TEKNILLINEN KORKEAKOULU

Sähkö- ja tietoliikennetekniikan osasto

Petri Strandén

Kertakäyttö- ja dynaamiset salasanat TKK:n palveluissa

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 6.11.2006

Työn valvoja Professori Patric Östergård

Työn ohjaaja DI Antti Tikkanen

TEKNILLINEN KORKEAKOULU Diplomityön tiivistelmä

Tekijä: Petri Mikael Strandén

Työn nimi:
Kertakäyttö- ja dynaamiset salasanat TKK:n palveluissa

Päivämäärä: 6.11.2006 Sivumäärä: viii + 74

Osasto: Sähkö- ja tietoliikennetekniikan osasto

Professuuri: S-72 Tietoliikennetekniikka

Työn valvoja: Prof. Patric Östergård

Työn ohjaaja: DI Antti Tikkanen

Diplomityön on tarkoitus selvittää kertakäyttö- ja dynaamisten salasanojen käyttöönoton kustannusrakenne Teknillisessä korkeakoulussa. Työ myös selvittää näiden mahdollisia hyötyjä ja haittoja, joita tarkastellaan myös käyttäjän näkökulmasta. Työ aloitettiin luomalla lista valmistajista, joiden tuotteisiin kuului kertakäyttö- tai dynaaminen salasanajärjestelmä. Näiltä valmistajilta tiedusteltiin järjestelmän toimivuutta ja sopivuutta TKK:n palveluihin sekä järjestelmän hintaa TKK:lle.

Diplomityössä toteutettiin myös käyttäjätutkimus, millä kartoitettiin käyttäjien käyttötottumuksia ja mielipiteitä salasanoista koko TKK:n mittakaavassa. Käyttäjätutkimus toteutettiin Internet-kyselynä, johon osallistujat kutsuttiin sähköpostilla. Tämän tutkimuksen tuloksia käytetään myös hyväksi TKK:n atk-keskuksen tulevaisuuden palveluja suunniteltaessa.

Lopputuloksena työ järjestää kertakäyttö- ja dynaamiset salasanatuotteet sopivuus-järjestykseen käyttökohteittain.

Avainsanat: kertakäyttösalasanat, dynaamiset salasanat, vahva todentaminen, käyttäjätutkimus

Helsinki University of Technology Abstract of the Master's Thesis

Author: Petri Mikael Strandén

Name of the Thesis:
One-Time and Dynamic Passwords in Services of TKK

Date: 6th November 2006 Number of pages: viii + 74

Department: Department of Electrical and Communications Engineering

Professorship: S-72 Communication Engineering

Supervisor: Prof. Patric Östergård

Instructor: DI Antti Tikkanen

This Master's Thesis defines the cost structure of introducing one-time and dynamic passwords into the services of TKK. The benefits and weaknesses of one-time and dynamic password systems are examined. Computer users in TKK are also taken into account. The conducted user study maps the password usage in TKK and reveals opinions on their usage.

The list of one-time and dynamic password system manufacturers was assembled first. These manufacturers were asked further about their systems and how they would fit into the services of TKK. Along technical information the price was enquired also.

User opinions and their habits regarding password usage were gathered in the user study, which was conducted as a survey. Randomly selected users were invited to participate by email. The results of this user study will also be used for planning the future services of Computing Centre of TKK.

In this Master's thesis strong authentication products are evaluated as to how well they would fit certain services. An overall comparison is made and in conclusion the best products for each service are suggested.

Keywords: one-time passwords, dynamic passwords, strong authentication, user study

Esipuhe

Tämä diplomityö on ollut minulle mitä suurin haaste. Suunnaton määrä hikeä on valunut ja työtä on tehty tämän paperinivaskan ja työn valmistumisen eteen. Valmistuminen TKK:sta häämöttää jo ihan lähitulevaisuudessa. Mutta onhan tätä jo odotettukin melkein seitsemän ja puoli vuotta.

Vuodet vierivät nopeasti ja aika häviää jonnekin. Onneksi sain opiskeluni aikana sentään jotain pysyvämpääkin aikaiseksi: tämän käsissäsi olevan diplomityön. Suuri kiitos tämän työn valmistumiselle kuitenkin kuuluu monelle eri taholle. Ensimmäiseksi tahdon kiittää tämän työn valvojaa professori Patric Östergårdia, koska hän ennakkoluulottomasti otti diplomityöaiheeni valvottavakseen ja antoi opastusta työn tekemiseen. Ilman häntä tätä diplomityötä ei kenties ikinä olisi pystytty tekemään. Suuret kiitokset myös ohjaajalleni DI Antti Tikkaselle, joka suurella työllä ja patistamisella sai minut pysymään kirjoitustahdissani ja välttämään kirjoittamisen tyveniä. Lisäkiitokset ansaitsevat myös DI Tikkasen työnantaja F-Secure Oyj, joka omalta osaltaan mahdollisti tämän työn tekemisen ja ansiokkaan ohjaamisen. Viimeisenä, mutta ei millään tavalla vähäisimpänä, vaikuttajana diplomityöhöni on toiminut TKK:n atk-keskus, jolle olen saanut etuoikeuden työskennellä. Mahdollisuus tehdä diplomityö työkseen on jo sinänsä suurta mutta lisäksi työ atk-keskuksessa on tukenut opiskelujani TKK:ssa varsin ansiokkaasti. Kiitokset myös U132-huonetovereilleni kaikkien tyhmien kysymyksieni kestämisestä.

Kiitos myös rakkaalleni Hennalle, koska kestit kaikkia minun oikkujani ja varsinkin diplomityön kirjoittamisen loppuvaiheessa laistamiani kotitöitä. Kannustuksen ja ymmärryksen määrä on ollut kaiken kaikkiaan suuri. Myös oma perhe ja sukulaiset ansaitsevat maininnan tässä. Kaikille muille diplomityöstäni kiinnostuneille: kiitos.

Espoossa 31. lokakuuta 2006

Petri Strandén

Sisällysluettelo

Lyhenteet ja määritelmät

Active Directory	Microsoftin hakemistopalvelu, jossa voidaan säilyttää mm. monipuolisia tietoja ja käyttöoikeuksia
Biometrinen todentaminen	Todentaminen, joka perustuu biometrisiin tunnisteisiin
Biometrinen tunniste	Ihmisen jokin fyysinen, mitattava ominaisuus
Dynaaminen salasana	Aikaperusteinen salasana, joka on voimassa vain tietyn aikaa
Eheys	Ominaisuus, ettei tietoa ole valtuudettomasti muutettu
Ihmisrajapinta	Tietokoneen ja ihmisen välinen vuorovaikutusalue
IMAP	Sähköpostin lukemiseen käytetty yhteysmenetelmä (engl. Internet Message Access Protocol)
Kalasteluhyökkäys	Jonkin tietojärjestelmän käyttäjiin kohdistuva huijausyritys, jonka tavoitteena on saada edes joku käyttäjistä luovuttamaan käyttäjätunnuksensa ja salasanansa hyökkääjälle (engl. phishing)
Kerberos	Joukko hajautetuissa tietojärjestelmissä käytettyjä tunnistuksen, pääsynvalvonnan, resurssien aidonnuksen ja avaintenjakelun toimintoja
Kertakäyttösalasana	Tapahtumaperusteinen salasana, joka on voimassa vain kerran
Kiistämättömyys	Varmuus siitä, että tietty henkilö on lähettänyt tai vastaanottanut tietyn viestin
Kvalitatiivinen tutkimus	Tutkimus, jonka tulokset ovat laadullisia ja kuvailevia
Kvantitatiivinen tutkimus	Tutkimus, jonka tulokset ovat numeerisia ja määrällisiä
Käytettävyys	Ominaisuus, että tieto on siihen oikeutetuille saatavilla haluttuna aikana ja vaaditulla tavalla

Käyttäjärooli	Henkilöllä voi olla useita virtuaalisia henkilöllisyyksiä
LDAP	X.500-hakemiston kanssa yhteensopiva yksinkertainen yhteystapa (engl. Lightweight Directory Access Protocol)
Luotettu taho	Taho, jolle uskotaan erityistä luottamusta vaativia tehtäviä
Luottamuksellisuus	Tietojen säilyminen luottamuksellisina ja tietoihin kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta
Luottamusverkosto	Joukko tahoja, jotka sopivat luottamusverkoston piirissä luottavansa toisiinsa sovituissa tapauksissa
OATH	Open Authentication järjestö, jonka tavoitteena on saada avoimet standardit vahvaan todentamiseen
PIN-luku	Tunnusluku, jota käytetään salasanan sijaan syötteiltään rajoitetuissa päätteissä (engl. Personal Identification Number)
PKI	Julkisen avaimen järjestelmä (engl. Public Key Infrastructure)
Poletti	Kertakäyttö- tai dynaamisia salasanoja luova laite (engl. token)
POP	Sähköpostin lukemiseen käytetty yhteysmenetelmä (engl. Post Office Protocol)
Protokolla	Menettelytapa, joka on ennalta sovittu
RADIUS	Yleinen todennusmenetelmä (engl. Remote Authentication Dial-in User Service)
S/KEY	Standardi, joka kertoo miten toteuttaa yksinkertainen kertakäyttösalasanajärjestelmä
Shibboleth	Kertakirjautumisen mahdollistava todennusmenetelmä verkkopalveluissa
SQL	Tietokantojen käsittelyyn tehty kieli (engl. Structured Query Language)
Todentaminen	Varmistuminen jonkin luotettavuudesta tai aitoudesta

Todentamismenetelmä	Menetelmä, jolla voidaan varmistua todennettavan henkilöllisyydestä todentajaa tyydyttävällä tavalla
Todentamispalvelu	Palvelu, joka varmistuu kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä
Todentamistapahtuma	Tapahtuma, jossa todennettavan tekemä väite henkilöllisyydestään varmistetaan
Toimikortti	Suorittimen ja muistipiirejä sisältävä luottokortin kokoinen muovikortti. Soveltuu esim. henkilöllisyyden sähköiseen todistamiseen.
Tunnistaminen	Erottaminen kaikista muista yksiselitteisen nimen tai tunnuksen perusteella
TUPAS	Suomen Pankkiyhdistyksen määrittelemä todennuspalvelu, jossa käyttäjä todennetaan verkkopankin tunnuksilla
Vahva todentaminen	Käyttäjän todennus, joka käyttää ainakin kahta seuraavista kolmesta menetelmästä: käyttäjä ilmoittaa tietämänsä asian, käyttäjä esittää omistamansa esineen tai käyttäjä omaa jonkin biometrisen tunnisteen
Viestintäkanava	Siirtotie, mitä pitkin tieto liikkuu kahden viestijän välillä
Virkamieskortti	Toimikortti, jota henkilö käyttää viranomaisena
VPN	Avoimeen verkkoon tiettyjen käyttäjien välille muodostettu suljettu aliverkko, jonka sisäinen liikenne on suljettu avoimelta verkolta (engl. Virtual Private Network)
WLAN	Langatonta yhteystapaa hyödyntävä lähiverkko

1 Johdanto

Teknillisen korkeakoulun atk-palveluissa käytetään useita eri salasanoja ja nykykäytäntö on vähintäänkin sekava. Tavoitteena onkin jo pitkään ollut salasanojen määrän vähentäminen. Salasanojen määrän vähentämisellä on kuitenkin yksi merkittävä ja pääasiallinen este. Kaikissa salasanaa käyttävissä palveluissa eivät tietoturvavaatimukset ole samanlaisia eikä tietoturva ole samalla tasolla. Tämä pakottaa eri palvelut edelleen käyttämään eri salasanoja.

Palvelujen tietoturvallisuus on vaihtelevaa ja järjestelmälle annettu salasana voi kulkea verkossa joko turvattomasti selkokielisenä tekstinä tai turvallisesti täydellisesti salatussa bittivuossa. Mutta ongelma ei aina ratkea turvallisen siirtotien käytöllä vaan ohjelmat saattavat jättää salasanan tietokoneen muistiin tai pahimmissa tapauksissa kirjoittaa sen suoraan tietokoneen kovalevylle salaamattomana. Myös käyttäjä on suuri tietoturvariski. Käyttäjät käyttävät tuttuja ja helposti muistettavia sanoja ja päivämääriä salasanoinaan sekä kirjoittavat salasanoja erilaisille paperilapuille ja kalentereihinsa.

Ratkaisuja palvelujen tietoturvan parantamiseen on useita. Käyttäjille helpoin tapa on yhden salasanan käyttäminen kaikissa palveluissa. Yhden salasanan mallia toteutettaessa on perinteisesti tällöin joko luovuttava tietoturvavaatimuksista tai tehtävä toisenlainen toteutus jo olemassa olevista palveluista, mikä saattaa olla hyvinkin työlästä jos mahdollista ollenkaan. Yksi ratkaisu tällaiseen on kertakäyttösalasanojen käyttöön ottaminen.

Kertakäyttösalasanat ovat salasanoja, jotka ovat voimassa nimensä mukaisesti vain kerran. Tällöin ei ole niin suurta väliä, jos joku onnistuukin saamaan selville käyttäjän salasanan, sillä se on voimassa vain kerran. Vanha toteutus kertakäyttösalasanoista on ennalta itse tulostettu salasanalista, mikä sitten piti pitää mukana. Tällainen toteutus on käytössä myös TKK:n atk-keskuksessa, missä kertakäyttösalasanoja voi käyttää sisäänkirjautumisessa unix-järjestelmiin.

Nykytekniikoilla kertakäyttösalasanoja voidaan luoda myös tarvittaessa, jolloin salasanoja ei tarvitse itse tehdä etukäteen vaan käyttäjille voidaan antaa henkilökohtaiset

”avaimet”, poletit (engl. token), joista käyttäjät saavat uudet, rajoitetun ajan voimassa olevat salasanat. Tällaisia henkilökohtaisia, mukana pidettäviä poletteja on saatavilla useita erilaisia: usb-muisteja, avaimenperiä, muistikortteja, luottokortin kokoisia laskimia ja ohjelmia kannettaviin päätelaitteisiin.

Käyttäjien todentamisen voi myös hoitaa joku ulkopuolinen taho. Tällaisia todentamispalveluja ovat mm. Suomen Pankkiyhdistyksen TUPAS, Microsoftin Passport ja HAKA-luottamusverkosto. Ulkopuolisen palvelun käyttö käyttäjien todentamiseen tosin vaatii luottamussuhteen luomisen palveluntarjoajien välille ja on harvoin ilmaista.

Tässä diplomityössä tutustutaan tarjolla oleviin kertakäyttösalasanaratkaisuihin ja niiden sopivuuteen TKK:n ja atk-keskuksen tarjoamiin palveluihin. Diplomityö myös selvittää kuinka käyttäjät kokevat nykyisen salasanakäytännön ja miten he suhtautuvat toisenlaisiin todentamismenetelmiin. Diplomityössä myös selvitetään ratkaisuiden käyttöönottomahdollisuuksia ja –kustannuksia TKK:n ja atk-keskuksen palveluissa. Diplomityö kertoo tarvittavat tiedot, joihin päätöksentekoprosessi kertakäyttösalasanojen käyttöönottamisesta voidaan perustaa.

Diplomityö kertoo luotettavan todentamisen vaikeuksista ja ongelmakohdista. Diplomityössä käsitellään vahva todentaminen kertakäyttösalasanojen osalta ja miten kertakäyttösalasanat soveltuisivat TKK:n palveluihin. Diplomityö myös kertoo miten paljon tiettyjen kertakäyttösalasanajärjestelmien käyttöönotto maksaisi tietyillä reunaehdoilla, jotka määritellään jäljempänä.

Diplomityö jakaantuu viiteen selvästi erilaiseen kokonaisuuteen. Ensimmäisenä käsitellään tietoturvan nykytilaa ja käydään läpi historiaa mitä kautta todentaminen on kehittynyt sekä perehdytään todentamisen teoriaan. Seuraavaksi käydään läpi käyttäjätutkimuksen teoriaa ja toteutetun käyttäjätutkimuksen tulokset. Neljännessä luvussa kerrotaan tämän hetkisistä teknisistä todennusratkaisuista TKK:ssa ja atk-keskuksessa sekä vahvan todentamisen käytöstä ja kokemuksista muualla maailmassa. Viides luku muodostuu kertakäyttö- ja dynaamisten salasanatuotteiden vertailusta. Kuudennessa luvussa diplomityössä kerrotaan johtopäätökset ja mihin nämä perustuvat. Tässä luvussa otetaan myös kantaa siihen miten todentaminen kuuluisi ratkaista

TKK:ssa tulevaisuudessa. Viimeisestä luvusta löytyy lyhyt yhteenveto, mitä diplomityössä on tehty, mitkä olivat työn tavoitteet ja mitkä ovat työn tärkeimpiä tuloksia.

2 Tietoturvan historia ja nykytila

2.1 Tietoturvasta

Turva tai turvallisuus on omaisuuden suojelemista. Turvattaessa täytyy tietää suojeltavan omaisuuden arvo, jotta turvaamistoimenpiteet voidaan mitoittaa oikein. Turvaamistoimenpiteet voidaan jakaa kolmeen luokkaan: estämis-, havaitsemis- ja reagoimistoimenpiteisiin (Gollmann, 1999). Estämistoimenpiteillä ehkäistään omaisuuteen kohdistuvaa vahinkoa. Esimerkiksi ovien lukot estävät varkaita pääsemästä helposti sisälle. Havaitsemistoimenpiteillä voidaan jo tapahtunut vahinko ja vahingon luonne havaita sekä saada selville vahingonaiheuttaja. Esimerkiksi varkaus havaitaan, kun varastettu esine on kadonnut; valvontakameroilla voidaan selvittää varas. Reagoimistoimenpiteiksi sanotaan menetelmiä, joilla korjataan vahingot ja palaudutaan normaalitilanteeseen. Esimerkkinä voidaan pitää edellistä tilannetta, kun varkaus on tapahtunut jolloin soitetaan poliisille. Poliisi voi saada varastetun esineen takaisin ja palauttaa sen.

Tietoturvalla tai –turvallisuudella tarkoitetaan hallinnollisia ja teknisiä toimenpiteitä, joilla taataan tiedon luottamuksellisuus, eheys ja käytettävyys (Viestintävirasto, 2001). Gollmann (Gollmann, 1999) on määritellyt luottamuksellisuuden, eheyden ja käytettävyyden seuraavasti. Luottamuksellisuudella tarkoitetaan, ettei tietoon pääse käsiksi kukaan kenellä ei ole siihen tarvittavia oikeuksia. Eheydellä tarkoitetaan, ettei kukaan voi muuttaa tietoa ilman tarvittavia oikeuksia. Käytettävyydellä tarkoitetaan tässä yhteydessä tiedon ja resurssien olemista oikeutettujen käyttäjien saatavilla tarvittaessa.

Tietoturvan luottamuksellisuuden mukaan tietoihin pitää päästä käsiksi vain sellaiset henkilöt, joilla on siihen tarvittavat oikeudet. Järjestelmien täytyy pystyä tunnistamaan ja todentamaan käyttäjät, jotta tiedon luottamuksellisuus ei vaarantuisi. Tunnistaminen on tapahtuma, jossa henkilö kertoo järjestelmälle olevansa tietty käyttäjä. Yleensä tunnistaminen on toteutettu järjestelmäkohtaisesti ainutkertaisella käyttäjätunnuksella, jonka järjestelmä yhdistää tiettyyn henkilöllisyyteen. Todentaminen puolestaan on tapahtuma, jossa järjestelmä todentaa käyttäjän väittämän henkilöllisyyden järjestelmää

tyydyttävällä tavalla. Yleisimmin todentaminen tapahtuu vertailemalla käyttäjän antamaa salasanaa järjestelmän tietämään salasanaan.

Kiistämättömyys on tietoturvakäsite, joka tarkoittaa, että kaikki käyttäjän toimet voidaan todistaa hänen itsensä henkilökohtaisesti tekemiksi (Anderson, 2001). Esimerkiksi pankkien täytyy pystyä todistamaan tietyn asiakkaan tekemät pankkikorttiostokset juuri hänen tekemikseen kiistattomasti.

Sama tieto on eri arvoista eri ihmisille ja eri tahoille. Kuitenkaan tiedon arvoa saa harvoin, jos koskaan, selville ennen tiedon tai sen osan saantia (Shapiro & Varian, 1999). Tutkimuksissa on todettu, että tiedosta ei kuitenkaan olla valmiita luopumaan samaan hintaan kuin mitä siitä ollaan valmiita maksamaan (Rafaeli et al., 2003).

Kaikkea arvokasta täytyy suojella. Vaikka tiedon arvo on erittäin subjektiivista, eli tiedon arvo määräytyy sen mukaan, miten arvokkaana tiedon käyttäjä sen kokee, tiedolle on aina olemassa ostajia. Ja sieltä, missä on jotain arvokasta, löytyy aina rikollisia.

2.1.1 Erilaisia tapoja parantaa tietoturvaa

Tietoturva on kokonaisuus, joka pitää sisällään erilaisia osa-alueita. Valtionhallinnon tietoturvallisuuden johtoryhmä on ohjeessaan riskien arvioinnista jakanut tietoturvallisuuden kahdeksaan osa-alueeseen: hallinnolliseen tietoturvallisuuteen, fyysiseen turvallisuuteen, henkilöstö-, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuuteen (VAHTI 7/2003).

Tietoturvaan pätee hyvin sanonta ”ketju on yhtä vahva kuin sen heikoin lenkki”. Tietoturvaa pitää ajatella kokonaisvaltaisena prosessina, missä eri osa-alueet muodostavat oman lenkkinsä. Tietotekniikassa ja –liikenteessä on pitkään panostettu tekniseen turvallisuuteen erilaisin keinoin. Nykyisin tietoliikenneyhteydet ovat järjestään salattuja. Salaamiseen ja tietoturvallisiin yhteyksiin käytetään hyväksi havaittuja protokollia ja salausalgoritmeja (Schneier, 2000).

Useiden asiantuntijoiden ja yleisön käytössä avoimesti kehittämien ja testaamien protokollien käyttö on todettu hyväksi keinoksi kehittää tietoturvallisia tuotteita. Yleisesti maailmalla on käytössä myös joitakin suljetussa ympäristössä kehitettyjä tuotteita, joiden käyttämät protokollat ja tekniikat eivät kuitenkaan ole kestäneet edes tuotteiden teoreettista tarkastelua saati laajaa käyttöä ilman tietoturvan heikentymistä. Tietoturvasta puhuttaessa ja päätettäessä kannattaa suosia pitkään käytössä olleita ja turvallisiksi todettuja protokollia ja niitä käyttäviä tuotteita (Schneier, 2000).

