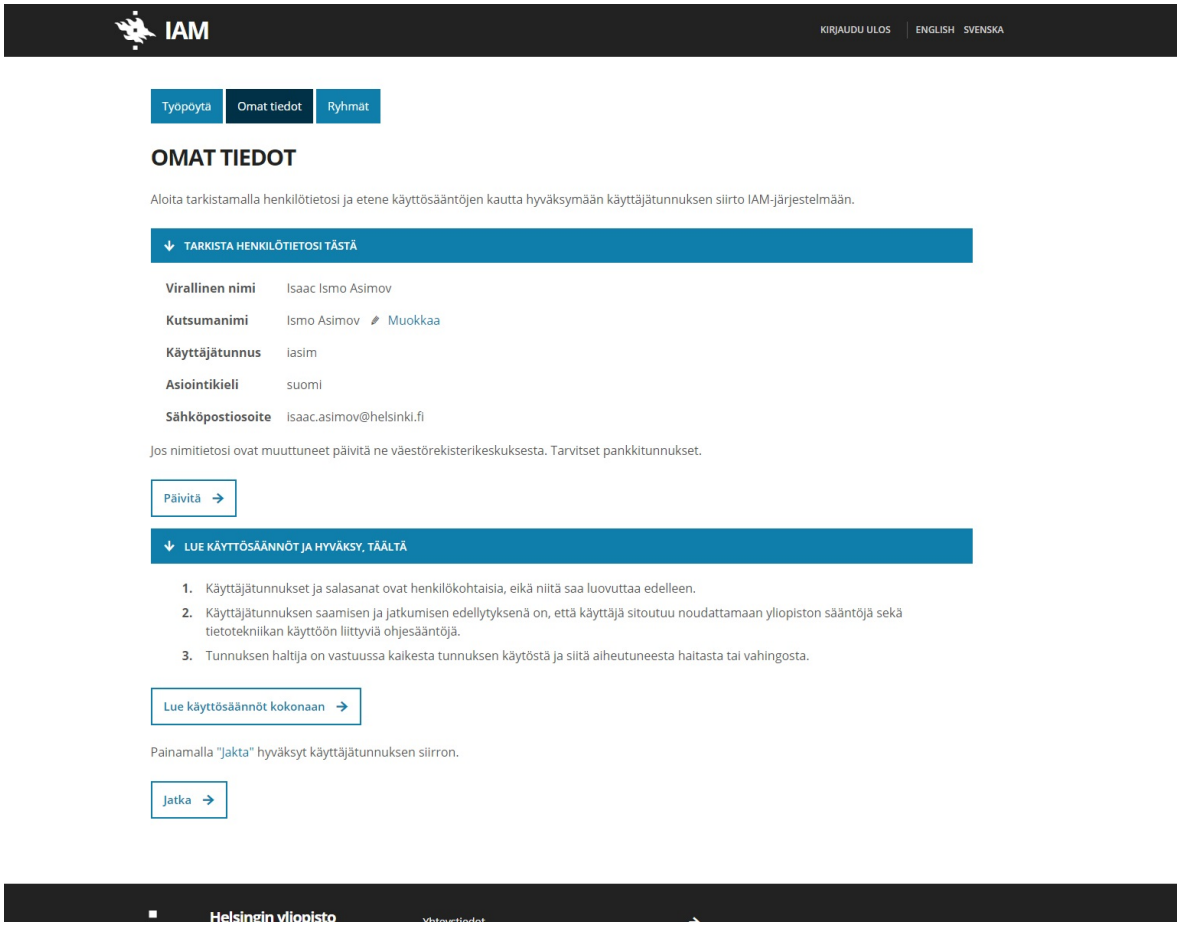
Liite 6. Käyttöliittymäsuunnitelman versio 8, tunnuksen siirto.



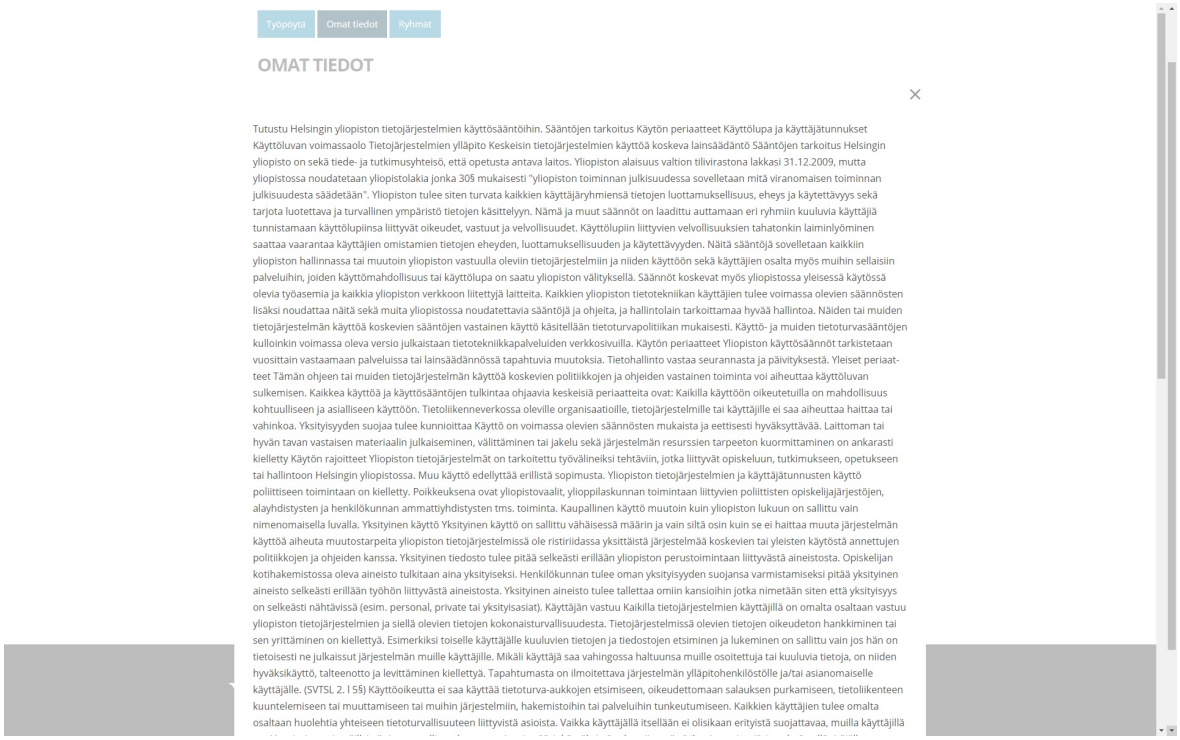
Kuva 35. Käyttötapaus jossa käyttäjä siirtää käyttäjätunnuksen.



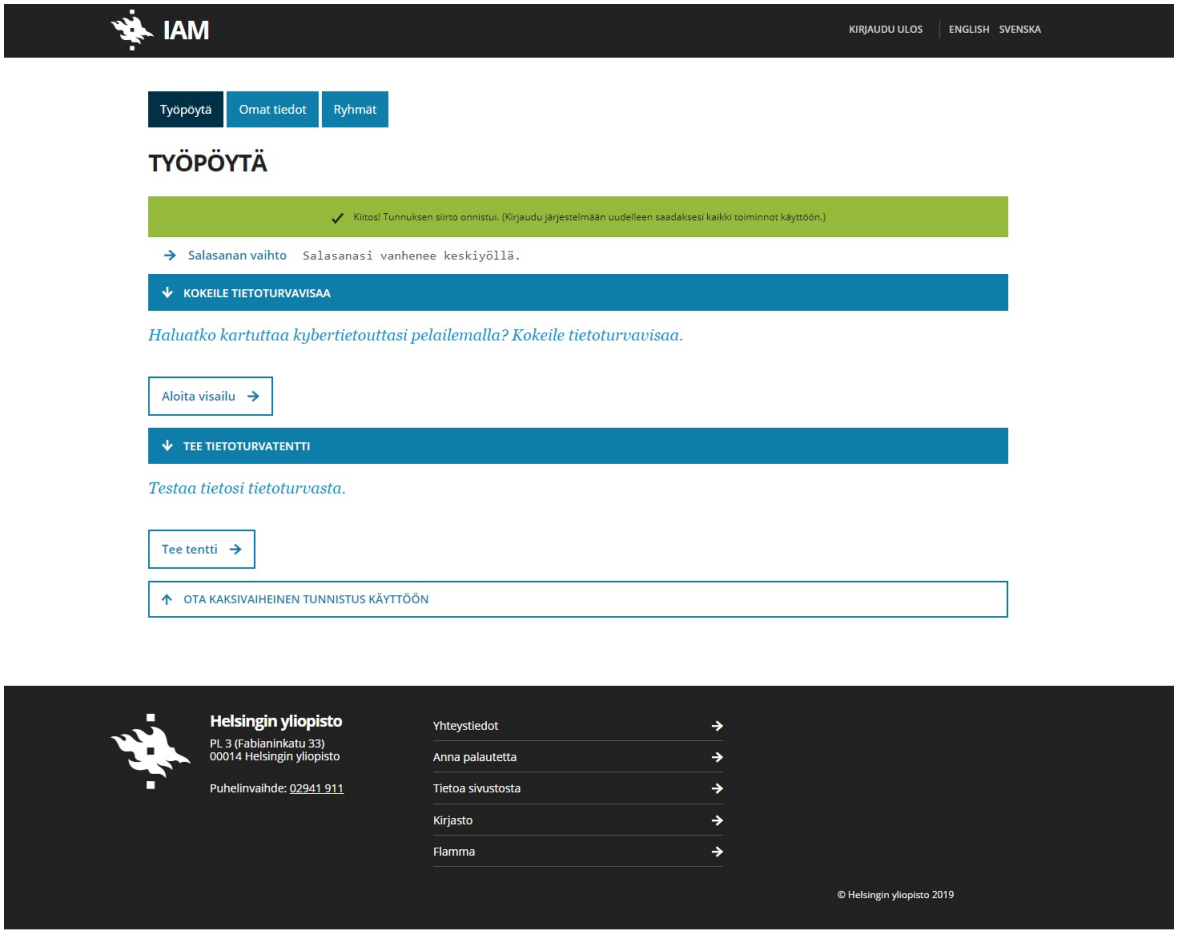
Kuva 36. Käyttäjän yrittäessä ohittaa henkilötietojen tarkistuksen näytetään huomautus.



Kuva 37. Huomautus katoaa, kun ensimmäinen haitarielementti avataan. Viralliset nimet ovat näkyvissä.

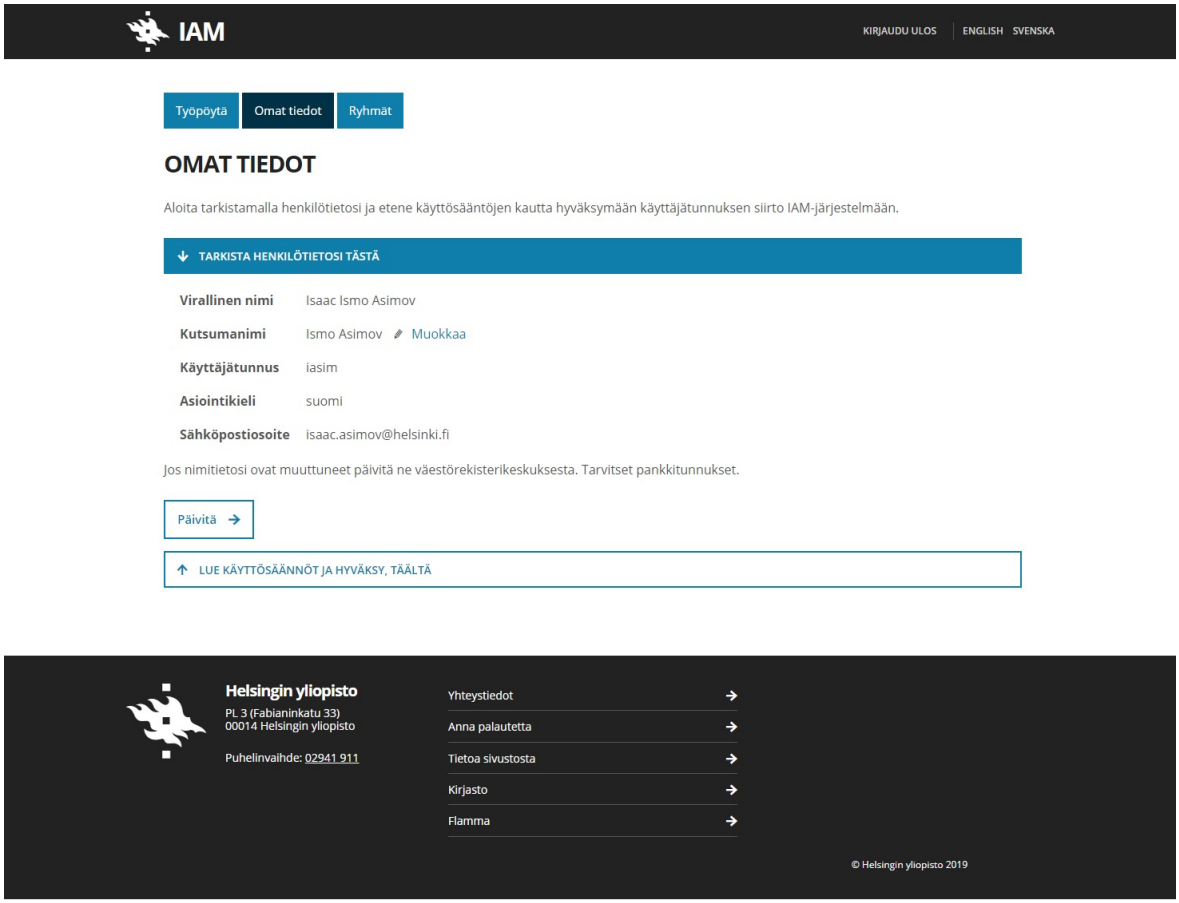


Kuva 38. Käyttösäännöt avataan modaali-ikkunaan.

