TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan osasto

MIKAEL LINDEN

Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa

Lisensiaatintutkimus

Tutkimusaihe hyväksytty osastoneuvostossa
13.2.2002
Tarkastajat: professori Jarmo Harju
dosentti Pekka Nikander
lehtori Jukka Koskinen

ALKULAUSE

Tämä lisensiaatintutkimus on syntynyt osana Henkilön sähköinen tunnistaminen yliopistoissa ja ammattikorkeakouluissa (HSTYA) -projektia, joka oli suomalaisten yliopistojen, ammattikorkeakoulujen, näiden opiskelijaliittojen ja Tieteen tietotekniikan keskus CSC:n yhteishanke, jonka päämääränä oli selvittää julkisen avaimen järjestelmän ja toimikorttien käyttöönottoa ja hyödyntämistä korkeakouluissa. Tutkimuksen on tarkoitus palvella korkeakouluyhteisöä paitsi akateemisena opinnäytteenä, myös korkeakoulujen tietojärjestelmien ylläpitäjien käteen sopivana taustoittavana yleiskuvauksena aihepiiristään. Erityisiä esitietovaatimuksia tutkimuksen lukemiseen ei ole – tavanomaisen tietoliikennetekniikkaan liittyvän yleistiedon omaaminen riittää.

Tahdon kiittää tutkimukseni tarkastaneita professori Jarmo Harjua, dosentti Pekka Nikanderia ja lehtori Jukka Koskista, joilta olen saanut runsaasti neuvoja tutkimukseeni liittyvissä asioissa. Kiitos myös tutkimukseen liittyviä kommentteja ja parannusehdotuksia esittäneille Kirsti Ala-Mutkalle, Antti Vähä-Sipilälle ja Martti Jokipiille. Saamastani tuesta tahdon kiittää lisäksi HSTYA-projektin projektiryhmää sekä Outi Kaikkosta, jonka lahjakkuus oikolukijana on vertaansa vailla.

Tampereella 15. tammikuuta 2003

Mikael Linden
Elementinpolku 15 C 25
33720 TAMPERE
puh. 040 552 4859

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

Tietoliikennetekniikka

LINDEN, MIKAEL JUHANI: Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa

Lisensiaatintutkimus, 129 sivua, 5 liitesivua

Tarkastajat: professori Jarmo Harju, dosentti Pekka Nikander, lehtori Jukka Koskinen

Tammikuu 2003

Avainsanat: Julkisen avaimen järjestelmä, PKI, toimikortti

Julkisen avaimen järjestelmä (public key infrastructure, PKI) on kryptografiaa soveltava teknologia, jota voidaan käyttää tietoverkon käyttäjien lähettämien viestien aitouden, eheyden ja luottamuksellisuuden varmistamiseen. Julkisen avaimen järjestelmän avulla on mahdollista toteuttaa muun muassa verkon käyttäjän henkilöllisyyden todentaminen, käyttäjien toisilleen lähettämien sähköpostiviestien salaaminen sekä digitaalinen allekirjoitus, jonka avulla verkon käyttäjä voi ilmaista sitoutumisensa lähettämäänsä viestiin perinteisen allekirjoituksen tapaan.

Julkisen avaimen järjestelmän toteuttamisessa voidaan käyttää apuna toimikorttia, joka on varsin turvallinen ja peruskäyttäjällekin kouriintuntuva väline kryptografisten avainten tallettamiseen ja käyttämiseen. Toimikorttien ja toimikortinlukijoiden hankkiminen käyttäjille ei kuitenkaan riitä: julkisen avaimen järjestelmän käyttöönotto aiheuttaa myös muutoksia verkon kautta tarjottavien palveluiden toteutukseen. Julkisen avaimen järjestelmän monipuolinen hyödyntäminen palveluja tarjoavassa organisaatiossa edellyttää julkisen avaimen järjestelmän niveltämistä organisaation käyttäjähallintoon.

Julkisen avaimen järjestelmä on vähitellen kypsymässä laajaan käyttöön. Tässä tutkimuksessa on koottu yhteen julkisen avaimen järjestelmän periaatteita ja nykyisiä toteutusmenetelmiä sekä syvennytty erityisesti sen toimikortteja hyödyntävään toteutustapaan. Tutkimuksen loppuosassa on tutkittu julkisen avaimen järjestelmän soveltamista ja siihen liittyviä erityiskysymyksiä organisaatiossa, joka tarjoaa tietoverkon välityksellä käyttäjille erilaisia henkilökohtaisia palveluja.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY

Department of Information Technology

Institute of Communications Engineering

LINDEN, MIKAEL JUHANI: Public Key Infrastructure, Smart Cards and Their Utilization in an Organization

Licentiate Thesis, 129 pages, 5 enclosure pages

Examiners: professor Jarmo Harju, docent Pekka Nikander, lecturer Jukka Koskinen

January 2003

Keywords: Public key infrastructure, PKI, smart card

Public key infrastructure (PKI) is a technology applying cryptography to make it possible to ensure the authenticity, integrity and confidentiality of messages sent in a network. Among other things PKI can be used in authenticating network users, encrypting messages exchanged by the users and implementing digital signatures, which are expressions of commitment to messages in the network.

An implementation of PKI can utilize a smart card, which is a fairly secure and tangible hardware module for storing cryptographic keys. However, acquiring smart cards and smart card readers to users is not enough; deploying public key infrastructure causes modifications to the services provided in the network as well. A large-scale utilization of PKI in an organization providing various kinds of services requires integration of PKI to the organization's user administration.

PKI is becoming developed enough for being used widely. This work gathers up the fundamentals of PKI, concentrating particularly on the implementation relying on smart cards. In the end of the work issues related to the utilization of PKI are studied especially in an organization providing different kinds of personal network services to the users.

SISÄLLYS

1. JOHDANTO

Internet siirtyi 1990-luvulla akateemisesta maailmasta myös suurten massojen saataville. Internetin käyttö on yleistynyt ja monipuolistunut: entistä suurempi joukko ihmisiä käyttää sitä myös entistä luottamuksellisempien asioiden hoitamiseen. Internetin lähtökohtaisesti tarjoama tietoturvallisuustaso on kuitenkin vaatimaton, ja nykyään entistä useammalla verkon käyttäjällä on tarvittava osaaminen ja välineet turvallisuuden heikoimpien kohtien murtamiseen. Tietoliikenteen turvallisuustason kohentamiseksi Internetissä onkin kehitetty monia eri menetelmiä.

Internetin kautta on tarjolla lukuisia erilaisia henkilökohtaisia palveluita, joiden osapuolet – palveluiden käyttäjät ja tarjoajat – edellyttävät varmuutta vastapuolen henkilöllisyydestä sekä siitä, että sivulliset eivät voi lukea tai peukaloida osapuolten välisiä viestejä. Tällä hetkellä yleisesti käytetty menetelmä palvelun käyttäjän henkilöllisyyden varmistamiseksi eli käyttäjän todentamiseksi on salasana, jonka tarjoamaa turvallisuustasoa ei kuitenkaan pidetä yleisesti kovin korkeana.

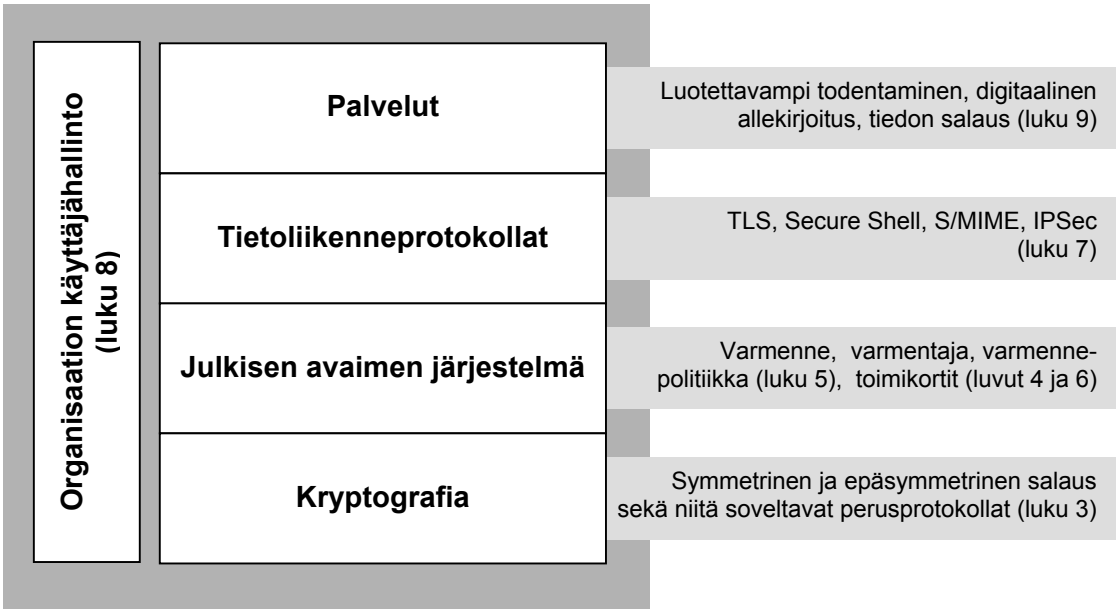
Kryptografian eli salakirjoitustieteen sovellukset ovat tuoneet myös Internetin kehittäjille uusia välineitä verkon tietoturvallisuuden kohentamiseen. Yksi niistä on julkisen avaimen järjestelmä, joka on saanut liittolaisen toimikorttitekniikan kehityksestä. Suomessa huomiota on herättänyt julkisen avaimen järjestelmää hyödyntävä sähköinen henkilökortti, jonka valtio on tuonut kansalaisten saataville.

Tämän tutkimuksen aiheena ovat julkisen avaimen järjestelmä ja sen hyödyntäminen. Tutkimuksessa syvennytään erityisesti toimikortteja hyödyntävän julkisen avaimen järjestelmän käyttöön päätelaitteissa, joiden keskinäinen kommunikointi tapahtuu Internetissä käytetyn protokollaperheen välityksellä.

Tutkimuksessa tarkastellaan julkisen avaimen järjestelmän tietoverkossa tarjoamia peruspalveluja: osapuolten henkilöllisyyden todentamista eli autentikointia, viestin alkuperän ja muuttumattomuuden takaavan digitaalisen allekirjoituksen toteutusta sekä julkisen avaimen järjestelmän käyttöä tiedon, kuten sähköpostin, salaukseen. Päähuomio tutkimuksessa keskittyy kuitenkin käyttäjän henkilöllisyyden todentamiseen, jolloin julkisen avaimen järjestelmä toimii salasanan ja muiden todentamismenetelmien korvaajana.

Tutkimuksen loppupuolella syvennytään julkisen avaimen järjestelmän hyödyntämiseen ja käyttökohteisiin organisaatiossa, kuten yrityksessä, jossa järjestelmää käyttävät esimerkiksi työntekijät tai asiakkaat, tai oppilaitoksessa, jossa käyttäjinä ovat muun muassa opiskelijat ja opettajat. Tällöin julkisen avaimen järjestelmä kytkeytyy kullekin tietoverkon käyttäjälle myönnettyjen käyttöoikeuksien hallinnointiin ja siten edelleen organisaation käyttäjähallintoon.

Tutkimuksen aihepiiri ja rakenne koostuu kokonaisuuksista, joiden keskinäistä riippuvuutta on pyritty hahmottamaan oheisella kuvalla (Kuva 1). Tutkimuksen keskeistä aihepiiriä – julkisen avaimen järjestelmää – käsitellään luvussa 5. Teknisessä mielessä julkisen avaimen järjestelmä nojaa kryptografiaan, erityisesti epäsymmetriseen eli julkisen avaimen salausmenetelmään. Luvussa 3 esitellään joitain kryptografian perusteita, joihin sisältyvät muun muassa symmetrinen ja epäsymmetrinen salaus, digitaalinen kirjekuori, tiivistefunktiot, digitaalinen allekirjoitus ja haaste/vaste-todentaminen.



Kuva 1. Tutkimuksen aihepiiri koostuu toisiinsa tukeutuvista tasoista.

Toimikortti on houkutteleva alusta korkeaa tietoturvaa vaativien sovellusten toteuttamiseksi. Toimikorttien tekniikkaa esitellään yleisellä tasolla luvussa 4 ja niiden käyttöä erityisesti julkisen avaimen järjestelmässä käsitellään luvussa 6. Julkisen avaimen järjestelmään nojaavia tietoliikenneprotokollia käsitellään luvussa 7, jossa näkökulmana on erityisesti tietoverkon käyttäjän henkilöllisyyden todentaminen varmenteen avulla. Esimerkkinä on käytetty TLS-, Secure shell- ja S/MIME-protokollia.