Nykyisin on tietoturvassa päästy teknisesti niin pitkälle, että parhaiden protokollien ja menetelmien rikkomiseen ja hyväksikäyttämiseen menee nykyisilläkin tietokoneiden laskentatehoilla useita vuosia. Uusia, ja mahdollisesti turvallisempia, protokollia ja käytäntöjä kehitetään jatkuvasti. Kuitenkin tietoturvan koostuessa erilaisista osa-alueista ei kaikkiin osa-alueisiin ole kiinnitetty samanlaista huomiota. Vähimmälle kehitykselle on jäänyt ihmisrajapinnan tietoturvallisuus ja sen kehitys aina viime vuosiin saakka (Schneier, 2000).

Ihminen inhimillisenä olentona on erittäin tietoturvaton. Ihmiset ovat kehittäneet kaikki käyttämänsä menetelmät ja protokollat ja ihmiset tekevät virheitä. Näistä virheistä johtuen on monien menetelmien ja protokollien väärinkäyttö mahdollista. Lisäksi ihminen haluaa vain tehdä työnsä ja sosiaalisena olentona auttaa muita suoriutumaan töistään mahdollisimman hyvin. Tästä johtuen ihmiset eivät usein noudata tietoturvaohjeita, koska se on vaivalloista ja haittaa työn tekoa. Tällöin ei ole tarpeellista edes yrittää murtaa käytettyä teknistä tietoturvaa, kun samaan ja jopa parempaan tulokseen päästään kysymällä asiaa suoraan käyttäjältä kertomalla jokin sopiva tekosyy, minkä käyttäjä on valmis hyväksymään (Anderson, 2001). Tätä kutsutaan käyttäjän manipuloinniksi.

Tunnistaminen ja todentaminen kuuluvat olennaisesti useaan tietoturvan osa-alueeseen. Kuitenkin tunnistaminen ja todentaminen on perinteisesti toteutettu käyttäjätunnuksilla ja salasanoilla. Tämä on kuitenkin tietoturvallisesti huono ratkaisu ihmisen muistirajoituksista johtuen; teknisesti paras salasana on täysin satunnainen, järjestelmälle ominaisen enimmäispituuden pituinen (Schneier, 2000).

Käyttäjän tunnistaminen ja todentaminen pelkän käyttäjätunnuksen ja salasanan avulla on muutenkin tietoturvaton menetelmä, koska käyttäjä kertoo ne niitä häneltä kysyttäessä (Mäkelä, 2003). Tietoturvaa saadaan jonkin verran parannettua opastamalla käyttäjiä ja ohjeistamalla esimerkiksi erilaisten muistisääntöjen käyttö salasanoja valittaessa (Yan et. al, 2000). On kuitenkin huomattava, että johtuen ihmisen ominaisuuksista pelkkään salasanaan perustuvaa todentamista ei ole mahdollista saada turvalliseksi (Anderson, 2001).

2.2 Identiteetti, tunnistaminen ja todentaminen

Jokaisella ihmisellä on oma henkilöllisyytensä, identiteettinsä, joka erottaa hänet muista ihmisistä. Ihmisen identiteetin määrittävät aikaisemmin koetut asiat ja hänen omat muistikuvansa ja kokemuksensa, joiden varaan ihminen rakentaa oman minäkuvansa. Identiteetti on tärkeä. Identiteetin avulla yhteiskunnan muodostavat ihmiset voidaan erottaa toisistaan. Identiteetti on aina sidoksissa fyysiseen ruumiiseen, jonka esittämällä ihminen voi todistaa identiteettinsä.

Tämän päivän yhteiskunta on rakentunut henkilöiden identiteettien erottamiselle toisistaan. Perusasiat kuten esimerkiksi omistusoikeus, kansalaisuus ja äänioikeus perustuvat kaikki sille periaatteelle, että henkilön identiteetti voidaan tarvittaessa todistaa. Identiteetin todistamiseen riittää fyysisen, identiteettiin sidonnaisen, ruumiin esittäminen. Käytännössä tämä tarkoittaa sitä, että kun kerrot poliisille nimesi ja poliisi lukee antamastasi henkilöllisyystodistuksesta saman nimen, on sinut tunnistettu. Kun hän vertaa todistuksessa olevaa kuvaa kasvoihisi, on sinut todennettu (Downes, 2005). Virtuaalisessa maailmassa, kuten Internetissä, identiteettiään ei voi todistaa esittämällä fyysisen itsensä.

Ihminen ilmaisee identiteettiään monin eri tavoin. Kehonkieli, pukeutumistapa ja harrastusvalinnat ovat esimerkkejä erilaisista identiteetin ilmaisutavoista ja viestintäkanavista. Samoin virtuaalisessa maailmassa hän valitsee erilaisia viestintäkanavia sen mukaan mitä ja miten hän haluaa ilmentää identiteettiään. Virtuaalisessa maailmassa ihmisellä voi olla monta eri identiteettiä, joista jokainen ilmentää vain yhtä osa-aluetta hänen identiteetissään (Suler, 2002).

Tunnistaminen on tapahtuma, jossa henkilö paljastaa henkilöllisyytensä, identiteettinsä; tunnistettava tekee väitteen identiteetistään. Todentamisella puolestaan tarkoitetaan tapahtumaa, jossa tarkistetaan henkilön väitetty identiteetti todentajaa tyydyttävällä tavalla. Todentaminen ei ole mahdollista ilman tunnistamista (Downes, 2005).

2.2.1 Henkilön todentamisen historia

Tarve tunnistaa ihmiset yksilöinä syntyi 1700-luvun alkupuolella Pietari Suuren uudistaessa Venäjän armeijaa ja arvojärjestystä. Armeijan tarvitsemia voimavaroja kontrolloitiin väestörekisterein ja rajoittamalla väestön liikkuvuutta erilaisin rajoituksin. Tunnistamisen tarve lisääntyi entisestään yleisen asevelvollisuuden keksimisen myötä Ranskan vallankumouksen aikana. (Torpey, 2000)

1700-luvulla vallinneen feodalismin aikana etenkin alempien väestöluokkien liikkuvuutta kontrolloitiin erilaisin virallisin dokumentein kuten passein. Passi oli aluksi jonkun virallisen tahon myöntämä matkustusasiakirja, joka tunnisti yksilön pikemminkin hänen yhteiskunnallisen asemansa (asuinpaikka, ammatti, perheen asema jne.) kuin fyysisten ominaisuuksiensa johdosta. (Torpey, 2000)

Ennen nationalismin ja nykyisten valtiomuotojen syntyä luotettiin miehen sanaan. Jos mies ei pitänytkään sanaansa, kukaan ei enää luottanut häneen (Downes, 2005). Väestön liikkumisrajoitusten vähentyessä ja paikallisen hallinnon vaihtuessa valtionhallintoon tarve ihmisten todentamiseen alkoi todella tulla esiin. 1800-luvulle tultaessa etenkin Ranskassa ihmisten täytyi todistaa henkilöllisyytensä erilaisissa yhteyksissä valtionhallinnon kanssa. Tuolloin ei kuitenkaan ollut mitään yhtenäistä todentamisasiakirjaa vaan sellaiseksi kävi joko passi tai aveu (jonkun hyvin tunnetun aatelisen tai kirkonmiehen antama suosituskirje). Varsinkin matkustusasiakirjojen väärentäminen oli yleistä. (Torpey, 2000)

Maailman ensimmäisen valokuvan ottajana pidetään yleisesti Nicéphore Niépcea. Valokuva on vuodelta 1826 ja vaati kahdeksan tunnin valotusajan. Keksinnöt, jotka paransivat kuvanlaatua ja lyhensivät tarvittavaa valotusaikaa vuosien 1839-1888

välisenä aikana, saivat valokuvauksen yleistymään räjähdysmäisesti (Coe, 1976). Ranska alkoi käyttää passeissa valokuvia vasta vuonna 1912 ja muut valtiot vielä myöhemmin. Tuolloin ensimmäistä maailmansotaa edeltävällä kaudella nähtiin ihmisten tunnistaminen ja todentaminen ensiarvoisen tärkeäksi. Yksi syistä, miksi valokuva otettiin käyttöön tunnistamisasiakirjoissa näinkin myöhään, oli että aiemmin poliisi ei luottanut valokuvien käyttöön todisteina (Torpey, 2000).

Nykyisin valokuva löytyy kaikista henkilöllisyyden todistavista virallisista asiakirjoista. Lisäksi esimerkiksi passeissa on Yhdysvallat jo ottanut käyttöön biometriset tunnisteet valokuvien lisäksi (Salin, 2004). Tämä on pakottanut myös muut valtiot aloittamaan biometristen tunnisteiden käyttöönottamisen passeissaan (EY, 2004).

2.3 Vahva todentaminen

Käyttäjän henkilöllisyys voidaan todentaa myös vahvalla todentamisella. Vahva todentaminen tarkoittaa todentamista useamman tekijän perusteella. Nämä tekijät ovat aina jollain tavalla käyttäjän identiteettiin, henkilöllisyyteen, liittyviä. Näitä tekijöitä ovat asiat, jotka käyttäjä tietää (esimerkiksi salasanat), esineet, jotka ovat käyttäjän hallussa (esimerkiksi kertakäyttösalasanoja tai dynaamisia salasanoja muodostavat laitteet eli poletit) tai biometriset ominaisuudet, jotka käyttäjällä on (esimerkiksi sormenjäljet ja silmän iiris) (Schneier, 2000). Lisäksi joissain tapauksissa käyttäjä voidaan myös todentaa hänelle ominaisen käyttäytymisen (esimerkiksi kirjoitusnopeuden, näppäinpainalluksen suunnan tai voimakkuuden tai keston yms.) mukaan mutta yleensä nämäkin luetaan biometrisiksi tunnisteiksi.

Todentaminen voi tapahtua monella eri tavalla. Todellisessa maailmassa henkilön todentamiseen kuitenkin liittyy aina fyysisen ruumiin ja henkilöllisyyden, identiteetin, välisen sidoksen osoittaminen (Downes, 2005). Virtuaalisessa maailmassa ei kuitenkaan näin voida toimia. Yleisin todentamistapa onkin vielä käyttäjätunnus ja salasana – yhdistelmä (Anderson, 2001). Todentaminen useamman tekijän perusteella tulee kyseeseen silloin, kun halutaan varmistua tietojärjestelmien käyttäjien henkilöllisyydestä hyvin suurella varmuudella (Anderson, 2001). Syitä tällaiseen voi

olla monia, suurimpina vaikuttimina ovat kuitenkin rahaa ja turvallisuutta koskevat asiat.

Biometriset tunnisteet ovat vanhimpia käytettyjä tunnisteita todentamisessa. Kasvojen ja äänen tunnistaminen ovat käytetyimpiä tunnisteita vielä nykyäänkin jokapäiväisessä elämässä ihmisten kesken. Asiayhteyksissä taas käsialan tunnistus nimikirjoituksissa on yksi vanhimmista edelleen käytössä olevista todentamistavoista. Uudempia tapoja todentaa henkilöllisyys ovat esimerkiksi sormenjäljet ja DNA (etenkin rikostutkimuksissa). Etätodentaminen biometristen tunnisteiden avulla esimerkiksi tietoverkoissa voi olla haastavaa ja siihen liittyy monia riskejä (Anderson, 2001). Yksi riskeistä on biometrisen ominaisuuden varkaus. Joku esimerkiksi voi onnistua varastamaan sormenjälkitunnisteen, jonka jälkeen kyseistä sormenjälkeä ei enää voi käyttää ainutlaatuisena tunnisteena yksilölle. Biometrisissä tunnisteissa on myös se huono puoli, että niitä on vain rajoitetusti käytettävissä (Schneier, 2000).

Vahva todentaminen voidaan kuitenkin toteuttaa myös muuten kuin biometristen tunnisteiden avulla. Henkilöä voidaan vaatia todentamistilanteessa esittämään fyysinen todiste henkilöllisyydestään. Tämä fyysinen todiste voi olla mikä vain: sinettisormus keskiajalla, nykyisin kotiavain tai vaikka verkkopankin avainlukulista. Pääasia on että todentaja tietää kenelle on antanut tämän fyysisen todisteen (Schneier, 2000). Tämän lisäksi henkilön tulee tietää jotain, mitä on todentajan kanssa aikaisemmin sopinut. Esimerkiksi käytettäessä kertakäyttö- tai dynaamisia salasanoja muodostavia laitteita, poletteja, on henkilön täytynyt aikaisemmin saada sellainen haltuunsa ja määrittää sen kanssa käytettävä salasana (polettien kanssa käytetään yleensä numerosarjaa salasanana, Personal Identification Number:ia eli PIN-lukua). Todentajajärjestelmä todentaa henkilön väittämän henkilöllisyyden, jos sekä PIN-luku että kertakäyttösalasana ovat oikein. Vahva todentaminen perustuu jaetun salaisuuden periaatteeseen, missä todentajaosapuoli luottaa käyttäjälle annettuun polettiin salaisuuden säilyttäjänä. Poletti muodostaa uusia kertakäyttösalasanoja juuri tuon salaisuuden pohjalta (Schneier, 2000).

Vahvan todentamisen etuna on suurempi varmuus todentamistilanteeseen liittyvistä osapuolista. Vahva todentaminen myös vaikeuttaa olennaisesti toiseksi tekeytymistä eli väärän henkilöllisyyden käyttämistä (Schneier, 2000).

Valtionhallinnon tietoturvallisuuden johtoryhmä on monissa ohjeissaan ottanut kantaa vahvan todentamisen puolesta. *Turvallinen etäkäyttö turvattomista verkoista* –ohjeessa sanotaan mm. ”viraston palveluja käytettäessä on olennaista, että etäkäyttäjä tunnistetaan ja todennetaan luotettavasti” ja ”käyttäjätunnus ja kiinteä salasana todentamismenetelmänä kelpaa vain julkisia aineistoja käsittelevien sovellusten käyttöön” (VAHTI 2/2003). Lisäksi *Valtionhallinnon keskeisten tietojärjestelmien turvaaminen* –ohjeessa sanotaan ”tietojärjestelmän suojaukset on mitoitettava turvaluokitukseltaan vaativimman käsiteltävän tiedon mukaisiksi” ja ”vahvoja todennusmenetelmiä, kuten kertakäyttösalasanoihin ja toimikortteihin perustuvia menetelmiä tulee suosia” (VAHTI 5/2004).

2.3.1 Kertakäyttö- ja dynaamiset salasanat

Kertakäyttösalasanoja voidaan luoda erilaisin menetelmin ja toteutuksin. Yksinkertaisin menetelmä on taulukoidut merkistöt, joista jokainen taulukon arvo kysytään vain kerran. Nämä ratkaisut ovat yleisesti tulostettu paperille ja muistuttavat laivanupotuspelin-ruudukkoja. Kertakäyttösalasanat voivat olla myös etukäteen paperille tulostettu salasanalista kuten S/KEY-ratkaisu (RFC 2289). Myös verkkopankkien käyttämät avainlukulistat toimivat tällä samalla periaatteella. Tulostetut salasanat ovat kuitenkin huonoja silloin, kun tunnistautumisia tapahtuu paljon. Esimerkiksi käyttäjän ei tarvitse yleensä käyttää verkkopankkia kuin vain joitakin kertoja kuukaudessa siinä missä sama käyttäjä saattaa lukea sähköpostinsa useita kertoja päivässä. Viimeksi mainitussa tapauksessa ennalta luodut salasanat eivät enää ole niin käytännöllisiä.

Kertakäyttö- ja dynaamisia salasanoja voidaan luoda myös sähköisesti PKI-varmenteiden pohjalta. Public Key Infrastructure on julkisen avaimen salausjärjestelmä, joka muodostuu digitaalisista julkisesta ja salaisesta -avaimesta. Julkisesta avaimesta ei voida päätellä salaista avainta mutta julkisella avaimella voidaan avata salaisella avaimella salattuja viestejä (RFC 2527). Tällaisessa ratkaisussa käyttäjän ja todentajan on ensiksi sovittava käytettävistä PKI-varmenteista. Tämän jälkeen käyttäjä luo uusia dynaamisia tai kertakäyttösalasanoja jollakin algoritmilla, mikä ottaa syötteinään käyttäjän PKI-varmenteen ja jonkun muun vaihtuvan ulkoisen tekijän. Tämä ulkoinen

tekijä voi olla todentamistapahtuma, jolloin kyseessä on kertakäyttösalasana (eli luotu salasana on voimassa vain kerran), tai aika, jolloin kyseessä on dynaaminen salasana (eli luotu salasana on voimassa vain tietyn ajan luomisesta). Ulkoinen tekijä voi myös olla järjestelmän antama syöte: haaste. Todentaja voi vastauksen saatuaan laskea, onko kertakäyttösalasana luotu käyttäjän PKI-varmenteesta ja haasteesta. Joidenkin järjestelmien toteutuksessa voidaan olla käytetty useampia tapoja yhdessä. Yhteistä kaikille menetelmille kuitenkin on jaettu salaisuus, jonka vain järjestelmä ja käyttäjä tietävät.

Kertakäyttö- ja dynaamisia salasanoja luodaan erilaisilla poleteilla. Poletit ovat joko pieniä mukana kuljetettavia laitteita tai käyttäjän päätelaitteessa toimivia ohjelmia. Tämä johtuu käytettävien algoritmien monimutkaisuudesta ja siitä, että poletin sisällä täytyy olla jokin salaisuus, mitä pystyy käyttämään vain, kun poletti on käyttäjän hallussa (Schneier, 2000). Poletteja on monenlaisia. Osassa laitteista on mahdollista syöttää käyttäjän tietämä salasana, PIN-luku, joka myös vaikuttaa luotavaan salasanaan muiden ulkoisten tekijöiden lisäksi. Lopuista laitteista pelkistetyimmillään ei löydy kuin näyttö ja yksi nappi, mitä painamalla poletti luo uuden salasanan. Käyttäjä joutuu luomaan lopullisen dynaamisen tai kertakäyttösalasanan lisäämällä poletin antamaan salasanaan oman henkilökohtaisen salasanansa, PIN-lukunsa. Tämä PIN-luku voidaan syöttää laitteen antamaa salasanaa ennen tai jälkeen riippuen toteutuksesta.

Tässä diplomityössä tarkoitetaan kertakäyttösalasanoilla poleteilla luotuja salasanoja, mitkä ovat voimassa kerran luomisensa jälkeen, ja dynaamisilla salasanoilla poleteilla luotuja salasanoja, mitkä ovat voimassa vain tietyn ajan luomisensa jälkeen. Dynaamiset kertakäyttösalasanat ovat salasanoja, jotka ovat voimassa vain tietyn ajan luomisensa jälkeen tai vain kerran.

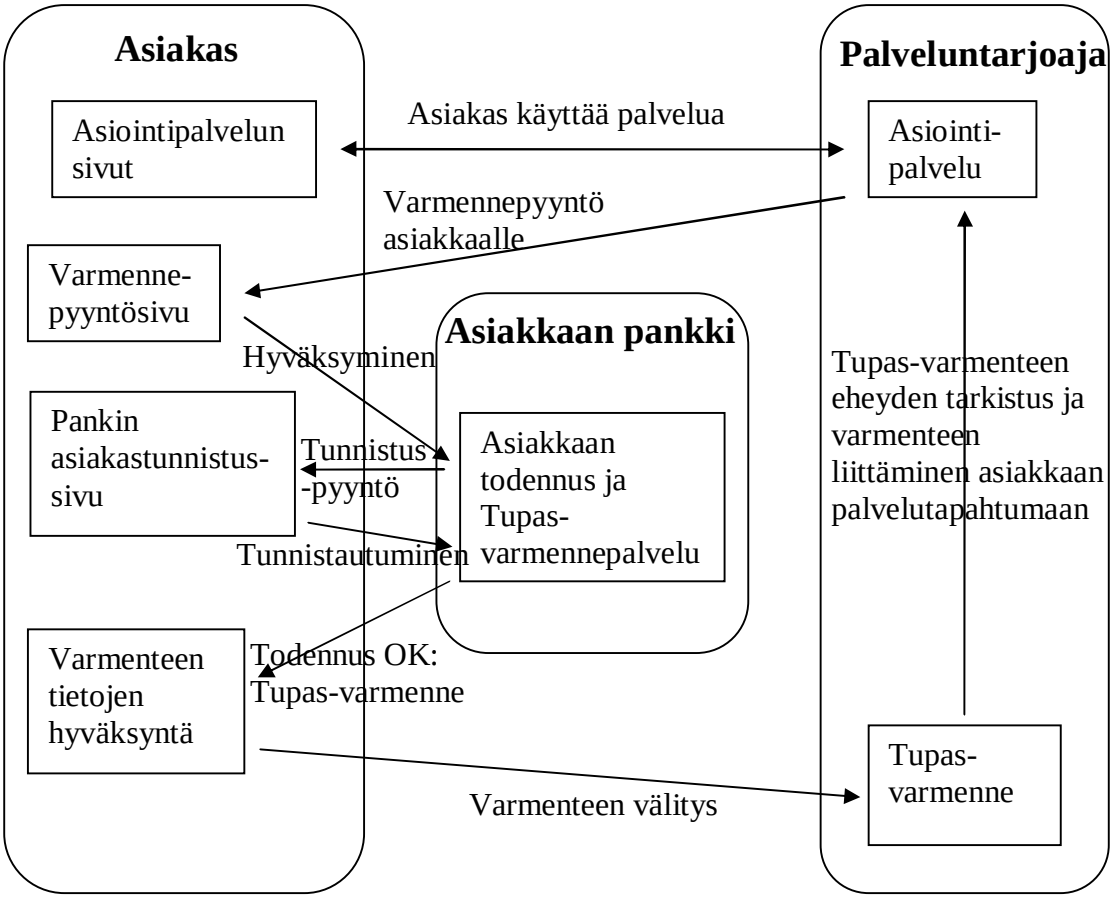
Kertakäyttö- ja dynaamisten salasanojen etuja on monia. Suurin etu on kuitenkin parantunut tietoturva, kun käyttäjien salasanat eivät enää ole arvattavissa tai selvitettävissä. Lisäksi kertakäyttö- ja dynaamisia salasanoja käytettäessä ei tarvitse muistaa monimutkaisia salasanoja vaan vain oma henkilökohtainen PIN-luku. Tämä ei vain vähennä käyttäjien muistikuormaa vaan vähentää myös muistiin kirjoitettujen salasanojen määrää. Suurin tietoturvariski, poletin häviäminen, ei kuitenkaan ole niin vakava riski kuin perinteisen salasanan joutuminen väärälle henkilölle, koska poletin

käyttämiseen tarvitaan edelleen myös käyttäjän salasana, PIN-luku. Yksi saavutettavista eduista ovat säästöt, kun päivystys unohtuneiden salasanojen ja lukkiutuneiden tunnuksien varalta jäävät pois. Tällöin ylläpito voi täysipainoisesti keskittyä ylläpitämään olemassa olevia palveluja ja kehittämään uusia.

