Lähiajan hankkeet käyttäjähallinnossa

Minna Harjuniemi
Tietotekniikkaosasto

Lähiajan keskeisimpinä hakkeina käyttäjähallinnossa on pankkien hyödyntämän Tupas-tekniikan käyttöönotto sekä kertakäyttösalanoja hyödyntävä tunnistautumisjärjestelmä.

Taustaa ja tavoitteita

Vuonna 2002 käynnistetty laaja kehittämishanke *HSTYA-valmistautuminen* on lähestymässä loppuaan. Vaatimukset ja menetelmät ovat muuttuneet huomattavasti siitä, mitä hanketta käynnistettäessä ajateltiin. Ensimmäisissä suunnitelmissa vahva tunnistautuminen oli etusijalla, ja budjettisuunnitelmissa varauduttiin mm. toimikorttien ja kortinlukijoiden hankintaan. Hyvin pian kävi kuitenkin ilmi, että ennen vahvan tunnistautumisen käyttöönottoa on lujitettava käyttäjähallinnon perusrakenteita. Niinpä hankkeessa keskityttiin käyttäjähakemiston ja erityisesti sen tarkemman tietosisällön luomiseen, ja hanke nimettiin uudelleen *Hakemisto*-hankkeeksi (ja edelleen *Tunnistamistekniikat*-hankkeeksi).

Vuonna 2004 toimineen käyttöoikeus- ja rooliryhmän suositusten mukaisesti eri tietojärjestelmissä pyritään hyödyntämään käyttäjähakemistoa sovelluksiin kirjautumisessa ja käyttöoikeuksien määrittelyssä. Tavoitteena on, että kaikkiin järjestelmiin pystyttäisiin kirjautumaan yhdellä tunnuksella ja salasanalla. Tässä yhteydessä puhutaan usein myös kertakirjautumisesta eli siitä, että tunnuksen ja salasanan joutuisi kirjoittamaan ainoastaan kerran työpäivänsä aluksi.

Käyttäjähakemiston kehittämisen ohella on kokeiltu Shibboleth-tekniikan hyödyntämistä monissa hankkeissa eri korkeakoulujen tarjoamissa palveluissa. Ajatus on, että yhden tunnuksen periaate voitaisiin ulottaa myös muiden korkeakoulujen järjestelmiin, vaikkapa verkko-oppimisympäristöihin tai erilaisiin ulkoisien toimijoiden sovelluksiin (esimerkiksi Fortime). Tulokset ovat olleet varsin rohkaisevia, ja tekniikan hyödyntämistä on kokeiltu tietotekniikkaosastolla myös yliopiston omien tietojärjestelmien pääsynvalvonnassa. Tästä esimerkkinä on tuleva ohjelmistojakelu.

Vahvaa tunnistautumista

Käyttäjähakemistoa hyödynnetään yliopiston sisällä monissa järjestelmissä, ja sen käyttö on lisääntymässä. Shibboleth-tekniikkaa käyttäviä palveluita on kehitetty ja niitä on valmistamassa lisää. Ollaan siis lähestymässä ”yksi tunnus, yksi salasana” -periaatetta, jossa käyttäjällä ei ole enää muistettavanaan pitkää listaa tunnuksia ja salasanoja.

Kertakirjautumisjärjestelyitä on rakennettu jonkin verran, ja esimerkiksi Almasta pääsee vaikkapa sähköpostiin ja käyttölupatyökaluihin ilman uutta kirjautumista. Hyvään tavoitteeseen liittyy kuitenkin riskinsä. Jos salasana joutuu vääriin käsiin tai selaimeen on jäänyt yhteys auki, voi mahdollinen väärinkäyttäjä saada aikaan paljon vahinkoa. Vähintään hän pääsee tietoihin, joita omistaja ei soisi muiden käsiin päätyvän. On siis aika palata kehityshankkeen alkuperäisille juurille, eli vahvaan tunnistamiseen. Näin

pyritään minimoimaan edellä mainitut riskit. Vahvaa tunnistamista kokeillaan sekä Shibboleth-tekniikkaan liitettynä että yksittäisissä palveluissa.

Tietotekniikkaosasto toteuttaa tänä vuonna osin Tieteen tietotekniikan keskuksen CSC:n rahoituksella kokeiluhankkeen, jossa tutkitaan vahvan tunnistuksen liittämistä Shibboleth-yhteyskäytäntöön. Tutkittavina tunnistusmenetelminä ovat ainakin pankkien kertakäyttösalasanoihin liittyvä Tupas-järjestelmä ja toimikorteilla olevat varmenteet sekä mahdollisesti myös mobiilivarmenteet. Jos, tai pikemminkin kun, tulokset osoittavat integroinnin mahdolliseksi, saatetaan tulevaisuudessa joissakin kriittisimmissä palveluissa edellyttää nimenomaan vahvaa tunnistautumista.