Luvussa 9 tarjotaan yksi näkökulma julkisen avaimen järjestelmän potentiaalisiin käyttötarkoituksiin organisaatiossa: mitä etua organisaatiolle koituu julkisen avaimen järjestelmän käyttöönotosta. Ennen käyttöönottamista organisaation on kuitenkin nivellettävä julkisen avaimen järjestelmä osaksi tietojärjestelmiensä käyttäjähallintoa. Tähän problematiikkaan syvennytään luvussa 8.

Tutkimus alkaa kuitenkin johdatuksella aihepiiriin: luku 2 käsittelee tutkimuksen aihepiirin keskeisiä käsitteitä, kuten käyttäjän henkilöllisyyden todentamista eli autentikointia, käyttäjän valtuuttamista eli auktorisointia ja näiden perusteella suori-

tettavaa pääsynvalvontaa. Luvun tarkastelu alkaa yleiseltä tasolta, ja syventyy sen jälkeen todentamisen, valtuuttamisen ja pääsynvalvonnan toteuttamiseen erityisesti tietojärjestelmissä.

2. PERUSKÄSITTEITÄ

Tässä luvussa tutustutaan tutkimuksen aihepiiriin liittyviin peruskäsitteisiin. Erityisesti tarkastellaan todentamista (authentication), valtuuttamista (authorization) ja pääsynvalvontaa (access control) ensin yleisesti ja sitten nimenomaan tietojärjestelmissä.

2.1. Valtuuden myöntäminen ja toteaminen

Päivittäisessä elämässä on lukuisia asioita, joita ovat oikeutettuja tekemään vain luvan saaneet henkilöt. Esimerkiksi useista ovista saavat kulkea vain kulkuluvan saaneet henkilöt. Auton ajoon valtuus on vain ajoluvan saaneilla, oikeus nostaa rahaa pankkitililtä puolestaan on tilinkäyttöoikeuden haltijoilla.

Luvan antamisessa on kyse valtuuttamisesta eli auktorisoinnista. Siitä huolehtii taho, jolle kyseinen tehtävä on uskottu valtuuksia edellyttävää asiaa hallinnoivassa organisaatiossa. Luvan kulkea ovista antaa yrityksissä tyypillisesti henkilöstöhallinto, valtuuden kotioven avaamiseen esimerkiksi vuokraisäntä. Oikeuden pankkitilin käyttöön puolestaan antaa tilin omistaja – joko luonnollinen henkilö itse tai yhteisöissä, kuten yhtiöissä tai yhdistyksissä, hallitus.

Valtuuden saamisen perusteet riippuvat asiayhteydestä. Luvan auton ajamiseen voivat saada henkilöt, jotka ovat esittäneet kuljettajatutkintoon kuuluvassa teoria- ja ajokokeessa riittävän ajoneuvon ja liikennesääntöjen hallintaan liittyvän osaamisensa. Oikeus kulkea ovesta on henkilöllä, joka asuu tai on vaikkapa töissä kyseisissä tiloissa. Voidaan myös ajatella, että junamatkustaja saa valtuuden nousta junaan ostaessaan junalipun kyseiselle matkalle.

Kerran myönnetyn valtuuden olemassaolo on pystyttävä myöhemmin toteamaan, kun valtuuksia halutaan käyttää. Valtuuttamattomilla henkilöillä ei saa olla pääsyä valtuuksia edellyttävään asiaan: oven tulee pysyä lukittuna henkilöille, joilla ei ole oikeutta kulkea siitä.

Joskus valtuus myönnetään toistaiseksi – näin on usein pankkitilin käyttöoikeuksien laita. Joissain tapauksissa valtuus on määräaikainen: kuukausilipulla voi matkustaa rajattomasti yhden kuukauden ajan, sen sijaan menolippu junassa on voimassa vain yhden matkan. Menolipun kertakäyttöisyydestä huolehtii lipuntarkastaja lippuun tekemällään leimalla.

Valtuuksien toteaminen voidaan järjestää periaatteessa kahdella eri tavalla. Joko tieto valtuuttamisesta kirjataan listaan, jossa myönnettyjä valtuuksia ylläpidetään

(access control list, ACL), tai valtuutetulle myönnetään valtuustieto (credential), jonka hän esittää halutessaan käyttää valtuuksiaan.

Perinteinen nikkeliavain on tyypillinen valtuustieto: oven lukko avautuu, kun lukkopesään työnnetään kyseiseen lukkoon tarkoitettu avain. Myös rautatieaseman lipunmyynnissä asiakkaalle kirjoitettu junalippu on valtuustieto.

Junalippu ja useammat muutkaan liput eivät yleensä ole sidottuja tiettyyn henkilöön, joka sitä käyttää. Palvelun tarjoajaa kiinnostaa lähinnä, että kaikki asiakkaat tulevat rahastetuiksi, eikä niinkään se, että lipun maksaa ja käyttää sama henkilö. Tällöin valtuustieto ei ole henkilö- vaan haltijakohtainen: valtuus voidaan siirtää eli delegoida toiselle. Avainten suhteen tilanne on toinen: lupa kulkea lukitusta ovesta annetaan avaimen haltijalle henkilökohtaisesti, eivätkä esimerkiksi yrityksen työntekijät ole oikeutettuja luovuttamaan avainta muille. Lukko ei kuitenkaan tiedä, käyttääkö avainta sen oikeutettu haltija vai onko avain vaikkapa varastettu.

Voidaan pyrkiä järjestelyihin, joiden myötä valtuustietoa voi käyttää vain valtuutettu käyttäjä itse. Esimerkiksi poliisi myöntää osoitukseksi suoritetusta kuljettajatutkinnosta ajokortin, johon sisältyy ajoneuvoluokan lisäksi kortin haltijan valokuva. Ajokorttia tarkastettaessa poliisi vertaa kortin haltijan kasvonpiirteitä kortin kuvaan pyrkimyksenään varmistua, että kortti todella on myönnetty ohjauspyörän takana istuvalla henkilölle. Ajokorttiin painettuja muita henkilötietoja, kuten kuljettajan nimeä, tarvitaan vasta, kun häntä on syytä sakottaa.

Vaihtoehtoinen tapa valtuutuksen toteamiselle on etsiä asianomainen henkilö pääsylistalta, johon on kirjattu kaikki valtuuden saaneet henkilöt. Ennen kuin tämä voidaan suorittaa, on asianomaisen henkilöllisyys todennettava eli autentikoitava.

Pankkitililtä rahaa nostavan henkilön valtuuksien toteaminen tapahtuu todentamalla hänen henkilöllisyytensä poliisin tai muun luotetun tahon myöntämän henkilöllisyystodistuksen avulla ja varmistamalla pankin tietojärjestelmästä, että kyseisellä henkilöllä on oikeus nostaa rahaa tililtä. Jos rahaa nostetaan pankkiautomaatista, ei tilinkäyttäjän henkilöllisyyden varmistamiseen käytetä henkilöllisyystodistusta vaan pankkiautomaattikorttia ja siihen liittyvää tunnuslukua. Tilinkäyttäjää on kielletty paljastamasta tunnuslukua kenellekään, jotta varastettua korttia ei voitaisi käyttää.

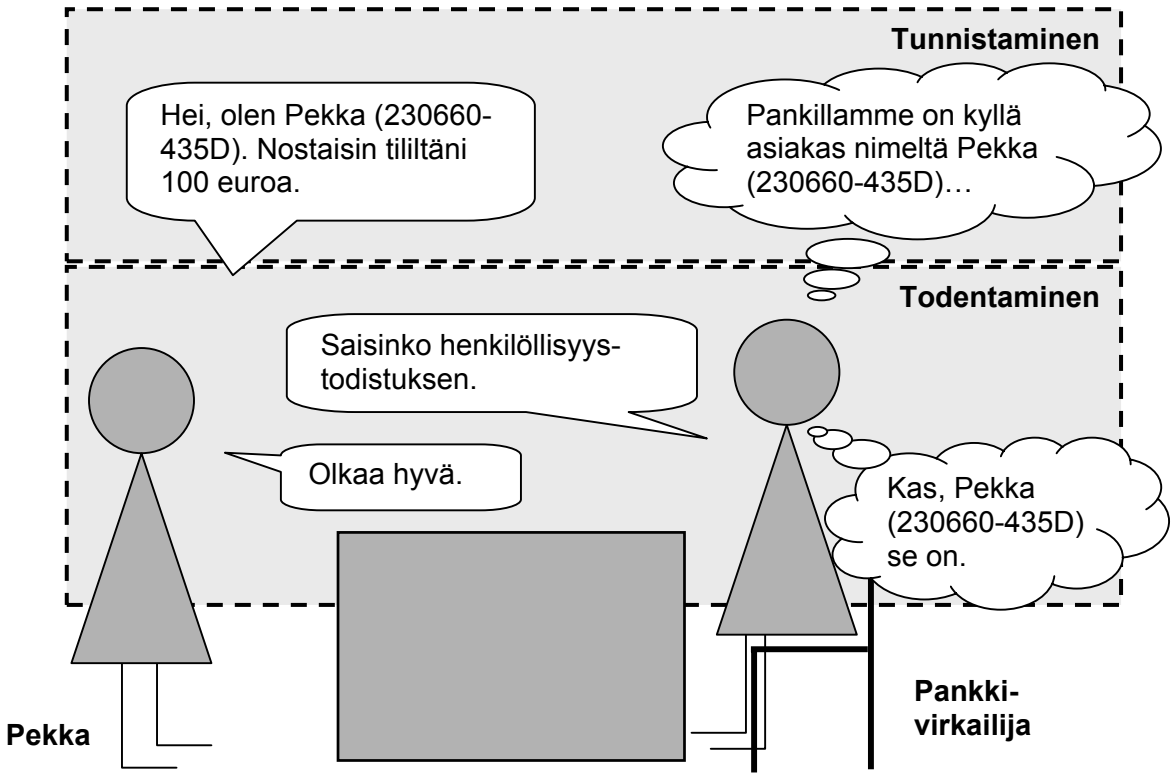
Todentaminen (authentication) ja tunnistaminen (identification) ovat kaksi eri käsitettä. Tunnistamisella tarkoitetaan menettelyä, jolla yksilöidään joku tai jokin, esimerkiksi tietojärjestelmän käyttäjä [VM00]. Tunnistamisen tarkoitus on siis erottaa käyttäjät toisistaan ja sen keskeinen apuväline on tunniste (identifier). Kaikki tunnisteet eivät välttämättä ole yksikäsitteisiä: kahdella eri henkilöllä voi olla sama ristimänimi. Henkilöille annettavia yksikäsitteisiä tunnisteita ovat mm. Väestöre-

kisterikeskuksen suomalaisille antama henkilötunnus ja yksittäisen tietojärjestelmän käyttäjälleen antama henkilökohtainen käyttäjätunnus. Tunnisteiden ja niistä muodostuvien nimiavaruuksien ongelmaan palataan luvussa 5.9.

Todentaminen puolestaan tarkoittaa järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen tunnistuksen varmistamista [VM00]. Elävässä elämässä henkilöllisyyden todentaminen voi perustua esimerkiksi todentajan omaan aikaisempaan kokemukseen (henkilö tuntee toisen kasvonpiirteistä tai äänestä) tai luotettavana pidetyn kolmannen osapuolen suorittamaan todentamiseen (poliisi on aikanaan todentanut henkilöllisyyden ja myöntänyt hänelle passin tai henkilöllisyystodistuksen). Todentamisessa on siis kysymys siitä, että tavalla tai toisella varmistetaan, että todennettava henkilö on sama, jonka todentaja itse tai hänen luottamansa kolmas osapuoli on aikaisemmin tunnistanut.

Henkilöllisyyden todentamiseen liittyy aina epävarmuus, jonka suuruus riippuu todennettavasta, todentajasta ja todentamistavasta. Todentaminen äänen avulla puhelimitse on yleensä vaikeampaa kuin kasvotusten kasvonpiirteiden avulla, mutta läheisetkään eivät aina erota identtisiä kaksosia toisistaan. Suomessa poliisin myöntämiä tunnistamisasiakirjoja on yleensä pidetty melko luotettavina, mutta myös poliisi joutuu henkilölle ensimmäistä henkilöllisyystodistusta myöntäessään luottamaan muihin järjestelyihin – esimerkiksi vanhempiin, jotka menevät takuuseen lapsensa henkilöllisyydestä.

