

## **SHAMAN-sovellusprojektin 1. workshop**

Aika: Maanantai 14.2.2005 klo 9.15 – 12.05

Paikka: Ag C223.1

Läsnä:

- Marko Andersson, puheenjohtaja
- Matti Törmä, 2. sihteeri
- Timo Valonen, 1. sihteeri
- Jukka-Pekka Santanen (saapui 9.20, poistui 11.55)
- Lassi Paavolainen
- Tero Toivonen
- Matti Levänen
- Sauli Takkinen (poistui 10.20)
- Seppo Kallio, Sähköpostijärjestelmät
- Tapani Tarvainen, Sähköpostijärjestelmät (poistui 9.45)
- Tuomas Kautto, UNIX-järjestelmät
- Mika Videnoja, UNIX-järjestelmät (poistui 11.50)
- Mika Mattila, Mikroverkot (poistui 10.45)

### ***Pöytäkirja***

#### **1. Workshopin aloitus**

Workshopin aloitti puheenjohtajana toiminut Marko Andersson klo 9.20. Puheenjohtaja pyysi lupaa saada nauhoittaa workshopissa käsitellyt asiat myöhempää tarkistusta varten. Osallistujat hyväksyivät nauhoituksen.

## **2. Paikallaolijat**

Paikallaolijat esittäytyivät pikaisesti toisilleen. Paikalla oli projektiryhmästä Marko Andersson, Matti Törmä ja Timo Valonen. Mika Rinkinen oli poissa sairauden takia. Tietotekniikan laitokselta paikalla olivat tekninen ohjaaja Lassi Paavolainen sekä projektin ohjaaja Jukka-Pekka Santanen. Tilaaajan edustajista paikalla olivat Matti Levänen sekä Tero Toivonen.

Sähköpostijärjestelmien asiantuntijoista paikalla olivat Seppo Kallio sekä Tapani Tarvainen.

UNIX-järjestelmien asiantuntijoista paikalla olivat Tuomas Kautto sekä Mika Videnoja.

Mika Mattila edusti mikroverkkojen asiantuntijoita.

## **3. Workshopin sisältöä**

### **3.1 Tunnukset**

Useista samalle henkilölle kuuluvista tunnuksista olisi päästävä eroon pitkällä aikavälillä, sillä useat eri tunnukset hankaloittavat ylläpitoa. Tällä hetkellä kuitenkin uuden AMAN-järjestelmän on tuettava useita tunnuksia, sillä niitä löytyy runsaasti vanhoista järjestelmistä.

Ideaalitilanteessa jokaisella käyttäjällä olisi vain yksi tunnus, ja käyttöoikeudet määritellään itse henkilölle, eikä eri käyttäjätunnuksille.

### **3.2 Ryhmät**

Uuteen järjestelmään tulisi toteuttaa ryhmiä, jotka kuvaisivat erilaisten käyttäjien ryhmiä ja niiden oikeuksia eri palveluihin. Ryhmiä lisäämällä ja tarkentamalla olisi mahdollista luoda tarkasti määritellyt oikeudet eri henkilöille ja ryhmille. Kuuluminen tiettyyn ryhmään tuo automaattisesti ryhmän oikeudet yksittäiselle ryhmän jäsenelle. Yksittäinen käyttäjä on myös itse ryhmä, joten käyttäjäkohtaisia oikeuksia voidaan myös hallita ryhmien avulla. Tämä selkeyttää oikeuksien suunnittelua, sillä erillisiä henkilökohtaisia oikeuksia ei tarvita vaan kaikki oikeudet voidaan määritellä ryhmien avulla.