Kertakäyttösalasanoissa ja dynaamisissa salasanoissa on myös huonoja puolia. Yksi huonoista puolista on se, että käyttäjät joutuvat kantamaan polettia mukanaan. Vaikka poletteja on myös pieniä avaimenperä-mallisia, joutuu käyttäjä silti huolehtimaan siitä. Lisäksi kertakäyttösalasanalaitteissa, jotka luovat salasanoja tapahtumien perusteella, voivat todentajan järjestelmä ja käyttäjän poletti mennä sekaisin siitä, mikä tapahtuma on menossa. Tämä voi tapahtua jos esimerkiksi käyttäjän lapsi saa poletin käsiinsä ja painelee poletin nappia. Dynaamisissa salasanoissa ei tällaista ongelmaa kuitenkaan ole, koska salasanan luominen perustuu aikaan.

2.3.2 Ulkopuoliset todentamispalvelut

Ulkopuoliset todentamispalvelut vaativat aina luottamussuhteen luomista. Lisäksi ulkopuoliset todentamispalvelut ovat usein maksullisia kuten Suomen Pankkiyhdistyksen TUPAS-järjestelmä (Suomen Pankkiyhdistys, 2005). TUPAS-järjestelmässä todentaminen tapahtuu suomalaisen verkkopankin tunnuksilla verkkopankin omalla sivustolla, josta tieto lähetetään TUPAS-todentamista käyttävällä sivulle. TUPAS-järjestelmän käyttö veloitetaan tapahtumakohtaisesti.



Kuva 1 Tupaspalvelun toiminta (Lähde: Suomen Pankkiyhdistys, 2005)

Kuva 1:n kaaviossa on kuvattu Suomen Pankkiyhdistyksen TUPAS-palvelun toiminta käyttäjän todentamistilanteessa. Palveluntarjoajan on täytynyt sopia asiakkaan pankin kanssa etukäteen todentamispalvelun käytöstä eli luottamussuhteen luomisesta mutta asiakkaan todentamistapahtumassa ei palveluntarjoajalla ja asiakkaan pankilla ole suoraa yhteyttä keskenään. Asiakkaan todentamistapahtumassa kuitenkin käytetään hyväksi asiakkaan pankin ja palveluntarjoajan ennalta luomaa luottamussuhdetta siten, että palveluntarjoajan tarvitsee vain luottaa asiakkaan pankkiin (Suomen Pankkiyhdistys, 2005). Tämä mahdollistaa monipuolisempien palvelujen tarjoamisen asiakkaalle.

Ulkopuolisten todentamispalveluiden käyttö on ollut suuressa nousussa. Tulevaisuudessa ulkopuolisten luotettujen tahojen palveluiden käyttö tulee olemaan

entistä suurempaa. Tällä hetkellä ulkopuolisia luotettuja tahoja ja heidän palveluitaan käytetään lähinnä rahaliikenteessä ja internetkaupankäynnissä (Schneier, 2000).

Ulkopuolisiksi todentamispalveluiksi voidaan myös laskea erilaiset luottamusverkostot. TKK kuuluu esimerkiksi Haka-luottamusverkostoon (Haka Federation) muiden suomalaisten yliopistojen kanssa. Tämän luottamusverkoston avulla voidaan TKK:n käyttäjä todentaa myös muiden yliopistojen verkkopalveluissa käyttäen Shibboleth-tekniikkaa. Shibboleth on verkkotekniikka, joka mahdollistaa käyttäjän todentamisen käyttäjän kotiorganisaation palvelussa. Esimerkiksi TKK:n käyttäjä todennetaan aina TKK:ssa. Tällä hetkellä TKK käyttää Shibbolethin kanssa normaaleja käyttäjätunnuksia ja salasanoja.

Ulkopuolisten todentamispalveluiden käyttö vaatii paljon luottamusta käyttäjän palveluntarjoajan ja todentamispalvelun toimittajan välillä. Esimerkiksi Suomen Pankkiyhdistyksen jäsenten tekemä TUPAS-palvelu vaatii maksua luottamussuhteen ylläpitoa vastaan. Luottamussuhteiden luonti ja ylläpito ovatkin vaikeimpia asioita ulkopuolisissa todentamispalveluissa (Schneier, 2000).

3 Käyttäjät

Koska käyttäjät ovat olennaisin osatekijä todentamisen varmuudesta puhuttaessa, tämä kappale käsittelee pelkästään heitä. Ensimmäisessä luvussa käydään läpi käyttäjätutkimuksen teoriaa. Toinen luku käsittelee TKK:n käyttäjiä käyttäjäryhmittäin. Viimeisestä luvusta löytyy suoritettu käyttäjätutkimus. Käyttäjätutkimuksesta käydään läpi olennaisimmat tulokset. Käyttäjätutkimus ja sen tulokset löytyvät liitteestä 1.

3.1 Käyttäjätutkimuksesta

Käyttäjätutkimus on osa käyttäjäkeskeistä suunnittelua, missä tuotteen käyttäjät otetaan mukaan tuotteen suunnitteluprosessiin. Käyttäjätutkimus on suhteellisen laaja käsite. Käyttäjätutkimus tarkoittaa niitä tutkimus- ja arviointimenetelmiä ja -toimintatapoja, joilla saadaan kerättyä tietoja suoraan käyttäjiltä (Tamminen, 2004).

Käyttäjätutkimusta voi painottaa eri tavoin. Riippuen tutkimuksen tavoitteista voidaan käyttäjätutkimuksessa keskittyä mm. käyttäjään, tuotteen käyttöön tai organisaatioon. Käyttäjään keskittyminen tutkii käyttäjien tarpeita, haluja, motivaatiota, tehtäviä ja odotuksia. Tuotteen käyttöön keskittyminen tutkii milloin ja mihin tiettyä informaatiota käytetään sekä millaisia esteitä ja mahdollisuuksia informaation käytölle on olemassa. Organisaatioon keskittyminen käyttäjätutkimuksissa paljastaa organisaation sisäisiä ja ulkoisia rakenteita kuten voimavarat, johdon toimenpiteet sekä sisäiset ja ulkoiset strategiat (Banwell & Coulson, 2004).

Käyttäjätutkimuksessa on tärkeää kohderyhmän oikea valinta. Kohderyhmän tulee koostua samoista ihmisistä, jotka käyttävät suunniteltavaa tuotetta. Erityisen tärkeää on etenkin kaupallisissa tuotteissa jo suunnitteluvaiheessa tietää se, että ostopäätöksen tekijät eivät useinkaan ole tuotteen varsinaisia käyttäjiä. Käyttäjätutkimukseen panostaminen ja samalla käytettävyyden parantaminen kannattaa aina (Nielsen, 1993).

Oikean käyttäjätutkimusmenetelmän valinta on onnistuneen käyttäjätutkimuksen edellytys. Käyttäjätutkimuksen aluksi kuuluu määritellä kohderyhmä, tutkimuksen tavoitteet ja tutkimukselta halutut tulokset. Tutkimukseen kutsuttavat kohderyhmän

edustajat tulee valita satunnaisesti ja otoskoon tulee olla riittävä. Riittävä otoskoko voi vaihdella tutkimuksen tavoitteista ja käytettävissä olevista resursseista johtuen. Ennen tutkimusmenetelmien valintaa pitää tietää tutkimukselta halutut tulokset. Tutkimusmenetelmien valintaan vaikuttavat millaista tietoa tutkimukselta halutaan ja miten kerättyä tietoa saadaan hyödynnettyä. Valintaan vaikuttaa olennaisesti myös käyttäjätutkimuksen käytössä olevat resurssit (Scheuren, 2004).

3.1.1 Haastattelu

Haluttaessa tietoa käyttäjistä on usein helpointa kysyä sitä heiltä itseltään. Haastattelussa käyttäjältä kysytään kysymyksiä ja vastaukset tallennetaan. Haastattelukysymykset täytyy suunnitella etukäteen mutta haastattelutilanteessa on se etu, että haastattelua voidaan johdatella johonkin suuntaan käyttäjän antamien vastausten perusteella. Haastattelut sopivatkin erityisesti tilanteisiin, missä tutkija ei vielä tiedä tarkalleen mitä tietoja hän haluaa (Nielsen, 1993).

Haastattelulla voidaan kerätä kvantitatiivista ja kvalitatiivista tietoa käyttäjiltä. Haastattelujen tulokset voivat kuitenkin vääristyä helposti ellei haastattelija tiedä mitä on tarkalleen tekemässä. Varsinkin tietokoneavusteiset puhelin- ja henkilöhaastattelut ovat nopeita toteuttaa ja niissä haastattelija ei pysty tekemään suuria virheitä, jotka olennaisesti vaikuttaisivat vastaajilta saatuihin tietoihin (Scheuren, 2004).

3.1.2 Kysely

Kyselytutkimuksessa joudutaan ottamaan moni asia huomioon jo sen suunnitteluvaiheessa. Kyselyillä saadaan selville käyttäjien mielipiteitä ja ajatuksia (Nielsen, 1993). Kysymysten on tärkeää olla mahdollisimman yksikäsitteisiä; koska henkilökohtainen kontakti käyttäjiin puuttuu, on mahdolliset väärinkäsitykset vaikeampi korjata jälkikäteen. Kyselyt ovat halpoja toteuttaa mutta niiden analysoiminen on vaikeampaa kuin haastattelujen (Faulkner, 2000).

Kyselytutkimus voidaan nykyisin toteuttaa eri tavoilla. Perinteinen tapa on lähettää kyselyyn osallistujille kirje, mikä sisältää kyselyn, ohjeet ja palautuskuoren. Nykyisin

moni kysely toteutetaan internetissä ja tällöin vain tapa millä osallistujat saavat tiedon kyselystä vaihtelee (Scheuren, 2004).

Kyselytutkimus on kvantitatiivinen käyttäjätutkimustapa, jonka edut ovat vähäiset tarvittavat resurssit ja tulosten tilastollisuus ja suora vertailtavuus. Haittoja ovat mm. virheherkkyys ja muita henkilökontaktin sisältäviä tutkimusmenetelmiä alhaisempi vastausaste (Scheuren, 2004).

3.1.3 Päiväkirja

Päiväkirjatutkimuksella pystytään keräämään kvantitatiivista tietoa. Päiväkirjatutkimuksen toteutuksen suunnittelussa joudutaan kiinnittämään paljon huomiota päiväkirjan yksikäsitteisyyteen ja helppotäyttöisyyteen. Käyttäjä täyttää päiväkirjaa toimiensa ohella, tekemänsä työn ohessa tai välittömästi sen jälkeen. Päiväkirjan täyttämisen tulisi olla käyttäjälle mahdollisimman miellyttävä kokemus, muutoin vaarana on haluttujen asioiden päiväkirjaan merkitsemättä jättäminen ja tutkimustulosten kyseenalaisuus. Nämä mainitut asiat yksinään pakottavat tutkijan ottamaan henkilökohtaisen kontaktin tutkimukseen osallistuviin. Henkilökohtainen kontakti myös parantaa luottamusta tutkijan ja käyttäjän välillä, jolloin päiväkirjamerkintöjen luotettavuus paranee (Rieman, 1993).

3.1.4 Havainnointi

Havainnointi sopii tutkimusmenetelmäksi, jos halutaan kerätä kontekstista l. asiayhteydestä riippuvaista tietoa kuten tietoa fyysisestä ympäristöstä, käyttäjien yhteysverkostoista ja työnkulusta. Havainnointia käytetään usein kontekstisuunnittelun yhtenä menetelmänä (Jääskö & Mattelmäki, 2003). Kontekstisuunnittelu on menetelmä, jolla saadaan selville käyttäjistä ja varsinaisesta tuotteen käyttöympäristöstä kattava kokonaisuus (Wixon et al., 2002).

Havainnointi tapahtuu käyttäjän omassa työpisteessä. Havainnoinnin tarkoitus on seurata ilman vuorovaikutusta, kuinka käyttäjä toimii omassa työympäristössään. Havainnoinnin haittana tosin on, että havainnointi vaikuttaa aina havainnoitavan

käyttäytymiseen. Havainnoinnilla ei välttämättä myöskään saada selville käyttäjän perimmäisiä syitä toiminnalleen (Faulkner, 2000).

3.1.5 Ryhmäkeskustelu

Ryhmäkeskustelu on tutkimusmenetelmä, jossa useampi käyttäjä kokoontuu puhumaan ohjatusti tutkittavasta aiheesta. Ryhmäkeskustelun tulokset riippuvat erittäin paljon keskustelun ohjaajan taitotasosta. Ryhmäkeskustelu on tutkimusmenetelmänä erittäin innovatiivinen mutta tulosten tarkempi analysointi voi olla erittäin vaikeaa ja aikaa vievää (Nielsen, 1993).

Ryhmäkeskustelut ovat kvalitatiivinen tutkimustapa. Niillä saadaan tehokkaasti selville mielipiteitä ja asenteita. Ryhmäkeskusteluista saadaan selville myös syyt mielipiteiden ja asenteiden takana. Vaikka tutkimuksessa järjestettäisiin useita ryhmäkeskusteluja, ei näiden tuloksia voida verrata keskenään kvantitatiivisesti liian pienen otoskoon vuoksi. Ryhmäkeskustelujen etuja ovat mm. tiedonkerääminen nopealla aikataululla, keskustelujen joustavuus ja ohjailtavuus sekä valmistelujen yksinkertaisuus. Ryhmäkeskustelujen haittoja puolestaan ovat että mikään ryhmä ei ole edustava otos kohderyhmästä, ja näin ollen tuloksia ei voida yleistää tai käsitellä tilastollisesti, kerätyn tiedon laatu riippuu täysin keskustelun ohjaajan taito- ja motivaatiotasosta keskustelutilaisuudessa ja myös tulosten käsittelytapa poikkeaa muista yleisesti käytetyistä käyttäjätutkimusmenetelmistä (Scheuren, 2004).

3.2 Käyttäjäryhmät TKK:ssa

Teknillisessä korkeakoulussa on monia erilaisia tietoteknisten palveluiden käyttäjäryhmiä, joiden tarpeet, käyttötavat ja –koulutus ovat toisistaan poikkeavia. Aikaisemmin eri käyttäjäryhmien erilaisiin tarpeisiin ei ole kiinnitetty suurempaa huomiota mutta toisaalta sellaiseen ei ole ollut mahdollisuuttakaan vähäisten tietoteknisten palveluiden vuoksi; käyttäjille on tarjottu kaikki, mikä on hyödylliseksi katsottu. Nykyisin erilaisten palveluiden kirjo on kuitenkin niin laaja, että yksittäisellä toimijalla ei ole minkäänlaisia mahdollisuuksia tarjota kaikkia mahdollisia palveluita.

Palveluita suunniteltaessa on niiden käyttäjät myös tunnettava. Usein palveluiden käyttäjät voidaan jakaa vielä pienempiin käyttäjäryhmiin jonkin kriteerin mukaan. Seuraavaksi käydään läpi TKK:n atk-palvelujen käyttäjät käyttäjäryhmittäin. Jako käyttäjäryhmiin on tehty käyttäjien roolin mukaan.

3.2.1 Opiskelijat

Opiskelijat ovat suurin käyttäjäryhmä Teknillisessä korkeakoulussa. Suurin osa opiskelijoista on nuoria, alle 28-vuotiaita. Opiskelijoissa voi olla useita pienempiä ryhmiä, joiden käyttötottumukset eroavat toisistaan mutta koko Teknillistä korkeakoulua ajatellen ovat opiskelijoiden tarpeet melko homogeenisiä. Opiskelijoiden perustarpeita tietotekniikan kannalta ovat kursseille ilmoittautumiset, harjoitustöiden tekemiset ja omien opintosuoritusten seuranta. Varsinkin ensimmäisen vuoden opiskelijoiden tietotekninen taitotaso saattaa olla hyvinkin matala, jolloin palveluiden käytettävyys korostuu. Opiskelijoiden tietotekniikan käyttö saattaa olla hyvinkin katkonaista päivän mittaan. Tietotekniikan käyttöä katkovat luennot ja harjoitukset. Opiskelijat voivat kuulua myös muihin käyttäjäryhmiin osa-aikatyönsä perusteella.

3.2.2 Opetushenkilökunta

Opetus- ja tutkimushenkilökunta on laaja käyttäjäryhmä, jolla on paljon erityistarpeita. Opiskelijoiden tarpeista useimmat ovat opetushenkilökunnan tekemien päätöksien ja toimien määräämiä. Eri kurssit käyttävät erilaisia elektronisia palveluja, joissa kaikissa opiskelijoiden täytyy pystyä yksilöitymään. Opiskelijoiden tarpeiden lisäksi opetushenkilökunnan täytyy pitää kirjaa opiskelijoiden kurssisuorituksista ja pystyä hallinnoimaan käyttämiään elektronisia palveluja. Tutkimushenkilökunnan tarpeet keskittyvät oman tutkimusalan erikoisohjelmien ja –laitteiden käyttöön. Henkilökunnalla on oma työasema, josta käyttö useimmiten tapahtuu. Henkilökuntaa koulutetaan työn kannalta olennaisten ohjelmien käyttöön.

3.2.3 Muu henkilökunta

TKK:n muu henkilökunta koostuu suurimmaksi osaksi opetus- ja tutkimushenkilökuntaa tukevasta henkilöstöstä ja hallinnosta. Muun henkilökunnan tarpeet ovat hyvin homogeenisiä. Toimisto-ohjelmat ja eri toimintoja varten olevat palvelut, kuten esimerkiksi laskutus, ovat tärkeitä. Muun henkilökunnan yleinen taitotaso vaihtelee tietotekniikan tehokäyttäjien vuosien kokemuksesta vasta-alkajien yleisimpien toimisto-ohjelmien tietämykseen.

3.2.4 Vierailijat

Vierailijat ovat käyttäjäryhmänä ehkä yksi tarpeiltaan hajanaisimmista. Vierailija voi olla esimerkiksi toisen yliopiston professori tai yrityselämän edustaja pitämässä vierailijaluentoa, opiskelija toisesta yliopistosta osallistumassa TKK:ssa järjestettävälle kurssille tai kokonaan ulkopuolinen. Vierailijoiden tarpeet rajoittuvat yleensä vain sähköpostin lukuun ja internetin käyttöön mutta voivat olla myös monimuotoisempiakin kuten oman kannettavan tietokoneen kytkeminen tietoverkkoon ja ennalta valmistetun esitelmän esittäminen luentosalin valkokankaalla.

3.2.5 Kansainväliset opiskelijat

TKK on määritellyt kansainväliset opiskelijat kahdella kriteerillä; kansainvälinen opiskelija ei ole Suomen kansalainen ja on suorittanut opintonsa ulkomailla. Kansainvälisillä opiskelijoilla ei näin ollen ole suomalaista henkilötunnusta. Kansainvälisten opiskelijoiden erityispiirre on suurempi vaihtuvuus kotimaisiin opiskelijoihin verrattuna. Useat kansainväliset opiskelijat ovat TKK:ssa vain yhden tai kaksi lukukautta. Tämä kansainvälisten opiskelijoiden vaihtuvuus on haaste etenkin tietoteknisten palveluiden käyttöön oikeuttavien lupien hallinnalle. Kansainväliset opiskelijat ovat kuitenkin käyttäjinä samanlaisia kuin opiskelijat ja jatko-opiskelijat erotuksena vain suurempi viestimistarve kotimaahansa. Tämä näkyy erilaisten pikaviestinten ja sähköpostien suurena käyttönä. Vieraskielisille käyttäjille on tärkeää myös löytää sama ohjeistus kuin suomenkielisille.

3.2.6 Ylläpitäjät

Ylläpitäjät muodostavat oman hyvin pienen alaryhmänsä. Ylläpitäjät kuuluvat usein myös johonkin muuhun käyttäjäryhmään mutta lisänä heillä on eritasoisia ylläpitämisvastuita, -käyttäjätunnuksia ja -rooleja. Lisäksi tähän ylläpitäjä-kategoriaan lasketaan mukaan myös erilaisten tietokantojen ja rekisterien pääkäyttäjät. Ylläpitäjät ovat usein tietotekniikan tehokäyttäjiä.

3.2.7 Virtuaaliset käyttäjät

Virtuaaliset käyttäjät ovat käyttäjiä, jotka suurimmaksi osaksi käyttävät TKK:n palveluja verkon välityksellä etänä. Virtuaaliset käyttäjät eivät tällöin ole fyysisesti käyttämässä TKK:n tiloja ja laitteita mutta etenkin tietojärjestelmät tulee mitoittaa myös etäkäyttö huomioiden. Virtuaalinen käyttäjä kuuluu tällöin aina myös johonkin muuhun käyttäjäryhmään vaikka hänellä onkin suuremmat tarpeet palvelujen toimimiseen missä vain ja milloin vain.

3.3 Toteutettu käyttäjätutkimus

Käyttäjätutkimuksen kohderyhmänä olivat kaikki TKK:n atk-palveluiden käyttäjät. Valitun tutkimusmenetelmän tuli tavoittaa kaikki käyttäjät yhtäläisesti ja asettaa heidät saman arvoiseen asemaan tutkimukseen nähden.

Tutkimuksen tavoitteena oli kartoittaa käyttäjien tapoja salasanojen käytössä ja mielipiteitä salasanoista TKK:n palveluissa. Lisäksi tutkimus kartoittaa käyttäjien tyytyväisyyttä niin TKK:n kuin atk-keskuksenkin tarjoamiin palveluihin. Tutkimuksen tulosten perusteella pitää voida arvioida käyttäjien tarpeet salasanojen käyttämisessä ja pystyä päättelemään käyttäjien mahdolliset reaktiot kertakäyttösalasanajärjestelmiin. Tutkimus tuli voida suorittaa nopeasti ja suhteellisen pienillä henkilöresursseilla.

Käyttäjätutkimuksen täytyi olla toistettavissa ja tutkimuksien tulosten sitten helposti vertailtavissa keskenään. Tutkimukselta haluttiin saada vastaukset seuraaviin tutkimuskysymyksiin:

1. Millainen tarve kertakäyttösalasanoilla on?
2. Miten käyttäjät kokevat nykyiset ja kertakäyttösalasanat?
3. Miten TKK hyötyy ja mitä kertakäyttösalasanoilla saavutetaan?

Käyttäjätutkimusmenetelmäksi valittiin Internetkysely. Kysely valittiin käyttäjätutkimusmenetelmäksi sen antamien kvantitatiivisten tulosten johdosta. Osasyinä valintaan olivat kyselyn nopeus, kyselyn mahdollistama suurempi otoskoko verrattuna muihin menetelmiin ja käytössä olevat resurssit.

Asetetuista tutkimuskysymyksistä kaksi ensimmäistä saavat vastauksensa suoritetusta käyttäjätutkimuksesta ja kolmas jäljempänä.