Henkilön tunnistamisen ja todentamisen eroa on pyritty selventämään oheisen kuvan avulla. Kuvassa henkilö, joka tulee pankkiin ja kertoo virkailijalle olevansa Pekka, on määritelmän mukaan tullut tunnistetuksi pankin asiakkaaksi. Todennetuksi hän tulee vasta sitten, kun virkailija on todennut hänen henkilöllisyytensä hänen esittämänsä henkilöllisyystodistuksen avulla (Kuva 2).



Kuva 2. Esimerkki tunnistamisesta ja todentamisesta pankissa.

Käyttäjän tunnistaminen ja hänen henkilöllisyytensä todentaminen kohtaavat toisensa muun muassa tietojärjestelmään kirjauduttaessa, joka nykyään tapahtuu useimmiten antamalla järjestelmälle käyttäjätunnus (tunnistaminen) ja salasana (todentaminen). Suomen kielessä tietojärjestelmään kirjautumista kutsutaan usein harhaan johtavasti "käyttäjän tunnistamiseksi". Tässä tutkimuksessa tunnistamisen ja todentamisen käsitteet pyritään kuitenkin pitämään erillä toisistaan.

2.2. Todentaminen, valtuuttaminen ja pääsynvalvonta tietoverkossa

Valtuuttaminen on keskeinen kysymys myös tietoverkoissa ja -järjestelmissä. Useimmissa tietojärjestelmissä valtuuksien hallinta perustuu valtuuksien myöntämiseen, käyttäjän henkilöllisyyden todentamiseen ja näiden perusteella tapahtuvaan pääsynvalvontaan. Tässä alaluvussa tarkastellaan näitä kolmea osakokonaisuutta, mutta muistutetaan kuitenkin myös käyttäjän yksityisyyden suojan ottamisesta huomioon.

2.2.1. Valtuuttaminen tietoverkossa

Valtuudella tarkoitetaan oikeutta tiettyjen tietojen tai tietojärjestelmäresurssien käyttöön [VM00]. Valtuus voi kohdistua esimerkiksi tietoon, tiedostoon, tietokantaan, tietojärjestelmään tai niiden muodostamaan toiminnalliseen kokonaisuuteen, kuten WWW-sivustoon. Käyttäjällä voi olla valtuudet esimerkiksi tiedon lukemi-

seen, muuttamiseen, lisäämiseen tai poistamiseen. Tässä tutkimuksessa sanoja valtuus, oikeus ja käyttöoikeus käytetään useimmiten toistensa synonyymeinä.

Valtuuttaminen tarkoittaa valtuuksien myöntämistä ja hallintaa [VM00]. Sen tekninen toteutus riippuu kyseessä olevasta järjestelmästä. Esimerkiksi Unix-käyttöjärjestelmässä tiedoston omistaja voi antaa kullekin tiedostolle luku-, kirjoitus- ja suoritus-oikeuden erikseen paitsi itselleen, myös hänen kanssaan samaan käyttäjäryhmään kuuluville sekä muille tietojärjestelmän käyttäjille. Käyttöoikeudet annetaan käyttöjärjestelmän tarjoamalla `chmod`-komennolla.

Valtuuksien myöntäminen on organisaatiossa paitsi tekninen, myös hallinnollinen kysymys. Yritykset antavat kaikille työntekijöilleen tyypillisesti oikeuden käyttää tiettyjä perustyökaluja ja -järjestelmiä. Tällöin valtuuksien myöntäminen käsittää sekä kerran tehdyn linjapäätöksen, jolla kaikille työntekijöille myönnetään tietojärjestelmiin käyttöoikeus, että päätöksen, jolla tietty henkilö palkataan yrityksen työntekijäksi. Kun uusi työntekijä palkataan ja hänelle luodaan käyttäjätunnus tietoverkkoon, ei verkon ylläpitohenkilökunta itse asiassa enää tunnusta luodessaan suorita valtuuden myöntämistä vaan pelkästään toteuttaa yrityksen aikaisemmin tekemää käyttäjätunnuslinjausta. Niinpä käyttäjätunnusten luominen uusille työntekijöille voidaan suorittaa myös täysin automaattisesti.

Joissain tilanteissa on tarkoituksenmukaista, että valtuutetulla on mahdollisuus siirtää eli delegoida valtuutensa jollekin toiselle. Toisaalta valtuuden myöntäjä voi myös kieltää valtuuden siirtämisen eteenpäin, tai peruuttaa siirtämänsä valtuuden. Erilaiset käyttäjähallinnon toteutusmallit tukevat delegointia vaihtelevalla tavalla.

2.2.2. Todentaminen eli autentikointi

Kun henkilö haluaa käyttää hänelle myönnettyjä valtuuksia, hän tunnistautuu järjestelmälle eli esittää väitteen henkilöllisyydestään. Väitteen totuudenmukaisuus selvitetään todentamalla henkilöllisyys.

Henkilöllisyyden todentaminen voi hyödyntää erilaisia periaatteita ja tekniikoita. Usein esitetty luokittelu todentamisen perusteelle koostuu kolmesta tekijästä, joiden tulee olla ainutlaatuiset: jotain, mitä henkilö tietää (kuten salasana), jotain, mitä henkilöllä on (kuten pankkiautomaattikortti) tai jotain, mitä henkilö on (kuten sormenjälki, käyttäytyminen tai muu henkilökohtainen biometrinen ominaisuus). Todentamisen luotettavuutta voidaan lisätä vaatimalla useamman tekijän yhtäaikaista käyttöä; pelkällä pankkiautomaattikortilla ei vielä saa rahaa pankkiautomaatista, vaan kortinhaltijan on tiedettävä myös korttiin liittyvä salasana eli tunnusluku.

Nykyisin pääosa tietojärjestelmistä todentaa käyttäjänsä henkilöllisyyden salasanan avulla. Salasana on tyypillisesti vaihtelevan määrän numeroita, kirjaimia ja yleisimpiä erikoismerkkejä sisältävä merkkijono, joka on vain todennettavan itsensä ja mahdollisesti todentavan tietojärjestelmän tiedossa. Käyttäjä esittää salasanansa tietojärjestelmälle todennuksen yhteydessä.

Salasanaan perustuvan todentamisen ongelma on salasanan pysyminen samana käyttökerrasta toiseen. Jos hyökkääjä saa salasanan haltuunsa, hän pystyy sen avulla esiintymään järjestelmän valtuutettuna käyttäjänä. Salasana saattaa paljastua verkkoliikennettä salakuuntelevalle tai todennettavan olan yli kurkkivalle sivulliselle. Todennettava voi myös kirjoittaa salasanansa paperinpalalle, joka saattaa joutua sivullisen käsiin.

Jos todennettava pääsee itse valitsemaan salasanansa, saattaa hän valita sen niin helpoksi, että se on arvattavissa. Hyökkääjillä on käytössään niin sanottuun sanakirjahyökkäykseen soveltuvia työkaluja, jotka muodostavat ja kokeilevat tietojärjestelmissä yleisimmin käytettyjä salasanoja kunnes oikea löytyy. Tietokoneiden laskentatehon kasvaessa salasanojen kokeileminen on entistä nopeampaa, joten salasanan on oltava aina vain pidempi ollakseen vaikeasti arvattava.

Joitakin keinoja salasanan turvallisuuden kohentamiselle on olemassa ja myös yleisesti käytössä. Salakuuntelun estämiseksi tietoliikenneyhteydet todennettavan ja todentajan välillä voidaan salata, tai käyttäjää voidaan estää valitsemasta liian lyhyt tai muuten helposti arvattava salasana. Tietoturvallisuuden heikoin lenkki on kuitenkin yleensä ihminen, ja ylläpidollisin keinoin on vaikea estää käyttäjää kirjoittamasta salasanaansa paperille, joka laitetaan näppäimistön alle piiloon.

Tietoverkon käyttäjä kohtaa päivittäin lukuisia eri järjestelmiä, jotka todentavat käyttäjänsä henkilöllisyyden salasanan avulla. Käyttäjällä on siis yhtä aikaa muistettavana iso joukko salasanoja eri järjestelmiin; erityisesti WWW:ssä niitä käytetään runsaasti. Samaa salasanaa ei saisi käyttää kahdessa eri järjestelmässä, sillä WWW-palvelimen pahantahtoinen ylläpitäjä tai palvelimeen murtautunut hakkeri saattaa esimerkiksi kokeilla, mihin muihin järjestelmiin kyseinen henkilö on asettanut saman salasanan.

Jos todennettavalla ja todentajalla on mahdollisuus jollain tavoin havaita salasanan paljastuminen sivulliselle, tarjoutuu mahdollisuus estää lisävahinkojen syntyminen. Usein jälkiä ei kuitenkaan jää tai huomata, eikä osapuolilla ole käytännössä mahdollisuutta todeta salasanan paljastumista. Niinpä monet tietojärjestelmät pakottavat käyttäjän varmuuden vuoksi vaihtamaan salasanansa säännöllisesti, esimerkiksi kolmen kuukauden välein, mikä lisää salasanojen opettelemista entisestään. Tietojärjestelmien määrän ja niiden edellyttämän turvallisuustason kasvaessa onkin lähdetty etsimään vaihtoehtoisia todentamismenetelmiä.

Kerrasta toiseen samana pysyvää salasanaa luotettavammin käyttäjän henkilöllisyys voidaan todentaa kertakäyttösalasanan avulla, jolloin käyttäjän tulee jokaisen todentamiskerran yhteydessä antaa eri salasana. Tietojärjestelmän ylläpitäjä on voinut antaa käyttäjälle luotettavaa kanavaa pitkin etukäteen listan käytettävistä kertakäyttösalasanoista. Koska kukin salasana kelpaa vain yhden kerran, ei salasanan sieppaamisesta verkossa ole hyötyä. Kertakäyttösalasanojen turvallisuutta voidaan lisätä protokollilla, jotka eivät edellytä, että todentaja tietää etukäteen todennettavan kertakäyttösalasanan (esim. One-Time Password System [RFC2289]). Käyttäjälle mahdollisesti paperilla toimitetun salasanalistan paljastumiseen liittyvää riski voidaan välttää tarjoamalla salasanalistan sijaan salasanoja pyydettäessä generoiva laite (esim. RSA Securityn kehittämä SecurID, [RSAS02]).

Todentamista kutsutaan vahvaksi (strong authentication), kun se hyödyntää kryptografista laskentaa, esimerkiksi julkisen avaimen salausmenetelmää [VM00]. Vahva todentaminen on olennaisesti luotettavampi kuin heikko todentaminen, koska osapuolten välistä tiedonsiirtoa mahdollisesti salakuunteleva hyökkääjä ei saa haltuunsa tietoa, jonka avulla hän pystyisi vahingoittamaan osapuolia esimerkiksi tekeytymällä myöhemmin todennettavaksi käyttäjäksi. Vahva todentaminen edellyttää yleensä monimutkaisia laskutoimituksia, ja sopiikin lähinnä tilanteeseen, jossa sekä todennettava että todentaja ovat koneita. Koska ihminen on epäluotettava ja hidas laskemaan, joudutaan ihminen todentamaan koneelle yleensä heikon eli yksinkertaisen todentamisen (weak/simple authentication), kuten salasanan, avulla.

Vahvaan todentamiseen perustuvia tekniikoita on kehitetty useita. Niihin palataan myöhemmin kryptografian ja julkisen avaimen järjestelmän yhteydessä.

2.2.3. Pääsynvalvonta

Pääsynvalvonta (access control) on tietojärjestelmissä oma, luotettu kokonaisuutensa, joka nojaa valtuuttamiseen ja todentamiseen. Pääsynvalvonta on mekaanista toimintaa, jonka tehtävä on viime kädessä huolehtia, että resursseihin pääsevät käsiksi vain valtuutetut käyttäjät.

Pääsynvalvonnan toimintaperiaate on yksinkertainen. Kun käyttäjä haluaa tehdä jotain tietojärjestelmässä, järjestelmä selvittää, kenestä on kyse (henkilöllisyyden todentaminen) ja mitkä ovat kyseisen käyttäjän valtuudet. Jos käyttäjällä on riittävät valtuudet, hänen sallitaan suorittaa kyseinen toimenpide.