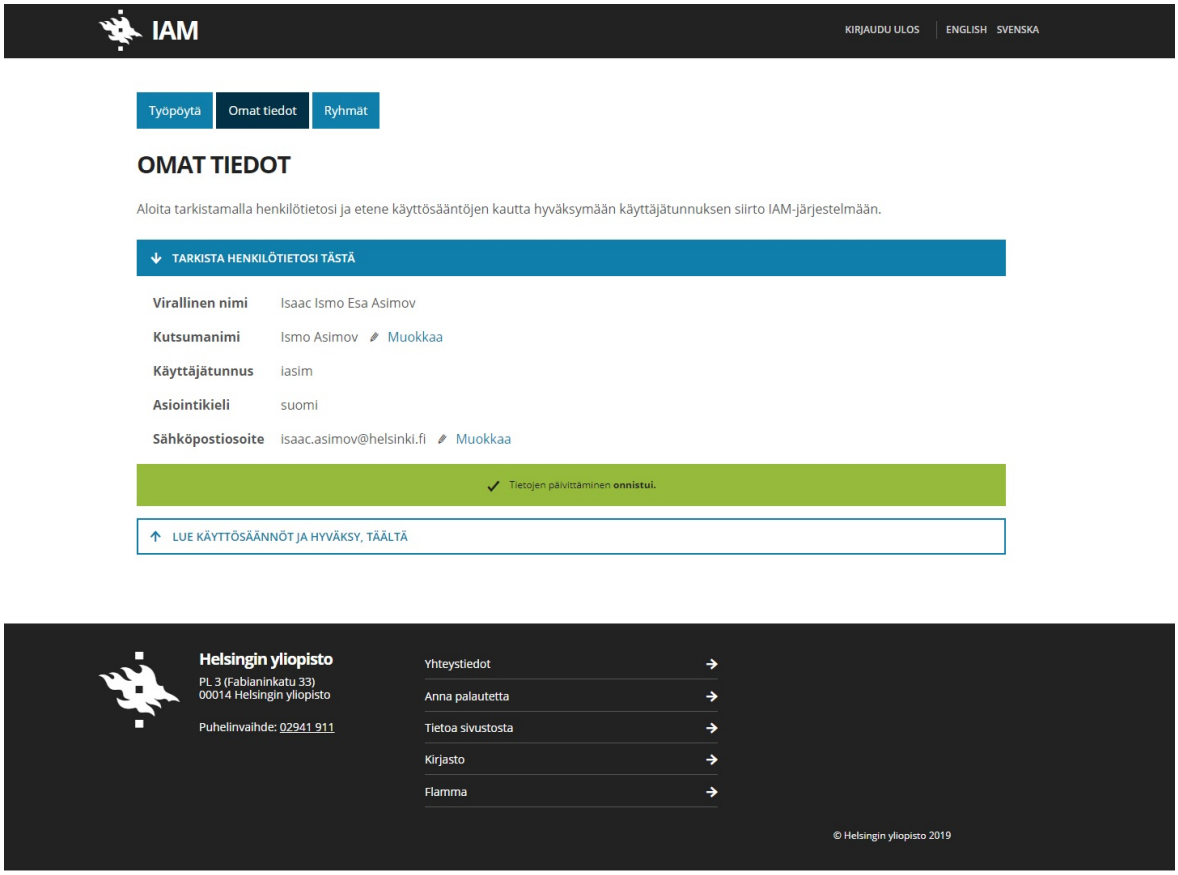


Kuva 39. Viimeinen sivu on samanlainen kuin edellisissäkin versioissa.

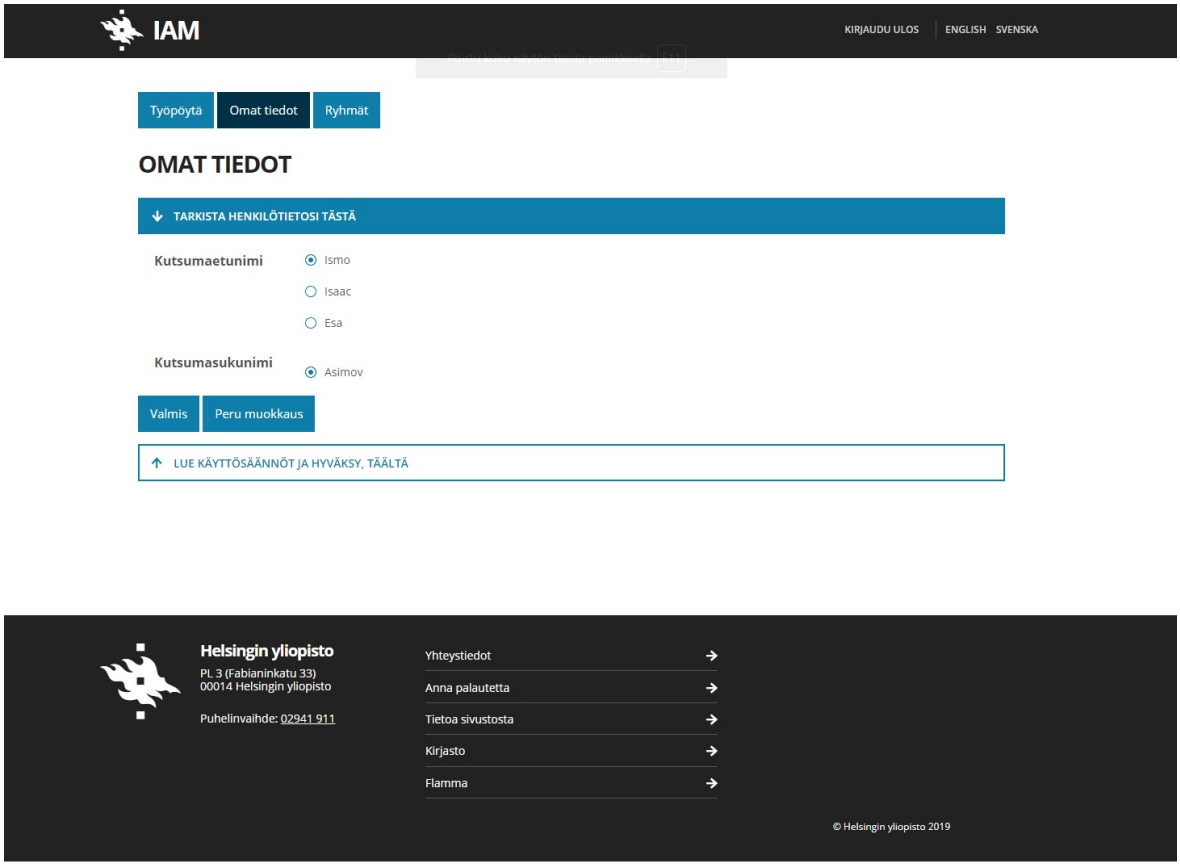
Liite 7. Käyttöliittymäsuunnitelman versio 8, tietojen päivittäminen



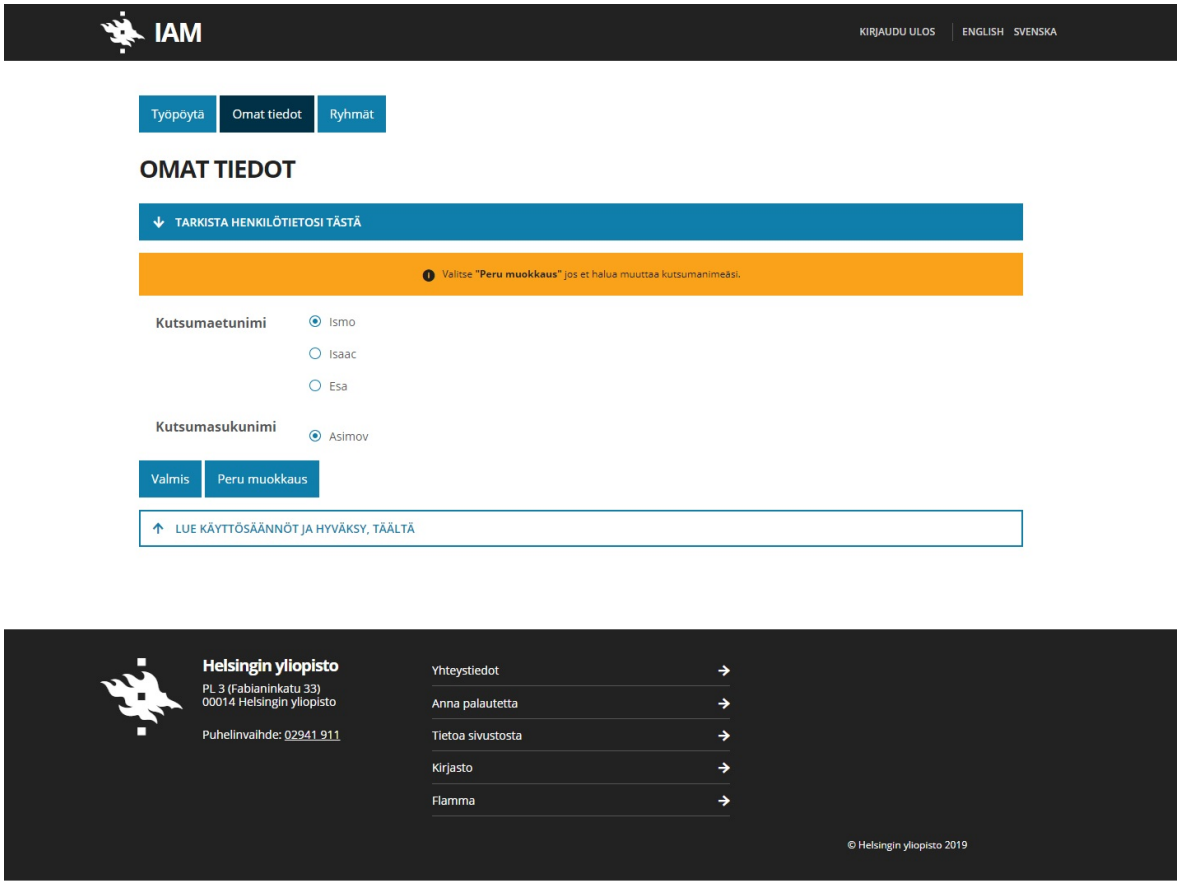
Kuva 40. Tietojen tarkistus ja valitaan tietojen päivittäminen painikkeesta.



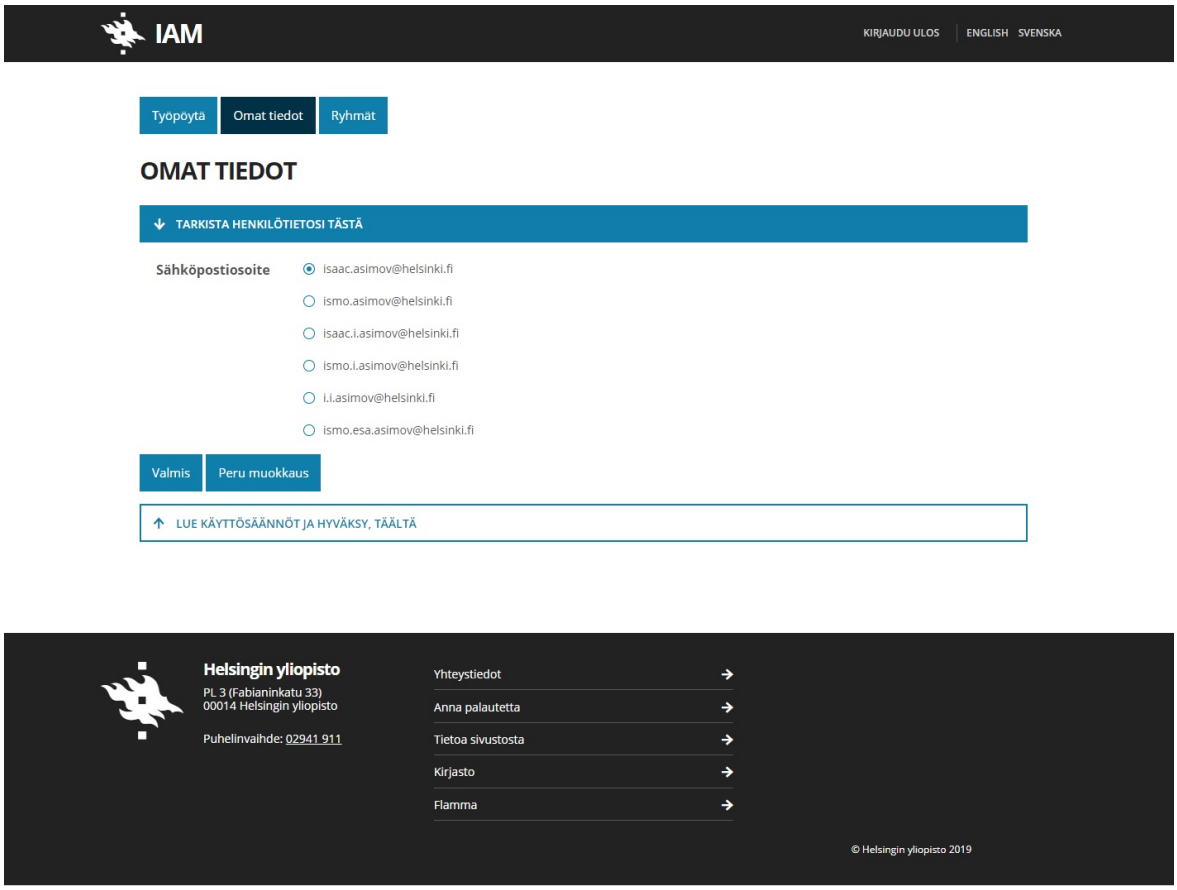
Kuva 41. Nimitiedot päivittyvät ja se kerrotaan ilmoituksella.