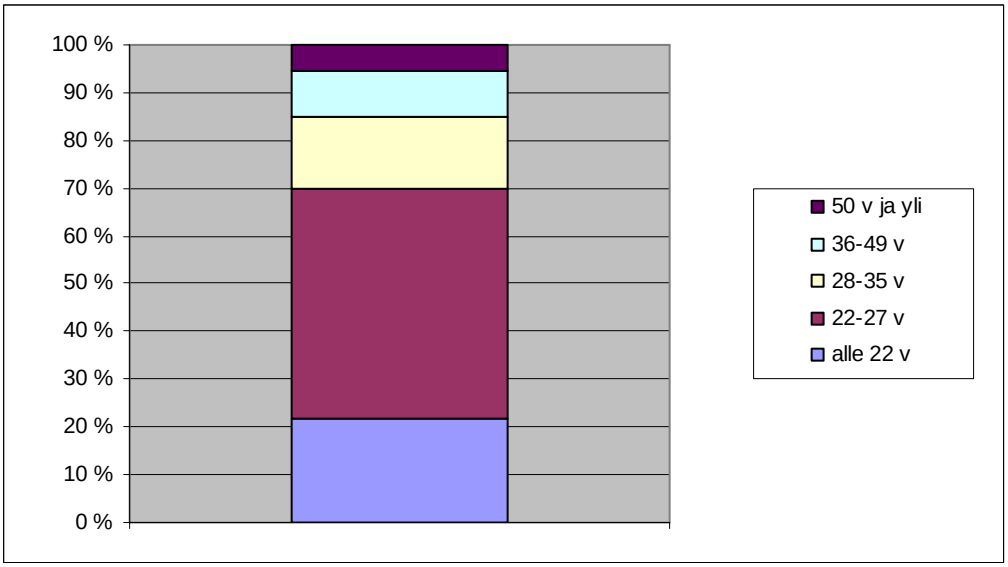
Tutkimuskysymyksien määrittelyn jälkeen aloitettiin kyselyn kysymyksien muodostaminen. Kysely muodostui kolmesta osasta tässä järjestyksessä: taustatiedoista, koko TKK:a koskevasta osasta ja atk-keskusta koskevasta osasta. Taustatiedoissa kysyttiin vastaajan sukupuolta, ikää sekä ensisijaista suhdetta TKK:uun. TKK:a koskevassa osassa kysyttiin yleisiä salasanan käyttötapoja ja suhtautumista salasanoihin sekä kuinka paljon vastaaja käyttää TKK:n salasanaa vaativia palveluja. Pelkkää atk-keskusta koskeva osa oli lyhyt, jossa keskityttiin lähinnä määrittämään tyytyväisyyttä nykyisiin palveluihin ja salasanojen käyttöön. Kyselyn kysymykset testattiin ensin atk-keskuksen henkilökunnan edustajilla ja viimeiseksi maallikolla TKK:n ulkopuolelta selkeätajuisuuden selvittämiseksi. Lopullisen kysymystenasettelun jälkeen samat kysymykset käännettiin myös englanniksi suuremman vastaajakunnan saamiseksi. Englanniksi olevista kysymyksistä 8 ja 9 kuitenkin jäi pois vastausohje, joten englanninkielisen kyselyn vastauksia näihin kysymyksiin ei ole otettu lopputuloksissa huomioon.

Kysely julkaistiin internetissä toukokuussa 2006, jolloin myös sähköpostitse lähetettiin osallistumiskutsut 400:lle satunnaisesti valitulle atk-keskuksen käyttäjälle. Kutsu oli laadittu sekä suomeksi että englanniksi ja sisälsi suorat linkit molemmankielisiin kyselyihin sekä kyselystä tarkemmin kertovalle verkkosivulle. Kutsussa ei ollut mainittu vastaustakarajaa mutta kolmen viikon kuluttua kutsun lähettämisestä ei uusia vastauksia enää saapunut kyselyyn.

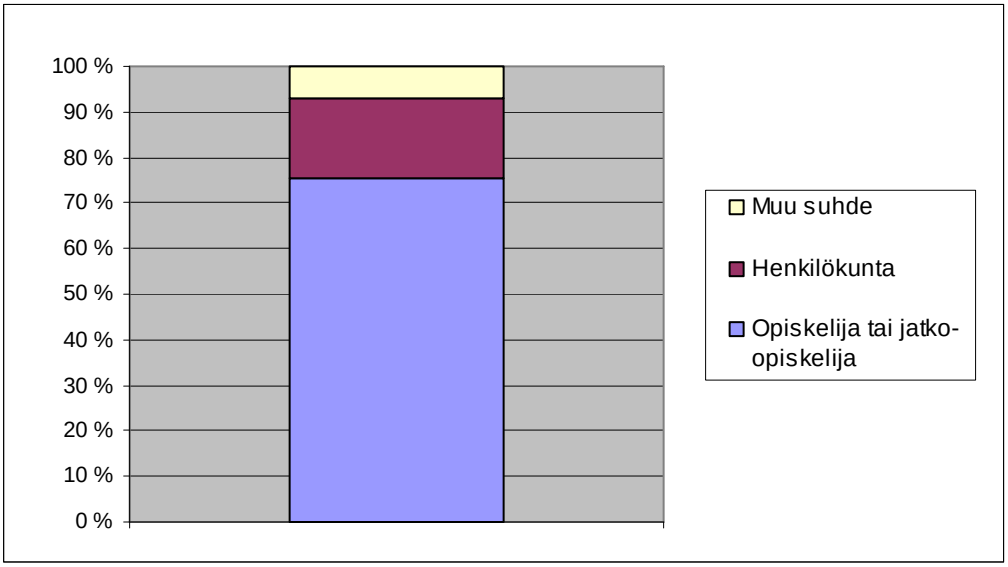
Seuraavaksi käydään läpi toteutetun kyselyn tulokset. Kyselyn kysymykset löytyvät liitteestä A. Seuraavassa kappaleessa olevat viittaukset viittaavat suoraan kyselyn kysymyksiin ja vastauksiin. Kyselyn tulokset löytyvät liitteestä B.

3.3.1 Kyselyn tulokset

400:stä kutsutusta tutkimukseen osallistui 73 henkilöä vastausprosentin ollessa tällöin 18 %. Miehiä vastaajista oli 73 % ja naisia 27 %. Vastaajien ikäjakauma oli kuvaajan 1 mukainen. Kuvaajassa 2 näkyy vastaajien ensisijainen suhde TKK:uun. Suhde TKK:uun on tässä pelkistetty opiskelijaan tai jatko-opiskelijaan, henkilökuntaan ja muuhun suhteeseen. Kyselyn tulokset löytyvät liitteestä B. Liitteessä kyselyn tulokset ovat lisäksi jaoteltu taustatiedoittain. Tässä kappaleessa käydään läpi kyselyn tärkeimpiä tuloksia.



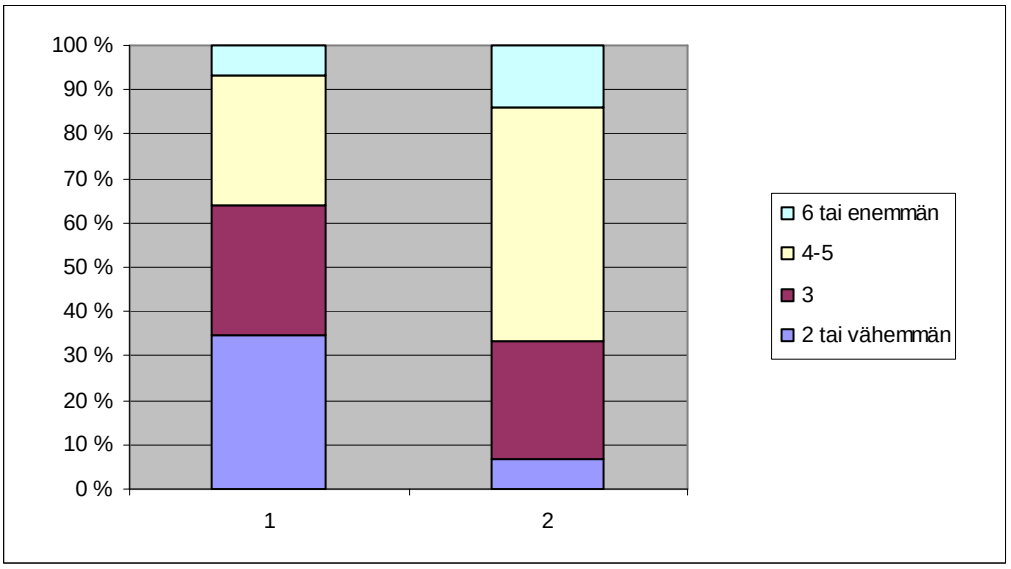
Kuvaaja 1 Ikäjakauma



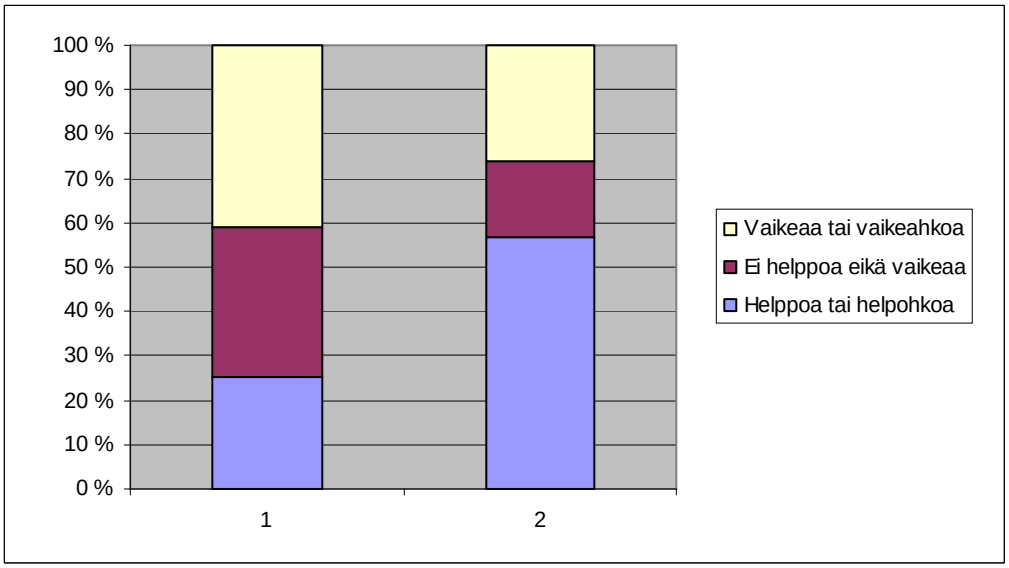
Kuvaaja 2 Ensisijainen suhde TKK:uun

Salasanojen määrä käyttäjillä on suuri. Vastaajista neljäsosalla on käytössään kolme ja yli puolella 4-5 salasanaa. Vain pienellä osalla vastaajista salasanoja on käytössä vielä tätäkin enemmän. Nämä salasanojen lukumäärät koskevat vain TKK:n palveluissa käytettäviä salasanoja. Koska salasanoja on käytössä näin paljon, on käyttäjillä vaikeuksia muistaa niitä kaikkia. Esimerkiksi salasanoja on kolme tai vähemmän käytössään yhteensä vain kolmasosalla vastaajista (kuvaaja 3, kohta 2). Kuitenkin vastaajista kolmannes muistaa vain kaksi salasanaa tai vähemmän (kuvaaja 3, kohta 1). Paljon salasanoja käyttävät vastaajat, joilla salasanoja on käytössään kuusi tai enemmän, eivät kuitenkaan muista salasanojaan yhtään sen paremmin; vain puolet heistä sanoi muistavansa salasanoistaan kuusi tai enemmän.

Tuloksista käykin ilmi selvästi, että harva muistaa kaikki käyttämänsä salasanat. Tämän myös vahvistaa, että kysyttäessä kuinka vaikeana käyttäjät pitivät salasanojen muistamista, suuri osa vastaajista piti muistamista vaikeana (kuvaaja 4, kohta 1). Kuitenkin toisinpäin asiaa kysyttäessä, eli kuinka helppona käyttäjät pitivät salasanojen muistamista, pienempi osa vastaajista piti muistamista vaikeana tai vaikeahkona. Suurin osa vastaajista piti muistamista päinvastoin helppona tai helpohkona (kuvaaja 4, kohta 2). Tästä voidaan päätellä, että reilu kolmannes vastaajista piti salasanojen muistamista yleensä vaikeana tai jonkin verran vaikeana. Vaikka enemmistö pitääkin salasanojen muistamista yleensä enemmän helppona kuin vaikeana, 64 % vastaajista myönsi, että joidenkin salasanojen muistaminen on vaikeata tai vaikeahkoa.



Kuvaaja 3 Muistettuja salasanoja (1) ja käytössä olevia salasanoja (2)



Kuvaaja 4 Salasanojen muistamisen vaikeus (1) ja helppous (2)

Koska käyttäjillä on vaikeuksia muistaa kaikkia salasanojaan, keksivät he erilaisia keinoja parantaa muistamistaan. Yksi keinoista on käyttää samaa salasanaa useassa eri palvelussa. Vastaajista ainoastaan neljännes ei ollut tehnyt näin. Toinen suosittu tapa on salasanojen kierrättäminen eli vanhemman, muistetun, salasanan käyttäminen uudelleen. Vastaajista vain alle viidennes ei ole kierrättänyt salasanoja. Näin ollen kaikkien käyttäjien salasanat eivät vaihdu suunnitellusti ja väärinkäytökset ovat helpompia.

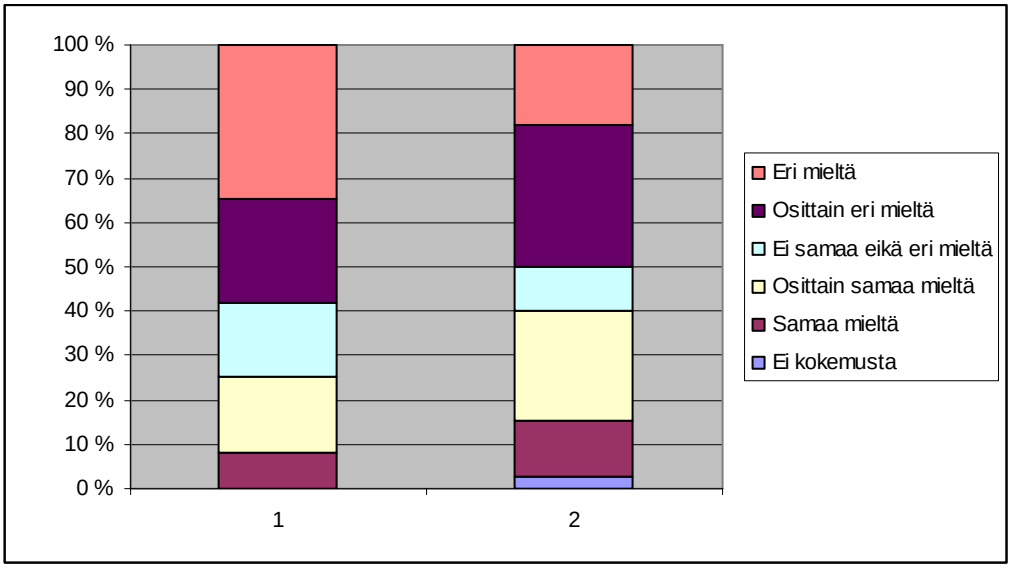
Salasanojen muistamista helpotetaan myös kirjoittamalla ne muistiin jonnekin. 46 % vastaajista kirjoittaa uuden salasanan muistiin ja lisäksi 28 % kirjoittaa uuden salasanan muistiin joskus. Useamman kerran viikossa käytettävät salasanat kuitenkin muistetaan suhteellisen hyvin. Tällaiset salasanat muistaa ulkoa 93 % vastaajista. Harvemmin käytetyt salasanat muistettiin huonommin. Vastaajista 45 % muistaa nämäkin salasanat ulkoa mutta 25 % säilyttää salasanojaan kalenterissa, 13 % lapulla lompakossa ja 14 % matkapuhelimessa. Valitettavasti myös tarralapuille kirjoitetut salasanat tietokoneen lähellä olivat saaneet TKK:n henkilökunnan osalta kannatusta.

Nykyinen salasanakäytäntö on rasittava paitsi käyttäjille niin myös atk-ylläpitäjille. Esimerkiksi TKK:n atk-keskuksen pää- ja windowssalasanat vanhenevat kuudessa kuukaudessa. Kun pääsalasana vanhenee, sulkeutuu myös käyttäjän tunnus. 41 %:lle vastaajista tämä on tapahtunut joskus. Sulkeutuneen tunnuksen voi aukaista vain ottamalla yhteyttä atk-keskuksen asiakaspalveluun. Vastaajista

- 12 % oli soittanut atk-keskuksen asiakaspalveluun.
- 22 % oli käynyt asiakaspalvelupisteessä.
- 14 % oli lähestynyt atk-keskusta sähköpostitse.

Vaikka osa vastaajista on käyttänyt useampaa palvelukanavaa, voidaan pitää todennäköisenä, että ainakin tämä 41 % kyselyyn vastanneista on ollut yhteydessä atk-keskuksen asiakaspalveluun.

Nykyiset salasanat eivät saaneet vastaajien keskuudessa kovinkaan suurta kannatusta. Vastaajista 8 % mielestä salasanojen vaihtaminen on hankalaa ja 17 % mielestä jonkin verran hankalaa (kuvaaja 5, kohta 1). Tämä luultavasti johtuu salasanan laadun tarkistuksesta, jolloin järjestelmä ei hyväksy kaikkia salasanoja. 13 % kyselyyn osallistujista vastasi, että usein järjestelmä ei hyväksy uutta salasanaa (kuvaaja 5, kohta 2). Näiden lisäksi 25 % vastaajista on ollut samanlaisia ongelmia mutta ei niin usein. Vastaajista vain 25 %:lle järjestelmä yleensä hyväksyi ensimmäisen käyttäjän ehdottaman salasanan. Suurimman osan salasananvaihtokerroista ilman hyväksymisongelmia sai lisäksi tehtyä 35 % vastaajista.



Kuvaaja 5 1) Salasanan vaihto on hankalaa. 2) Järjestelmä usein ei hyväksy uutta salasanaa.

Käyttäjien mielestä eri salasanoja on käytössä liikaa. Vastaajista vain kolmannes oli sitä mieltä, että salasanojen määrä on sopiva tai melkein sopiva. 60 % vastaajista oli sitä mieltä, että salasanoja on liikaa tai jonkin verran liikaa. 39 % tosin myös vastasi, että pystyisi muistamaan enemmänkin salasanoja, jos sellaiseen vain olisi tarvetta.

Salasanojen unohtaminen ei kuitenkaan ole ainoa ongelma. Salasanoja käytetään myös suoraan samoina muihinkin palveluihin. Tällöin voi käydä niin, että käyttäjä ei muista palvelun käyttämää salasanaa ennen kokeilemista. Kyselyyn vastanneista joka viides kirjoittautui johonkin palveluun väärällä salasanalla usein tai useahkosti. Vaikka salasanojen käyttö on yli puolelle vastaajista helppoa tai helpohkoa, reilu kuudennes vastaajista pitää salasanojen käyttöä työläänä. Neljännes vastaajista myös kokee salasanojen käytön hidastavan työskentelyään ainakin jollain tasolla.

Tällaisiin mielipiteisiin voi osasyynä olla myös salasanojen käyttöä koskevan tiedon vaikea saatavuus. Tähän saattaisi antaa viitteitä se, että 14 % kyselyyn vastanneista ei pitänyt tietoa salasanoista helposti saatavana.

Tutkimus myös kartoitti käyttäjien etäkäyttötottumuksia. Puolet vastaajista ei ollut koskaan käyttänyt TKK:n salasanallisia palveluita ulkomailta. Suurin osa vastaajista, jotka käyttivät TKK:n palveluja ulkomailta, käyttivät niitä 1-4 kertaa vuodessa. Tosin 10 % vastaajista ilmoitti käyttävänsä TKK:n palveluja ulkomailta useammin kuin kerran kuukaudessa. Palveluiden etäkäyttö onkin TKK:ssa varsin yleistä. Melkein puolet

vastaajista ilmoitti käyttävänsä TKK:n verkkopalveluita pääosin etänä. Etäopiskelu tai –työskentely ei kuitenkaan ole aivan yhtä yleistä. Tutkimukseen vastanneista käyttäjistä reilu viidennes ilmoitti työskentelevänsä tai opiskelevansa etänä. Suurin osa (72 %) vastaajista ei pitänytkään itseään etäopiskelijana tai –työläisenä. Kuitenkin läsnäoloa TKK:ssa kysyttäessä neljännes vastaajista ilmoitti käyvänsä TKK:ssa vain kerran viikossa tai harvemmin siinä missä suurin osa (69 %) useita kertoja viikossa.

Käyttäjätutkimuksessa kartoitettiin myös käyttäjien tyytyväisyyttä niin TKK:n kuin atk-keskuksenkin palveluihin. TKK:n palveluihin ja saatuun palveluun oli valtaosa vastaajista pääosin tyytyväisiä. Vaikka atk-keskuksen palveluihin oltiin tyytyväisiä samoissa määrin kuin TKK:n palveluihin yleensä, oli tyytymättömyys atk-keskuksesta saatuun palveluun suurempaa kuin koko TKK:sta puhuttaessa.

3.4 Tutkimuksen luotettavuus

Suoritetun käyttäjätutkimuksen virhemarginaali on noin 11 %. Tämä on laskettu 95 % luottamusvälillä, kun otoskoko on 73 käyttäen kaavaa:

$virhemarginaali \approx \frac{0{,}98}{\sqrt{n}}$ (Moore & McCabe, 2005).

Vaikka tutkimuksen otoskoko oli suhteellisen pieni, vastaavat tutkimuksessa kysytyt taustatiedot ja TKK:n tilastot toisiaan virhemarginaalin puitteissa. Kyselyn tulokset voivat silti olla vääristyneitä, koska 400:sta kutsutusta vain 73 käyttäjää vastasi kyselyyn ja vastaamatta jättäneiden käyttäjien tilastoja ei tiedetä muilta osin. Käyttäjätutkimuksen tuloksiin voivat vaikuttaa myös muut asiat kuten kutsumistapa tutkimukseen, pelko nimettömyydestä kyselyssä, haluttomuus vastata kysymyksiin, mitkä kartoittivat käyttösääntöjä rikkovia tapoja, ja vastaajien halu miellyttää kysymyksen asettajaa vastaamalla suuremmassa osassa vastauksia myötäilevästi.