Esimerkiksi Unix-käyttöjärjestelmässä tiedostojärjestelmä huolehtii tiedostojen pääsynvalvonnasta. Oletetaan, että tiedoston omistaja on asettanut itselleen täydet luku-, kirjoitus- ja suoritus-oikeudet tiedostoon `index.html`, mutta muille kyseiseen tiedostoon on annettu pelkästään lukuoikeus. Kun käyttäjä haluaa muokata tiedostoa ja tallentaa muokatun version vanhan tilalle, on tiedostojärjestelmän pää-

synvalvonnan tehtävä tarkistaa, kuka tekstieditorin on käynnistänyt (henkilöllisyyden todentaminen, jonka Unix suorittaa heti järjestelmään kirjauduttaessa ennen komentotulkin käynnistystä) ja onko kyseisellä käyttäjällä kirjoitusoikeus (valtuutus) kyseisen tiedoston kirjoittamiseen. Ellei valtuuksia ole, pääsynvalvonta palauttaa virheilmoituksen.

2.2.4. Yksityisyyden suoja

Tietotekniikan käytön ja tietoverkossa tarjottavien palvelujen laajeneminen kasvattaa palveluntarjoajien mahdollisuuksia kerätä asiakkaistaan tietoa, jota voidaan käyttää asiakkaiden profilointiin. Esimerkiksi asiakkaan kulutustottumuksista laadittua profiilia voidaan hyödyntää suoramarkkinoinnin kohdentamisessa. Monet kokevat kuitenkin henkilötietojen liiallisen keräämisen ja taltioinnin loukkauksena yksityisyydelleen (privacy), jota Suomessa suojelee perustuslaki [PERU99 §10]. Henkilötietolaki [HETI99] kieltääkin muiden kuin tarpeellisten henkilötietojen keräämisen ja säätelee kerättyjen henkilötietojen käsittelyä ja käyttöä.

Monien verkossa tarjottavien palveluiden, kuten tavallisten WWW:n välityksellä toteutettujen tiedotuspalvelujen, käyttäminen ei edellytä, että palvelun tarjoajien tarvitsisi tietää asiakkaiden henkilöllisyyttä. Tällaisia palveluja sanotaan anonyymipalveluiksi [VM00]. Jotkut palvelut kuitenkin edellyttävät, että asiakas pystytään yksilöimään ja todentamaan tietyksi palvelulle jo entuudestaan tunnetuksi käyttäjäksi ilman, että palvelun tarjoajan tarvitsee tietää asiakkaan oikeaa nimeä ja henkilöllisyyttä. Tällöin asiakas voi käyttää oikean nimensä sijaan peitenimeä (pseudonym) [VM00].

Julkishallinnon sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje muistuttaa, että asiakkaan perusoikeutena on anonyymi palvelu aina, kun henkilön yksilöivä todentaminen ei ole välttämätöntä. Vaikka todentamisen ja personoinnin avulla voitaisiin tarjota parempaa palvelua, neuvoo yleisohje tarjoamaan mahdollisuuksien mukaan myös anonyymin palveluvaihtoehdon, jonka palvelutaso voi olla heikompi. [VM01b, s 15-16]

2.3. Muita peruskäsitteitä

Tietoturvallisuutta koskeville termeille ja käsitteille on kirjallisuudessa annettu runsaasti erilaisia ja keskenään ristiriitaisiakin määritelmiä. Tässä esitetyt, tutkimuksen kannalta keskeiset määritelmät ja erityisesti englanninkielisten termien suomennokset perustuvat valtionhallinnon tietoturvakäsitteistöön, ellei muuta mainita [VM00].

Luottamuksellinen (confidential) tieto on tarkoitettu vain tietyn henkilön tai tiettyjen henkilöiden tietoon, ja **luottamuksellisuus** (confidentiality) tarkoittaa tietojen säilymistä luottamuksellisina [VM00]. Anderson korostaa luottamuksellisuuden ja yksityisyyden välistä eroa: luottamuksellisuudella tarkoitetaan henkilön tai organisaation kolmannelle osapuolelle antamaa sitoumusta asian pitämisestä salassa, kun taas yksityisyys tarkoittaa henkilön oikeutta pitää henkilökohtaiset asiansa salassa sivullisilta. Esimerkiksi potilaan hoitosuhteeseen liittyvät seikat ovat potilaan itsensä näkökulmasta yksityisiä ja hoitavan lääkärin näkökulmasta luotaamuksellisia [ANDE01, s. 10].

Eheys (integrity) tarkoittaa, että tietoa tai viestiä ei ole valtuudettomasti muutettu. Eheyden menettämistä kutsutaan **rämettymiseksi** (corrupt). Esimerkiksi sähköpostiviesti rämettyy, jos joku tai jokin onnistuu matkan varrella **peukaloimaan** (tamper) sitä ennen kuin vastaanottaja avaa ja lukee viestin. Tiedon eheyden tarkastamiseen ja mahdollisen rämettymisen paljastamiseen voidaan soveltaa kryptografiaa.

Aitous eli alkuperäisyys (authenticity) puolestaan tarkoittaa viestin tai sen lähettäjän luotettavaa tunnistettavuutta tietoverkossa. Aitous ja eheys liittyvät läheisesti toisiinsa: ehyt viesti on lisäksi aito, jos voidaan varmistaa, että se on **tuore** (fresh), eikä esimerkiksi aikaisemmasta viestistä uudelleenlähetetty kopio [ANDE01, s. 11].

Viestin eheyden avulla voidaan toteuttaa **kiistämättömyys** (non-repudiation), joka tarkoittaa tietoverkossa eri menetelmin saatavaa varmuutta siitä, että tietty henkilö on lähettänyt tai vastaanottanut tietyn viestin, tai että tietty viesti tai tapahtuma on jätetty tietojärjestelmään käsiteltäväksi. Kiistämättömyyttä tarvitaan, kun tietoverkon muut käyttäjät haluavat varmistua osapuolen sitoutumisesta tiettyyn viestiin tai asiaan, esimerkiksi sopimukseen. Yksi kiistämättömyyden hyödyntäjä on sähköinen allekirjoitus, jolla siirretään perinteisessä maailmassa kynällä tehdyn allekirjoituksen oikeudellinen muotovaikutus tietoverkossa tapahtuvaan toimintaan. **Sähköinen allekirjoitus** (electronic signature) on tietokoneen luettavassa muodossa oleva henkilön nimikirjoitus tai sen vastine, esimerkiksi digitaalinen allekirjoitus, todisteena nimikirjoitukseen liittyvän asiakirjan tai viestin yhteydestä tiettyyn henkilöön. Digitaaliseen allekirjoitukseen syvennytään tarkemmin teknisestä näkökulmasta luvussa 4.5 ja lainsäädännön näkökulmasta luvussa 6.5.

Luotettu tietojenkäsittelyalusta (trusted computing base, TCB) on niiden komponenttien (esimerkiksi laitteisto, ohjelmisto, ja ihminen) muodostama joukko, joiden oikea toiminta riittää takaamaan asetetun tietoturvapäämäärän toteutumisen – tai kääntäen: joista jossain tapahtuva virhetoiminto saattaa aiheuttaa asetetun tietoturvapäämäärän murenemisen [ANDE01, s. 140]. Tietoturvapäämäärä saattaa esi-

merkiksi olla, että vain tietyllä tietojärjestelmän käyttäjällä on mahdollisuus lukea tietty tiedosto tai vain ylläpitäjällä on oikeus asentaa työasemaan sovellus, joka asioi sarjaporttiin kytketyn laitteen kanssa. Yhden keskeisen TCB:n muodostaa käyttöjärjestelmän ydin (kernel), jonka tehtävä on suorittaa järjestelmässä oleviin resursseihin liittyvää pääsynvalvontaa.

Luotettu järjestelmä on **luotettava** (trustworthy), mikäli se todellisuudessa on myös siihen kohdistuvan luottamuksen arvoinen [ANDE01, s. 10]. Luotettavassa järjestelmässä ei tapahdu tietoturvapäämäärän vaarantavia virhetoimintoja.

3. KATSAUS TOIMIKORTTEIHIN

Toimikortti, jota kutsutaan myös älykortiksi, sirukortiksi tai suoritinkortiksi (smart card, integrated circuit card), on yleensä luottokortin kokoinen suorittimen sisältävä laite. Euroopassa toimikortti on yleistynyt erityisesti GSM-tekniikan myötä, joka käyttää toimikorttia matkapuhelinliittymän todentamisessa. Tässä luvussa luodaan yleissilmäys toimikortin tekniikkaan, käsitteisiin, turvallisuuteen ja tyypillisimpiin toimikorttisovelluksiin. Luku perustuu pitkälti ISO-standardiin [IS7816].

3.1. Toimikortin edut

Toimikortin kiinnostavuus erityisesti korkeaa tietoturvaa vaativien sovellusten alustana perustuu toimikortin kolmeen perusominaisuuteen: toimikortin peukalointia sietävään rakenteeseen ja pieneen kokoon sekä sen sisäiseen laskentakapasiteettiin ja muistiin.

Toimikortin sisäinen laskentakapasiteetti ja muisti tekevät toimikortista pienen tietokoneen. Toimikortilla on oma suorittimensa, joka suorittaa kortin ROM-muistiin tai haihtumattomaan RAM-muistiin talletettua ohjelmaa. Toimikortin ja ulkomaailman välinen tiedonsiirto on sarjamuotoista ja tapahtuu joko kontaktillisten toimikorttien kontaktipintojen välityksellä tai kontaktittomissa toimikorteissa sähkömagneettisella induktiolla.

Toimikorttien lisäksi on olemassa myös muistikortteja, jotka toimikortteja muistuttavasta ulkonäöstään huolimatta eivät kuitenkaan sisällä suoritinta. Muun muassa puhelinautomaateissa ja digitaalikameroissa käytettävät kortit ovat muistikortteja. Muistikortit sisältävät kyllä tietoa – esimerkiksi puhelinkortti käyttämättä olevien maksusykäysten määrän – mutta eivät kykene laskutoimituksiin, minkä vuoksi ne eivät ole tässä tutkimuksessa mielenkiinnon kohteina. Myöskään magneettiraitaan talletettua tietoa sisältäviä magneettiraitakortteja ei tässä käsitellä.

Toimikortin peukaloinnin sietoisuus (tamper-resistance) on toimikortin tietoturvasovelluksia ajatellen vähintään yhtä haluttu tekninen ominaisuus kuin laskentakapasiteetti. Toimikortti on rakenteeltaan sellainen, että hyökkääjän on vaikea väkivalloin tai muulla tavalla päästä käsiksi kortin sisältämään tietoon. Toimikortin käyttö edellyttää, että kortti todentaa käyttäjänsä esimerkiksi PIN-koodilla tai sormenjäljen avulla (jos käyttäjä on ihminen) tai vahvan todentamisen avulla (jos kortti todentaa esimerkiksi palvelimen). Toimikortin peukaloinnin sietoisuutta tarkastellaan luvussa 3.8.

Toimikortin lisäksi on olemassa muitakin peukalointia sietäviä laitteistotason turvamoduuleja (hardware security module, HSM). Tällaisia ovat mm. suoraan työaseman USB-porttiin kytkeytyvät eri valmistajien toimiavaimet (USB token), Yhdysvaltojen hallinnon toteuttama, PCMCIA-korttipaikkaan kytkettävä Fortezza-kortti [ANDE01] ja muun muassa pankkien käyttämät kooltaan suuremmat turvamoduulit. Tässä tutkimuksessa keskitytään kuitenkin toimikortteihin.

Toimikortin pieni koko helpottaa toimikortin kuljettamista mukana. Tyypillisesti luottokortin kokoinen toimikortti mahtuu mukavasti lompakkoon kortinhaltijan muiden korttien joukkoon. Tämän ominaisuuden myötä toimikortilla on hyvät edellytykset muodostua käyttäjälleen henkilökohtaiseksi esineeksi perinteisen avainnipun, lompakon ja matkapuhelimen tavoin.

Näiden kolmen ominaisuuden yhteisvaikutuksesta toimikortti on muodostunut varsin houkuttelevaksi alustaksi haltijansa henkilökohtaisen ja arkaluontoisenkin tiedon tallettamista ajatellen. Tietoturvan sovelluksissa yksi tällainen tieto on salausavain.

3.2. Toimikortin teknisiä ominaisuuksia

Toimikortin tekniikka kehittyy muun tietotekniikan tavoin jatkuvasti. Erityisesti tämä näkyy toimikortin haihtumattoman muistin eli EEPROM:n kapasiteetissa, joka tyypillisesti on toimikortin kriittinen resurssi. GSM-matkapuhelintekniikka on ollut yksi toimikorttien laajimmista hyödyntäjistä Euroopassa. Muistamme GSM-puhelinten alkuajoilta SIM-liittymäkortit, joiden haihtumaton muisti rajoittui 8 kilotavuun. Kortin muistiin mahtui tuolloin varsin vaatimaton määrä tekstiviestejä ja puhelinnumeroita. Nykyiset SIM-kortit sisältävät 16 kilotavun muistin, ja 32 ja 64 kilotavun toimikortit ovat tulossa.