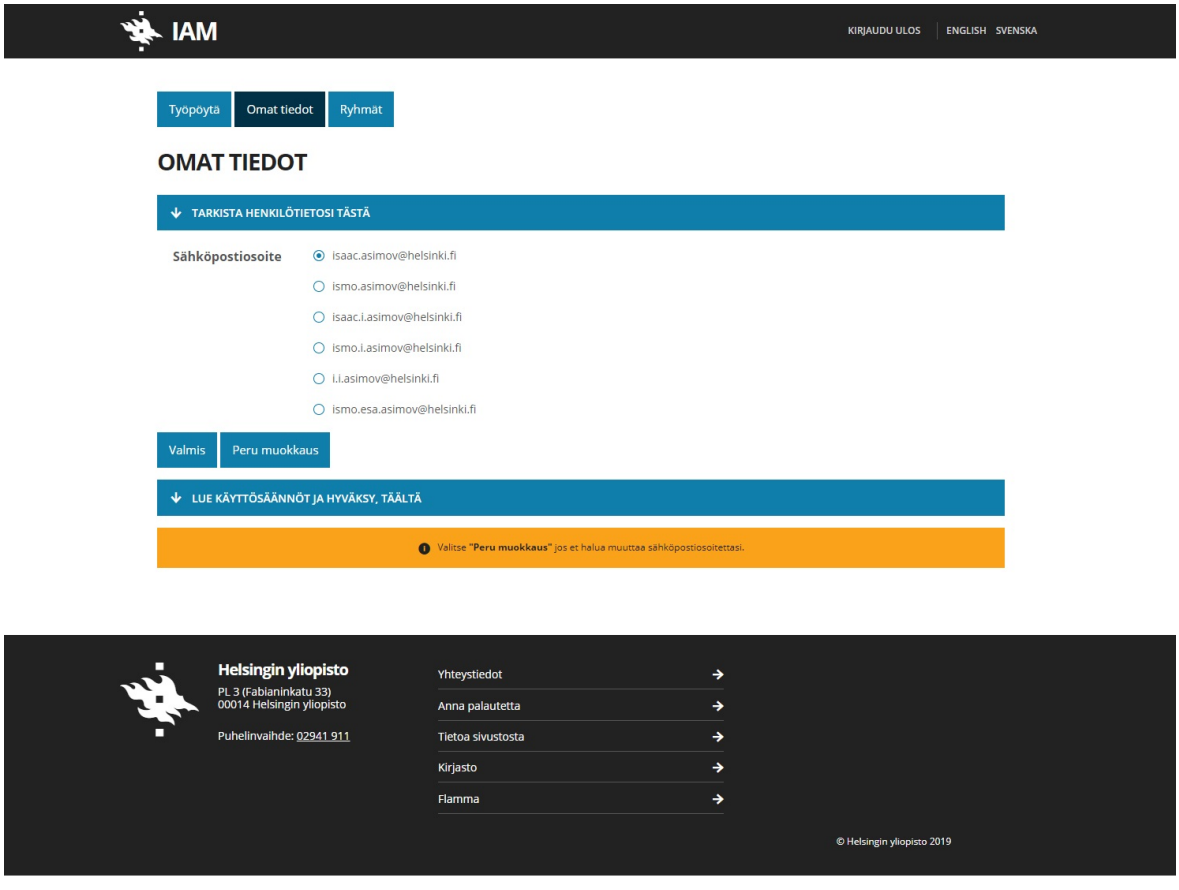
Kuva 42. Kutsumanimien muokkausnäkymä.



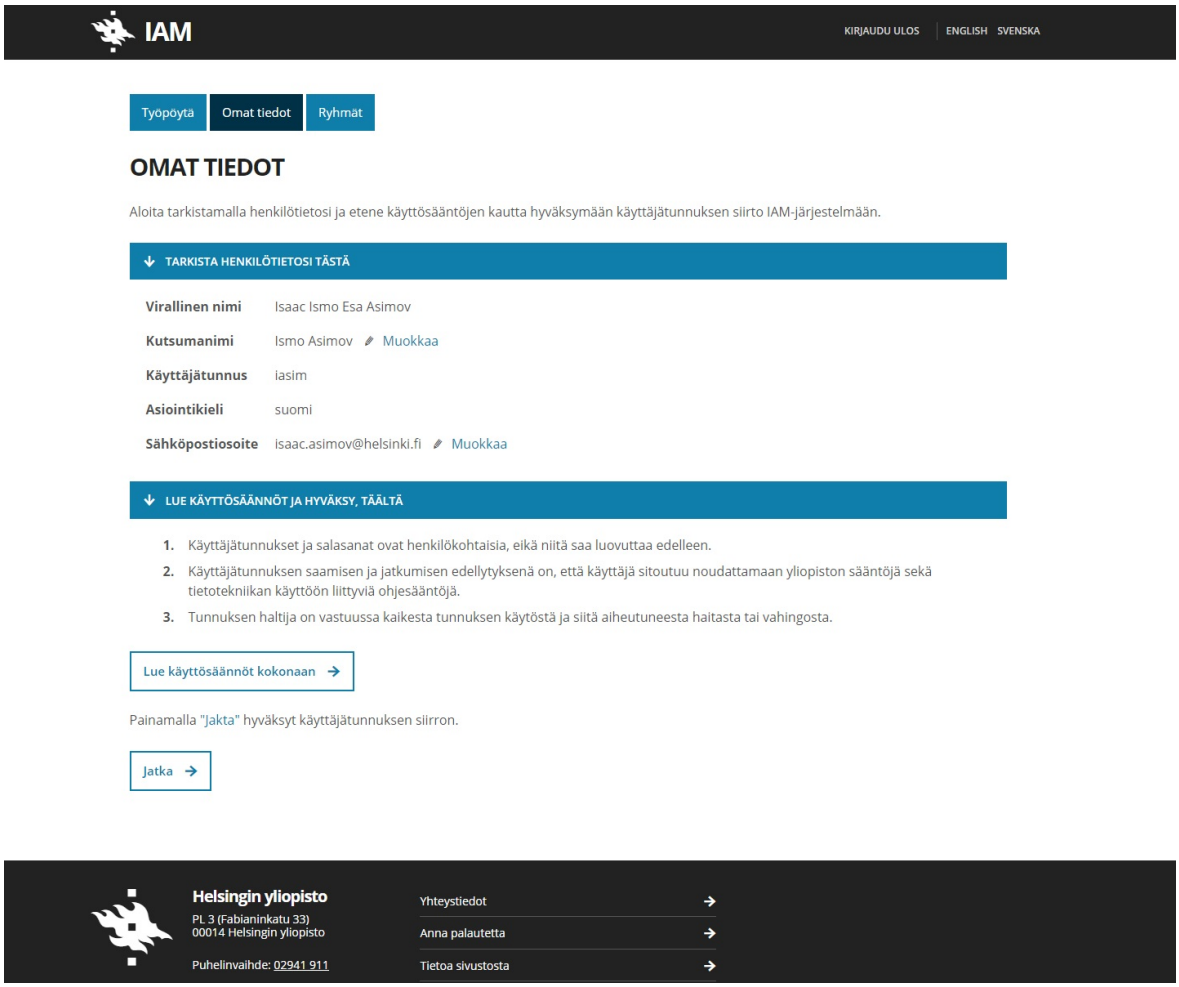
Kuva 43. Käyttäjän klikatessa jotakin muuta elementtiä, kuin ”Valmis”- tai ”Peru muokkaus” -painikkeita näytetään huomautus. Näitä kehotteita järkevöitettiin.



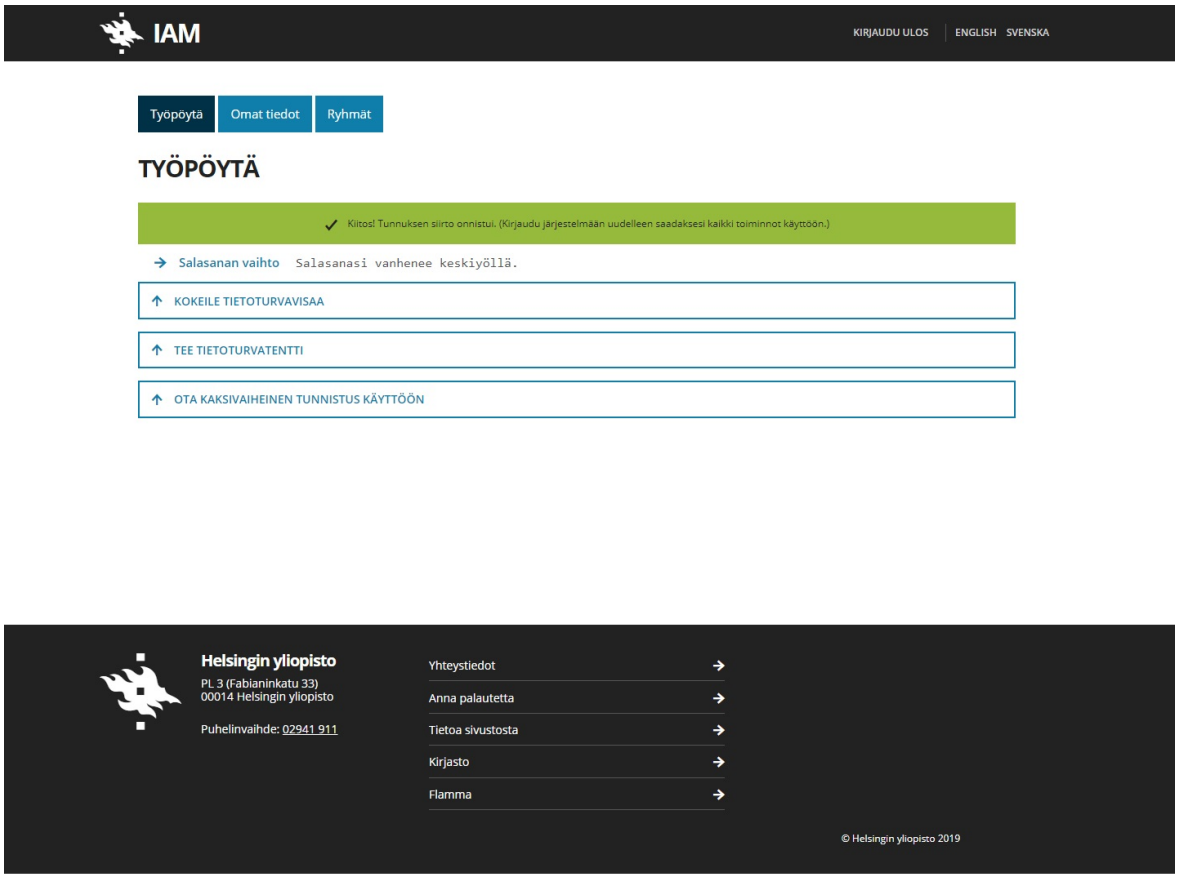
Kuva 44. Sähköpostiosoitteen muokkausnäkymä.



Kuva 45. Haitarielementin painaminen näyttää huomautuksen.

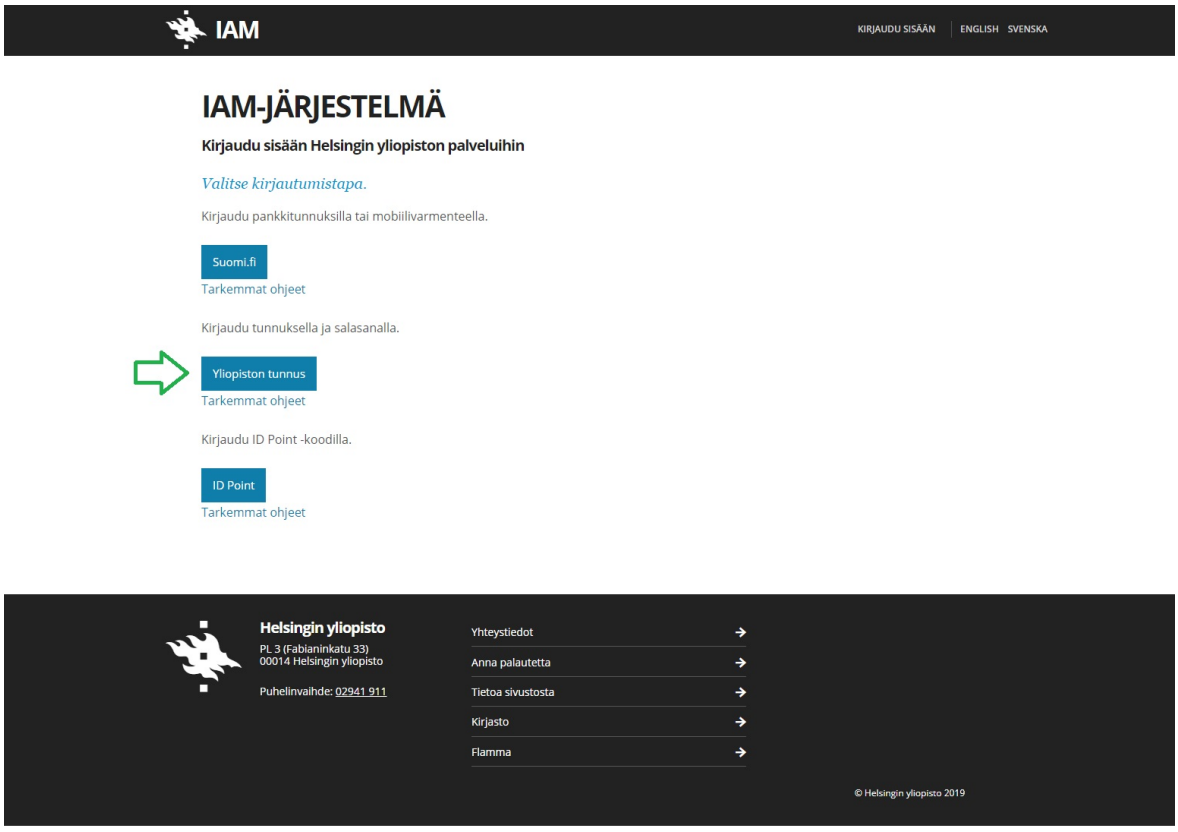


Kuva 46. Tästä näkymästä toiminnon saa vietyä loppuun ”Jatka”-painikkeella tai perus norjalla, mikä on painovirhe.

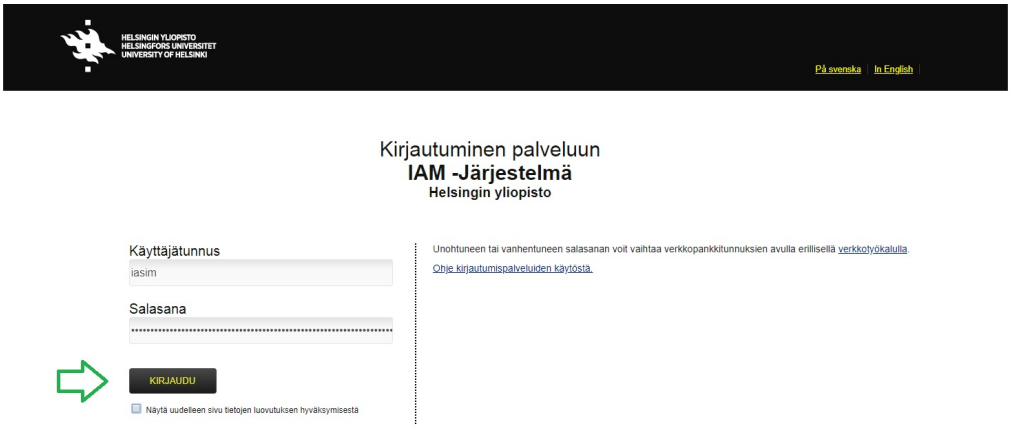


Kuva 47. Viimeinen sivu.