Kyselyyn valikoitui kutsujen kautta atk-keskuksen käyttäjiä, koska kutsu lähetettiin sähköpostilla käyttäjän atk-keskuksen sähköpostiosoitteeseen. Olisivatko tulokset olleet toisenlaisia, jos kutsu tutkimukseen olisi esitetty atk-keskuksen uutisryhmässä tai verkkosivuilla? Mahdollisesti vastaajat olisivat ensin mainitussa tapauksessa olleet

aktiivisimpia atk-keskuksen palvelujen käyttäjiä ja jälkimmäisessä tapauksessa aktiivisimpia atk-keskuksen verkkosivuilla vierailleita ihmisiä. Tämä olisi ollut parempi vaihtoehto suoritettaessa kvalitatiivista tutkimusta, koska kaikki erilaiset mielipiteet ja vastaukset olisivat saaneet saman painoarvon. Kvantitatiivisessa tutkimuksessa yleisin mielipide on painavin ja huomionarvoisin.

Kyselyn ajankohta toukokuussa 2006 saattoi myös vaikuttaa joidenkin opiskelijoiden vastaamiseen, koska tenttikaudella kaikki opiskelijat eivät välttämättä käy TKK:ssa tai lue sähköpostejaan joka päivä.

4 Laiteympäristö TKK:ssa ja atk-keskuksessa

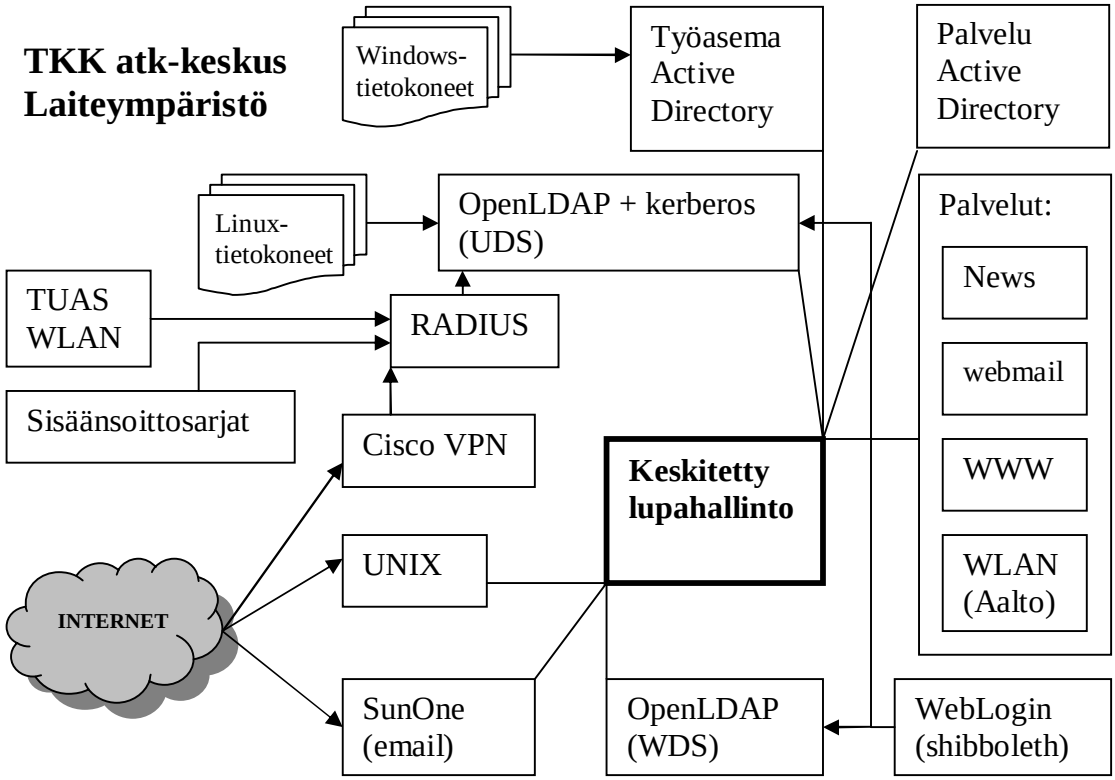
Käyttäjien lisäksi myös jo olemassa olevat järjestelmät ovat tärkeitä. Uutta todentamismenetelmää mietittäessä ei vanhojen järjestelmien yhteensopivuuksia voida unohtaa. Pahimmillaan yhteensopimattomuus voi johtaa kalliisiin muutostöihin joko olemassa oleviin järjestelmiin tai hankittavaan todentamismenetelmään. Tämän takia jo olemassa olevien järjestelmien todennusmenetelmät täytyi selvittää. Tässä luvussa käydään läpi olennaisimmat järjestelmät TKK:ssa ja niiden käyttämät todennustekniikat.

Teknillinen korkeakoulu tarjoaa useita erilaisia salasanoja käyttäviä palveluita. Osa palveluista on pelkästään sisäiseen käyttöön ja osalla palveluista tietoturvavaatimukset ovat korkeammat. Palvelut on toteutettu monien erilaisten tekniikoiden avulla. Keskeisiä palveluja TKK:ssa ovat sähköposti, Linux-kotihakemistot sekä luokka- ja työhuonetietokoneet. Lisäksi on olemassa lukuisia palveluja suunnattuina TKK:n eri käyttäjäryhmille. Näiden toimintojen turvaaminen tapahtuu taustalla olevien palvelujen ja järjestelmien avulla. Kuva 2 selventää eri palvelujen käyttämiä todentamismenetelmiä. Kuvassa on viivoilla kuvattu käyttäjä- ja salasanatietojen siirtoa järjestelmiin ja nuolilla todentamistapahtumia.

TKK:n atk-keskuksen luokka- ja työhuonewindowstietokoneet tarkistavat käyttäjän salasanan Active Directorystä[1], AD:stä. Tällä hetkellä atk-keskuksessa ei ole kuin yksi Windowstoimialue käytössä mutta tulevaisuudessa opiskelijoille ja henkilökunnalle voi olla olemassa omansa kummallekin. Luokka- ja työhuonelinuxtietokoneet puolestaan tarkistavat salasanan OpenLDAP[2]-palvelimelta. Unix-yleispalvelimissa salasanan tarkistus hoidetaan perinteisemmin vertaamalla syötettä paikalliseen kopioon salasanatietokannasta. Lisäksi TKK:ssa on joillakin osastoilla vielä käytössä paikallisesti asennettuja työasemia, omia järjestelmiä ja lupahallintoja. Näissä järjestelmissä olevat salasanat ja käyttäjätunnukset toimivat vain paikallisesti. Nykyisin keskitetty lupahallinto hallinnoi kuitenkin suurta osaa TKK:n tietokoneiden

[1] Active Directory on Microsoftin hakemistopalvelin, josta käsin voi hallinnoida koko Windows-toimialuetta. (Microsoft, 2006)
[2] OpenLDAP on avoimen lähdekoodin toteutus hakemistopalvelusta käyttäen LDAP-yhteyskäytäntöä. Verkkosivut: http://www.openldap.org/ (Saatavuus 30.10.2006)

käyttöoikeuksista vaikkakaan ei kaikkia. Tulevaisuuden tavoite on, että TKK:ssa on yhtenäinen keskitetty lupahallinto.



Kuva 2 Laiteympäristö TKK:ssa keskitetyn lupahallinnon näkökulmasta

Luokka- ja työhuonetietokoneiden lisäksi käytetyin palvelu tällä hetkellä on sähköposti. Sähköpostia myös käytetään ulkomailta vaikka sähköpostin käyttämät yhteystavat eivät ole tietoturvallisimpia. Sähköpostipalvelu on TKK:n atk-keskuksessa rakennettu SunOne-järjestelmän päälle. Sähköposti toimii POP-[3] tai IMAP-[4] protokollia tukevilla asiakasohjelmilla tai Sunin toimittamalla omalla webmaililla.

Tulevaisuudessa tärkeää roolia etäkäytön kannalta näyttelee TKK:n VPN-ratkaisu. VPN (Virtual Private Network) tarkoittaa näennäistä yksityisverkkoa eli etäkäyttäjän tietokone näkyy verkossa kuin se olisi paikallisessa verkossa TKK:ssa. VPN toteutetaan yleensä ohjelmistollisesti. Vahvan todennuksen tulee toimia myös käytettävän VPN-ratkaisun kanssa, joka tällä hetkellä on Ciscon toimittama.

[3] Post Office Protocol on käytetyimpiä sähköpostin lukemiseen käytettyjä yhteyskäytäntöjä.
[4] Internet Message Access Protocol on POP-protokollaa uudempi ja monipuolisempi sähköpostin lukemiseen tarkoitettu yhteyskäytäntö.

TKK:ssa on myös tehty päätös Exchange[5]-palvelun käyttöönotosta (THJR, 2006). Exchange Microsoftin tuotteena todentaa käyttäjät käyttäen Windowstoimialueen AD:ä. Tällöin Exchange-palvelu ei tuo uusia vaatimuksia kertakäyttö- ja dynaamisille salasanajärjestelmille.

Palvelimia on lisäksi monia muitakin. Erilaisia ohjelmistoalustoja on palvelimilla käytössä vain muutamia, jotka jakaantuvat kolmeen pääasialliseen ryhmään: Windows-, Linux- ja unixohjelmistoalustoihin. Käyttäjien todentamismenetelmät näissä ohjelmistoalustoissa ovat kuitenkin jo edellä mainittu (Windows-alusta vertaa salasanatietoa AD:stä löytyvään tietoon, Linux- ja unixalusta joko OpenLDAP-palvelimelta tai paikallisesta käyttäjätietokannasta löytyvään tietoon).

Atk-keskuksessa on lisäksi käytössä Oracle-tietokanta[6]. Oracle-tietokanta käyttää omia käyttäjätunnuksia ja salasanoja, jotka ovat lupahallinnosta erillään omassa järjestelmässään.

Kertakäyttö- tai dynaamisen salasanajärjestelmän tulee pystyä toimimaan varsin monipuolisessa laiteympäristössä. Todentamisjärjestelmän tulee tukea useampaa Microsoftin Active Directoryä, OpenLDAPia, RADIUSta[7], Cisco VPN:ia, Unixeja (Tru64, Solaris 9/10) ja SunOne järjestelmää. Lisäksi todentamisjärjestelmän tulee olla helposti muokattava tai tarjottava ohjelmointirajapinta muiden mahdollisten palvelujen varalta.

4.1 Vahva todentaminen maailmalla

Vahva todentaminen on otettu käyttöön etenkin verkkopankeissa ympäri maailman. Tämä on ymmärrettävää, koska nykyisin käytännöllisesti katsoen kaikki raha liikkuu pankkien kautta. Yliopistot poikkeavat pankeista siinä, että rahaa ei käsitellä suoraan

[5] Exchange on Microsoftin viestintäratkaisu, joka tarjoaa mm. sähköpostin ja kalenterin keskitetysti. (Microsoft, 2006)
[6] Oracle-tietokanta on Oraclen tekemä tietokantaohjelmisto. Verkkosivut http://www.oracle.com/ (Saatavuus 30.10.2006)
[7] RADIUS on yhteyskäytäntö, jota voidaan käyttää tietojen todennusta, valtuutusta ja kirjausta vaativissa ohjelmistoissa.

niin paljon mutta tietomäärät ovat huikeat ja voivat olla joillekin osapuolille ratkaisevan arvokkaita.

Siinä missä pankit ja erilaiset rahalaitokset käyttävät vahvaa todentamista asiakkaiden henkilöllisyyksien todentamiseen, käyttävät ne vahvaa todentamista myös asiakkaiden sähköisiin allekirjoituksiin. Korkeaa turvallisuutta vaativat laitokset ovat käyttäneet vahvaa todennusta jo pitkään. Nämä laitokset ovat suurimmalta osaltaan militaarisia, joissa luotettavalle todentamiselle on suuri tarve. Etenkin Yhdysvalloissa on vahva todentaminen käytössä myös valtion virastoissa yleisesti. Lisäksi Yhdysvalloissa toimivien lääkintälaitosten täytyy noudattaa HIPAA-lainsäädäntöä, mikä asettaa niille erittäin tarkat vaatimukset potilastietojen käsittelyyn (Health Insurance Portability and Accountability Act, 1996). Monet lääkintälaitokset ovatkin siirtyneet käyttämään erilaisia kertakäyttö- tai dynaamisia salasanoja niitä vaativissa sovelluksissa.

Turvallisuusteknologian yritykset käyttävät vahvaa todentamista omissa järjestelmissään. Etenkin turvallisuuskonsultointiyritykset ovat vahvan todentamisen osalta edelläkävijöitä. Yksi syy käyttää vahvaa todentamista onkin sen yritykselle antama myönteinen julkisuus tietoturvallisuuden osalta. Varsinkin turvallisuusteknologian yrityksille suuren yleisön mielikuvat yrityksen turvallisuudesta ovat erittäin arvokkaita.

Suomen viranomaisetkin ovat heränneet kasvavaan luotettavan todentamisen tarpeeseen. Valtiovarainministeriö, joka vastaa Suomessa Valtionhallinnon tietoturvallisuuden johtoryhmästä VAHTIsta, on puoltanut vahvan todentamisen käyttöönottoa valtion virastoissa ja tietojärjestelmissä julkaisemissaan tietoturvaohjeissa. Esimerkiksi VAHTI ohjeessa 5/2004 sanotaan ”mikäli jokin erityistapaus ehdottomasti vaatii etäyhteyttä keskeisiin järjestelmiin joko käyttöä tai hallintaa varten, tulee noudattaa seuraavaa periaatetta: etäyhteyden muodostamiseen vaaditaan vahva käyttäjätodennus, johon tarvitaan salasanan tai PIN-koodin lisäksi fyysinen elementti, kuten toimikortti tai kertakäyttösalasanoja generoiva laite”.

Suomessa ei vahvaa todentamista tiettävästi ole otettu oppilaitoksissa vielä käyttöön, vaikka alan toimijoiden mukaan kyseisiä vahvan todentamisen käyttöönottoon tähtääviä projekteja on käynnissä parissakin paikassa (Vilander, 2006). Oppilaitokset, kuten

yliopistot, poikkeavat kaupallisista yrityksistä siinä, että niiden ei tule tehdä voittoa vaan antaa opetusta. Tällöin oppilaitoksissa voi myös olla vaikeampi perustella päätöstä kertakäyttösalasanapalvelun tai dynaamisen salasanapalvelun hankkimisesta, koska ei voida suoraan laskea siitä tulevia hyötyjä.

Israelissa yliopistot käyttävät vahvaa todentamista etäyhteyksiin. Esimerkiksi Haifan yliopistossa yhteyspaketti maksaa opiskelijoille $30 (Fried, 2006), joka sisältää poletin ja ohjelmisto-cd:n. Henkilökunnalle yhteyspaketti on ilmainen. Muut yliopistot Israelissa käyttävät samaa mallia, jossa opiskelijat joutuvat ostamaan käyttämänsä poletin. Etäyhteydet yliopistolle toimivat vain vahvaa todentamista käyttämällä. Muualla maailmassa oppilaitokset eivät ole näin suurissa määrin toteuttaneet vahvaa todennusta kertakäyttö- tai dynaamisia salasanoja käyttämällä. Luultavasti Israelin herkkä turvallisuustilanne pakottaa oppilaitoksetkin käyttämään vahvaa todennusta palveluissaan.

5 Kertakäyttö- ja dynaamiset salasanatuotteet

Kertakäyttö- ja dynaamisia salasanoja voidaan käyttää moniin eri tarkoituksiin. Kertakäyttö- ja dynaamisten salasanojen suurin etu on niiden tarjoama vahva todentaminen. Tulevaisuudessa, kun asiointi keskittyy yhä enemmän verkkoon, tulee sähköinen henkilöllisyys olemaan paljon tärkeämpi kuin nykyisin. Tämä jo yksistään asettaa vaatimuksia luotettavalle todentamiselle.

Tässä luvussa käydään läpi tarjolla olevat kertakäyttö- ja dynaamiset salasanatuotteet. Arvioitaville tuotteille määritellään aluksi vertailukriteerit, jonka mukaan tuotteiden vertailu on suoritettu. On huomattava, että kaikki tarjolla olevat ja tässä diplomityössä arvioidut tuotteet eivät sovellu kaikkiin käyttötapauksiin. Erilaisia käyttötapauksia käsitellään tarkemmin seuraavassa luvussa.

5.1 Vertailukriteerit

Turvallisuustuotteita on olemassa monenlaisia ja monella eri toimintatavalla. Kuitenkin kun valitaan käyttöönotettavaa tuotetta, tulee tuotteet voida arvioida paremmuusjärjestykseen. Jotta tuotteet voidaan laittaa paremmuusjärjestykseen, täytyy niiden arviointiin määritellä vertailukriteerit ja kriteerien väliset painoarvot.

TKK on valtion laitos, joten TKK:ssa joudutaan kilpailuttamaan hankittavat tuotteet ja palvelut. Ensimmäinen vertailukriteeri on siis tuotteen hinta. Hintaan sisältyy tuotteen hankinta-, käyttöönotto- ja ylläpitohinta. Hankintahinta ja ylläpitohinta ovat helpompia laskettavia kuin käyttöönottohinta. Hankintahinta saadaan suoraan tuotetta myyvältä osapuolelta. Ylläpitohinta puolestaan voidaan laskea keskimääräisinä henkilötyövuosina, mikä voidaan muuttaa edelleen euromääräiseksi hinnaksi. Käyttöönottohinta on hieman vaikeampi laskea. Käyttöönottohinta koostuu henkilöstön koulutuskuluista, mahdollisista logistiikkakuluista ja muista yllättävistä käyttöönottovaiheessa ilmenevistä kuluista ja viivytyksistä.

Mikään tuote ei voi kestää loputtomiin, joten tuotteiden elinkaari täytyy voida selvittää. Tärkeitä elinkaaren vertailumittareita ovat tuotteiden kesto, tuotetuen ja –takuun

kattavuus ja tuotteenvalmistajan luotettavuus sekä markkinatilanne. Pidempi elinkaari on parempi puhuttaessa TKK:n suuruisesta yksiköstä.

Tuotteiden valinnassa tärkeää osaa esittää myös hankittavan tuotteen yhteensopivuus TKK:n jo olemassa oleviin palveluihin ja atk-infrastruktuuriin. Yhteensopivuudelle voidaan laskea arvo, mikä tulee hankittavan tuotteen tekemisestä yhteensopivaksi TKK:n palveluille.

Tuotteiden käytettävyyttä ei sikäli voida mitata suoraan. Käytettävyys on aina käyttäjän kokema subjektiivinen arvo. Tuotteiden käytettävyyttä voidaan kuitenkin arvioida yleisesti hyväksytyillä arviointimenetelmillä. Nämä arviointimenetelmät sisältävät käytettävyyteen liittyviä sääntöjä, joiden mukaan tuotteiden käytettävyyttä voidaan arvioida (Faulkner, 2000). Yksi tärkeimmistä käytettävyyden mittareista on se, että käyttäjille jaettavien polettien tulee olla ulkonäöltään ja muotoilultaan sellaisia, että käyttäjät pitävät ne mielellään mukana eivätkä hyljeksi niiden käyttöä.

Yhtenä tärkeänä kriteerinä pitää myös mainita tuotteen tietoturvallisuus. Tuotteen toimintaperiaatteiden tulee olla tietoturvallisia ja yleisesti hyväksyttyjä, jotta ylimääräisiin tuotteen korjauksiin kesken tuotantokäytön ei jouduttaisi.

TKK:n atk-keskus käyttää todennusmenetelminään erilaisin tavoin toteutettuja käyttäjätunnuksia ja salasanoja. Tässä diplomityössä keskitytään atk-keskuksen todennusmenetelmiin ja oletetaan niiden kattavan suurimman osan todennusmenetelmistä TKK:ssa.

5.1.1 Kustannusten laskeminen

Tuotteiden lopullisia kustannuksia ei voi saada tarkasti selville ennen tuotteiden lopullista käyttöönottoa. Ylimääräisiä kustannuksia voi ilmetä vielä onnistuneen käyttöönoton jälkeenkin, kun kyseessä on näin laaja-alaisesti vaikuttava palvelu. Kustannuksia tulee kuitenkin pääasiassa kolmessa eri vaiheessa: käyttöönotto-, ylläpito- ja lopetus-/uusimisvaiheessa (Grand, 2001).

Käyttöönottovaiheen kustannukset ovat melko helposti laskettavissa. Käyttöönottokustannuksiin kuuluvat hankintahinta, lisenssimaksut, jakelusta kertyvät logistiikkakulut ja kulut muutostöistä, joita olemassa oleviin järjestelmiin joudutaan tekemään tuotteen käyttöönottovaiheessa. Lisäksi käyttöönottokustannuksiin tulee laskea käyttäjien koulutus uuden tuotteen käyttöön. Hankintahinnat ja lisenssimaksut saadaan suoraan tuotetta myyvältä taholta ja jakelusta kertyvät logistiikkakulut ovat kaikilla tuotteilla suunnilleen yhtä suuret. Muutostyökustannukset voivatkin olla hankintahinnan lisäksi eri tuotteilla eri suuruiset. Yhteensopivuus-kriteeri voidaan tällöin pelkistää hinnaksi käyttöönottovaiheen kustannuksiin lisättäväksi.

Ylläpitovaiheen kustannukset voidaan laskea tietyillä oletuksilla. Ylläpitokustannukset luultavasti ovat samaa suuruusluokkaa kaikilla tuotteilla johtuen niiden teknisistä ominaisuuksista. Perusoletuksena voidaan kuitenkin pitää päivystystä hävinneiden ja rikkoutuneiden polettien varalle. Päivystys vaatii yhden henkilön työpanoksen arkisin virka-aikaan. Käytännössä tämä henkilö voi tehdä muitakin työtehtäviä ja olla samaan aikaan tavoitettavissa poletteja koskevissa asioissa.

Lopetus- ja uusimisvaiheen kustannukset ovat sellaisia kustannuksia, joita tulee kun tuotteen käyttö lopetetaan kokonaan tai takuuajan jälkeen tuote uusitaan ja päivitetään vastaamaan sen hetkistä tilannetta. Lopetus- ja uusimiskustannukset voivat vaihdella tuotteittain, koska tuotteet eivät keskenään välttämättä ole suoraan yhteensopivia. Jos saman toimittajan tuotteen käyttöä jatketaan, pysyvät uusimiskustannukset yleensä maltillisen pieninä.

Tuotteiden elinkaarelle voidaan myös yrittää laskea hintaa. Esimerkiksi kun arvioidaan kolmen ja viiden vuoden takuiden eroja voidaan laskea lyhyemmästä takuusta tulevat säästöt ja arvioida lyhyemmästä takuusta syntyvät lisäkustannukset ylläpitovaiheessa. Ylläpitovaiheen kustannukset kuitenkin ovat selvästi alemmat kuin käyttöönotto- tai lopetus- ja uusimisvaiheen, joten on perusteltua pyrkiä tuotteisiin joiden elinkaari on mahdollisimman pitkä.