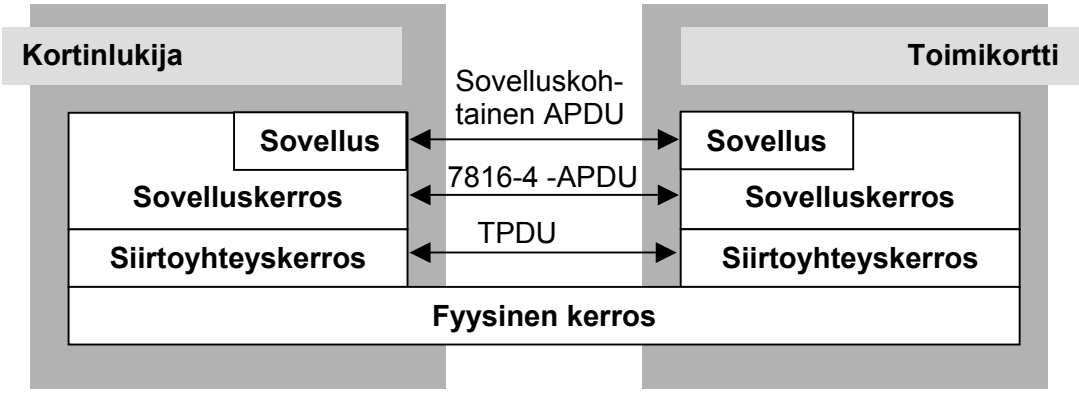
Haihtumattoman muistin lisäksi toimikortilla on tyypillisesti 6-24 kilotavua ROM-muistia sekä muutamia satoja tavuja tai kilotavuja RAM-muistia, jota tarvitaan lähinnä välitulosten tallettamiseen. RAM -muisti tyhjenee, kun toimikortti poistetaan kortinlukijasta. [NICH99, s. 491]

Kolmen tai viiden voltin ulkoisen jännitelähteen lisäksi toimikortilla on myös ulkoinen kellopulssi, joka johdetaan toimikortille sen kontaktipinnan kautta. Ulkoinen kello, jonka taajuus on tyypillisesti noin viisi megahertsiä, käyttää toimikortin tavallisesti 8 tai 16-bittistä suoritinta. Kommunikointi ulkomaailman kanssa tapahtuu sarjamuotoisesti kontaktipinnan kautta 9600 bitin sekuntinopeudella tai jollain sen monikerralla. Kontaktittomassa toimikortissa, kuten joukkoliikenteessä laajasti käytetyissä matkakorteissa, virransyöttö, kellopulssi ja muu kommunikointi tapah-

tuu sähkömagneettisen induktion välityksellä. Tässä tutkimuksessa keskitytään lähinnä kontaktillisiin toimikortteihin. [NICH99, s. 491—494]

3.3. Kontaktillisen toimikortin protokollat

Toimikortin ja kortinlukijan välinen tietoliikenne käyttää protokollapinoa, joka on varsinkin alimpien protokollatasojen osalta varsin vahvasti standardoitu ISO 7816-standardiperheessä. Protokollapino on esitetty oheisessa kuvassa (Kuva 3).

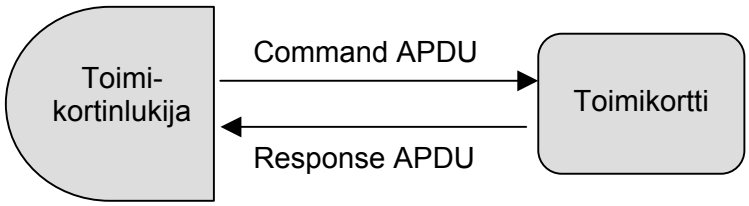


Kuva 3. Toimikortin ja kortinlukijan välinen protokollapino.

Fyysisen kerroksen päällä ajettavan siirtoyhteyskerroksen protokollasta käytetään ISO 7816 -standardissa nimeä T-protokolla (transmission protocol) ja protokollan datayksiköstä nimeä TPDU (transmission protocol data unit). Sen tehtävä on peittää alleen yksinkertaisempien ja monimutkaisempien toimikorttien väliset fyysisen kerroksen erot. Sen päällä ajetaan sovellusprotokollaa (application protocol), jonka datayksikkö on nimeltään APDU (application protocol data unit). Sovellusprotokollan tavallisimmat primitiivit ja vastaavat APDU:t (esimerkiksi "Lue tiedosto", "Syötä PIN") on standardoitu ISO 7816-4 -standardissa. Standardissa määritellään myös puitteet, joita noudattaen sovellukset voivat muodostaa omia sovelluskohtaisia APDU:jaan.

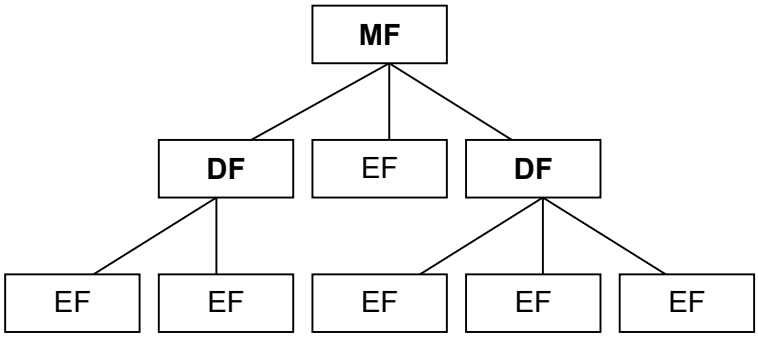
3.4. Toimikortti sovelluksen näkökulmasta

Sovelluksen näkökulmasta toimikortti on master/slave-arkkitehtuurin mukainen orja (Kuva 4), joka vastaa kortinlukijan lähettämään komentoon (command APDU) lähettämällä vastauksen (response APDU). Toimikortin kanssa käytävä kommunikointi koostuu sarjasta tällaisia komentoja, joihin sisältyy komennon tunnuksen lisäksi parametreja ja muuta dataa. Vaikka standardi mahdollistaa myös pidemmät rakenteet, koostuu yksi APDU yleensä muutaman tavun mittaisesta otsakkeesta ja enintään 255 tavun datakuormasta.



Kuva 4. Toimikortti on master/slave-arkkitehtuurin mukainen orja, joka vastaa kortinlukijan esittämään komentoon.

ISO 7816-4 -standardi määrittelee toimikortille myös hierarkkisen tiedostorakenteen (Kuva 5), joka on periaatteessa samanlainen kuin työasemista tuttu puumainen tiedostohierarkia. Hierarkian juurena olevaa tiedostoa kutsutaan nimellä MF (master file), ja alihakemistoon rinnastettavat tiedostot tunnetaan nimellä DF (dedicated file). Varsinainen tieto on tallennettu hierarkian lehtiin EF-tiedostoihin (elementary file). Tiedostot tunnistetaan niille annetun kahden tavun mittaisen nimen avulla.



Kuva 5. Toimikortin hierarkkinen tiedostorakenne.

Hierarkialle on tunnusomaista, että tarvittavat valtuudet komennon antamiseen voidaan määritellä jokaisen tiedoston kohdalta erikseen. Esimerkiksi tiedostoon, joka sisältää salausavaimen, voidaan tyypillisesti kohdistaa komento ”salakirjoita” (parametrina salattava data) vain, jos kortin käyttäjä on ensin todennettu kortille PIN-koodin avulla. Vastaavasti PIN-koodin syöttäminen kortille tapahtuu omalla komennollaan.

3.5. Tyypillisiä toimikorttisovelluksia

Toimikorteille voidaan keksiä mitä erilaisimpia sovelluskohteita, joista tyypillisimmät ovat maksamiseen käytettävät ja kortin haltijan henkilöllisyyden todentamiseen liittyvät sovellukset. Muita toimikorttisovelluksia ovat esimerkiksi erilaisten bonusten keräämiseen käytettävät kanta-asiakassovellukset, kortinhaltijan terveystietojen taltiointiin käytettävät terveystietosovellukset jne.

Kukkarosovellus (electronic purse) toimii siten, että kortin haltija käy erityisessä kortinlatauspisteessä, esimerkiksi pankkiautomaatilla, lataamassa pankkitililtä kor-

tilleen sähköistä käteistä, jolloin maksujärjestelmän (clearing) ylläpitäjä veloittaa hänen pankkitiliään vastaavalla summalla. Kortilla maksettaessa sähköinen käteinen "siirtyy" salattuna asiakkaan kortilta kauppiaan maksupäätteen turvamoduuliin, jolloin kukkaron saldoa vähennetään ja turvamoduulin saldoa kasvatetaan samalla summalla. Kauppias purkaa turvamoduulinsa saldon aika ajoin esimerkiksi modeemin avulla maksujärjestelmän ylläpitäjälle, joka puolestaan hyvittää kauppiaan pankkitiliä vastaavalla summalla. Kukkarosovelluksessa on siis kyse maksa etukäteen (pay before) -tyyppisestä maksamisesta: raha lähtee kortinhaltijan tililtä ennen kuin tuote tai palvelu vaihtaa omistajaa.

Suomessa tunnetuin kukkarosovellus on Avant [AVAN02], jota ylläpitää Nordean, Osuuspankkien ja Sammon omistama Automatia Rahakortit Oy. Maailmalla on runsaasti kansallisia, Avant-kortin tyyppisiä kukkarosovelluksia, joille yhteistä on lähinnä keskinäinen tekninen yhteensopimattomuus. Myös muutamilla ylikansallisilla luottokorttiyhtiöillä on omat sovelluksensa, kuten Visalla VisaCash [VISA02].

EMV-sovellus on osa Europay-, Mastercard- ja Visa-luottokorttiyhtiöiden myötävaikutuksella syntynyttä laajaa määritystä infrastruktuurista, joka muun muassa mahdollistaa maksukortti- (debit) ja luottokorttityyppisen (credit) maksamisen toimikortilla. Magneettiraidallisten pankki- ja luottokorttien tietoturvaongelmat ovat suunnanneet kehityksen kohti sirullisia kortteja maailmanlaajuisesti. Pankkien mukaan EMV-sovelluksen sisältävien pankki- ja luottokorttien jakaminen alkanee Suomessa vuoden 2002 aikana. Siirtymäajan on suunniteltu päättyvän vuoden 2004 lopussa, jonka jälkeen vastuu magneettiraitakorttien väärinkäytöksistä on suunniteltu siirrettäväksi liikkeellelaskijalta maksun vastaanottavalle kauppiaalle. [EMV00]

Tunnistamissovellus on toimikorttisovellusten toinen valtavirta. Sitä käytetään henkilön tai muun toimijan sähköiseen tunnistamiseen ja tunnistamisen todentamiseen. Monelle suomalaiselle tuttu tunnistamissovellus on GSM-puhelimen SIM-kortti [ETSI00], jonka avulla GSM-verkko todentaa matkapuhelinliittymän ja PIN-koodin myötä edelleen liittymän käyttäjän. SIM-korttia uudempi tunnistamissovellus matkapuhelinympäristössä on WAP-standardiin kuuluva WIM (wireless identity module), jonka avulla WAP-palvelin voi muun muassa tunnistaa WAP-päätelaitteen vahvan todennuksen perusteella [WAPF01].

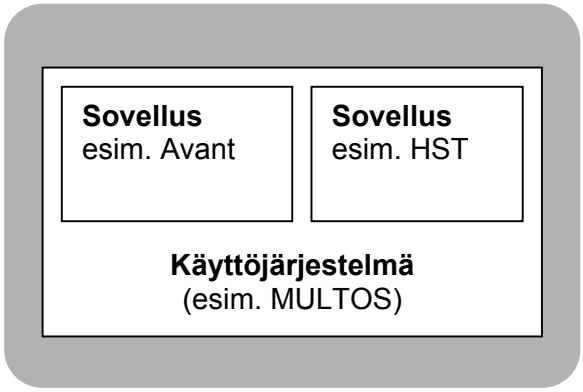
Samoihin aikoihin WIM:n kanssa esiteltiin Väestörekisterikeskuksen kehittämä sähköinen henkilökortti, joka kuuluu valtionhallinnon henkilön sähköinen tunnistaminen -projektiin [VRK02]. Sähköinen henkilökortti eli HST-kortti on ollut 1.12.1999 alkaen jokaisen kansalaisen ulottuvilla, ja se on vaihtoehto perinteiselle

henkilökortille. Sähköiseen henkilökorttiin ja muihin vastaaviin toimikortteihin syvennytään tuonnempana.