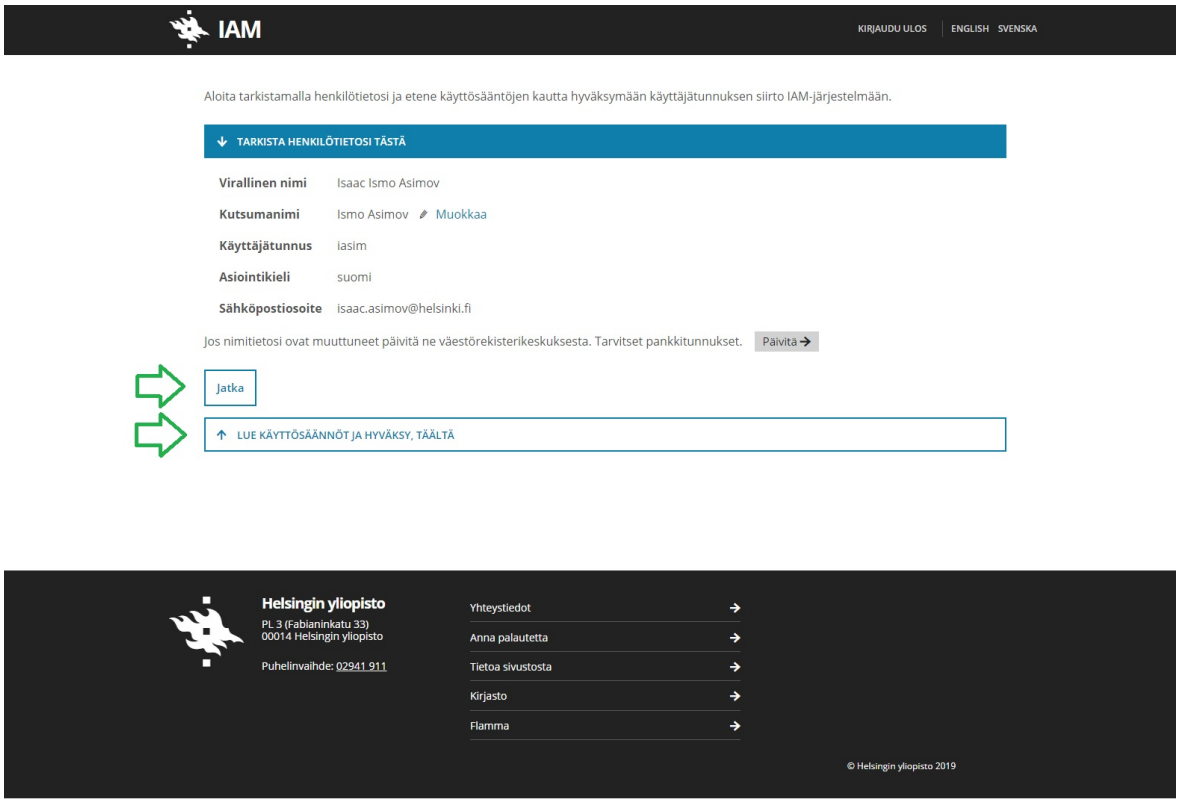
Liite 8. Käyttöliittymäsuunnitelman versio 9, tunnuksen siirto.



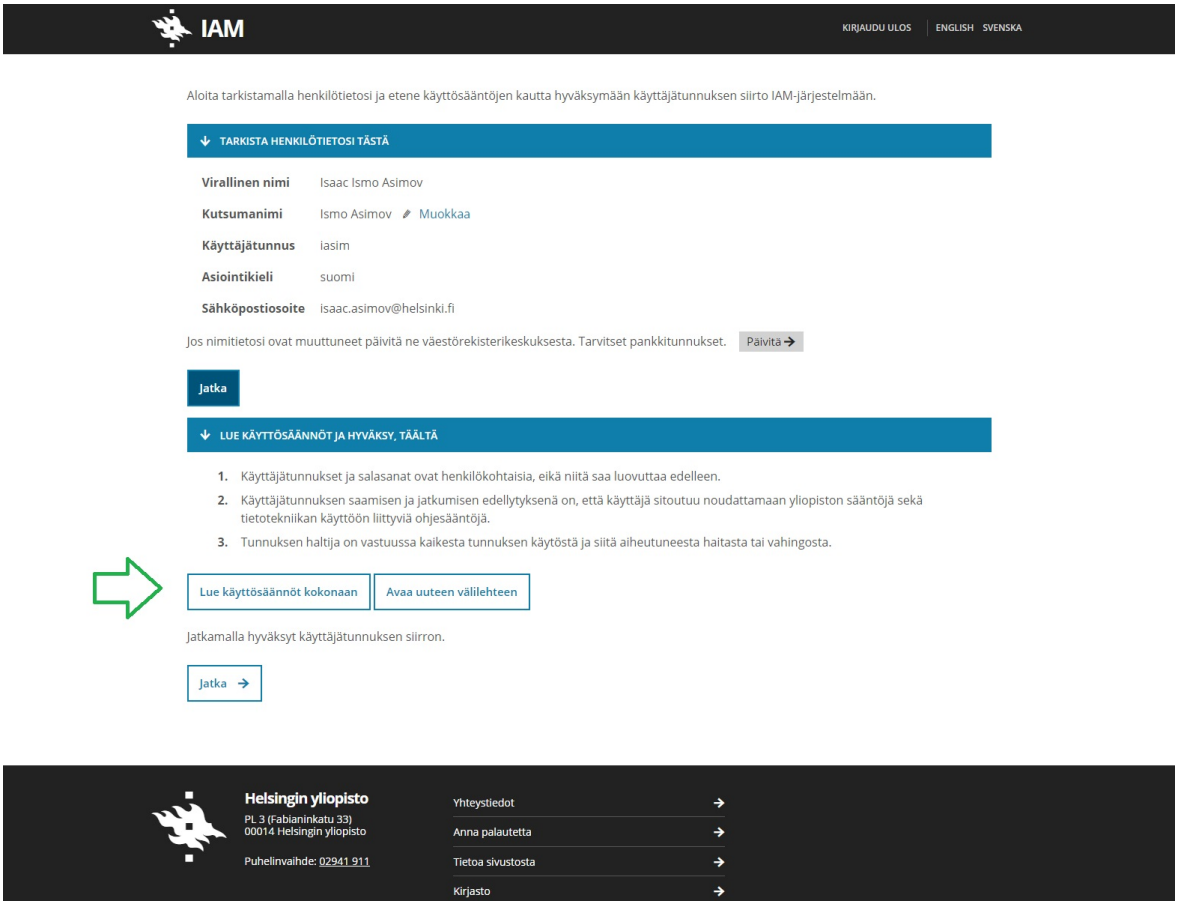
Kuva 48. Kirjautumistapa.



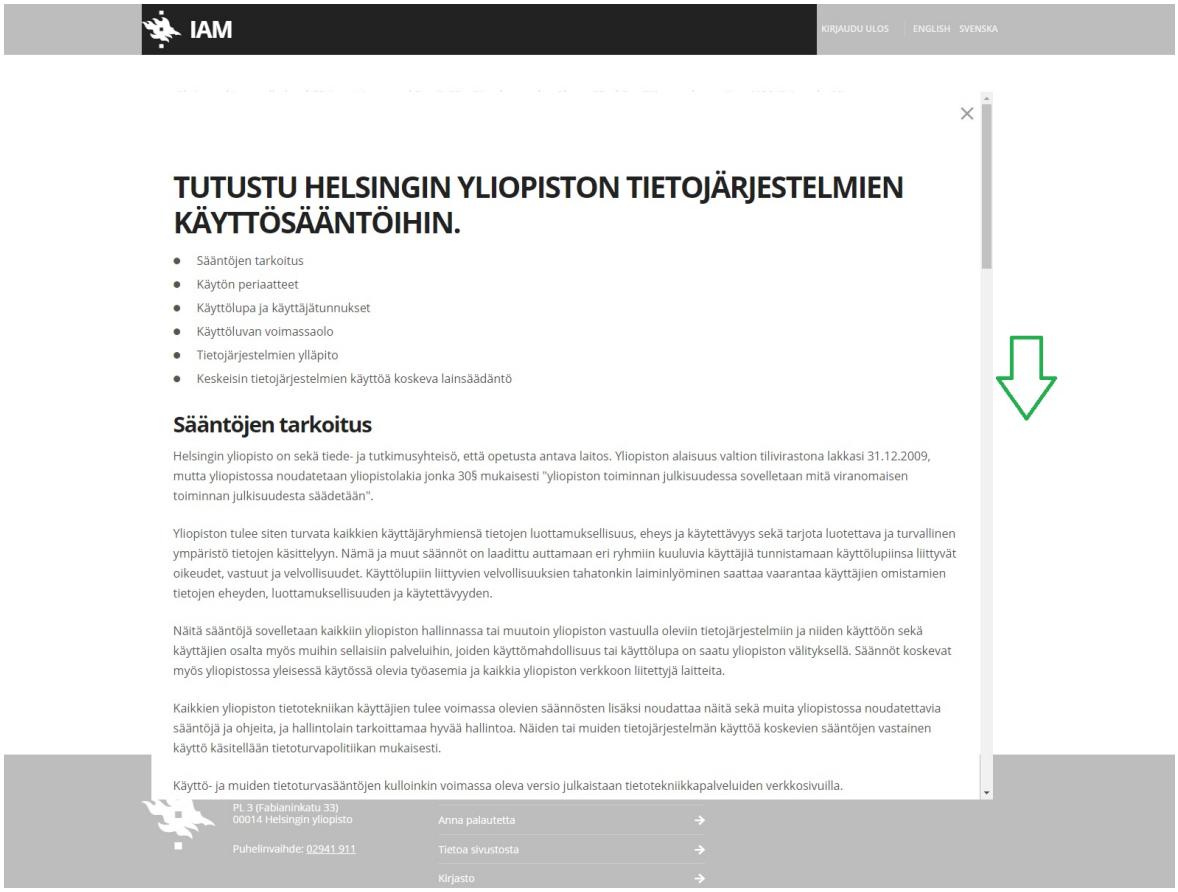
Kuva 49. Yliopiston kirjautuminen.



Kuva 50. Ylärivin elementit on karsittu. Ensimmäinen haitarielementti näytetään avonaisena. ”Jatka”-painike tekee saman asian, kuin haitarielementin klikkaaminen.

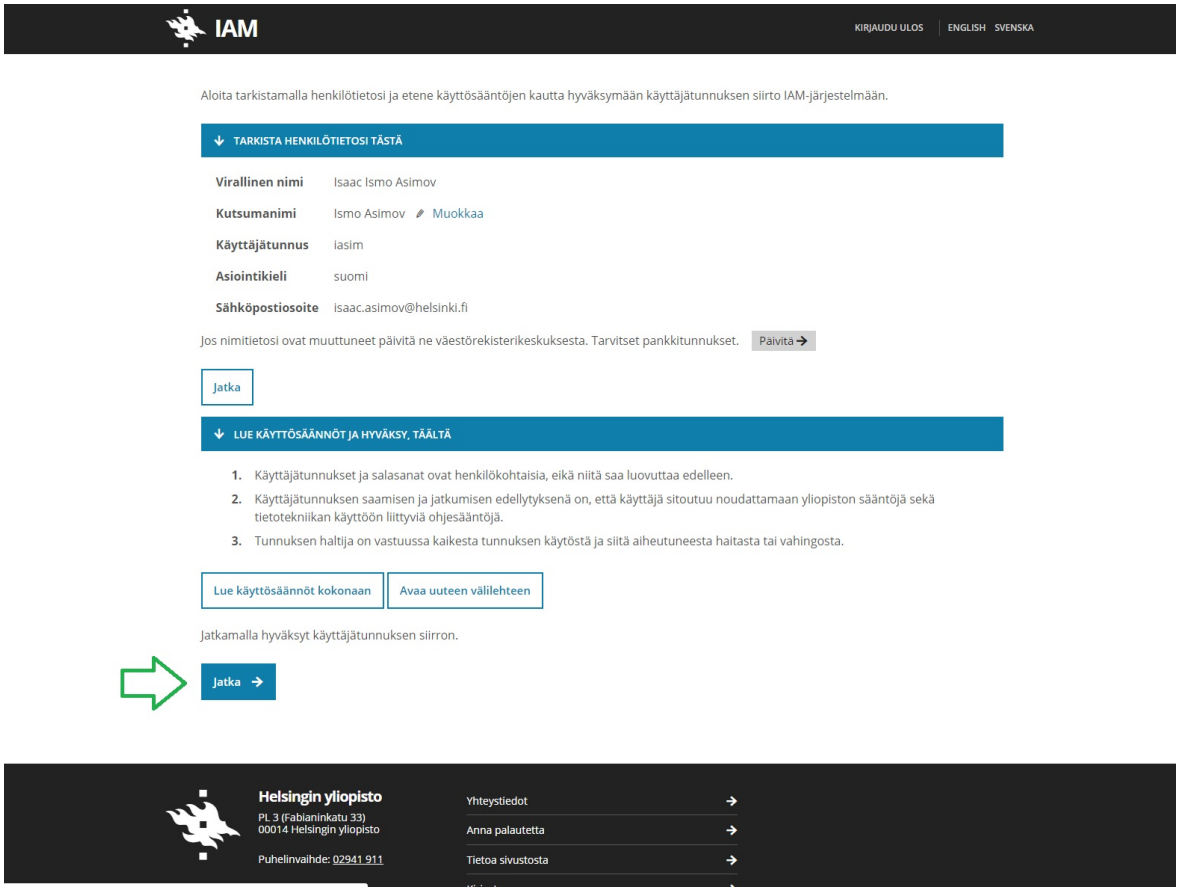


Kuva 51. Käyttösäännöt voi avata modaali-ikkunaan tai toiseen välilehteen.