Atk-yhdyshenkilöitä ja käyttölupaneuvojia työllistävät varsin paljon unohtuneet salasanat. Tällä hetkellä käyttäjän on käytävä tunnistautumassa henkilökohtaisesti joko yhdyshenkilön luona tai käyttölupapisteissä saadakseen uuden salasanan. Tupas-tunnistautumisen avulla mahdollistetaan se, että käyttäjä voi itse vaihtaa unohtuneen salasanansa. Tämä toki edellyttää, että käyttäjällä on suomalainen henkilötunnus ja käytössään Tupas-palvelua tarjoavan pankin kertakäyttösalasanat.

Ajatuksena on, että Tupas-tekniikkaa hyödynnettäisiin myös uusien käyttölupien jaossa. Tupas-tunnistuksella tehty käyttölupasitoumuksen sähköinen allekirjoitus on juridisesti pätevä, ja tämä vähentäisi paperilomakkeiden käsittelyä. Toteutusaikataulu ei tältä osin ole varmistunut, eli vielä ei ole tiedossa, saadaanko järjestely käyttöön jo ensi syksynä uusien opiskelijoiden lupien jaossa.

Omia kertakäyttösalasanoja

Julkisia WWW-kioskeja käyttävät joutuvat aina arvioimaan käyttöön liittyvät riskit. Vaarana on, että työasemassa on jokin salasanoja ja käyttäjätunnuksia keräävä ohjelma. Tällaisissa tilanteissa on usein toivottu mahdollisuutta käyttää kertakäyttösalasanoja Tupas-tekniikan tapaan. Yhtenä ongelmana on se, että Tupas-käyttö edellyttää suomalaista henkilötunnusta, eli aivan kaikkiin tarpeisiin tekniikka ei ole riittävä. Jokainen Tupas-tunnistustapahtuma maksaa yliopistolle jonkin verran, joten toistuvaan käyttöön se ei ole hyvä ratkaisu. Ajatuksena onkin, että kehitetään tällaisiin erityistarpeisiin soveltuva yliopiston oma kertakäyttösalasanajärjestelmä. Tämä on tarkoitus ottaa käyttöön syksyllä 2006.

Käyttäjien roolitietojen määrittelyä jatketaan yliopistossa yhteistyössä henkilöstö- ja kehittämisosastojen kanssa ja myös kansallisella tasolla (ns. funetEduPerson-skeema). Melko yleisluontoisten ”henkilökunta” ja ”opiskelija” -roolien lisäksi yliopistolla on käytössä useita erityisrooleja, kuten atk-yhdyshenkilö, laskujen hyväksyjä tai henkilöesimies. Näiden hallintaa halutaan keskittää ja siihen halutaan lisää automatiikkaa. Ainakin osa roolihallinnasta tullaan toteuttamaan organisaatiorekisterin avulla.

Kertakirjautumisen edistämiseksi tietotekniikkaosastolla harkitaan myös jonkin tikettipohjaisen järjestelmän käyttöönottoa WWW-palveluissa. Vahvimpana ehdokkaana on tällä hetkellä alun perin Yalen yliopistossa kehitetty CAS, joka on sittemmin siirtynyt JA-SIG-yhteisön projektiksi.

Lopuksi

Käyttäjätunnistukseen ja sähköiseen asiointiin liittyvät projektit ovat usein erittäin kiinnostavia ja kiitollisia. Uudet tekniikat ovat mielenkiintoisia ja ne avaavat uusia mahdollisuuksia verkkopalveluiden kehittämisessä. Myös käyttäjät ovat pääsääntöisesti

tyytyväisiä toiminnan helpottuessa. Kehitystyössä ei kuitenkaan voi jäädä lepäämään laakereilleen, ja kehittämisessä tarvitaan edelleenkin sekä palveluiden käyttäjien että ylläpitäjien yhteistyötä ja työpanosta.

Lisätietoa

Minna.Harjuniemi@helsinki.fi
Tupas, *http://www.pankkiyhdistys.fi/sisalto/upload/pdf/tupasV21.pdf*
CSC:n hankkeet, *http://www.csc.fi/suomi/funet/middleware/projektit/index.phtml*
CAS, *http://www.ja-sig.org/products/cas/*