3.6. Toimikortin sovellukset ja käyttöjärjestelmät

Aikaisemmin toimikortit olivat tyypillisesti yhden sovelluksen kortteja: toimikorttia, jossa on esimerkiksi GSM SIM -sovellus, voitiin kutsua SIM-kortiksi, ja toimikorttia, jossa on Avant-sovellus, voitiin kutsua Avant-kortiksi. Nykyään kehitys kulkee kuitenkin kohti useampia sovelluksia sisältäviä toimikortteja, jolloin samalla kortilla voi olla esimerkiksi sekä Avant- että HST-sovellus. Tässä yhteydessä onkin selkeämpää puhua esimerkiksi Avant-kortin sijaan kortilla olevasta Avant-sovelluksesta.

Monen sovelluksen kortista puhuttaessa nousee esiin myös kysymys kortin käyttöjärjestelmästä. Arkkitehtuuria on havainnollistettu oheisessa kuvassa (Kuva 6).



Kuva 6. Monen sovelluksen toimikortti.

Käyttöjärjestelmän tehtävänä on muun muassa pitää kortilla olevat sovellukset huolellisesti erillään toisistaan, huolehtia toimikortin tiedostojärjestelmästä ja hoitaa muitakin käyttöjärjestelmälle tyypillisiä tehtäviä, kuten syöttö ja tulostus (input/output) jne. Monen sovelluksen kortille voidaan ladata sen elinaikana käyttöjärjestelmän avulla sovelluksia ja poistaa vanhoja sovelluksia. [NICH99, s. 495]

Vielä nykyään toimikorteilla on tyypillisesti valmistajakohtainen käyttöjärjestelmä, jonka päälle toteutetut sovellukset on vaikea siirtää muihin käyttöjärjestelmiin. Niinpä sovellusten tuottajat ovat sidoksissa tiettyyn kortinvalmistajaan. Esimerkiksi Automatia rahakortit Oy:n Avant-kukkaro on toteutettu suomalaisen toimikorttivalmistaja Setec Oy:n SetCOS-käyttöjärjestelmälle.

Korttisovellusten vahvaa sidosta tiettyyn käyttöjärjestelmään on pidetty eräänä toimikorttialan kasvua rajoittavana tekijänä. Tilanne on kuitenkin vähitellen muut-

tumassa, kun tilaa valtaavat avoimet käyttöjärjestelmät, joita korttivalmistajat ja sovelluskehittäjät alkavat tukea.

Avoimia toimikorttikäyttöjärjestelmiä ovat esimerkiksi JavaCard, Multos ja Windows for Smart Cards. JavaCard-käyttöjärjestelmän päällä ajettavat sovelmat (”cardlet”) luodaan Java-ohjelmointikielen kevennetyllä versiolla ja suoritetaan toimikortille toteutetulla Java-virtuaalikoneella. Multos-käyttöjärjestelmän kehitystä vie eteenpäin MasterCardin johdolla MAOSCO-konsortio, ja kyseinen muun muassa maksamissovelluksien alustana toimiva käyttöjärjestelmä tunnetaan korkean turvallisuuden toteuttavasta arkkitehtuuristaan. Myös Microsoft on mukana toimikorttien käyttöjärjestelmäkehityksessä Windows for Smart Cards-käyttöjärjestelmällään.

3.7. Toimikortin standardeista

Vaikka toimikortin joillakin sovellusalueilla käytetään valmistajakohtaisia ratkaisuja ja de facto -standardeja, luo perustan kontaktillisen toimikortin soveltamiselle ISO 7816 -standardiperhe [IS7816], johon tässä luodaan silmäys. Standardiperheen pohjalle rakentuu edelleen joukko muita määrityksiä, kuten GSM-matkapuhelimien SIM-liittymäkortit määrittävä ETSI-standardi [ETSI00] ja luvussa 3.5. mainittu EMV-sovellus.

Kontaktillisten toimikorttien fyysiset ominaisuudet, kuten koko, kontaktipintojen sijainti ja kortilta vaadittava lämpötilan ja mekaanisen rasituksen sietoisuus määritellään ISO 7816 -standardin osissa 1 ja 2. Kortin sähköiset perusominaisuudet, kuten kontaktipintojen sallitut jännitetasot ja -toleranssit sekä ulkoisen kellopulssin hyväksyttävät taajuudet, määritellään osassa 3. Sama osa yhdessä osan 10 kanssa määrittelee myös toimikortin siirtoyhteyskerroksen T-protokollat.

Standardin osassa 4 määritellään toimikortin ja kortinlukijan välinen sovellusprotokolla sekä toimikortilta ulospäin näkyvä sisäinen rakenne, kuten tiedostorakenne ja siihen liittyvä pääsynvalvonta. Osassa 5 määritellään menetelmä toimikorttisovellusten nimeämiseksi yksiselitteisellä tavalla ja osassa 6 standardeja tietorakenteita muille yleisimmille toimikortin sisältämille tiedoille. Tiedon esitysmuotona on ASN.1 (Abstract Syntax Notation One) [IS8824], joka on ISO:n niin ikään standardoima, laajasti käytetty esitystapa verkossa siirrettävälle tiedolle. ASN.1-tietorakenteet talletetaan toimikortille DER-koodattuina (Distinguished Encoding Rules).

Osan 7 määrittelemä toimikortille sijoitetun tietokannan käyttöön tarkoitettu SQL-tyyppinen kyselykieli on jäänyt vähemmälle huomiolle. Toimikorttien tuntemat, turvallisuuteen liittyvät viestit ja tietorakenteet ovat sitäkin keskeisimpiä tämän

tutkimuksen kannalta, ja ne määritellään osassa 8. Osa 9 laajentaa osaa 4 määrittelemällä muun muassa toimikortin ja sen tiedostojen elinkaaren asiaankuuluvine viesteineen ja tietorakenteineen.

Standardiperheen kehitys ei kuitenkaan ole vielä päättynyt. Kehitteillä oleva osa 11 ottaa kantaa biometristen menetelmien käyttöön kortinhaltijan henkilöllisyyden varmistamisessa. Nykyisin kortin haltija todentaa henkilöllisyytensä toimikortille antamalla PIN-koodinsa toimikortinlukijalle, joka välittää sen toimikortille. Biometrisen menetelmän, kuten sormenjäljen, käyttöä pidetään tätä turvallisempana menetelmänä [ISO01].

3.8. Toimikortin turvallisuus

Toimikortin sovellusalueet hyödyntävät tyypillisesti sen peukalointia sietävää rakennetta: toimikorttia käytetään sellaisen tiedon tallettamiseen, jonka paljastuminen vahingoittaisi jotain sovellusalueen osapuolta, kuten kortinhaltijaa tai toimikortin tai sen sovelluksen liikkeellelaskijaa. Esimerkiksi toimikortilla olevan kukkarosovelluksen murtaminen saattaisi mahdollistaa "väärän rahan painamisen" maksujärjestelmään, joka koituisi kukkarojärjestelmän ylläpitäjän tappioksi.

Toimikortin pieni koko ja helppo liikuteltavuus aiheuttaa lisähaasteen sen peukaloinnin sietoisuudelle. Pankkiautomaatin kimppuun sorkkarauta aseenaan käyvä murtomies havaitaan nopeasti, ja vartijat lähetetään ottamaan hänet kiinni ennen kuin hän pääsee käsiksi rahoihin. Toimikortin turvallisuus sen sijaan perustuu ensisijaisesti sen peukalointia sietävään rakenteeseen, jolla murtautujaa koitetaan estää pääsemästä käsiksi kortin sisältämään tietoon: itse murtoyritys voidaan suorittaa kaikessa rauhassa laboratorio-olosuhteissa ilman, että kortin liikkeellelaskijalla olisi mahdollisuutta sen havaitsemiseen ja siihen reagoimiseen.

Toimikortti tarjoaa hintaansa nähden varsin hyvän suojan sisältämilleen tiedoille. Valitettavasti täysin murtovarmaa toimikorttia ei kuitenkaan ole, ja markkinat pakottavat valmistajia hakemaan kompromissia tuotantokustannusten ja turvallisuuden väliltä. Toimikortteja vastaan on raportoitu erilaisia hyökkäyksiä, jotka voidaan jaotella neljään ryhmään: anturointi, ohjelmistohyökkäykset, signaalien kuuntelu ja virheiden generointi [KÖMM99].

Anturointi on aktiivinen hyökkäys, joka suoritetaan erikoistyövälinein varustetussa laboratoriossa ja jossa toimikortin sirua manipuloidaan fyysisesti. Siru irrotetaan kortista ja sitä suojaavat kerrokset poistetaan typpihapolla. Tämän jälkeen sirun arkkitehtuuria voidaan tutkia mikroskoopilla ja sen väylien signaaleja mitata ja muuttaa mikroanturilla. Tarvittavien välineiden hinnat alkavat käytettyinä kymmenestä tuhannesta eurosta. Monimutkaisemmilla välineillä, kuten fokusoidulla io-

nisuihkulla (focused ion beam, FIB) päästään käsiksi myös syvemmällä sirussa oleviin johtimiin.

Ohjelmistohyökkäykset ovat passiivisia hyökkäyksiä, jotka eivät vahingoita sirua. Toimikorttisovelluksen käyttämistä tietoturvaprotokollista, salausalgoritmeista ja niiden toteutuksista etsitään virheitä ja heikkouksia, jotka avaavat hyökkääjälle esimerkiksi pääsyn toimikortin sisältämiin tietoihin.

Signaalien kuuntelu kiinnittää huomiota toimikortin kontaktipintojen signaalien analogisiin ominaisuuksiin ja prosessorin tuottamaan sähkömagneettiseen säteilyyn. Toimikortin virrankulutuksesta ja sen muutoksista voidaan edullisissa olosuhteissa tehdä päätelmiä toimikortin sisäisestä rakenteesta ja toiminnasta sekä sen käsittelemästä tiedosta.

Virheiden generoinnissa toimikortin kontaktipintojen signaaleihin aiheutetaan transientteja, jotka ovat nopeita muutoksia esimerkiksi toimikortin analogisissa signaaleissa, kuten kello- ja virtasignaaleissa. Sopivalla tavalla valittu transientti saattaa johtaa hyökkääjän tavoittelemaan vikatoimintoon, kuten kortille talletettujen tietojen tulostumiseen kortinlukijalle.

Hyökkäyksiä voidaan yhdistellä. Yhden toimikortin rakenteen selvittäminen anturoimalla saattaa viedä asiantuntijaryhmältä viikkoja, mutta sen tuloksena voi esimerkiksi paljastua alttius tietyntyyppiselle transientille, minkä jälkeen samaa mallia edustavat muut toimikortit pystytään murtamaan sekunneissa. Ääritapauksessa kortinhaltija ei välttämättä itsekään ole tietoinen onnistuneesta hyökkäyksestä: pahantahtoinen kauppias voi esimerkiksi käyttää modifioitua maksupäätettä murtaakseen kukkarokortin tavanomaisen maksusuorituksen yhteydessä.

Myös toimikortit ovat turvatekniikan kehittäjien ja murtajien välisen kilpajuoksun temmellyskenttänä. Toimikorttien arkkitehtuuriin ja toimintaan voidaan esimerkiksi lisätä epädeterministisyyttä vaikeuttamaan signaalien kuuntelua ja transienttien generointia. Anturointia vastaan voidaan suojautua ympäröimällä siru metalliverkolla, jonka peukalointi saa haihtumattoman muistin tyhjenemään. Tällöin toimikortin turvallisuus ei nojaa enää pelkästään hyökkäykseltä suojautumiseen, vaan myös hyökkäysyrityksen havaitsemiseen ja siihen reagoimiseen.

Kaukaa viisas toimikorttijärjestelmän suunnittelija ei kuitenkaan rakenna järjestelmänsä turvallisuutta yhden kortin varaan, vaan rakentaa järjestelmän arkkitehtuurin sellaiseksi, että se tarjoaa puolustuskeinoilleen syvyyttä. Esimerkiksi yhden kukkarokortin murtuminen ei saa tehdä kaikkia järjestelmän kukkaroita käyttökelvottomiksi.

3.9. Toimikortin käyttäminen työasemassa

Toimikortin käyttö tietokoneeseen kytkettävänä lisälaitteena on yleistymässä. Kattavien standardien syntyminen on parantanut laitteiden ja ohjelmistojen yhteensopivuutta, ja tuonut markkinoille kilpailevia tuotteita erityisesti Windows-käyttöjärjestelmään pohjautuviin työasemiin. Tässä luvussa käsitellään työasemaan kytketyn toimikortinlukijan standardeja ja turvallisuutta.