Käyttäjille näkyvin osa vahvaa todentamista on poletti ja sen käyttäminen. Tuotteiden käytettävyydelle on hieman hankalampi laskea vertailukelpoista hintaa. Tuotteiden huono käytettävyys voi vaikuttaa tuotteen käyttöönottovaiheen koulutuskustannuksiin

lisäävästi sekä ylläpitovaiheen kustannuksiin vaatimalla lisää henkilöresursseja tuotteen käyttäjätukeen. Tuotteen käytettävyyden arvioinnilla voi siis olla suuri merkitys etenkin ylläpitokustannuksille.

5.2 Vertailtavat tuotteet

Tämän diplomityön aluksi kartoitettiin tarjolla olevat vahvan todentamisen tuotteet. Tuotteita oli monenlaisia, joiden käyttämät menetelmät vaihtelivat suuresti. Sivumainintana tässä voidaan mainita erilaiset haaste-vastemenetelmät, joissa vasteen sai luettua esimerkiksi laivanupotus-ruudukkoa muistuttavalta kortilta (Entrust) tai menetelmät, joissa käyttäjä sai kertakäyttösalasanan vaihtoehtoista paluureittiä pitkin esimerkiksi tekstiviestinä ennaltamääritettyyn puhelinnumeroon (NordicEdge). Seuraavaksi kuitenkin käydään läpi kertakäyttö- ja dynaamiset salasanatuotteet toimintaperiaatteineen. Vertailtavat tuotteet ovat järjestettynä valmistajan mukaan aakkosjärjestykseen.

Aloitettaessa kertakäyttösalasanojen käyttöönottoa eri valmistajien järjestelmien vaatimukset ovat erilaisia. Kriteereiden arvioimisen lisäksi tuotteista käydään läpi vaatimukset jo olemassa oleville järjestelmille. Kaikkien vertailtavien tuotteiden toimittajat eivät vastanneet kyselyyn tuotteiden hinnasta ja yhteensopivuudesta TKK:n tekniseen ympäristöön, joiden osalta tässä vertailussa on jouduttu turvautumaan tuotteiden valmistajien tarjoamaan mainosmateriaaliin.

Open Authentication

Open Authentication, eli OATH, on useiden eri ohjelmisto- ja laitevalmistajien muodostama organisaatio, jonka tarkoituksena on luoda avoin standardi vahvaan todentamiseen (Open Authentication, 2006). Tämän hetkinen OATH-standardi määrittelee tapahtumakohtaisesti luotavia kertakäyttösalasanoja mutta tulossa on myös standardi dynaamisten salasanojen luomiseksi. Eri valmistajien OATH-tuotteet ovat keskenään yhteensopivia, jolloin OATH-yhteensopivan tuotteen hankkiminen ei sido mihinkään yhteen ja samaan valmistajaan. Suurin osa tässä diplomityössä vertailtavista tuotteista ovat OATH-yhteensopivia. OATH ei kuitenkaan ole mikään yksittäinen tuote

tai tuotemerkki vaan pakollinen maininta ennen eri valmistajien kertakäyttö- tai dynaamisten salasanatuotteiden läpikäyntiä ja esittelyä.

ActivIdentity

ActiveIdentityn vahvan todentamisen ratkaisu koostuu AAA Server –palvelinohjelmistosta sekä käyttäjille jaettavista poleteista. Poletit luovat kertakäyttösalasanoja tapahtumakohtaisesti. Polettien käyttämä algoritmi käyttää myös aikaa kertakäyttösalasanan luomiseen mutta vain osana tapahtumakohtaista kertakäyttösalasanan luontia. ActivIdentityn tuotteissa on myös OATH-yhteensopiva toimintatila.

ActiveIdentityn palvelinohjelmistoon voidaan määrittää eri käyttäjille eri todennustavat. Tuettuja todentamistapoja ovat kertakäyttösalasanat ActivIdentityn poleteilla, OATH kertakäyttösalasanat jonkun muun valmistajan poleteilla sekä staattiset salasanat. Ratkaisuun sisältyy itsepalveluportaali, missä käyttäjät voivat synkronoida polettinsa järjestelmän kanssa. ActivIdentityn ohjelmisto tukee kaikkia TKK:n atk-keskuksessa käytössä olevia todennusmenetelmiä. Lisäksi ActivIdentityn palvelinohjelmistoa varten on saatavilla dokumentoitu ohjelmointirajapinta omia sovelluksia varten.

ActivIdentityn Mini Token –poletissa on kahdeksannumeroinen näyttö ja painallusnäppäin. Näppäimestä painamalla poletti luo uuden kertakäyttösalasanan. Polettien toiminta-aika on neljä vuotta, kun kertakäyttösalasanoja luodaan keskimäärin kaksi kertaa päivässä. Tämän jälkeen polettien virtalähde on vaihdettava.

Aladdin

Aladdinin ratkaisu vahvaan todentamiseen on eToken-tuoteperhe. Ratkaisun käyttö vaatii eToken TMS (Token Management System) –palvelinohjelmiston käytön. Palvelinohjelmisto perustuu Microsoftin Active Directoryyn mutta toimii myös ilman AD:ä itsenäisenä ohjelmistona. eToken-poletit ovat USB-poletteja, jotka toimivat sirukortin tavoin PKI-perusteisesti. Palvelinohjelmisto on RADIUS ja LDAP yhteensopiva. Lisäksi eToken-järjestelmään on saatavissa ohjelmistokehitysrajapinta omia sovelluksia varten.

Poletit ovat Aladdinin eToken-ratkaisussa USB-poletteja, joista yhdessä mallissa on myös sisäänrakennettu kertakäyttösalasanan luomismahdollisuus. Kertakäyttösalasana toimii vain OATH-yhteensopivasti eli tapahtumakohtaisesti. Poletin antaman kertakäyttösalasanan pituus on kuusi merkkiä.

Authenex

Authenex tarjoaa Aladdinin tavoin vahvaa todennusta, joka perustuu OATH-yhteensopiviin kertakäyttösalasanoihin tai PKI-pohjaisiin USB-poletteihin. Authenexin ratkaisu koostuu ASAS-palvelinohjelmistosta (Authenex Strong Authentication System) ja WMC-järjestelmänhallintasivuista (Web Management Console). Authenexin ratkaisu on suunnattu lähinnä PK-yrityksille ja mitä luultavimmin ratkaisu ei skaalaudu TKK:n vaatimuksiin. Palvelinohjelmisto toimii Microsoftin SQL:n tai AD:n kanssa.

Poletit ovat USB-poletteja, joista yhteen malliin on sisäänrakennettu kertakäyttösalasanan luomismahdollisuus. Tässä poletissa on kuusinumeroinen näyttö ja virtalähde kestää viisi vuotta.

CryptoCard

CryptoCardin Cryptoserver palvelinohjelmisto on saatavana niin Windows kuin unix/Linux tai Macintosh -puolellekin. Cryptocardin ratkaisu on erittäin skaalautuva sekä tukee kaikkia TKK:n atk-keskuksessa käytössä olevia todennusmenetelmiä. CryptoCardin ratkaisu ei kuitenkaan ole OATH-yhteensopiva.

Poletit luovat kertakäyttösalasanoja eli luonti on tapahtumakohtaista. Järjestelmä on erittäin skaalautuva tietoturvavaatimuksiin ja poletit voidaan ohjelmoida näyttämään 5-8 numeroisia kertakäyttösalasanoja. Käytettävässä PIN-luvussa voi olla muita merkkejä kuin numeroita muistuttaen enemmän salasanaa. Polettien virtalähde kestää yli viisi vuotta. Virtalähteet ovat vaihdettavia pattereita. Järjestelmälle tulee viiden vuoden täystakuu.

Diversinet

Diversinetin ohjelmistopoletit mainitaan tässä ihan lyhyesti, koska Diversinet ei tarjoa sellaista vahvan todentamisen palvelua, mikä sopisi TKK:uun. Diversinet valmistaa OATH-yhteensopivia ohjelmistopoletteja, joita voidaan käyttää kannettavissa mobiilipäätelaitteissa. Diversinetin ohjelmistopoletit vaativat toimiakseen OATH-yhteensopivan todennuspalvelun. Polettien hyvä puoli on, että käyttäjä ei tarvitse uutta laitetta mutta huono puoli on ylläpidon vaikeutuminen.

PassGo

PassGon ratkaisu vahvaan todentamiseen on Defender-palvelinohjelmisto. Defender on OATH-yhteensopiva ja Microsoft Active Directoryyn asentuva tuote, jonka kanssa voi käyttää muiden valmistajien OATH-yhteensopivia poletteja. Defender on hyvin skaalautuva ja tukee TKK:n atk-keskuksen käyttämiä todennusmenetelmiä. Vaikka Defender vaatii toimiakseen Microsoftin Active Directoryn, sisältyy siihen tuki myös Linux- ja unixtietokoneille sisäänkirjautumiseen. Defender-palvelinohjelmisto tukee osittaista siirtymistä polettien käyttöön sillä, että järjestelmä osaa myös staattisten salasanojen käytön.

Defender-tuoteperheeseen kuuluu myös kertakäyttösalasanoja luovia poletteja. Poletteja, jotka luovat dynaamisia salasanoja, ei PassGo:lla ole valikoimissaan. Yhdessä polettimallissa on mahdollisuus syöttää käyttäjän PIN-luku polettiin ennen kertakäyttösalasanan luomista.

Portwise

Portwisen ratkaisu koostuu PortWisen todennuspalvelimesta ja ohjelmistopoleteista. Poletit toimivat OATH-yhteensopivasti eli luovat kertakäyttösalasanoja tapahtumien perusteella. Portwisen ratkaisu on suunnattu selvästi PK-yrityksille ja se ei välttämättä skaalaudu TKK:n vaatimuksiin ja palveluihin.

RSA Security

RSA Securityn tarjoama SecurId tuoteperhe on pitkäikäisimpiä vahvan todentamisen tuotteita. SecurId-tuoteperhe on erittäin skaalautuva ja pohjautuu dynaamisten salasanojen käyttöön. SecurId-ratkaisu sisältää RSA Securityn todennuspalvelimen ja käyttäjille jaettavat poletit. SecurId on Microsoftin Active Directoryn kanssa integroituva. Todennusratkaisu on yhteensopiva TKK:n atk-keskuksen käyttämien palveluiden kanssa. RSA Securityltä on saatavana niin kolmen kuin viidenkin vuoden ylläpitosopimukset.

Poletit ovat helppokäyttöisiä ja ne luovat uuden dynaamisen salasanan 60 sekunnin välein. Ainoa haittapuoli on, että RSA SecurId polettien virtalähde ei kestä kuin kolme vuotta, jonka jälkeen poletti täytyy vaihtaa uuteen. Virtalähteen vaihtaminen ei ole mahdollista.

Secure Computing

SafeWord on Secure Computing:n vahvan todentamisen ratkaisu. Ratkaisu käyttää kertakäyttösalasanoja. Vaikka SafeWord perustuukin Microsoftin Active Directoryyn, tukee se kaikkia TKK:n atk-keskuksen käyttämiä todennusmenetelmiä. Ratkaisu koostuu joko palvelinohjelmistosta tai erillisestä todennuspalvelimesta, johon palvelinohjelmisto on asennettu jo valmiiksi.

SafeWord poletteja on kahdenlaisia. Toinen on pelkkä näppäimen painalluksella ja toinen käyttäjän PIN-luvun perusteella kertakäyttösalasanan luova poletti. Secure Computing:n takuu poleteille on kattava. Poletti voidaan vaihtaa ilman erikseen mainittua syytä uuteen milloin vain ilmaiseksi. Ainoa ehto vaihdon onnistumiseksi on voimassaoleva huoltosopimus Secure Computing:n kanssa.

Vasco

Vascon DigiPass tuoteperhe on kattava ratkaisu vahvaan todentamiseen. Ratkaisu koostuu VACMAN Controller todennuspalvelimesta tai VACMAN Radius Middleware palvelinohjelmistosta ja käyttäjille jaettavista poleteista. DigiPass-tuotteet tukevat

kaikkia ohjelmistoalustoja vaikka todennuspalvelin toimiikin Windows-alustalla. DigiPass tuotteet tukevat kaikkia TKK:n atk-keskuksen käyttämiä todennusmenetelmiä. Vascon ratkaisu voidaan ottaa käyttöön vähittäisesti sillä se tukee myös staattisia salasanoja.

Vascon DigiPass-poletit pystyvät luomaan kertakäyttö-, dynaamisia ja dynaamisia kertakäyttösalasanoja. Vaikka Vascon tuotteet eivät vielä ole OATH-yhteensopivia on se mukana OATH-yhteisössä.

Verisign

Verisign Unified Authentication on Verisignin tarjoama vahvan todentamisen ratkaisu. Ratkaisu koostuu todennuspalvelimesta, joka voi sijaita omissa tai Verisignin tiloissa käyttäjätietoineen, sekä poleteista. Poletit voivat luoda sekä kertakäyttö- että dynaamisia salasanoja. Verisign toimii huoltosopimuksen perusteella, jonka pituus voi olla kolme tai viisi vuotta. Tuona aikana päivitykset ovat ilmaisia. Ratkaisu tukee TKK:n atk-keskuksen käyttämiä todennusmenetelmiä.

5.3 Tuotteiden kustannusvertailu

Käyttöönottokustannus on hankintahinta ja käyttöönottohinta yhteenlaskettuna. Hankintahintaa eivät kaikki valmistajat paljastaneet. Hankintahinta on ilmoitettu taulukossa 1 euromääräisenä, kun käyttäjiä on 20000. Taulukko 1:een on laskettu ylläpitohinnat järjestelmille kolmeksi vuodeksi niiltä osin kuin se tuotteen myyvän tahon antamien hintatietojen perusteella on ollut mahdollista. Hankintahintoja ei diplomityössä pyydetty työntekijöille mitoitettuun järjestelmään. Käyttöönottohinta puolestaan pitää sisällään kaikki muut kulut käyttöönottokustannuksissa. Ylimääräisen työn määrää tuotteiden tekemisestä sopiviksi TKK:uun on vaikea arvioida. Tämä menoerä on kaikilla parhaiten TKK:n käyttöön sopivilla tuotteilla suurin piirtein sama, koska tuotteiden tukemat todennusmenetelmät ovat samoja ja kaikille tuotteille on saatavana ohjelmointirajapinnat. Tässä luvussa lasketuissa esimerkeissä työntekijän kuukausikustannukseksi TKK:lle oletetaan 3000 €.

Valmistaja	Hankintahinta	Ylläpitohinta (Huoltosopimus)	Uusimiskustannus (3v)	Vaihdettava virtalähde	OATH-yhteensopiva	Kertakäyttösalasanat	Dynaamiset salasanat	API-rajapinnat
ActivIdentity	Ei tietoa	-	Ei tietoa	Kyllä	Kyllä	Kyllä	Ei	Kyllä
Aladdin	1443718	160000	160000	Kyllä	Kyllä	Kyllä	Ei	Kyllä
Authenex	Ei tietoa	-	Ei tietoa	Ei	Kyllä	Kyllä	Ei	Kyllä
Cryptocard	640676	Ei tietoa	Ei tietoa	Kyllä	Ei	Kyllä	Ei	Kyllä
PassGo	1046200	161280	161280	Ei	Kyllä	Kyllä	Ei	Kyllä
Defender (PassGo)	358400	161280	161280	-	Kyllä	-	-	Kyllä
Portwise	Ei tietoa	-	Ei tietoa	-	Kyllä	Kyllä	Ei	Kyllä
RSA Security	405500	240000*	400000	Ei	Ei	Ei	Kyllä	Kyllä
Secure Computing	Ei tietoa	-	Huoltosopimus	Ei**	Ei	Kyllä	Ei	Kyllä
Vasco	Ei tietoa	-	Ei tietoa	Ei	Ei***	Kyllä	Kyllä	Kyllä
Verisign	Ei tietoa	-	Huoltosopimus	Ei	Kyllä	Kyllä	Kyllä	Kyllä

Taulukko 1 Hintavertailu kertakäyttö- ja dynaamisten salasanavalmistajien kesken (luvut euromääräisiä) * = Laskettu korvaavien polettien hinta samaksi kuin koko sopimuksen hinta käyttäjää kohden. ** = Vaikka virtalähdettä ei poleteista ei pysty vaihtamaan, voi poletit vaihtaa ilman syytä uuteen, jos huoltosopimus on voimassa. * = Vasco kuuluu OATH jäseniin nykyisin.**

Käyttöönottohinta kiinteiltä kuluiltaan on seuraava, kun käyttäjiä on 20000: (Kiinteisiin kuluihin lasketaan käyttäjien koulutus, koulutusmateriaalin valmistus ja tuotteisiin kuuluvien polettien jakaminen käyttäjille.)

- Koulutusmateriaalin valmistus (1 viikko) $3000 € / 4 \approx 750€$
- Koulutus ja polettien jako (5 min / käyttäjä) $5 \text{ min} * 20000 * 3000 € / kk \approx 30000 €$

Vastaavasti, jos tuote otetaan käyttöön vain henkilökunnalle, ovat kiinteät kulut 3600:lle käyttäjälle:

- Koulutusmateriaalin valmistus (1 viikko) $3000 € / 4 \approx 750 €$
- Koulutus ja polettien jako (5 min / käyttäjä) $5 \text{ min} * 3600 * 3000 € / kk \approx 5700 €$

Tällöin tulevaisuudessa opiskelijat olisi helppo siirtää käyttämään vahvaa todentamista vuosikurssi kerrallaan fuksilupien jaon yhteydessä. Tällöin voitaneen laskea jakokulut

vuositasolla uusien opiskelijoiden vuoksi seuraavasti (koulutus voisi kuulua fuksien ”Tietokone työvälineenä” –kurssille):

- Polettien jako fuksilupien jaossa (1 min / käyttäjä) $1\ \text{min} * 2000 * 3000\ € / \text{kk} \approx 633\ €$

Ylläpitokustannus voidaan laskea seuraavasti. Oletetaan pahimmassa tapauksessa poleteista 20 % rikkoutuvan tai häviävän vuodessa Portwisen julkaiseman ”A Total Cost of Ownership Analysis On Strong Authentication with One Time Passwords” tutkielman mukaisesti. Oletetaan myös, että yhden poletin vaihtamiseen menee aikaa noin 5 minuuttia. Tästä saadaan laskettua tarvittava työkustannus vuositasolla:

- Poletin vaihtaminen $5\text{min} * 0{,}20 * 20000 = 333h \approx 6300\ €$

Ja vastaavasti pelkällä henkilökunnalla (3600 henkilöä) ylläpitokustannukset olisivat:

- Poletin vaihtaminen $5\text{min} * 0{,}20 * 3600 = 60h \approx 1200\ €$

Tämä ei kuitenkaan kata polettien hankinnasta koituvia kuluja (paitsi Secure Computing:in SafeWord-polettien takuu) vaan pelkästään työn osuuden atk-keskuksessa.

Uusimiskustannus onkin hieman vaikeampi laskettava. Suurin osa valmistajista myy em. tuotteilleen kolmen tai viiden vuoden huoltosopimusta. Useimpien järjestelmien kohdalla uusimiskustannus on sama kuin uuden huoltosopimuksen hinta. Joillakin valmistajilla koko tuote myydään huoltosopimuksena eli tuotetta voi käyttää niin pitkään kuin huoltosopimus on voimassa. RSA Securityn SecurId on esimerkiksi yksi näistä. Toinen ääripää valmistajista myy kerralla koko järjestelmän ja huoltosopimus kattaa melkeinpä vain takuun ja tuotepäivitykset sopimuskautena.

Nykyisen järjestelmän ylläpitokustannukset ovat suunnilleen seuraavanlaiset: Lokakuussa 2006 atk-keskuksen palvelupisteessä TKK:n päärakennuksessa oli käynyt reilut 360 käyttäjää vaihtamassa salasanansa tai avaamassa lukittuneen tunnuksensa. Lokakuu on melko keskimääräinen kuukausi salasanan vaihtamisessa ruuhkahuippujen keskittyessä syyskuun alkuun ja helmi-maaliskuun vaihteeseen. Lisäksi pelkästään uusia työntekijätunnuksia tulee päivittäin. Uuden tunnukseen luomiseen menee kauemmin kuin pelkän salasanan vaihtoon. Keskimäärin salasanan vaihtaa noin neljässä minuutissa

käyttäjän opastuksineen. Koska tilastoja uuden tunnuksen avaamisen ajallisesta pituudesta ei ole, arvioidaan siihen kuluvan aikaa kahdeksan minuuttia. Tästä saadaan:

- Salasananvaihtokustannukset vuodessa $360 * 4\ \text{min} * 12 = 288\ \text{h} \approx 5500\ €$
- Uusien työntekijätunnuksien luonti $1\text{-}2 * 8\ \text{min} * 20 * 12 = 32 - 64\ \text{h} \approx 600 - 1200\ €$

Tämän päälle tulevat tietysti kaikki työt fuksilupien jakamisessa.

- Fuksilupajakokustannukset (vuosikustannus) $1000 * 1\ \text{min} \approx 320\ €$
- Fuksilupien luonti ja jaon valmistelu $\approx 800\ €$

Tässä fuksilupien luonti ja fuksilupajaon valmistelu on laskettu vievän noin yhden työviikon. Kaikki salasanan vaihtamiset eivät kuitenkaan näy tämän laskemiseen käytetyssä tilastossa. Atk-keskuksen Maarintalolla olevassa toimipisteessä vaihdetaan useita salasanoja päivittäin. Tästä johtuen pelkät salasananvaihtokustannukset voivat todellisuudessa olla jopa 10000 € vuodessa. Tässä ei kuitenkaan ole huomioitu ylläpitotyötä, jonka nykyinen salasanajärjestelmä vaatii.

6 Pohdinta

Tässä luvussa käydään läpi tämän diplomityön keskeiset tulokset ja niistä vedetään johtopäätöksiä, joita voidaan käyttää uusia palveluja suunniteltaessa.

Käyttäjien mielestä nykyisten salasanojen ongelmat kiteytetysti ovat niiden määrä, huono muistettavuus ja vaihdon hankaluus. Koska salasanoja käytetään liikaa käyttäjienkin mielestä, on niiden määrää hyvä pienentää. Keinoja on monia, joista yksi on kertakäyttö- tai dynaamisten salasanojen käyttöönottaminen ainakin jossain mittakaavassa. Jos nykyistä salasanajärjestelmää halutaan kuitenkin ylläpitää, tulisi seuraavia asioita pohtia. Onko käytössä olevista salasanoista tarpeeksi tietoa saatavilla ja miten helposti? Miksi käyttäjät kokevat salasanat hankaliksi? Käyttäjät käyttävät samoja salasanoja yhä uudelleen ja uudelleen eri palveluissa, kierrättävät salasanoja, syöttävät vääriä salasanoja vääriin palveluihin ja kirjoittavat salasanat muistiin. Muun muassa nämä asiat nousivat esiin tehdyssä käyttäjätutkimuksessa. Perimmäinen syy tällaisiin salasanojen ”väärinkäytöksiin” lienee käyttäjien rajallinen muisti ja käytettävän salasanajärjestelmän sopimattomuus ihmiskäyttäjille.