Käyttäjän oikeudet ovat eri ryhmien oikeuksien summa. Jos käyttäjällä on henkilökohtaisia oikeuksia, ne kuuluvat vain käyttäjän omaan ryhmään, eivätkä ne koske muita eri ryhmissä olevia. Ryhmän oikeudet taas periytyvät koko ryhmälle ja jokaisella ryhmän jäsenellä on ainakin ryhmän oikeudet tiettyyn resurssiin. Ryhmään voi kuulua myös henkilöitä, joilla on erityisoikeuksia joihinkin resursseihin, nämä oikeudet eivät

koske muita ryhmässä olevia.

Ryhmät voivat olla myös rooleja, joita voidaan määritellä käyttäjille ja jotka voidaan siirtää käyttäjien kesken helposti. Tällaisia ovat esimerkiksi erilaiset virat, jolloin voidaan määritellä tietylle henkilölle viran tuoma rooli. Henkilön lopettaessa virassa voidaan rooli siirtää toiselle henkilölle, joka perii kaikki ensimmäisen käyttäjän oikeudet ja dokumentit. Rooleilla voisi myös olla omia sähköpostiosoitteita, jotka ohjautuvat henkilölle, jolla on kyseinen rooli.

Ryhmät voidaan esittää verkkona, jolloin kaikki ryhmät kuuluvat samaan yliryhmään, esimerkiksi "käyttäjä", josta voidaan periä ryhmät "opiskelija" ja "työntekijä". Yksittäinen käyttäjä voi kuulua useampaan ryhmään. Esimerkiksi opiskelija, joka myös opettaa yliopistolla voi kuulua kumpaankin em. ryhmään.

Ryhmien oikeuksia määriteltäessä on pyrittävä antamaan ylemmille ryhmille mahdollisimman vähän oikeuksia, jotka periytyisivät koko ryhmälle. Sen sijaan oikeuksien jakamista on keskitettävä pienemmille ryhmille, jolloin erilaisten yhdistelmien hallinta on helpompaa.

Ryhmä voi olla myös kurssi, tai osa kurssia, jolloin kurssilla oleville opiskelijoille voidaan antaa jokin erityisoikeus kurssin ajaksi.

Ryhmille voidaan myös määritellä quotat, jolloin kaikki ryhmän jäsenet saavat saman quotamäärän.

Ryhmien avulla on myös mahdollista toteuttaa erilaisia rajoitettuja oikeuksia esimerkiksi kesäopiskelijoille, joilla on vain pääsy päätteille, muttei sähköpostilaatikkaa tai kotisivutilaa.

### **3.3 Järjestelmän tiedot**

Järjestelmän tulisi sisältää mahdollisimman abstraktia tietoa, jotta tulevaisuudessa tietokantaa tai sen tietoja ei tarvitse muuttaa, jos kohdejärjestelmien toteutustavat muuttuvat. Tämä tulee esille esimerkiksi erilaisten UNIX- ja LDAP-järjestelmien attribuuteissa.

### **3.4 Tietojen lisäys**

AMAN-järjestelmä saa tiedot käyttäjistä Fortime-, Jore-, Acta-, sekä Korppi-järjestelmiltä. Järjestelmistä tuleva tieto ei välttämättä ole oikeaa, sillä kenttien vapaasta

muokkauksesta on seurannut epäyhtenäinen nimeämistapa esimerkiksi laitosten nimissä. Uuden järjestelmän tulee sisältää vain yksikäsitteistä tietoa, joten tiedon lisäys vaiheessa on tietojen oikeellisuus tarkastettava. Erilaisia laitosten nimiä voidaan konvertoida valmiiden listojen avulla. Jos järjestelmä ei osaa päätellä, mihin kategoriaan tieto kuuluu, on se siirrettävä odottamaan ylläpitäjän toimenpiteitä.