3.9.1. Kortinlukijat

Koska toimikortit käyttävät ulkoista jännitelähdettä ja kellopulssia ja koska sekä syöttö että tulostus tapahtuvat sarjamuotoisen signaalin välityksellä, toimikortti tarvitsee aina toimikortinlukijan kommunikoidakseen ympäristönsä kanssa. Kontaktilliset toimikortit työnnetään kortinlukijan sisälle, jolloin kortinlukijan nastat painuvat toimikortin kontaktipintoja vasten. Kontaktittoman toimikortin ja kortinlukijan välinen kommunikaatio tapahtuu sähkömagneettisen induktion välityksellä muutaman tai muutaman kymmenen senttimetrin etäisyydeltä.

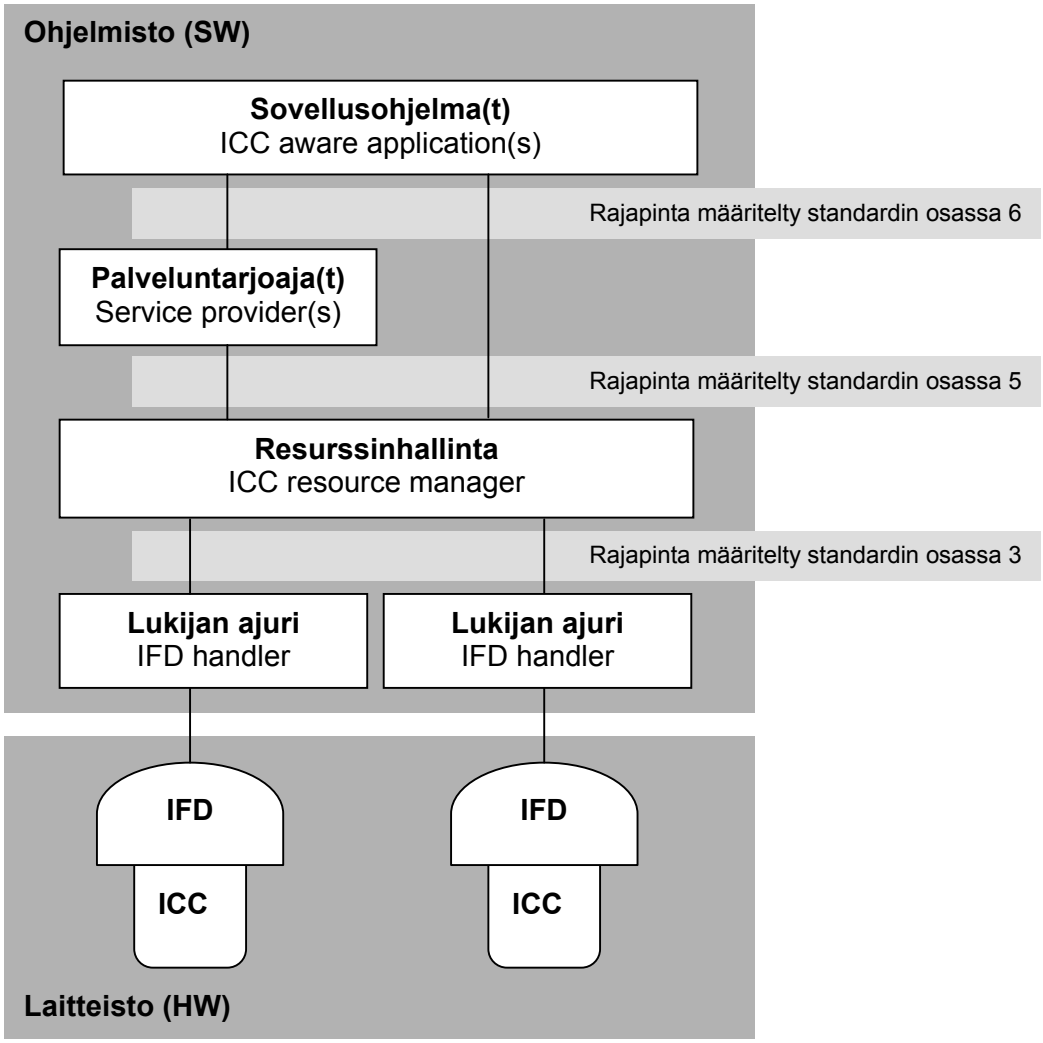
Termi toimikortinlukija on sikäli harhaanjohtava, että sama laite osaa tyypillisesti paitsi "lukea", myös "kirjoittaa" toimikortin tiedostoja, sekä suorittaa muitakin korttiin liittyviä operaatioita, kuten välittää kortille käyttäjän antaman PIN-koodin. Lukemisen ja kirjoittamisen käsitteleminen erillisinä toimintoina ei ole kovin mielekästä, koska molemmat operaatiot ovat vain tietyn merkityksen sisältäviä APDU-komentoja, kuten kappaleessa 3.3. selostettiin. Totuudenmukaisempi nimitys kortinlukijalle saattaisi olla rajapintalaite (interface device, IFD), mutta nimitys toimikortinlukija (smart card reader) on jo ehtinyt vakiintua suomen kieleen.

Toimikortinlukijan olemus riippuu suuresti järjestelmästä ja laitteesta, johon toimikortti kytketään. Pankkiautomaateissa toimikortinlukija on upotettu osaksi automaatin etupaneelia, matkapuhelimessa SIM-kortin lukija on puhelimen sisällä. Yksinkertainen kukkarokortin saldon näyttävä kortinlukija mahtuu avaimenperään.

PC-työasemiin liitettävät toimikortinlukijat käyttävät hyväkseen työasemien normaaleja laajennuspaikkoja. Nykyään kortinlukija kytketään työasemaan yleensä sarjaportin (COM, USB) kautta. Vaihtoehtoisesti kortinlukija voidaan myös integroida työaseman tai sen näppäimistön kotelointiin. Matkamikroissa kortinlukija sijoitetaan yleensä PCMCIA-laajennuspaikkaan, jolloin kortinlukija saadaan työnnettyä näppärästi kokonaan mikron kuorien sisälle.

3.9.2. PC/SC – työaseman ohjelmistoarkkitehtuuri

Keskeiset työasemia ja niiden käyttöjärjestelmiä sekä toimikortteja valmistavat yritykset ovat vuonna 1997 sopineet toimikortin työasemakäyttöön liittyvistä arkkitehtuurikysymyksistä. PC/SC-määrityksenä tunnettu teollisuusstandardi [PCSC97], johon tässä esitettävä perustuu, määrittelee joukon toiminnallisuuksia ja rajapintoja, joita noudattamalla valmistajat voivat varmistua tuotteidensa yhteensopivuudesta muiden valmistajien tuotteiden kanssa.



Kuva 7. PC/SC-spesifikaation määritys toimikortteja hyödyntävän työaseman arkkitehtuurista [PCSC97, s. 9].

Spesifikaation versio 1.0 koostuu kahdeksasta osasta, jotka hahmottavat oheisessa kuvassa esitetyn arkkitehtuurin (Kuva 7.). Toimikortti (ICC, integrated circuit card) työnnetään toimikortinlukijaan (IFD, interface device), johon liittyvä ajuri (IFD handler) tarjoaa resurssinhallinnalle (ICC resource manager) pääsyn toimikortin resursseihin. Palveluntarjoaja (service provider) toteuttaa resurssinhallintaan

nojaavan ohjelmointirajapinnan, jota sovellusohjelmat, esimerkiksi WWW-selain, voivat hyödyntää.

PC/SC-arkkitehtuurissa keskeinen rooli on resurssinhallintakomponentilla, joka on luonteeltaan käyttöjärjestelmään läheisesti liittyvä komponentti. Resurssinhallinnan tehtävä on tietää, mitä kortinlukijoita ja kortteja järjestelmässä on kullakin hetkellä asennettuna ja käytettävissä. Mikäli työasemassa on useita toimikorttia käyttäviä sovelluksia ja palveluntarjoajia, resurssinhallinta huolehtii tarvittaessa näiden keskinäisestä poissulkemisesta, koska toimikortin kanssa voi yleensä asioida vain yksi sovellus kerrallaan ja koska asiointi koostuu tyypillisesti monesta komennosta, jotka on annettava kortille peräjälkeen.

Spesifikaation osa 3 määrittelee rajapinnan, jonka kortinlukijan ajuri tarjoaa resurssinhallinnalle kortinlukijan ja edelleen toimikortin käyttämistä varten. Ajurin toteuttaa tyypillisesti kortinlukijan valmistaja, jonka päätettäväksi jää kortinlukijan fyysisen olemuksen (kytketäänkö se sarjaporttiin, PCMCIA-porttiin jne) lisäksi myös rajapinnan toteutuksen jakaantuminen ohjelmiston (ajuri) ja laitteiston (kortinlukija) välillä. Yksinkertaisimmillaan kortinlukija ei sisällä kovinkaan paljon elektroniikkaa – lähinnä vain kontaktipinnat, joiden välityksellä kommunikointi toimikortin kanssa tapahtuu. Tällöin muu toiminnallisuus, esimerkiksi luvussa 3.3. esitetyn siirtoyhteyskerroksen T-protokollan toteutus, tapahtuu ajurissa.

PC/SC ei siis ota kantaa siihen, miten esimerkiksi sarjaporttiin kytketty kortinlukija kommunikoi työaseman kanssa. Tällöin uuden kortinlukijan liittäminen työasemaan tarkoittaa aina myös kortinlukijan ajurin asentamista, mikä on vaivalloista ja myös hidastaa kortinlukijoiden käytön laajenemista uusiin käyttöjärjestelmiin. USB-väylään liitettävien kortinlukijoiden yhteensopivuuden mahdollistamiseksi onkin tehty CCID-määritys (USB Chip/Smart Card Interface Devices [CCID01]), joka pyrkii standardoimaan kortinlukijan ja ajurin USB-väylän kautta tapahtuvan kommunikoinnin. Ajatus on, että yhtä käyttöjärjestelmään sisältyvää yleiskäyttöistä ajuria voisi käyttää eri valmistajien tekemien kortinlukijoiden kanssa, mikä helpottaisi Plug and Play -tyyppisten kortinlukijoiden tekemistä.

Spesifikaation osa 5 määrittelee rajapinnan, jonka resurssinhallintakomponentti tarjoaa palveluntarjoajille ja sovellusohjelmille. Tämä rajapinta on kuitenkin vielä melko epämiellyttävä sovellusohjelmoijan kannalta, koska kommunikoiminen itse kortin kanssa tapahtuu antamalla rajapinnalle luvussa 3.3. kuvattuja, binääridatasta koostuvia APDU-komentoja.

Palveluntarjoajan tehtävä on toteuttaa resurssinhallinnan tarjoaman matalan abstraktiotason rajapinnan päälle korkean tason rajapinta, joka sisältää sovellusohjelmoijan kannalta helppokäyttöisiä funktioita. Tietty funktioiden perusjoukko, kuten "Lue tiedosto" tai "Syötä PIN-koodi", on riippumaton toimikortin sovelluksesta,

mutta pääsääntö on, että tietty toimikorttisovellus vaatii tietyn palvelutarjoajan. Esimerkiksi käyttäjän henkilöllisyyden todentamisen toteutuksessa käytettävät PKI-toimikortit, joihin syvennytään myöhemmin luvussa 6, vaativat toimiakseen kryptografisen palveluntarjoajan (cryptographic service provider, CSP), jonka rajapinta määritellään PC/SC-spesifikaation osassa 6.

PC/SC-määritystä laatineen työryhmän yksi jäsen on Microsoft, ja PC/SC- arkkitehtuuri on viime aikoina yleistynyt erityisesti Windows-käyttöjärjestelmää käyttävissä työasemissa. Resurssinhallintakomponentti, joka Microsoftin tuotteissa sisältyy toimikortin käyttöön tarvittavaan peruspakettiin (Smart card base components), asentuu automaattisesti Windows 2000:n ja tämän seuraajien mukana. Vanhempiin Windows-versioihin se on haettavissa Microsoftin WWW-sivuilta. Lähestulkoon kaikilla toimikortinlukijoiden valmistajilla on tarjolla ainakin Windowsiin sopivat ajurit lukijalleen. Windows-ympäristössä toimikortinlukijoiden yhteensopivuus onkin melko hyvä.