Tilannetta voidaan kuitenkin helpottaa myös muilla tavoin TKK:ssa, kuten siirtymällä käyttämään yhtä salasanaa. Tämä aiheuttaa suuremman salasanan väärinkäytösriskin eikä myöskään poista nykyhetken salasanoilla tunnistamisen perimmäistä ongelmaa: lukuisat muut palvelut muualla maailmassa. Tällä hetkellä alkavat Internetin ne palvelut, jotka eivät vaadi käyttäjien tunnistamista, olla vähissä ja tulevaisuus näyttää yhä pahemmalta. Verkkohenkilöllisyys tulee tulevaisuudessa olemaan yhtä oleellinen osa henkilöä kuin fyysinen henkilöllisyyskin. Tämä on jo osin nähtävissä erilaisissa Suomen virastojen verkkopalveluissa. Salasanoja ja käyttäjätunnuksia tulee tulevaisuudessa vain olemaan aivan liikaa, jotta tavallinen käyttäjä pystyisi muistamaan ne.

Erilaisia vahvaan todentamiseen perustuvia palveluita on jo olemassa useita verkkopankeilla ja jo mainituilla Suomen virastoilla. Paljon puhuttu Web 2.0[8], joka tarjoaa parempia palveluja yksilöllisesti suunnattuna, perustuukin paljolti käyttäjien tunnistamiselle ja todentamiselle. Vahvalla todentamisella voidaan todentaa käyttäjän henkilöllisyys suurella varmuudella. Tällöin myöskin mahdolliset väärinkäyttötilanteet voidaan selvittää paremmin, kun tiedetään luotettavammin kuka teki mitä. Käyttäjien todentamisessa on kuitenkin ongelmia, joita ei vielä ole ratkaistu ja joista kiistellään maailmalla. Kiistan aiheita on useita mutta yksi niistä on todentajan rooli; kuka todentaa käyttäjän? Kaikissa palveluissa ei myöskään ole mahdollista tai edes tarpeellista käyttää vahvaa todentamista.

Vahva todentaminen on keino vähentää käyttäjien muistikuormaa ja parantaa palvelujen käytettävyyttä samalla kuitenkin tehostaen tietoturvaa. Tällä hetkellä lupaavin taloudellisesti kannattavin vahvan todentamisen muoto on erilaisten polettien käyttäminen.

Polettien käyttäminen edellyttää todentamispalvelimen ja käyttäjille jaettavien polettien hankkimista. Lisäksi tulee nykyisten järjestelmien yhteensovittamistyö uuteen todentamisjärjestelmään. Tämä työ kannattaa parantuneena tietoturvallisuutena mutta sen taloudellista kannattavuutta pitää harkita aina tapauskohtaisesti.

Tietoturva on kuitenkin vasta viime aikoina alkanut saada suuren yleisön huomiota, joten tietoturvatuotteiden markkinat ovat vasta kehittymässä. Tästä aiheutuu markkinoilla olevien tuotteiden yhteensopimattomuus, suhteellisen kalliit hinnat ja lyhyet sopimusajat tuotteiden käytölle. Tieto ja turvallisuus ovat lisäksi niin abstrakteja käsitteitä, että tuotteiden hinnat vaihtelevat rajusti tietoturvatuotteiden valmistajien välillä. Toinen syy tuotteiden suuriin hintaeroihin ovat markkinoiden suuri kysyntä ja tällä hetkellä vielä pieni tarjonta.

Turvallisuuden mitoituksessa ensiarvoisen tärkeää onkin suojaamistoimien mitoittaminen vastaamaan turvallisuusriskejä. Turvallisuusriskejä mitataan yleensä

[8] Web 2.0, O'Reilly-kustantamon käyttöönottama termi uusista käyttäjille suunnatuista Internet-palveluista. Verkkosivu: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (Saatavuus 30.10.2006)

rahassa. Paljonko korjaus maksaa? Minkä arvoinen tämä tieto on minulle tai pahimmalle kilpailijalleni? Minkä arvosta työtä menetettiin? Nämä ovat esimerkkejä kysymyksistä, joihin jokaisen organisaation olisi kyettävä vastaamaan. Turvallisuustoimet tulee mitoittaa siten, että niistä saatavat hyödyt ovat pienempiä kuin niiden kiertämiseen tarvittavat resurssit. Tämä tarkoittaa, että organisaatioiden on tiedettävä arvonsa tämän päivän maailmassa. Nykyisin ulospäin annettu mielikuva onkin erittäin tärkeä ja arvokas. Tällöin on tärkeää luoda uskottava ja turvallinen kuva TKK:n käyttämästä tietoturvasta.

TKK:ssa ei välttämättä kuitenkaan olla vielä valmiita panostamaan tietoturvaan niin, että kaikki tietojärjestelmien käyttäjät todentaisivat henkilöllisyytensä poleteilla. Suositeltavaa kuitenkin olisi, että vähintään järjestelmien ylläpitäjät todennettaisiin vahvasti. Ylläpitotunnukset ovat kaikissa järjestelmissä toteutettu normaaleilla salasanoilla ja käyttäjätunnuksilla. Ylläpitotunnuksilla on mahdollista tehdä huomattavasti enemmän vahinkoa TKK:n tietojärjestelmille kuin tavallisilla käyttäjätunnuksilla. Jos ylläpitäjän salasana jostain syystä päätyisi vihamieliselle hyökkääjälle, voisi hyökkääjä esimerkiksi vaihtaa TKK:n verkkosivujen sisällön tai tehdä jotain muuta vielä pahempaakin. Vaikka teknisesti kaikki tällaiset tilanteet ovat korjattavissa työllä ja rahalla, ei tällaisista tilanteista aiheutuvaa negatiivista julkisuutta voida väheksyä. Nykymaailmassa, missä tuotemerkin arvo voi olla suurin osa yrityksen arvoa, suuren yleisön mielipiteellä on väliä.

TKK:n atk-keskuksen vastuulla on monia palveluja. Kaikki näistä palveluista eivät välttämättä ole kaikille käyttäjille tai näy ulospäin. Lukuisat palvelut pyörivät virtuaalipalvelimissa. Virtuaalipalvelimet ovat ohjelmistollisia palvelimia. Yhdessä virtuaalipalvelimia ajavassa palvelimessa saattaa olla jopa kymmeniä eri palveluja ajossa, jolloin ylläpitotunnusten turvallisuus nousee yhä enemmän esille.

Tehty käyttäjätutkimus myös paljasti, että vaikka työntekijöillä on saman verran salasanoja käytössään kuin opiskelijoilla, muistavat he vähemmän salasanoja. Työntekijät myös tarvitsevat salasanoja työssään, joten he kirjoittavat ne pääsääntöisesti muistiin ja säilyttävät niitä kukin missä sattuu. Kuitenkin salasanojen vaihtaminen ei heiltä onnistu yhtä hyvin kuin opiskelijoilta, joten melkein 90 % työntekijöistä onkin

joskus käyttänyt atk-keskuksen asiakaspalvelua (osa on jopa ”kanta-asiakkaita” ja asioivat palvelupisteessä puolen vuoden välein, kun pääsalasana vanhenee).

Käyttäjät ovat pohjimmiltaan epäluotettavia. Vaikka käyttäjiä ohjeistetaan toimimaan ja käyttämään palveluita oikein he kiertävät annettuja sääntöjä ja ohjeita eri syihin vedoten. Suurin osa käyttäjistä haluaa kuitenkin tehdä vain työnsä mahdollisimman helposti ja vaivattomasti, joka joissakin tapauksissa tarkoittaa opitusti, joten työtä hankaloittavia ohjeistuksia ei noudateta. Suoritetussa käyttäjätutkimuksessa kävikin ilmi, että noin viidennes vastaajista ei jollain tasolla noudattanut annettuja tietoturvaohjeita. Käyttäjätutkimukseen osallistuneista 46 % vastasi kirjoittavansa uuden salasanan jonnekin (kalenteri, kännykkä, lompakko) muistiin. 93 % puolestaan sanoi muistavansa ulkoa salasanat, joita käyttää useita kertoja viikossa. Kuitenkin miten käy kaikkien muistiinkirjoitettujen salasanojen? Huolehtivatko käyttäjät enää salasanamuistiinpanoistaan, kun eivät enää niitä tarvitsekaan vai mihin ne joutuvat?

Mahdollisen hyökkääjän tulee kertakäyttö- tai dynaamisia salasanoja käytettäessä käyttää enemmän resursseja järjestelmän murtamiseen kuin vain unohtuneiden muistiinpanojen etsiminen. Nykyisin käyttäjät käyttävät samaa salasanaa useassa eri palvelussa. Tällainen käyttö estyy kun salasana ei ole staattinen. Myös monet staattisiin salasanoihin kohdistuvat hyökkäykset eivät toimi kertakäyttö- tai dynaamisia salasanoja vastaan. Mm. salasanan kalasteluhyökkäykset (engl. phishing) vältetään niiden käytöllä, koska hyökkäyksessä annettu salasana ei ole voimassa kuin kerran tai rajoitetun ajan.

Kertakäyttösalasanoilla voidaan vähentää tarvittavien salasanojen määrää, kun salasanoja ei enää tarvitse luokitella eri palvelujen erilaisien tietoturvatasojen perusteella. Tämä paitsi helpottaa käyttäjien muistikuormaa ja työn tekemistä niin myös tekee todentamisesta yhtenäisempää. Kertakäyttösalasanoja voidaan myös esimerkiksi käyttää pelkissä turvattomissa yhteyksissä, jolloin salasanojen määrää voidaan laskea, kun muita salasanoja tai salasanaa käytetään turvallisessa ympäristössä. Tämä ratkaisu kuitenkin on heikompi kuin kertakäyttösalasanojen käyttäminen kaikissa palveluissa mutta sen mahdollistama käyttäjien muistikuorman pienentäminen on kiistaton etu.

Kertakäyttö- tai dynaamisten salasanojen käyttöönotto ei kuitenkaan onnistu hetkessä. Vähittäisessä käyttöönotossa on myös se hyvä puoli, että jo saatuja kokemuksia voidaan

hyödyntää seuraavassa vaiheessa. Ensimmäinen luonnollinen käyttäjäryhmä, jolle vahva todennus kannattaisi ottaa käyttöön, ovat ylläpitäjät, koska heidän käyttäjätunnuksillaan voidaan saada eniten vahinkoa aikaan, ja joka kertakäyttö- tai dynaamisia salasanoja käytettäessä olisi estettävissä. Toisena käyttöönottavana käyttäjäryhmänä pitäisin etätyöntekijöitä ja vasta sitten loppua henkilökuntaa. Suuri osa työntekijöiden työssään käsittelemästä materiaalista on kuitenkin luottamuksellista, josta valtiovarainministeriön VAHTI ohjeet sanovat ”tietojärjestelmien suojaukset on mitoitettava turvaluokitukseltaan vaativimman käsiteltävän tiedon mukaisiksi” (VAHTI 5/2004). Luottamuksellisen tiedon käsittelyssä pitäisi olla käytössä vahva todentaminen.

Suomessa valtionhallinnon puolelta tarve työntekijöiden vahvalle todentamiselle on jo tiedostettu. Valtionhallinto on ottamassa käyttöön virkamieskorttia: toimikorttia, joka jaetaan jokaiselle valtionhallinnon virkamiehelle. Virkamieskortin käyttöönoton aikataulu tosin tällä hetkellä on vielä auki. Virkamieskortin käyttöönotto ei kuitenkaan ratkaise vahvan todentamisen ongelmaa opiskelijoille. Kuinka opiskelijat voidaan tulevaisuudessa todentaa luotettavasti?

Jos kertakäyttö- tai dynaamisilla salasanoilla halutaan vähentää käyttäjille tarjottavaa asiakaspalvelua, voidaan asiassa edetä toisin. Vahvaa todentamista voi nykyisin käyttää esimerkiksi Tampereen ja Oulun yliopistoissa unohtuneen salasanan vaihtamiseen. Palvelu on toteutettu Suomen Pankkiyhdistyksen TUPAS-rajapintoja käyttämällä. Samanlainen palvelu hyödyttäisi etenkin TKK:n palvelujen etäkäyttäjiä, kun muuten pakolliset asiointimatkat TKK:uun vähenevät. Tällainen vahva todentaminen ei kuitenkaan välttämättä sovellu aivan kaikkiin käyttötapauksiin vaan vain tällaisiin melko harvoin tapahtuviin todentamistarpeisiin.

Vertailluista tuotteista TKK:n käyttöön sopivimmat ovat Vascon, Secure Computing:n, Verisign:n ja RSA Securityn dynaamiset salasanatuotteet juuri tässä järjestyksessä. RSA Securityn valitseminen olisi melko varma ratkaisu tietoturvallisesti mutta myös sieltä kalleimmasta päästä pitkän ajanjakson tarkastelulla, kun esimerkiksi poletteja kolmen vuoden toiminta-ajan jälkeen ei voi huoltaa vaan vain uusia. Vascon tuotteet tukevat hyvin TKK:n käyttämiä yhteysmenetelmiä ja Vasco on lisäksi liittynyt osaksi OATH-organisaatiota, mikä antaa tulevaisuudessa luultavasti etua harkittaessa OATH-standardin mukaisten laitteiden käyttämisestä. Secure Computing:n ratkaisun

kustannusmalli on polettien osalta parempi, koska huoltosopimuksen voimassaoloajan poletit voi päivittää ja vaihtaa uusiin tarvittaessa. Dynaamisten salasanojen etu kertakäyttösalasanoihin on, että ne eivät pysty menemään salasanan luomistapahtumista sekaisin. Tosin monet tässä työssä mainituista kertakäyttösalasanatuotteista pystyvät tahdistumaan automaattisesti, jos järjestelmä ja poletti olivat luomistapahtumista vain vähäisesti sekaisin.

Valittaessa kertakäyttösalasanat todentamistavaksi päällimmäiseksi vertailussa nousi OATH-yhteensopiva Defender todennuspalvelinohjelmisto PassGo:lta. Defenderin etuja ovat mm. sen tukemat todennusmenetelmät ja tuettujen polettimallien määrä. Lisäksi sen käyttö ei sido mihinkään tiettyyn polettivalmistajaan vaan poletit voi ostaa sieltä mistä ne halvimmalla saa. Myös Defenderin huoltosopimus on houkuttelevan hintainen: 15 % hankintahinnasta, joka määräytyy järjestelmän käyttäjämäärän mukaan.

Tällä hetkellä ei kuitenkaan kannata välttämättä lukittautua yksittäisten valmistajien kalliisiin dynaamisiin salasanajärjestelmiin. Virkamieskortin käyttöönoton viipyessä kannattanee myös harkita OATH-standardin seuraavan version odottamista. Se määrittelee myös dynaamisten salasanojen toteutusmenetelmät.

6.1 Odotettavissa olevat ongelmat

Kertakäyttö- tai dynaamisen salasanapalvelun käyttöönotossa on myös ongelmia. Vaikka tietoturva ja ylläpidettävyys paranisivat, voivat käyttäjät olla kaikkea muutosta ja uuden opettelua vastaan. Muutosvastarinta voi etenkin vapaassa yliopisto-organisaatiossa olla hyvinkin huomattavaa ja käyttöönottoa viivyttävää.

Käyttäjille tulee kertakäyttö- tai dynaamisia salasanoja luovista laitteista, poleteista, myös ylimääräistä harmia. Jos käytetty poletti ei ole tyylikäs tai muuten helposti mukana kulkeva, ei käyttäjä välttämättä halua kantaa sitä mukanaan. Poletin valinta onkin suoritettava huolellisesti ja mielellään siten, että poletin hävittäminen hävittää myös jotain muutakin käyttäjältä. Tällaisia poletteja ovat esimerkiksi avaimenperät, jolloin käyttäjät osaavat huolehtia poleteistaan huolehtiessaan avaimistaan.

Tämä polettien häviäminen voi olla suurikin ongelma etenkin isoissa organisaatioissa. Tällaisissa tilanteissa tulisi myös järjestää mahdollisuus käyttää ”varapolettia”, jolloin työnteko ei esty vaikka poletti unohtuisi kotiin. Opiskelijoille tällaista mahdollisuutta ei olisi välttämätöntä tarjota. Poletin kestävyyden tulisi myös olla hyvä, sillä pienikokoisena laitteena se voi usein tippua ja joutua muutenkin koville.

Kun jokin asia uudistuu ja käytännön järjestelyt muuttuvat, vaatii muutos käyttäjien sopeutumista ja koulutusta uuden järjestelmän käyttöön. Vaikka polettien käyttö sinänsä on helppoa, ei hyvää tiedotusta järjestelmän käytöstä ja käyttöönotosta aikatauluineen voi unohtaa. Käyttäjille moni pieni asia, joka olisi voitu estää tiedottamisella ja opastamisella, aiheuttaa paljon harmia ja turhaa työtä.

Vaikka suurin osa palveluista pystytäänkin toteuttamaan kertakäyttö- tai dynaamisilla salasanoilla kuten ennenkin, ei kaikkia nykyisin olemassa olevia palveluja voida tarjota muutoksen jälkeen sellaisinaan. Yksi näistä palveluista, johon todentamistavan muutos vaikuttaa, on sähköpostin luku sähköpostiasiakasohjelmilla. Sähköpostin lukuun tarkoitetut ohjelmat käyttävät sähköpostipalvelimien kanssa sellaisia yhteystapoja, mitkä eivät tue istuntokohtaisia salasanoja. Näitä ovat POP- ja IMAP-yhteystavat. Erilaisiin webmailien toteutuksiin kertakäyttö- tai dynaamisilla salasanoilla on vain vähän merkitystä, koska käyttäjät todennetaan istuntokohtaisesti istunnon aluksi.

Muita ongelmia ovat polettien jakelu ja luovutus käyttäjille. Se miten tällainen työ hoidetaan, sen suunnittelu ja käytännön toteutus ovat isoja operaatioita jo itsessään. Parhaiten tämä käy ottamalla vahva todentaminen vähittäisesti käyttöön pieni käyttäjäryhmä kerrallaan.

7 Yhteenveto

Tämän diplomityön oli tarkoitus selvittää kertakäyttösalasanojen tai dynaamisten salasanojen käyttöönoton kustannusrakenne TKK:ssa. Samalla tuli selvittää vahvan todentamisen tuomat hyödyt ja haitat sekä tarkastella vahvaa todentamista myös käyttäjän näkökulmasta.

Diplomityössä tehtiin käyttäjätutkimus, jolla kartoitettiin käyttäjien tyytyväisyyttä ja mielipiteitä tämän hetken todentamisratkaisuun käyttäjätunnuksilla ja salasanoilla. Tutkimus onnistui siinä mielessä hyvin, että vastaajiksi saatiin kaikkien TKK:n pääkäyttäjäryhmien edustajia sopivasti. TKK:n atk-keskuksen tulisi kuitenkin käyttää tästä tutkimuksesta saatua tietoa omien palveluidensa kehittämiseen ja seurata kehitystä uusilla samantapaisilla käyttäjien tyytyväisyyttä ja mielipiteitä kartoittavilla käyttäjätutkimuksilla aika ajoin.

Työssä otettiin myös yhteyttä kertakäyttösalasana- ja dynaamisten salasanatuotteiden valmistajiin ja tuotteista tehtiin vertailu. Vertailussa käytiin läpi tuotteiden ominaisuudet ja poikkeavuudet toisistaan. Tämän hetken ongelmana vahvan todentamisen turvallisuustuotteissa kuitenkin on korkea hinta ja markkinoilta puuttuvat yhtenäiset standardit.

Käyttäjien muistikuorma nykyisen salasanoja täynnä olevan maailman kanssa on huomattava. Ottamalla käyttöön kertakäyttösalasanoilla tai dynaamisilla salasanoilla tapahtuva todentaminen parannettaisiin niin tietoturvaa kuin vähennettäisiin käyttäjien muistin kuormitusta. Tällöin myös TKK:n palveluiden käytettävyys paranisi ja käyttäjätyytyväisyys lisääntyisi.

Kertakäyttösalasanat tai dynaamiset salasanat ovat kuitenkin kalliita hankintoja, jotka vaativat TKK:n ylimmän johdon päätöksen, koska vahvan todentamisen käyttöönotto on kuitenkin osaksi myös tietynlaisen julkisuuskuvan rakentamista. Vahvan todentamisen käyttöönoton kalleuden perusteella onkin mahdollisen siirtymisen sen käyttöön tapahduttava vähittäin tietyt käyttäjäryhmät kerrallaan.

Viitteet

ActivIdentity. 2006. Verkkosivut: http://www.actividentity.com/ (Saatavuus: 30.10.2006)

Aladdin. 2006. Verkkosivut: http://www.aladdin.com/ (Saatavuus: 30.10.2006)

Anderson, R. 2001. *Security Engineering, A Guide to Building Dependable Distributed Systems*. New York: Wiley & Sons.

Authenex. 2006. Verkkosivut: http://www.authenex.com/ (Saatavuus: 30.10.2006)

Banwell, L., Coulson, G. 2004. *Users and user study methodology: the JUBILEE Project*. Information Research. Vol. 9, No. 2. http://informationr.net/ir/9-2/paper167.html (Saatavuus: 3.11.2006)

Chan, S., Srinivasan, J. 2004. *One Time Password Authentication for Open High Performance Computing Environments.* http://www.es.net/raf/OTP-final.pdf (Saatavuus: 30.10.2006)

Coe, B. 1976. *The Birth of Photography*. London: Ash & Grant.

Cryptocard. 2006. Verkkosivut: http://www.cryptocard.com/ (Saatavuus: 30.10.2006)

Downes, S. 2005. *Authentication and Identification*. http://www.downes.ca/cgi-bin/page.cgi?db=post&q=crdate=1115168586&format=full (Saatavuus: 30.10.2006)

EY. 2004. *Neuvoston asetus N:o 2252/2004*. Euroopan unionin virallinen lehti. L 385. 6 s.

Faulkner, X. 2000. *Usability Engineering*. Basingstoke: Palgrave.

Fried, R. 2006. *"Remote Access" (connection from home) for students*. http://research.haifa.ac.il/~rfried/cd/index_eng.html (Saatavuus: 27.10.2006)

Gollmann, D. 1999. *Computer Security*. West Sussex: Chichester: Wiley & Sons.

Grand, J. 2001. *Authentication Tokens: Balancing the Security Risks with Business Requirements*. Julkaistu: @stake-verkkosivulla 18.9.2001. Kopio: http://malpaso.ru/securid/rr2001-04.pdf (Saatavuus: 3.11.2006)

Haka Federation. 2005. Verkkosivut: http://www.csc.fi/suomi/funet/middleware/haka/index.phtml (Saatavuus: 30.10.2006)

Health Insurance Portability and Accountability Act. 1996. US Public Law 104-191.