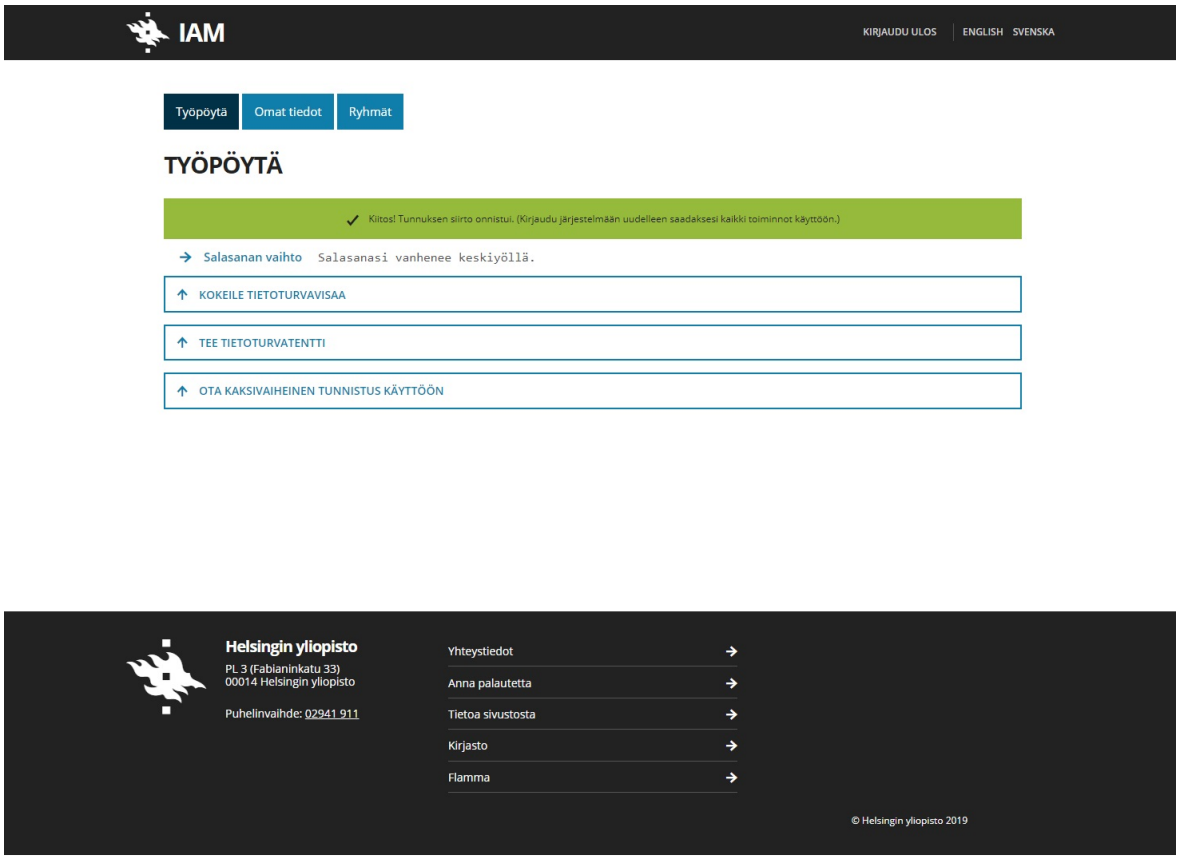


Kuva 52. Vanhat käyttösäännöt.

Kuva 53. Käyttösääntöjen lopussa on ylimääräinen ”Sulje”-painike selkeyden vuoksi.

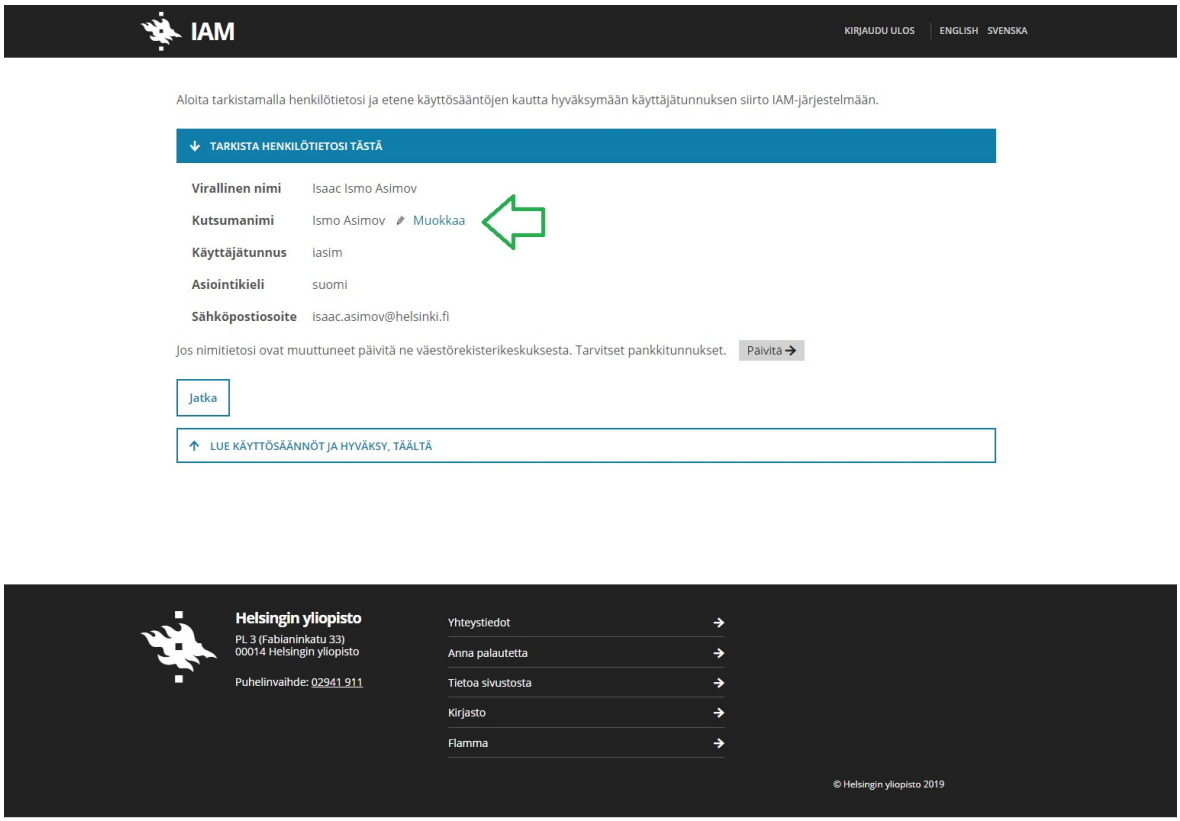


Kuva 54. ”Jatka”-painike viimeistelee tunnuksen siirron.

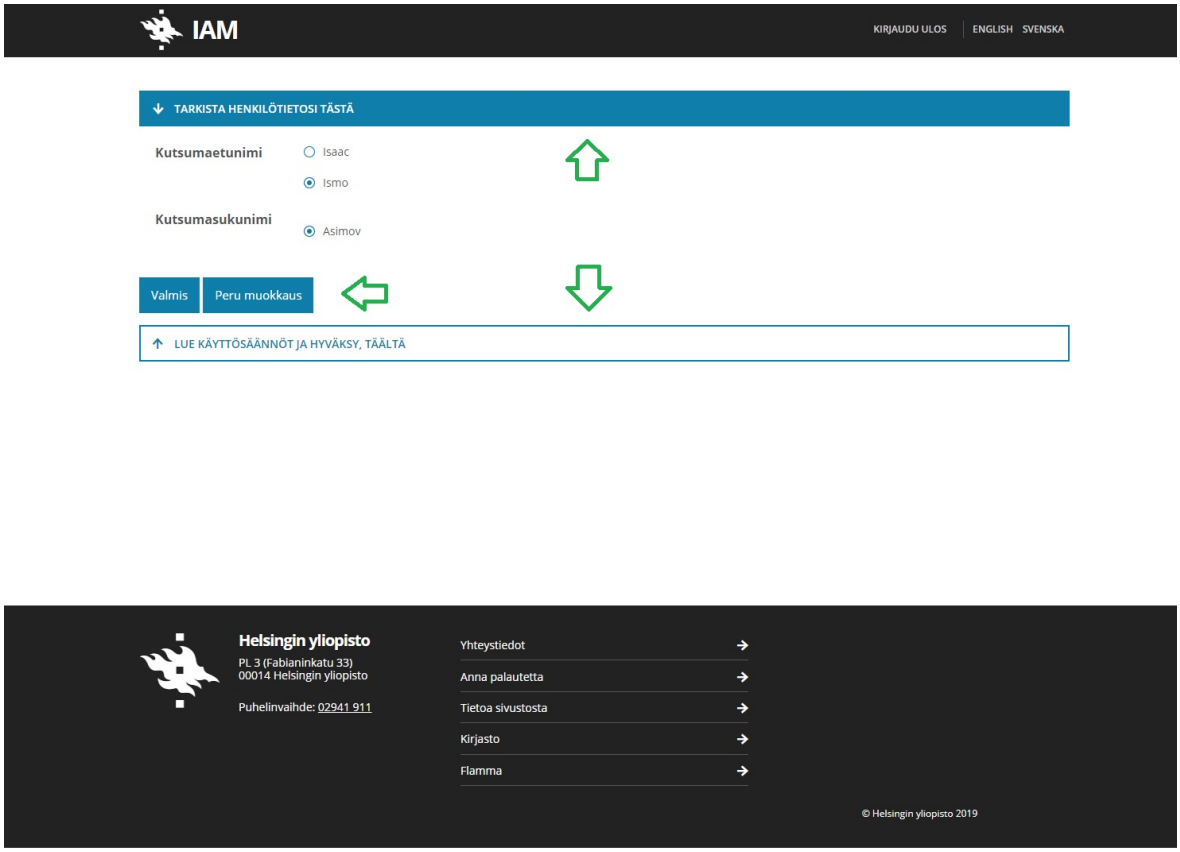


Kuva 55. Viimeinen sivu. Ylärivin elementit tulevat näkyviin.

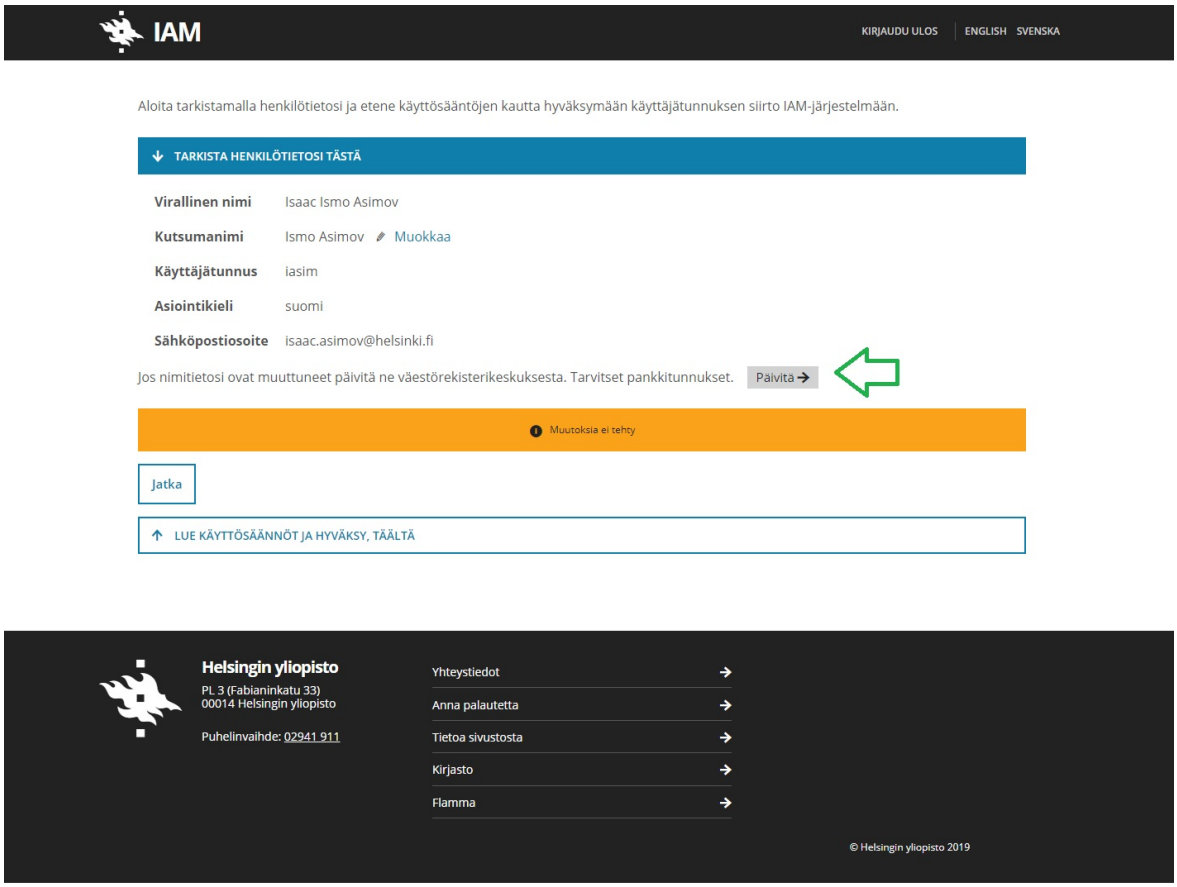
Liite 9. Käyttöliittymäsuunnitelman versio 9, tietojen päivittäminen.



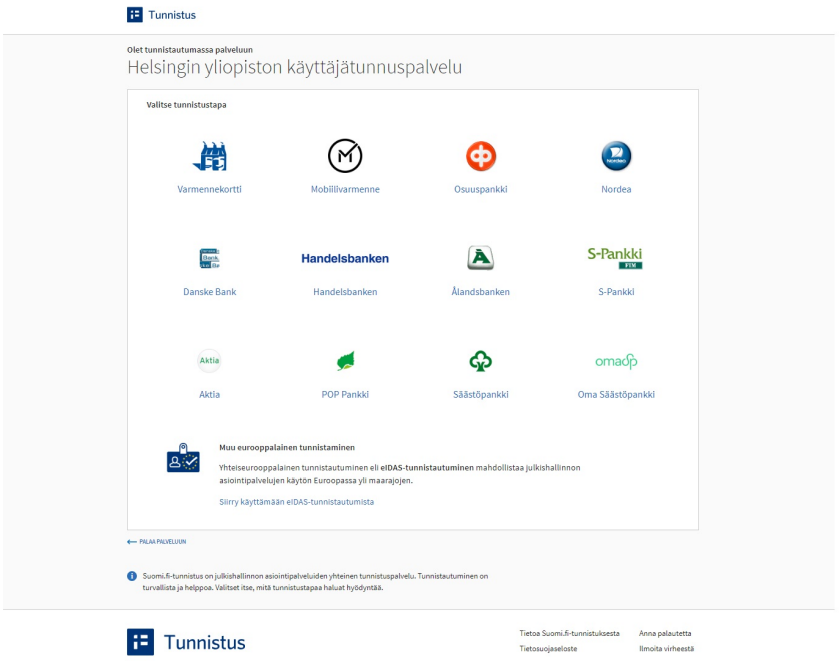
Kuva 56. Käyttäjä tarkistaa ”Muokkaa”-linkin.