Myös järjestelmässä jo olevien käyttäjien päivittäminen vaillinaisin tai väärillä tiedoilla pitää olla mahdollista. Esimerkiksi ulkomaalaisten opiskelijoiden henkilötunnus muuttuu usein ja on monissa tapauksissa väärä. Myös heidän nimensä kirjoitetaan usein väärin. Näissä tapauksissa jos järjestelmä epäilee, että tietokannassa on jo tunnus ko. opiskelijalle, on lisäys vähintään laitettava odottamaan ylläpidon toimenpiteitä. Jos on todennäköistä, että lisättävä tieto kuuluu jo järjestelmässä olevalle, voidaan se muokata suoraan järjestelmään (esimerkiksi jos nimessä on kirjoitusvirhe). Uuden tunnuksen lisäys täytyy tapahtua vain, jos ollaan varmoja, ettei henkilöllä ole ole jo tunnusta järjestelmässä.

Korpista voidaan myös välittää tietoa, mille kurssille käyttäjä kuuluu, jolloin käyttäjälle voidaan automaattisesti lisätä ko. kurssin oikeudet.

Tietoja voidaan myös lisätä käyttämällä siirtotiedostoja, joita voidaan ajaa suoraan käyttöliittymän kautta.

### **3.5 Sähköposti**

Nykyiset järjestelmät tarvitsevat tietoa, millä koneilla käyttäjien sähköpostilaatikat sijaitsevat. Koska uuteen AMAN-järjestelmään ei ole mielekästä toteuttaa sähköpostilaatikoiden ja käyttäjien kotihakemistojen luontia, on niiden tehtävät siirretty erillisille moduuleille, jotka hoitavat järjestelmiin tehtävät muutokset. Näin uuden AMAN-järjestelmän ei tarvitse tietää, millaisia kohdejärjestelmiä on käytössä, vaan järjestelmien muuttuessa toiminnan muutokset tehdään moduuleihin.

Uuden AMAN-järjestelmän tulee päättää, mille koneelle uuden käyttäjän sähköpostilaatikko luodaan. Päätös tehdään ryhmiin tallennettavan tiedon perusteella. Tämän jälkeen AMAN lähettää pyynnön sähköpostilaatikoita luovalle moduulille, joka hoitaa laatikoiden fyysisen luonnin. Tämän jälkeen moduuli palauttaa polun, jonne laatikko luotiin ja AMAN tallentaa sen tietokantaansa. Laatikon luonnin aikana tunnus ja postilaatikko ovat varattuna käyttäjälle, mutta AMAN ei aktivoi tunnusta, ennenkuin sähköpostimoduuli lähettää kuittauksena postilaatikon polun. Sähköpostilaatikon luonnista vastaava moduuli myös päivittää tiedon sähköpostilaatikon sijainnista suoraan gateway-koneeseen.

Sähköpostilaatikoiden luomisjärjestelmässä tullaan pyrkimään noin tunnin vasteaikaan.

AMAN-järjestelmän tulee myös tarkkailla luotavia sähköpostiosoitteita, jottei kukaan pysty varaamaan osotteita, jotka ovat varattu esimerkiksi verkon ylläpitäjälle. Tällaisia osoitteita ovat mm. admin, postmaster.

### **3.6 Lokitiedot**

Tietokannassa tulee säilyttää lokia muuttuneista tiedoista tietokannassa. Näin ylläpitäjät voivat tarkistaa esimerkiksi käyttäjän tekemät toimenpiteet virhetilanteissa. Myös statuksen vaihdot ja ryhmien vaihdot tulee näkyä lokissa. Järjestelmän lokissa tulee näkyä ainakin seuraavat tiedot: aika, tekijä, muutetut kentät ja tekijän kirjoittama vapaamuotoinen kommentti. Kentistä tallennetaan vain ne, joihin on tullut muutoksia. Tietokantaan tallentuu myös kenttien vanha-arvo.

AMANin tulee myös kirjoittaa normaalia tekstilogia, josta voidaan nähdä kaikki järjestelmässä tapahtuvat toiminnot, jolloin virheiden tutkinta helpottuu huomattavasti.

## **4. Workshopin päättäminen**

Workshop päättyi klo 12.05