IETF. 1995. RFC 1760. *The S/KEY One-Time Password System*.

IETF. 1998. RFC 2289. *A One-Time Password System*.

IETF. 1999. RFC 2527. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.

Krebs, B. 2006. *The New Face of Phishing*. The Washington Post, Brian Krebs on Computer Security. http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html (Saatavuus: 14.2.2006)

Microsoft. 2006. Verkkosivut: http://www.microsoft.com/ (Saatavuus: 30.10.2006)

Moore, D. & McCabe G. 2005. *Introduction to the Practice of Statistics*. New York: W. H. Freeman.

Mäkelä, J. 2003. *Suomalainen antaa salasanansa ja tunnuksensa vaikka puhelimessa*. Digitoday. http://www.digitoday.fi/showPage.php?page_id=14&news_id=25944 (Saatavuus: 5.4.2006)

Nielsen, J. 1993. *Usability Engineering*. London: Academic Press.

Open Authentication. 2006. Verkkosivut: http://www.openauthentication.org/ (Saatavuus: 30.11.2006)

PassGo. 2006. Verkkosivut: http://www.passgo.com/ (Saatavuus: 30.10.2006)

Portwise. 2006A. *A Total Cost of Ownership Analysis On Strong Authentication with One Time Passwords*. http://www.portwise.com/downloadcenter/docs/PortWise-Strong-Authentication-TCO.PDF (Saatavuus: 30.10.2006)

Portwise. 2006B. Verkkosivut: http://www.portwise.com/ (Saatavuus: 30.10.2006)

RSA Security. 2006. Verkkosivut: http://www.rsasecurity.com/ (Saatavuus: 30.10.2006)

Salin, M. 2004. *Kansalaisten yksityisyys säilyy*. SEAL. 2/2004. s. 12-13.

Scheuren, F. 2004. *What is a Survey*. American Statistical Association. http://www.amstat.org/sections/srms/pamphlet.pdf (Saatavuus: 28.8.2006)

Schneier, B. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley Computer Publishing.

Schneier, B. *Two-Factor Authentication: Too Little, Too Late*. Communications of the ACM. 2005. Vol. 48. No. 4. s. 136.

Secure Computing. 2006. Verkkosivut: http://www.securecomputing.com/ (Saatavuus: 30.10.2006)

Shapiro, C. & Varian, H. R. 1999. *Information Rules: a Strategic Guide to the Network Economy*. Boston: Harvard Business School Press.

Suler, J.R. 2002. *Identity Management in Cyberspace*. Journal of Applied Psychoanalytic Studies. Vol. 4. No. 4. s. 455-459.

Suomen Pankkiyhdistys. *TUPAS Pankkien Tunnistuspalvelu Asiointipalveluntuottajille, Palvelun kuvaus ja palveluntuottajan ohje*. http://www.pankkiyhdistys.fi/sisalto/upload/pdf/tupasV2.pdf (Saatavuus: 31.10.2005)

Tietohallinnon johtoryhmä, THJR. 2006. *TIETOHALLINNON PÖYTÄKIRJA 2/2006*. Teknillinen korkeakoulu. http://www.tkk.fi/Yksikot/Kehittamisyksikko/thjr/pk/2006/02/THJR_pk_2-2006.pdf (Saatavuus: 19.10.2006)

Torpey, J. 2000. *The Invention of the Passport: Surveillance, Citizenship and the State*. Cambridge: Cambridge University Press.

Vasco. 2006. Verkkosivut: http://www.vasco.com/ (Saatavuus: 30.10.2006)

Verisign. 2006. Verkkosivut: http://www.verisign.com/ (Saatavuus: 30.10.2006)

Viestintävirasto. 2001. Verkkosivut: http://www.ficora.fi/ (Saatavuus: 3.1.2006)

Vilander, P. 2006. *Sähköpostikirjeenvaihto*. Sähköposti 6.7.2006. RSA Security.

Williams, C. *WHO GOES THERE? Authentication in the On-Line World*. The Business Forum. http://www.bizforum.org/whitepapers/cylink002.htm (Saatavuus: 31.10.2005)

Yan, J., Blackwell, A., Anderson, R., Grant, A. 2000. *The Memorability and Security of Passwords – Some Empirical Results*. University of Cambridge. Computer Laboratory. Technical Report. No. 500.

Liite 1

Salasanat Teknillisen korkeakoulun palveluissa

	Kaikki	Kaikki (%)
Taustatiedot:		
1. Sukupuoli		
Mies	53	72,6 %
Nainen	20	27,4 %
Yhteensä:	73	
2. Ikä		
->22	16	21,9 %
22-27	35	47,9 %
28-35	11	15,1 %
36-49	7	9,6 %
50->	4	5,5 %
Yhteensä:	73	
3. Ensisijainen suhde Teknilliseen korkeakouluun		
Opiskelija	52	71,2 %
Jatko-opiskelija	3	4,1 %
Opetushenkilökuntaa	4	5,5 %
Muuta henkilökuntaa	9	12,3 %
Muu suhde	5	6,8 %
Yhteensä:	73	
Kysymykset:		
4. Kuinka monta eri salasanaa sinulla on käytössäsi TKK:n palveluissa? (esim. sähköposti, windows, ssh-etäyhteys)		
En käytä salasanaa vaativia TKK:n palveluja	0	0,0 %
1	0	0,0 %
2	5	6,9 %
3	19	26,4 %
4-5	38	52,8 %
6-7	8	11,1 %
8->	2	2,8 %
Yhteensä:	72	

5. Montako TKK:n palvelujen salasanaa muistat ulkoa?

0	3	4,2 %
1	6	8,3 %
2	16	22,2 %
3	21	29,2 %
4-5	21	29,2 %
6->	5	6,9 %
Yhteensä:	72	

6. Käytätkö tai oletko käyttänyt samaa salasanaa useassa eri palvelussa?

Kyllä	24	33,3 %
Joskus	29	40,3 %
En	19	26,4 %
Yhteensä:	72	

7. Oletko kierrättänyt salasanoja? (Oletko vaihtaessasi uutta salasanaa käyttänyt vanhempaa, muistamaasi salasanaa uudelleen?)

Kyllä	39	54,9 %
Joskus	19	26,8 %
En	13	18,3 %
Yhteensä:	71	

8. Miten vaikeaa mielestäsi yleensä on salasanojen muistaminen? (1=helppoa, 3=ei helppoa eikä vaikeaa, 5=vaikeaa)

1	5	7,4 %
2	12	17,6 %
3	23	33,8 %
4	20	29,4 %
5	8	11,8 %
Yhteensä:	68	

9. Miten vaikeaa mielestäsi on luoda uusi salasana, jonka järjestelmäkin hyväksyy? (1=helppoa, 3=ei helppoa eikä vaikeaa, 5=vaikeaa)

1	16	23,5 %
2	15	22,1 %
3	13	19,1 %
4	19	27,9 %
5	5	7,4 %
Yhteensä:	68	

10. Kirjoitatko vasta vaihtamasi salasanan yleensä muistiin? (esim. paperille, kännykkään, kalenteriin tms.)

Kyllä	33	45,8 %
Joskus	20	27,8 %

En	19	26,4 %
Yhteensä:	72	

11. Salasanani on joskus vanhentunut. (Ylläpito on joskus avannut tunnukseni.)

Kyllä	30	41,7 %
Ei	38	52,8 %
En ole varma	4	5,6 %
Yhteensä:	72	

12. Miten säilytät salasanoja, joita käytät useita kertoja viikossa? (Valitse, mikä parhaiten vastaa tapojasi.)

Muistan ulkoa	67	93,1 %
Kalenterissa	4	5,6 %
Lapulla lompakossa	0	0,0 %
Matkapuhelimessa	0	0,0 %
Tarralapu(i)lla lähellä tietokonetta	1	1,4 %
Yhteensä:	72	

13. Miten säilytät salasanoja, joita käytät harvemmin? (Valitse, mikä parhaiten vastaa tapojasi.)

Muistan ulkoa	32	45,1 %
Kalenterissa	18	25,4 %
Lapulla lompakossa	9	12,7 %
Matkapuhelimessa	10	14,1 %
Tarralapu(i)lla lähellä tietokonetta	2	2,8 %
Yhteensä:	71	

14. Oletko käyttänyt jonkun toisen tai onko joku toinen käyttänyt sinun henkilökohtaista TKK:n käyttäjätunnusta? (esim. sähköpostin käyttö, tiedostonsiirto, työaseman käyttö toisen tunnuksilla tms.)

En koskaan	44	61,1 %
Kerran	10	13,9 %
2-3 kertaa	12	16,7 %
Noin puolen kymmentä kertaa	5	6,9 %
Useammin	1	1,4 %
Yhteensä:	72	

15. Onko sinulla tai tuntemallasi henkilöllä ollut tarvetta päästä ilman käyttäjätunnuksia käyttämään TKK:n atk-palveluita? (esim. sähköpostin luku, internetin selaus)

Ei koskaan	49	68,1 %
Muutaman kerran	17	23,6 %
1-2 kertaa vuodessa	2	2,8 %

Useammin kuin kaksi kertaa vuodessa	4	5,6 %
Yhteensä:	72	

16. Kuinka usein käytät tai olet käyttänyt TKK:n salasanallisia verkkopalveluita ulkomailta. (esim. sähköposti, ssh, tiedonsiirto)

En koskaan	36	50,0 %
Kerran vuodessa	9	12,5 %
2-4 kertaa vuodessa	18	25,0 %
Kerran kuussa	1	1,4 %
Useammin	8	11,1 %
Yhteensä:	72	

Valitse seuraavasta kaikki parhaiten sopivat:

17. Käytän useasti viikossa seuraavia TKK:n palveluita:

Sähköposti	70	95,9 %
Luokka- tai työhuonewindows	27	37,0 %
Luokka- tai työhuonelinux	17	23,3 %
Langaton verkko	10	13,7 %
Webnews/tkknews	14	19,2 %
VPN-yhteys	0	0,0 %
Modeemi-internetyhteys	3	4,1 %
Tulostus	27	37,0 %
Tietokantahaut (esim. kirjasto)	20	27,4 %
TKK:n internetsivut	47	64,4 %
Muut TKK:n työntekijöille tarkoitetut palvelut	13	17,8 %
Muut TKK:n opiskelijoille tarkoitetut palvelut	17	23,3 %
Yhteensä:	73	

Väittämät (Valitse itsellesi parhaiten sopiva vaihtoehto)**:**
(0=ei kokemusta, 1=täysin samaa mieltä, 2=jonkin verran samaa mieltä, 3=en samaa enkä eri mieltä, 4=jonkin verran eri mieltä, 5=täysin eri mieltä)

18. Salasanani on vaikeasti arvattava.

0	3	4,2 %
1	37	51,4 %
2	18	25,0 %
3	7	9,7 %
4	5	6,9 %
5	2	2,8 %
Yhteensä:	72	

19. Vaihtaessani salasanaa järjestelmä usein ei hyväksy uutta salasanaa.

0	2	2,8 %
1	9	12,5 %
2	18	25,0 %
3	7	9,7 %
4	23	31,9 %
5	13	18,1 %
	72	

20. Salasanojen muistaminen on yleensä minulle helppoa.

0	1	1,4 %
1	15	20,8 %
2	26	36,1 %
3	11	15,3 %
4	14	19,4 %
5	5	6,9 %
Yhteensä:	72	

21. Olen tyytyväinen Teknillisessä korkeakoulussa tarjottaviin palveluihin yleensä.

0	0	0,0 %
1	27	37,5 %
2	27	37,5 %
3	6	8,3 %
4	10	13,9 %
5	2	2,8 %
Yhteensä:	72	

22. Mielestäni salasanoja on sopiva määrä.

0	1	1,4 %

1		9	12,5 %
2		13	18,1 %
3		14	19,4 %
4		25	34,7 %
5		10	13,9 %
	Yhteensä:	72	

23. Käyn harvoin Teknillisessä korkeakoulussa (kerran viikossa tai harvemmin).

0		1	1,4 %
1		13	18,1 %
2		5	6,9 %
3		4	5,6 %
4		10	13,9 %
5		39	54,2 %
	Yhteensä:	72	

24. Salasanojen vaihtaminen on yllättävän hankalaa.

0		0	0,0 %
1		6	8,3 %
2		12	16,7 %
3		12	16,7 %
4		17	23,6 %
5		25	34,7 %
	Yhteensä:	72	

25. Verkkopankkien kertakäyttösalasanalistat ovat helppokäyttöisiä.

0		1	1,4 %
1		25	34,7 %
2		13	18,1 %
3		8	11,1 %
4		17	23,6 %
5		8	11,1 %
	Yhteensä:	72	

26. Joidenkin salasanojen muistaminen on vaikeaa.

0	1	1,4 %
1	24	33,3 %
2	22	30,6 %
3	10	13,9 %
4	12	16,7 %
5	3	4,2 %
Yhteensä:	72	

27. Muistan useimmin käyttämäni salasanan/salasanat parhaiten.

0	0	0,0 %
1	63	87,5 %
2	3	4,2 %
3	1	1,4 %
4	2	2,8 %
5	3	4,2 %
Yhteensä:	72	

28. Mielestäni verkkopankkiin kirjautuminen sisään on työlästä.

0	2	2,8 %
1	2	2,8 %
2	13	18,3 %
3	14	19,7 %
4	20	28,2 %
5	20	28,2 %
Yhteensä:	71	

29. Pidän salasanoistani yhtä hyvää huolta kuin kotiavaimistani.

0	0	0,0 %
1	31	43,1 %
2	25	34,7 %
3	5	6,9 %
4	8	11,1 %
5	3	4,2 %
Yhteensä:	72	

30. Pääosin etäkäytän TKK:n verkkopalveluita.

0	3	4,2 %
1	24	33,3 %
2	11	15,3 %
3	7	9,7 %
4	19	26,4 %
5	8	11,1 %
Yhteensä:	72	

31. Pystyisin muistamaan salasanoja enemmänkin, jos siihen olisi tarvetta.

0	1	1,4 %
1	10	13,9 %
2	18	25,0 %
3	17	23,6 %
4	19	26,4 %
5	7	9,7 %
Yhteensä:	72	

32. Teknillisessä korkeakoulussa käytetään liian paljon eri salasanoja.

0	0	0,0 %
1	18	25,0 %
2	25	34,7 %
3	14	19,4 %
4	13	18,1 %
5	2	2,8 %
Yhteensä:	72	

33. Kirjoittaudun usein väärällä salasanalla palveluun ensimmäisen kerran.

0	0	0,0 %
1	2	2,8 %
2	13	18,1 %
3	14	19,4 %
4	21	29,2 %
5	22	30,6 %
Yhteensä:	72	

34. Salasanojen käyttö on helppoa ja vaivatonta.

0	0	0,0 %
1	11	15,5 %
2	27	38,0 %
3	20	28,2 %
4	11	15,5 %
5	2	2,8 %
Yhteensä:	71	

35. Tietoa Teknillisessä korkeakoulussa käytettävistä salasanoista on helposti saatavilla.

0	15	20,8 %
1	8	11,1 %
2	25	34,7 %
3	14	19,4 %
4	8	11,1 %
5	2	2,8 %
Yhteensä:	72	

36. Käytän usein samanlaisia tai samankaltaisia salasanoja muistaakseni ne paremmin.

0	0	0,0 %
1	24	33,3 %
2	22	30,6 %
3	5	6,9 %
4	14	19,4 %
5	7	9,7 %
Yhteensä:	72	

37. Järjestelmä yleensä hyväksyy ensimmäisen ehdottamani salasanan vaihtaessani sitä.

0	0	0,0 %
1	18	25,0 %
2	25	34,7 %
3	15	20,8 %
4	10	13,9 %
5	4	5,6 %
Yhteensä:	72	

38. Salasanojen käyttö hidastaa työni tekemistä.

0	1	1,4 %
1	4	5,6 %
2	13	18,1 %
3	9	12,5 %
4	24	33,3 %
5	21	29,2 %
Yhteensä:	72	

39. Tietoa käytettävistä salasanoista löytyy yleensä helposti.

0	10	13,9 %
1	12	16,7 %
2	24	33,3 %
3	16	22,2 %
4	8	11,1 %
5	2	2,8 %
Yhteensä:	72	

40. Käytän TKK:n verkkopalveluita päivittäin. (esim. luen sähköpostini)

0	0	0,0 %
1	60	83,3 %
2	5	6,9 %
3	1	1,4 %
4	0	0,0 %
5	6	8,3 %
Yhteensä:	72	

41. Olen tyytyväinen Teknillisestä korkeakoulusta saamaani palveluun.

0	0	0,0 %
1	22	30,6 %
2	37	51,4 %
3	6	8,3 %
4	6	8,3 %
5	1	1,4 %
Yhteensä:	72	

42. Olen tyytyväinen Teknillisessä korkeakoulussa tarjottaviin palveluihin.

0	0	0,0 %
1	23	31,9 %
2	34	47,2 %
3	7	9,7 %
4	7	9,7 %
5	1	1,4 %
Yhteensä:	72	

43. Luen TKK:n sähköpostini käyttäen enimmäkseen internet-selainta (esim. http://webmail.tkk.fi)

0	0	0,0 %
1	21	29,2 %
2	12	16,7 %
3	6	8,3 %
4	12	16,7 %
5	21	29,2 %
Yhteensä:	72	

44. Haluaisin TKK:n palveluissa käytettävän vähemmän eri salasanoja.

0	0	0,0 %
1	25	34,7 %
2	24	33,3 %
3	13	18,1 %
4	7	9,7 %
5	3	4,2 %
Yhteensä:	72	

45. En käy Teknillisessä korkeakoulussa kuin tärkeimmissä kokouksissa ja tenteissä, joissa läsnäoloni on välttämätön. (Etäopiskelen tai –työskentelen.)

0	1	1,4 %
1	10	14,1 %
2	6	8,5 %
3	3	4,2 %
4	16	22,5 %
5	35	49,3 %
Yhteensä:	71	

TKK atk-keskus:

(Seuraavat kohdat koskevat pelkästään TKK:n atk-keskuksen palveluita)

46. Olen käyttänyt seuraavia atk-keskuksen palveluita: (Valitse kaikki, joita olet käyttänyt ainakin kerran viimeksi kuluneen vuoden aikana.)

Luokkatietokone	60	82,2 %
Työhuonetietokone	30	41,1 %
Sähköposti	71	97,3 %
Langaton Aalto-verkko	24	32,9 %
VPN-yhteys	5	6,8 %
Modeemi-internetyhteys	5	6,8 %
Webnews/tknews	36	49,3 %
SSH-etäyhteys	63	86,3 %
FTP-tiedonsiirto	35	47,9 %
Atk-keskuksen internetsivut	55	75,3 %
Asiakaspalvelunumerot	9	12,3 %
Asiakaspalvelupisteet	16	21,9 %
Helpdesk (helpdesk@tkk.fi)	10	13,7 %
Yhteensä:	73	

47. Jatka parhaiten sopivalla: Käytän eniten …

…pääsalasanaa. (linux/unix)	27	37,5 %
…windowssalasanaa.	7	9,7 %
…sähköpostisalasanaa.	38	52,8 %
…verkkosalasanaa. (langaton Aalto-verkko, VPN)	0	0,0 %
…palvelusalasanaa. (webnews, tknews)	0	0,0 %
En tiedä tai käytä mitään mainituista.	0	0,0 %
Yhteensä:	72	

48. Käytän viikoittain seuraavia atk-keskuksen palveluita:

Luokkatietokone	31	42,5 %
Työhuonetietokone	20	27,4 %
Sähköposti	65	89,0 %
Langaton Aalto-verkko	7	9,6 %
VPN-yhteys	0	0,0 %
Modeemi-internetyhteys	2	2,7 %
Webnews/tkknews	9	12,3 %
SSH-etäyhteys	38	52,1 %
FTP-tiedonsiirto	13	17,8 %
Atk-keskuksen internetsivut	7	9,6 %
Asiakaspalvelunumerot	3	4,1 %
Asiakaspalvelupisteet	1	1,4 %
Helpdesk (helpdesk@tkk.fi)	3	4,1 %
Yhteensä:	73	

Väittämät:
(0=ei kokemusta, 1=täysin samaa mieltä, 2=jonkin verran samaa mieltä, 3=en samaa enkä eri mieltä, 4=jonkin verran eri mieltä, 5=täysin eri mieltä)

49. Atk-keskuksen internetsivut (http://www.tkk.fi/atk/) ovat helppokäyttöiset.

0	9	12,5 %
1	9	12,5 %
2	31	43,1 %
3	12	16,7 %
4	11	15,3 %
5	0	0,0 %
Yhteensä:	72	

50. Olen tyytyväinen atk-keskuksen salasanojen määrään.

0	1	1,4 %
1	4	5,6 %
2	17	23,6 %
3	15	20,8 %
4	27	37,5 %
5	8	11,1 %
Yhteensä:	72	

51. Atk-keskuksen palveluissa käytettävät viisi (5) eri salasanaani muistan helposti. (Sinulla voi olla käytössä vähemmän salasanoja käyttämiesi palvelujen mukaan.)

0	2	2,8 %
1	8	11,1 %
2	25	34,7 %
3	6	8,3 %
4	20	27,8 %
5	11	15,3 %
Yhteensä:	72	

52. Olen tyytyväinen atk-keskuksesta saamaani palveluun.

0	3	4,2 %
1	17	23,6 %
2	30	41,7 %
3	16	22,2 %
4	5	6,9 %
5	1	1,4 %
Yhteensä:	72	

53. Löydän tarvitsemani tiedon helposti atk-keskuksen internetsivuilta (http://www.tkk.fi/atk/).

0	10	13,9 %
1	7	9,7 %
2	29	40,3 %
3	16	22,2 %
4	8	11,1 %
5	2	2,8 %
Yhteensä:	72	

54. Olen tyytyväinen atk-keskuksen tarjoamien palveluiden laatuun.

0	3	4,2 %
1	19	26,4 %
2	29	40,3 %
3	17	23,6 %
4	3	4,2 %
5	1	1,4 %
Yhteensä:	72	

55. Olen tyytyväinen atk-keskuksen tarjoamien palveluiden määrään.

0	4	5,6 %
1	17	23,9 %
2	34	47,9 %
3	12	16,9 %
4	3	4,2 %
5	1	1,4 %
Yhteensä:	71	

56. Tieto atk-keskuksen palveluissa käytetyistä salasanoista löytyy helposti.

0	9	12,5 %
1	13	18,1 %
2	28	38,9 %
3	11	15,3 %
4	9	12,5 %
5	2	2,8 %
Yhteensä:	72	