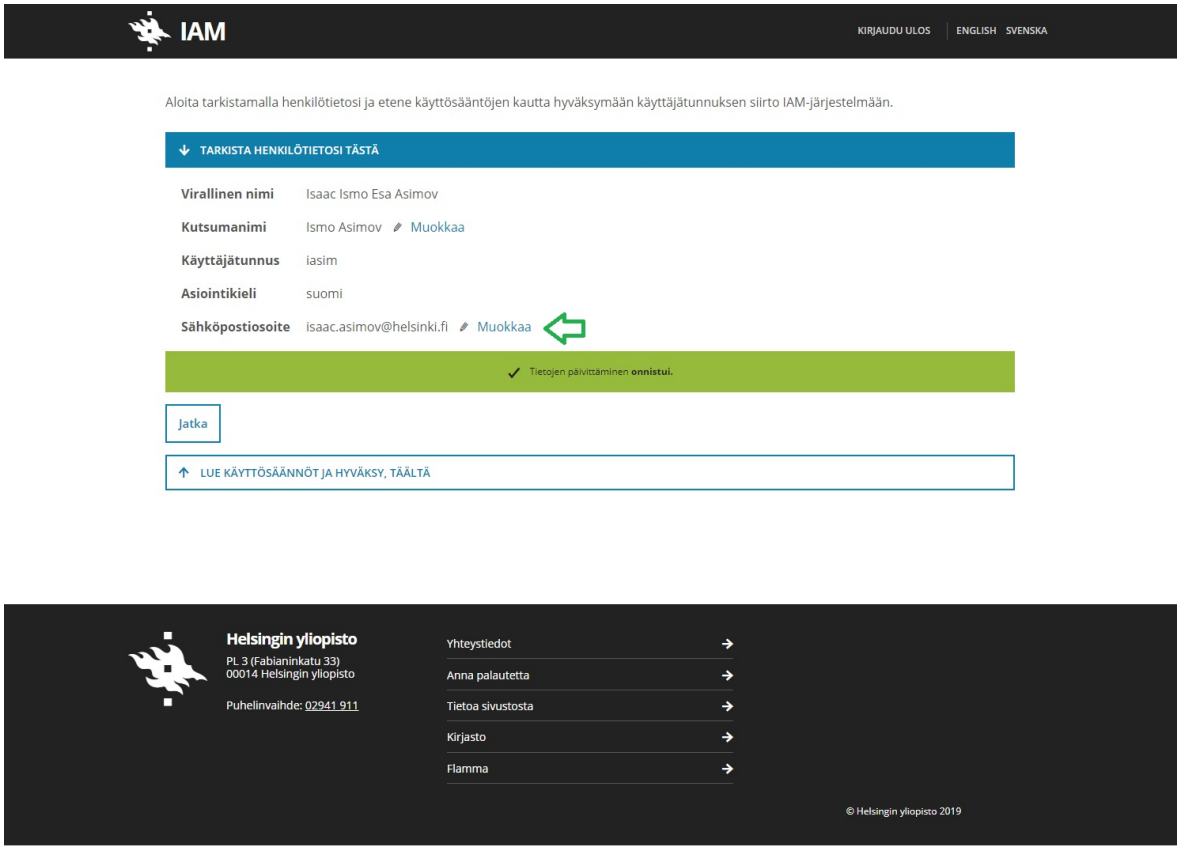
Kuva 57. ”Peru”-painike ja haitarielementtien klikkaaminen tuottavat saman lopputuloksen.



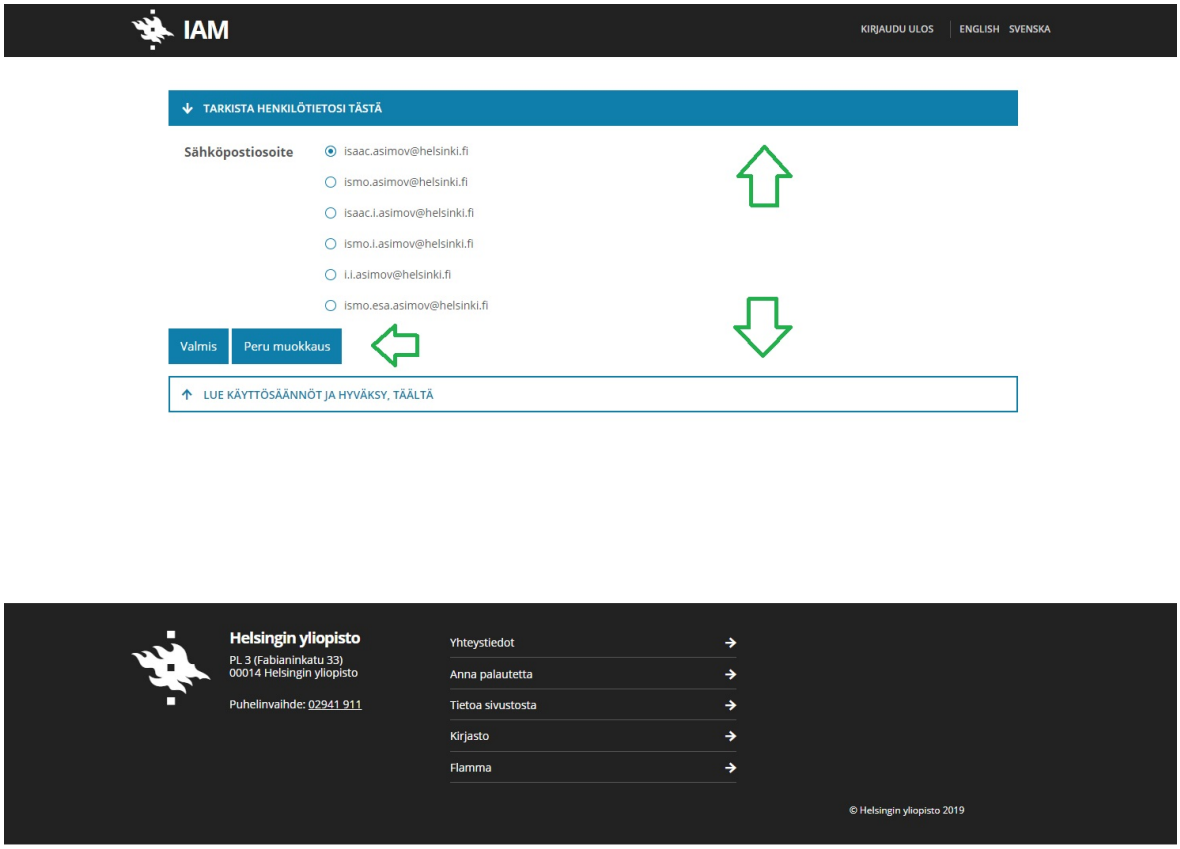
Kuva 58. Haitarielementin klikkaaminen palaa edelliseen näkymään ja näyttää huomautuksen. ”Päivitä”-painike on siirtynyt oikealle.



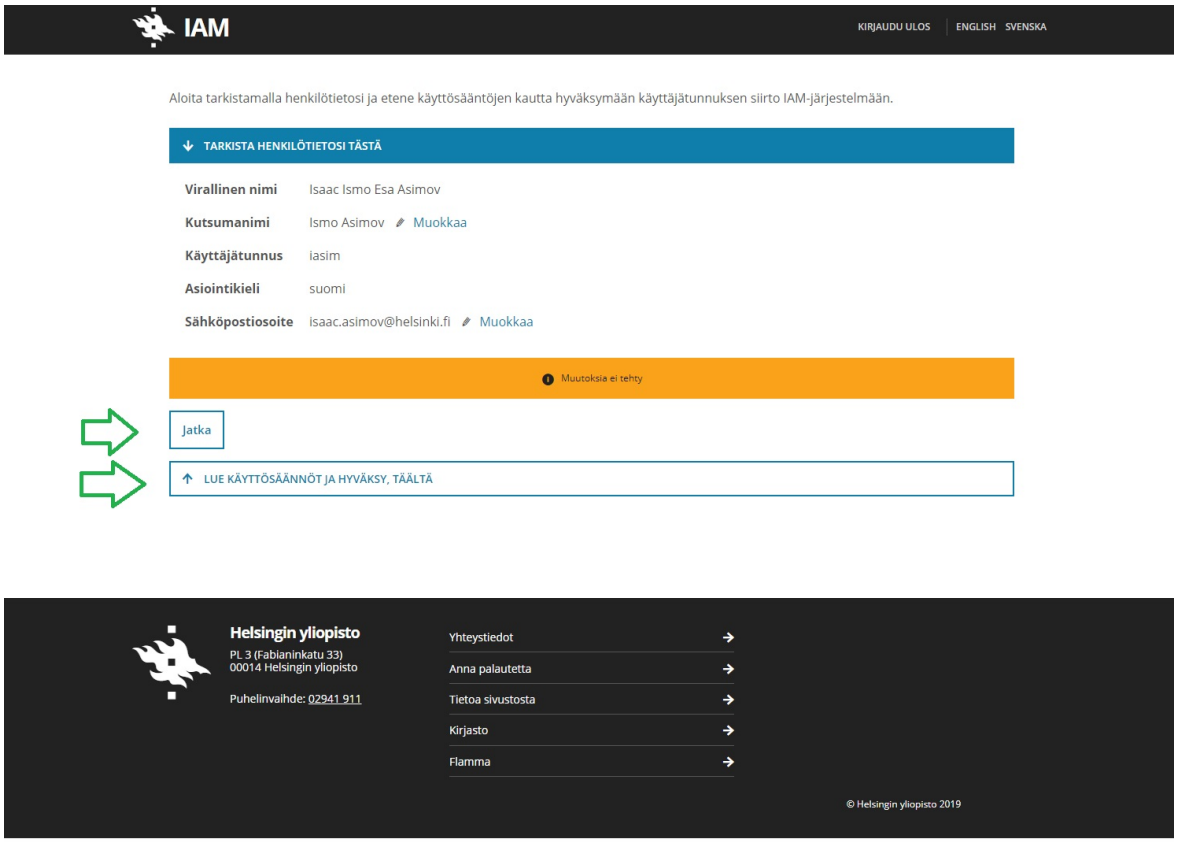
Kuva 59. Käyttäjä klikkaa mitä tahansa.



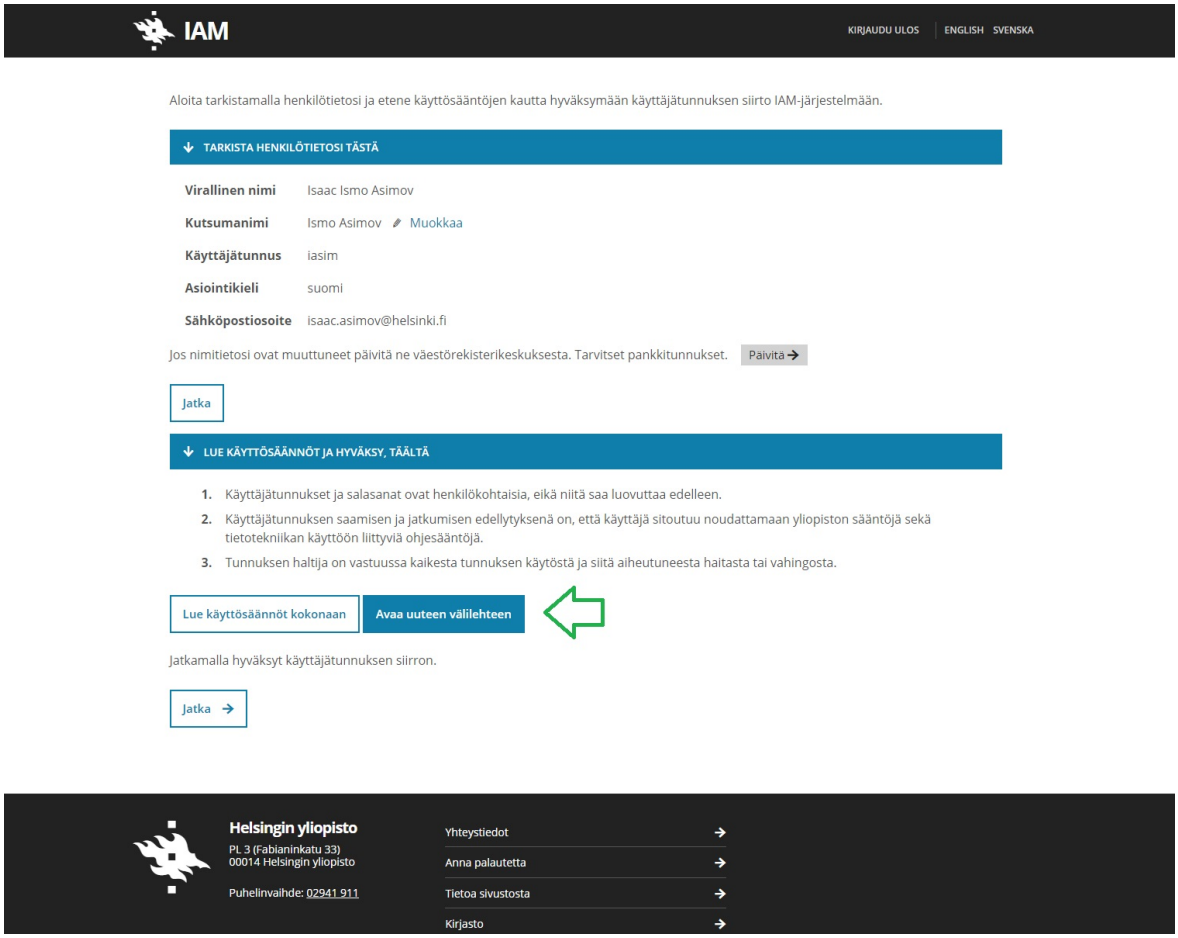
Kuva 60. Näytetään ilmoitus tietojen päivittymisestä. Tarkistetaan mahdolliset sähköpostit.



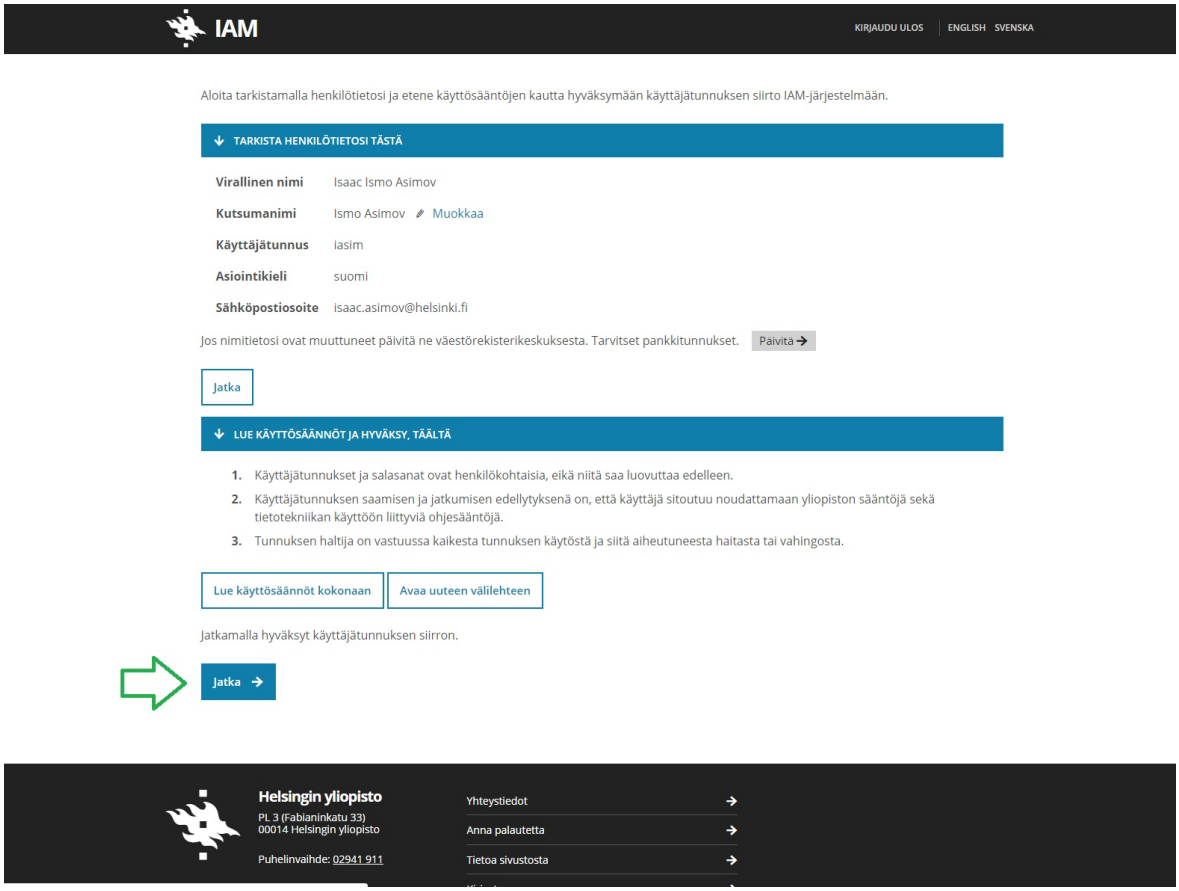
Kuva 61. Käyttäjä voi tässä yhteydessä muuttaa sähköpostiosoitteensa.



Kuva 62. Huomautus näytetään taas, jos asianmukaista painiketta ei valittu. Ylimääräinen ”Jatka”-painike avaa seuraavan haitarielementin.



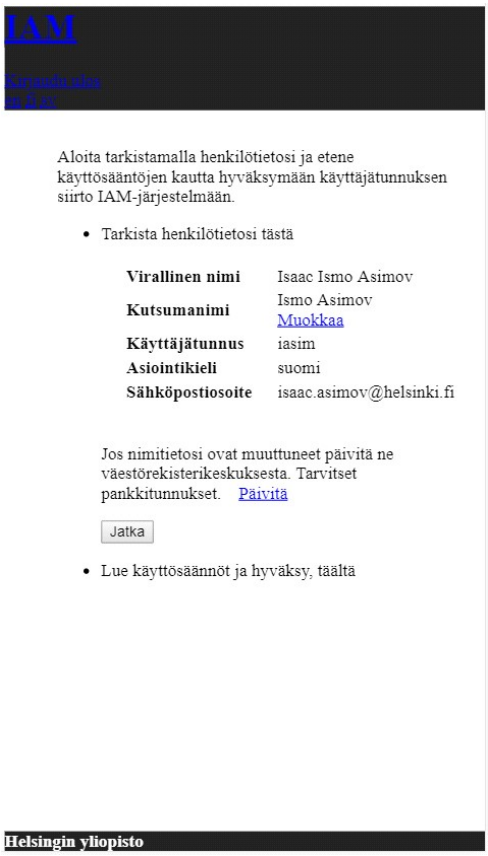
Kuva 63. Käyttösäännöt luetaan.

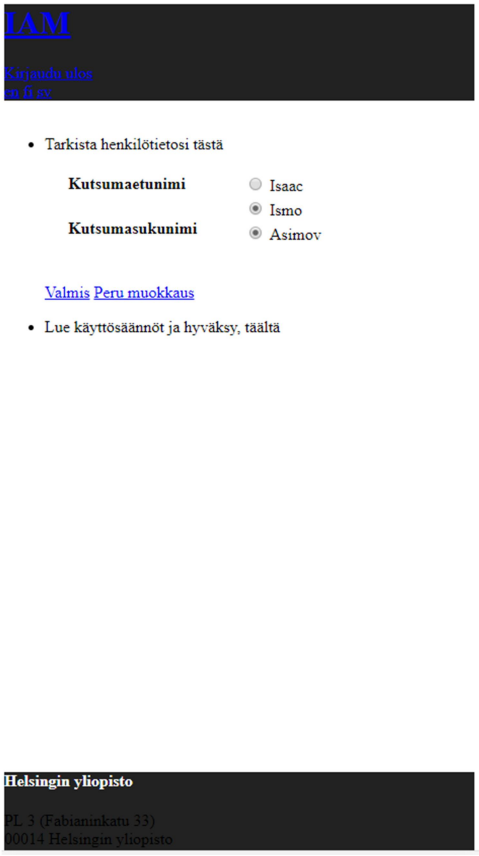


Kuva 64. ”Jatka”-painike viimeistelee tunnuksen siirron.

Liite 10. Käyttöliittymäsuunnitelman versio 9, riisuttu, mobiili.

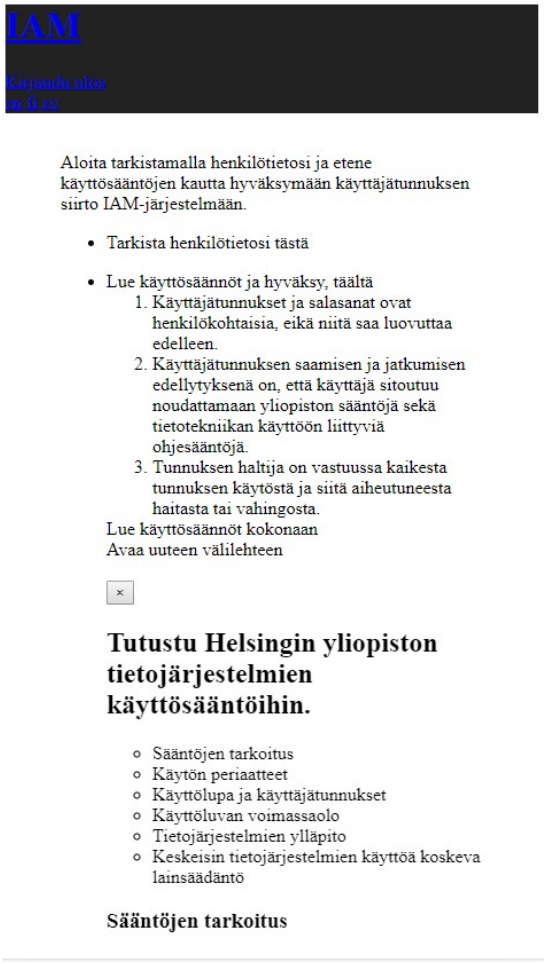
Kuva 65. Käyttöliittymään lisättiin nappeja.

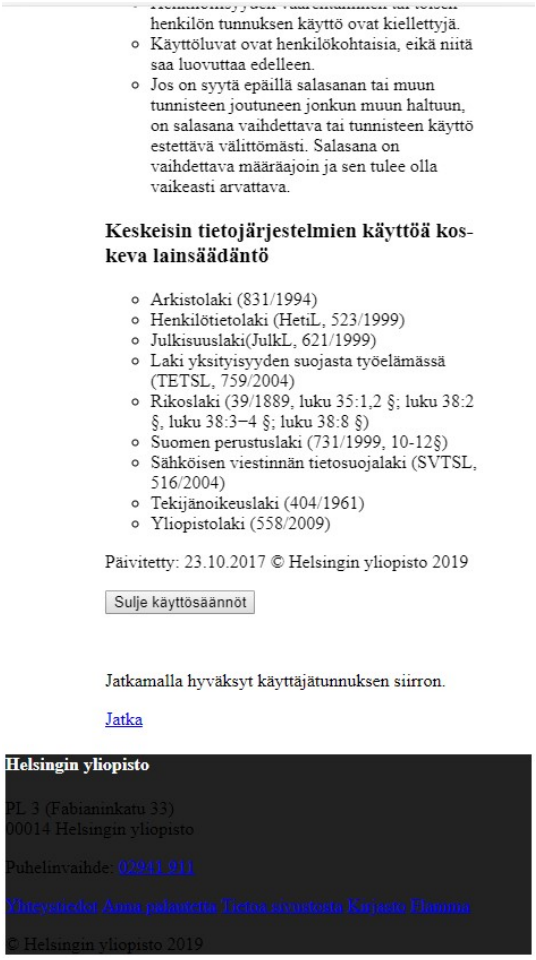




Kuva 66. Oikealla.

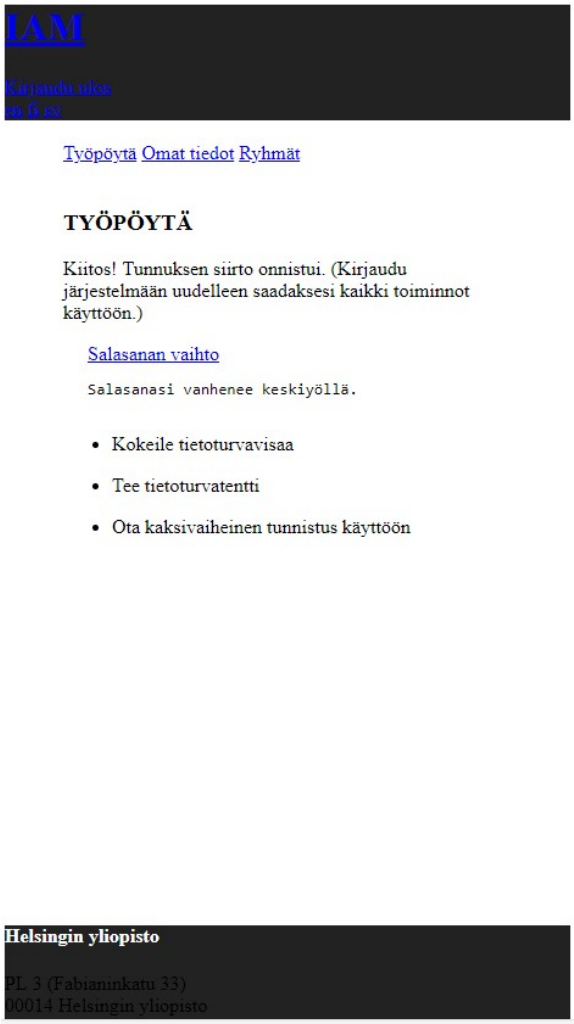
Kuva 67.





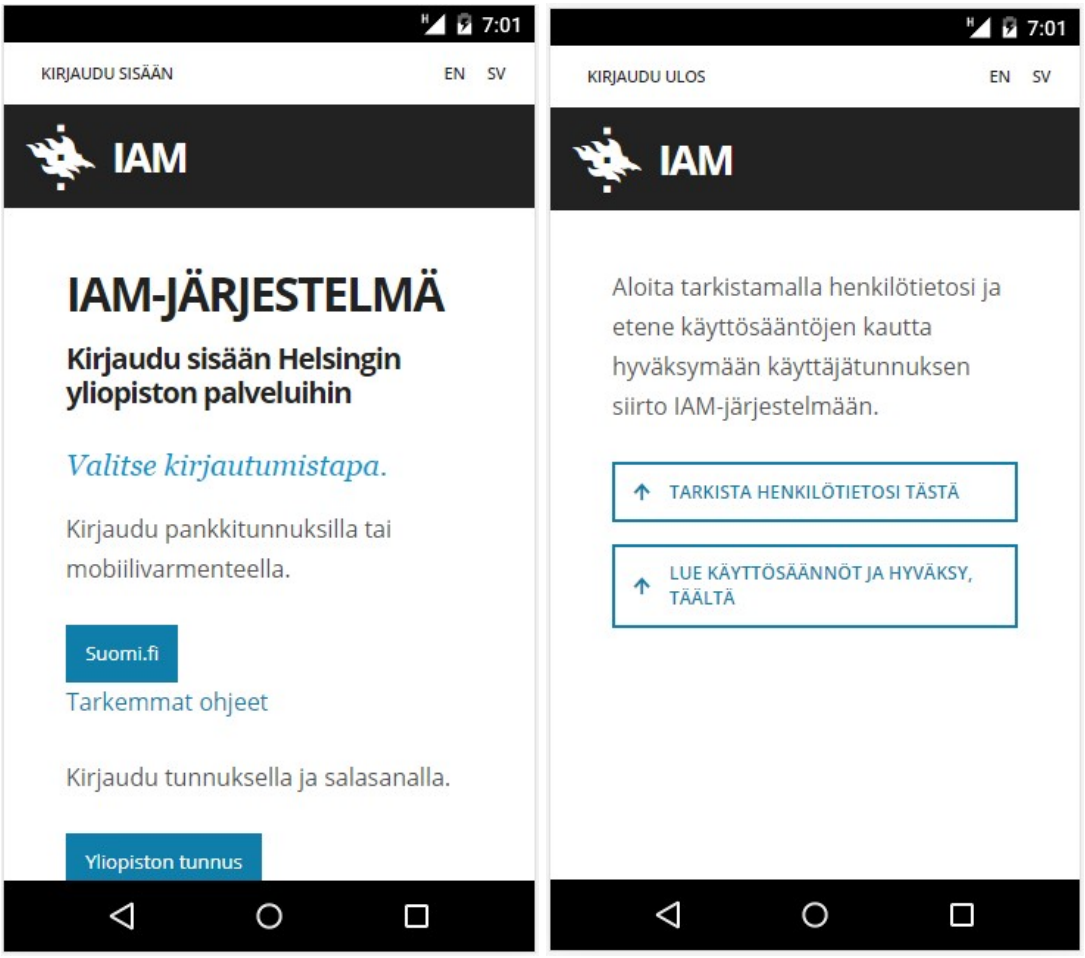
Kuva 68. Oikealla. Vanhat käyttösäännöt.

Kuva 69.


IAM
Kirjaudu ulos
en fi sv
Työpöytä Omat tiedot Ryhmät
TYÖPÖYTÄ
Kiitos! Tunnuksen siirto onnistui. (Kirjaudu järjestelmään uudelleen saadaksesi kaikki toiminnot käyttöön.)
Salasanan vaihto
Salasanasi vanhenee keskiyöllä.
Kokeile tietoturvavisaa
Tee tietoturvatentti
Ota kaksivaiheinen tunnistus käyttöön
Helsingin yliopisto
PL 3 (Fabianinkatu 33)
00014 Helsingin yliopisto

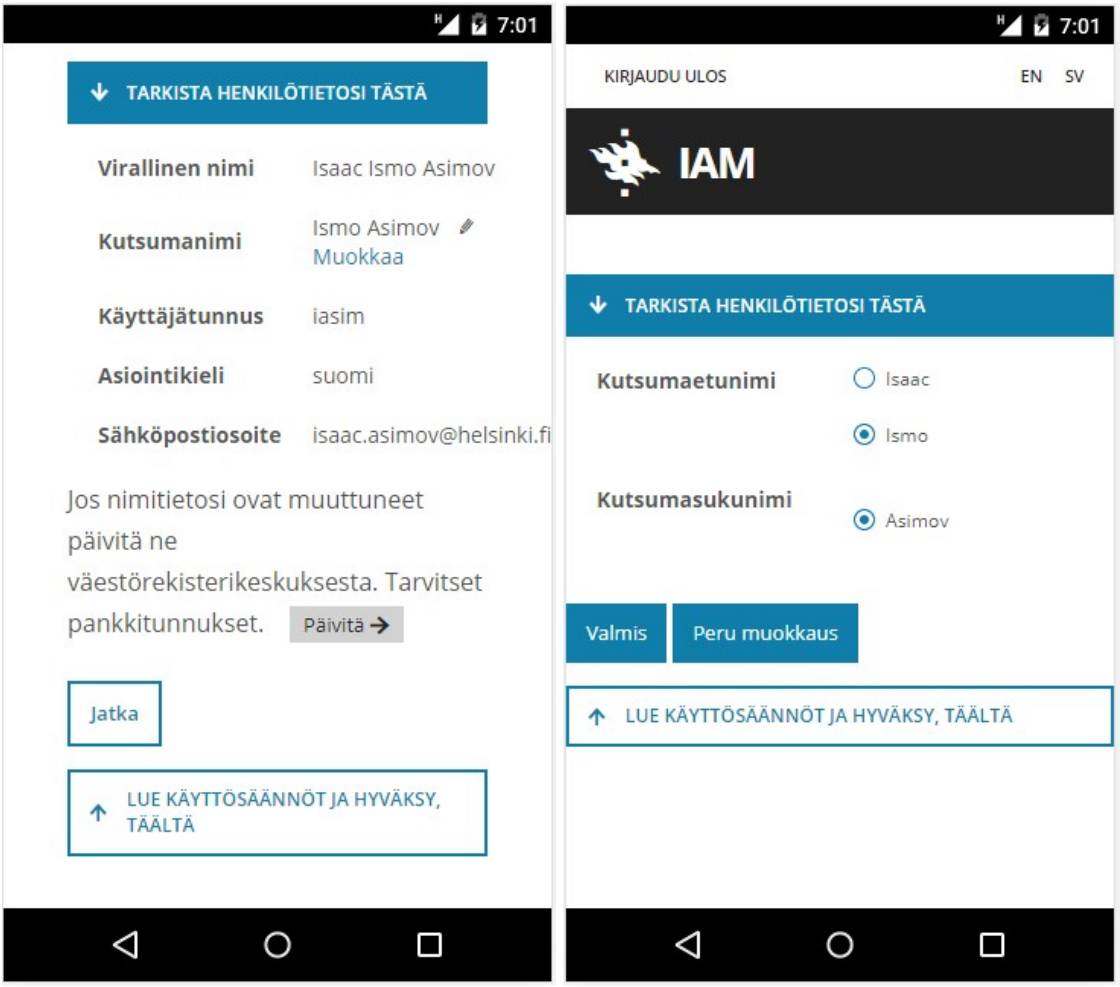
Liite 11. Käyttöliittymäsuunnitelman versio 9, mobiili.

Kuva 70. Kirjautuminen.



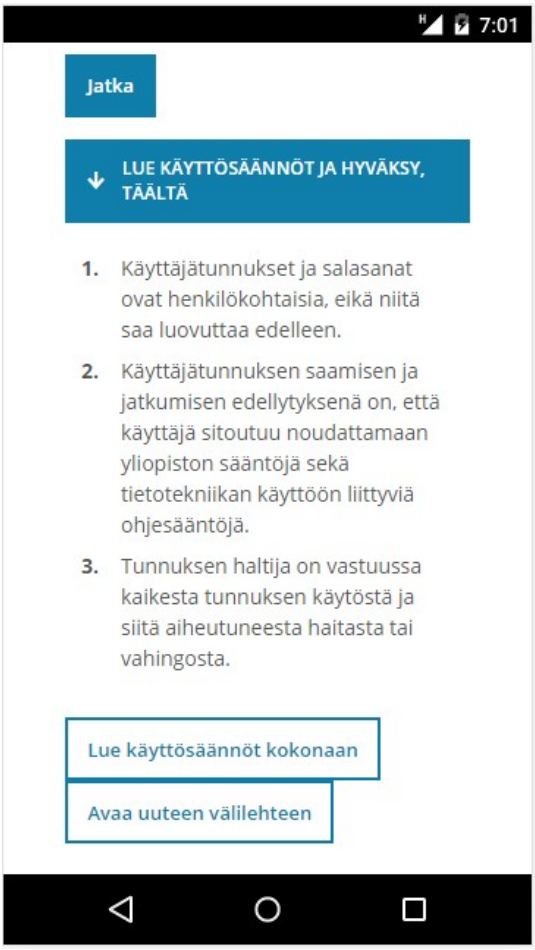
Kuva 71. Oikealla. Vaihtoehtoinen aloitusnäkymä 1.

Kuva 72. Vaihtoehtoinen aloitusnäkymä 2.



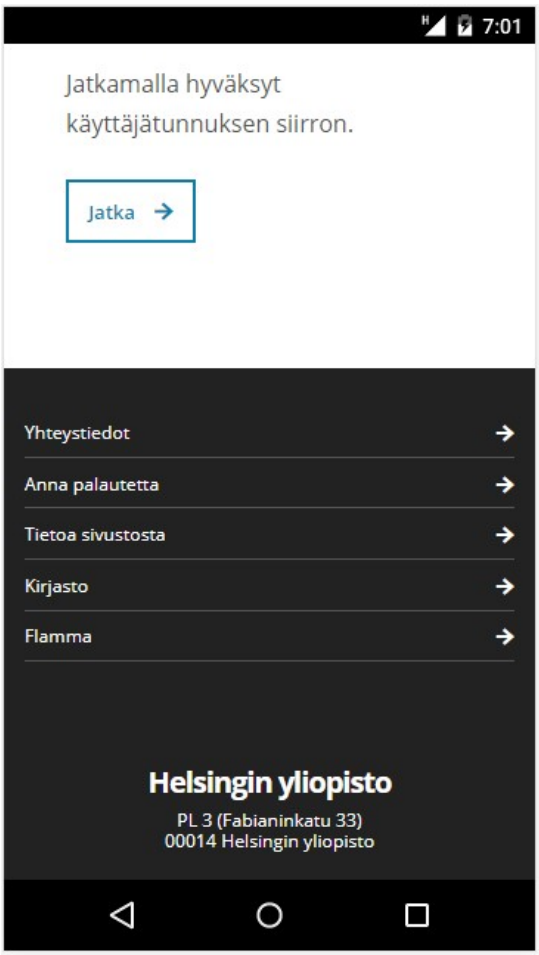
Kuva 73. Oikealla.

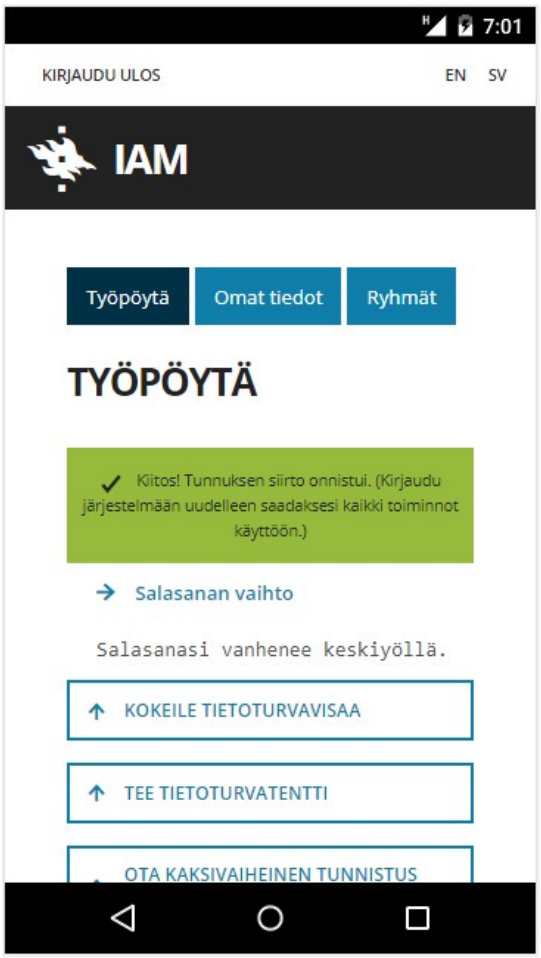
Kuva 74.



Kuva 75. Oikealla.

Kuva 76.





Kuva 77. Oikealla.

Liite 12. Käyttötapaukset.

Taulukko C. Käyttötapaukset taulukko.

Käyttötapaus	Käyttötapauksen kuvaus
Case 1A	Käyttäjän tiedoissa ei ole tapahtunut muutoksia.
Case 1B	Käyttäjän tiedoissa ei ole tapahtunut muutoksia. Suomi.fi -palvelun käyttö ei ole mahdollista.
Case 1C	Käyttäjän tiedoissa ei ole tapahtunut muutoksia. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan.
Case 1D	Käyttäjän tiedoissa ei ole tapahtunut muutoksia. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan. ID Point -tunnistaminen ei ole käytettävissä.
Case 2A	Käyttäjän nimitiedoissa on muutos.
Case 2B	Käyttäjän nimitiedoissa on muutos. Suomi.fi -palvelun käyttö ei ole mahdollista.
Case 2C	Käyttäjän nimitiedoissa on muutos. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan.
Case 2D	Käyttäjän nimitiedoissa on muutos. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan. ID Point -tunnistaminen ei ole käytettävissä.
Case 3A	Käyttäjä on saanut uuden henkilötunnuksen.
Case 3B	Käyttäjä on saanut uuden henkilötunnuksen. Suomi.fi -palvelun käyttö ei ole mahdollista.
Case 3C	Käyttäjä on saanut uuden henkilötunnuksen. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan.
Case 3D	Käyttäjä on saanut uuden henkilötunnuksen. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan. ID Point -tunnistaminen ei ole käytettävissä.
Case 4A	Henkilötunnus puuttuu.
Case 4B	Henkilötunnus puuttuu. Suomi.fi -palvelun käyttö ei ole mahdollista.
Case 4C	Henkilötunnus puuttuu. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan.
Case 4D	Henkilötunnus puuttuu. Suomi.fi -palvelun käyttö ei ole mahdollista. Käyttäjä on menettänyt käyttäjätunnuksensa hallinnan. ID Point -tunnistaminen ei ole käytettävissä.

Liite 13. Käyttötapauksien riskimatriisi.

Taulukko E. Käyttötapausten riskimatriisi. Taulukon kuvaus on luvussa 3.3.

Käyttötapaus/ Riskitekijä	Suomi.fi	Käyttäjätunnus ja salasana	ID Point - tunnistaminen	Riski pa-himmillaan
Case 1A / (+0)	palvelu alhaalla (+1)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+3
Case 1B / (+1)	palvelu alhaalla (+0)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+3
Case 1C / (+2)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+1)	+3
Case 1D / (+3)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+0)	+3
Case 2A / (+1)	palvelu alhaalla (+1)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+4
Case 2B / (+2)	palvelu alhaalla (+0)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+4
Case 2C / (+3)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+1)	+4
Case 2D / (+4)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+0)	+4
Case 3A / (+1)	palvelu alhaalla (+1)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+4
Case 3B / (+2)	palvelu alhaalla (+0)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+4
Case 3C / (+3)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+1)	+4
Case 3D / (+4)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+0)	+4
Case 4A / (+1)	palvelu alhaalla (+0)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+3
Case 4B / (+1)	palvelu alhaalla (+0)	palvelu alhaalla (+1)	palvelu estynyt (+1)	+3
Case 4C / (+2)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+1)	+3
Case 4D / (+3)	palvelu alhaalla (+0)	palvelu alhaalla (+0)	palvelu estynyt (+0)	+3

Liite 14. Käyttötapauksien ja tunnistamisen riskimatriisi.

Taulukko F. *Hybridisodassa* voidaan käyttää vastaavia menetelmiä. Tämä on taidetta.

Käyttötapaus	Suomi.fi	Käyttäjätunnus ja salasana	ID Point - tunnistaminen	Riski pa-himmillaan
1 Case A	OK 2	OK 2	OK 1	+5
2 Case A	OK 2	OK 2	- 1	+3
3 Case A	OK 2	- 2	- 1	-1
4 Case A	- 3	- 3	- 1	-7
5 Case A	- 3	- 3	OK 1	-5
6 Case A	- 2	OK 2	OK 1	+3
7 Case A	OK 2	- 2	OK 1	+1
8 Case A	- 2	OK 2	- 1	-1
9 Case B	OK 3	OK 1	OK 2	+6
10 Case B	OK 3	OK 1	- 2	+2
11 Case B	OK 3	- 1	- 2	+0
12 Case B	- 3	- 1	- 2	-6
13 Case B	- 3	- 1	OK 2	-2
14 Case B	- 3	OK 1	OK 2	+0
15 Case B	OK 3	- 1	OK 2	+4
16 Case B	- 3	OK 1	- 2	-4
17 Case C		OK 2	OK 3	+5
18 Case C		OK 2	- 3	-1
19 Case C		- 2	OK 3	-1
20 Case C		- 3	- 3	-6
21 Case D		OK 3	OK 1	+4
22 Case D		OK 3	- 1	+2
23 Case D		- 3	OK 1	-2
24 Case D		- 3	- 2	-5