Unix- ja Linux-ympäristöissä tarjonta on vähäisempää. Resurssinhallintakomponentti on toteutettu avoimeen lähdekoodiin perustuvassa MUSCLE-projektissa ja kantaa nimeä PC/SC Lite [MUSC02]. Ajureita kortinlukijoihin on vaihtelevasti, palveluntarjoajan toteutuksia vähemmän.

PC/SC-spesifikaation 1.0-versiossa on joitakin puutteita, ja PC/SC-työryhmä on valmistelemassa spesifikaation versiota 2.0. Uusi versio mahdollistaa monisovelluskorttien joustavamman käytön työasemassa ja ottaa huomioon myös erityistoiminnallisuuksia, kuten PIN-koodin syöttämiseen tarkoitetun näppäimistön sisältävät kortinlukijat. Lisäksi uudessa versiossa on mukana tuki kontaktittomille ja synkronista tiedonsiirtoa tukeville toimikorteille [PCSC99].

3.9.3. Työasemaan kytketyn toimikortin turvallisuus

Toimikortti tarjoaa hintaansa nähden melko hyvän suojan peukalointiyrityksiä vastaan. Työasemien suojaaminen hyökkääjiltä on paljon vaikeampaa: peruskäyttäjällä on vähäiset mahdollisuudet varmistua työasemansa kaikkien prosessien vilpittömistä aikeista. Käyttöjärjestelmien ja sovellusten turvamekanismit, kuten epäilyttäville sovelmille eristetyn ajoympäristön tarjoavat järjestelyt (esim. Javan hiekkalaatikko), tähtäävät hyökkäysten estämiseen ja vahinkojen rajaamiseen. Internetiin kytkettyyn työasemaan pyrkii kuitenkin viruksia ja muita tuho-ohjelmia, jotka sivuuttavat suojaukset hyödyntämällä työaseman mitä erilaisimpia tietoturva-aukkoja kuten ohjelmointivirheitä. Työaseman turvattomuus osaltaan perusteleekin arkaluontoisimpien tietojen sijoittamista peukalointia sietävälle toimikortille.

Toisaalta toimikortti on täysin riippuvainen kortinlukijasta ja siihen kytkeytyvästä työasemasta, jonka läpi kaikki kommunikointi ulkomaailman kanssa tapahtuu.

Koska nykyisissä toimikorteissa ei ole näyttöä, näppäimistöä eikä muutakaan syöttö- tai tulostuslaitetta, altistuu myös toimikortin ja kortinhaltijan välinen kommunikaatio työasemassa mahdollisesti oleville tuho-ohjelmille. (Gobioff ja kumppanit ovat kyllä ehdottaneet, että toimikortin työntämistä sisään lukijaan ja vetämistä ulos lukijasta käytettäisiin kortin ja kortinhaltijan välisenä suorana turvallisena kommunikointikanavana [GOBI96], mutta järjestelyn käyttömahdollisuudet ovat rajalliset, koska toimikortin työntäminen lukijaan aiheuttaa kortin resetoinnin ja kortin vetäminen pois lukijasta katkaisee siitä virran.)

Toimikortilla ei yleensä ole keinoa varmistaa sovellusohjelmalta tai palveluntarjoajalta vastaanottamiensa Command APDU:jen (luku 3.3) aitoutta ja eheyttä, ja sama pätee myös sovellusohjelman tai palveluntarjoajan toimikortilta saamiin Response APDU:ihin. Jokainen näiden välissä oleva komponentti voi halutessaan muuttaa APDU:ja, ja niinpä ne kaikki kuuluvat TCB:hen (luku 2.3), jonka päämäärä on varmistaa toimikortin ja palveluntarjoajan tai sovellusohjelman välisen kommunikoinnin eheys ja aitous.

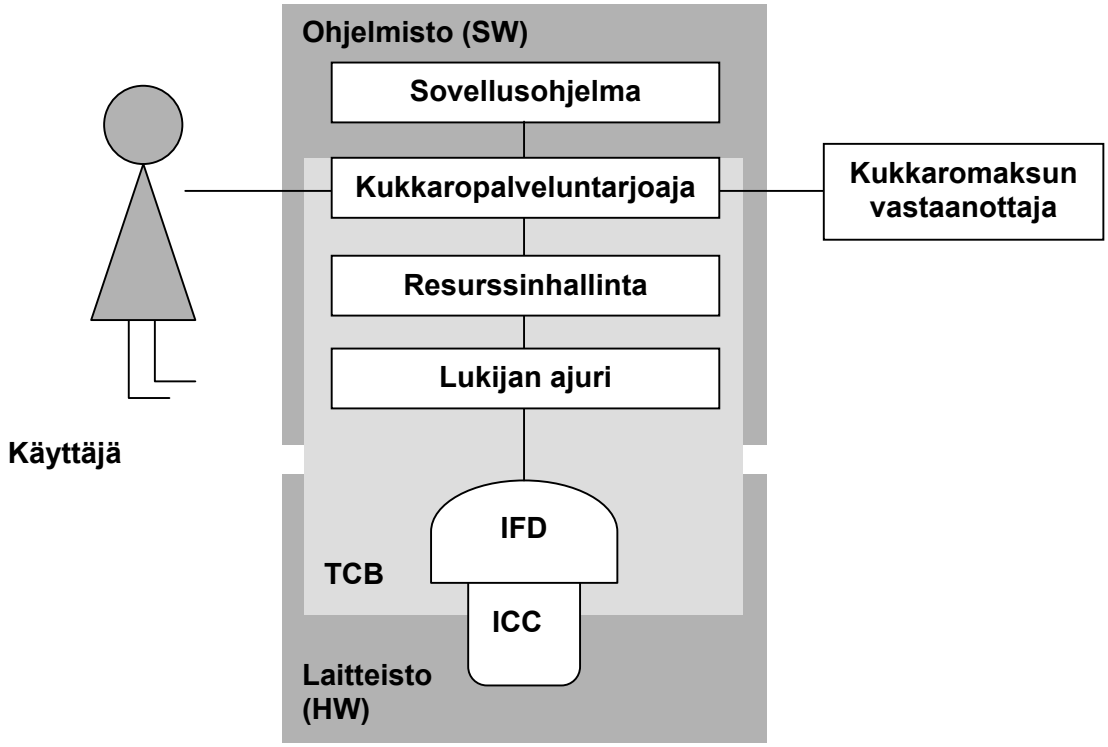
Otetaan esimerkiksi kuvitteellinen kukkarokortti, jota varten työasemaan on toteutettu erityinen kukkaropalveluntarjoaja. Kukkaropalveluntarjoaja toteuttaa sovellusohjelmia varten ohjelmointirajapinnan, joka tarjoaa erilaisia funktioita (mm. funktion, jolla voi tarkistaa kortinlukijaan työnnetyn kukkarokortin saldon, ja toisen funktion, jolla voi tiedustella kukkaron viittä viimeistä tapahtumaa). Yksi funktioista on `makeTransaction(amount, receiver)`, jonka kutsumisen tuloksena kukkarolta siirretään amount-parametrin osoittama summa vastaanottajan (receiver) turvamoduuliin, joka saattaa sijaita esimerkiksi toisessa Internetiin kytketyssä verkkoasemassa. Tällöin seuraa tapahtumaketju:

1. Kukkaropalveluntarjoaja esittää käyttäjälle dialogin, jolla käyttäjää pyydetään vahvistamaan sovellusohjelman palveluntarjoamalle ehdottama maksu.

2. Palveluntarjoaja ottaa yhteyden (esimerkiksi TCP/IP-protokollan välityksellä) maksun vastaanottajaan ja lähettää toimikortille APDU:n, jolla käynnistetään sovellusohjelman pyytämä maksutapahtuma.

3. Palveluntarjoaja välittää (asiaankuuluvien sovelluskohtaisten APDU:jen avulla) kukkaron ja maksun saajan turvamoduulin välisiä salattuja viestejä, joiden aitouden ja eheyden kukkaro ja turvamoduuli molemmat tarkistavat. Viestien vaihdon tuloksena kukkaron saldo pienenee, ja turvamoduulin saldo kasvaa.

4. Kukkaro antaa palveluntarjoajalle Response-APDU:n, jossa maksun kerrotaan onnistuneen. Palveluntarjoaja ilmoittaa onnistuneesta maksusta käyttäjälle ja sovellusohjelmalle.



Kuva 8. Esimerkki TCB:stä, jonka päämäärä on taata kukkaron ja kukkaropalveluntarjoajan välisen kommunikoinnin eheys ja aitous.

Kukkarokortin ja kukkaropalveluntarjoajan kommunikoinnin aitouden ja eheyden takaava TCB on kuvattu ohessa (Kuva 8). Troijan hevosen sisältävä kukkaropalveluntarjoaja, resurssinhallinta, lukija-ajuri tai niiden välissä oleva muu komponentti kuten käyttöjärjestelmä pystyy peukaloimaan kukkarosta kannettavan maksun suuruutta: vaikka palveluntarjoaja pyytää käyttäjältä valtuutuksen 5 euron maksusuoritukselle, saatetaankin kukkarolta periä käyttäjän tietämättä 50 euroa. Sen sijaan sovellusohjelma ei kuulu TCB:hen, koska valtuutusta maksun kantamiseen kukkarosta pyytää palveluntarjoaja, ei sovellus.

Ohjelmiston lisäksi TCB:hen kuuluu myös laitteistoa. Kortinlukijaa ei yleensä ole rakennettu sietämään peukalointia, ja niinpä lukijan modifiointi on mahdollista. Jos kortinlukija kytkeytyy esimerkiksi työaseman sarjaporttiin, voidaan sarjaportin ja kaapelin väliin kiinnittää helposti vihamielinen välikappale. Koska kortinlukijan ja ajurin väliseen kommunikointiin ei yleensä liity eheys- ja aitoustarkistusta, voi välikappale tarkkailla ja modifioida työaseman ja kortinlukijan välistä liikennettä. Jos työasemaa ei ole suojattu fyysisesti, välikappaleen asettajan ei tarvitse sivuuttaa työaseman käyttöjärjestelmän turvajärjestelyjä, vaan kumarrus työaseman taakse riittää.

Työasema ja siihen kytketty toimikortti muodostavat siis varsin epätasapainoisen aisaparin. Sisällölleen melko hyvän suojan tarjoava toimikortti joutuu kaikessa kommunikoinnissaan luottamaan turvattomaan työasemaan. Tietoturvallisuutta

verrataan usein ketjuun, joka katkeaa heikoimman lenkin kohdalta. Tässä tapauksessa toimikortin melko hyvä turvallisuus menettää osaksi merkityksensä, kun se on kortinlukijan kautta yhteydessä huomattavasti heikomman turvallisuuden tarjoavaan työasemaan.

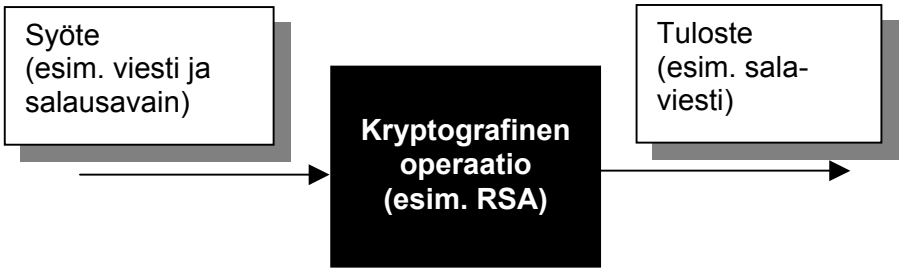
Tilanteen korjaamiseksi toimikorttiin, johon käyttäjä luottaa, pitäisi liittää eheyden ja aitouden takaava suora kommunikointikanava käyttäjän kanssa, kuten pieni näyttö (itse asiassa yksi LED riittää) ja ainakin yksi näppäin (tai muu mekanismi, jonka kautta voidaan siirtää yhden bitin mittainen hyväksymistieto) [GOBI96]. Jos tämä ei ole teknisesti, taloudellisesti tai heikon käytettävyyden vuoksi mahdollista, voidaan TCB pyrkiä siirtämään työasemasta johonkin turvallisempaan ympäristöön, kuten oman näytön ja näppäimistön sisältävään terminaaliin, johon toimikortti liitetään. Tällainen terminaali voisi olla esimerkiksi kortinhaltijan oma kämmenmikro tai matkapuhelin, johon hän luottaa ja johon asennettavia ohjelmia hän ainakin periaatteessa pystyy kontrolloimaan. Toisaalta kämmenmikrojen ja matkapuhelinten monimutkaistuminen lisää myös niiden alttiutta tuho-ohjelmille.

4. KRYPTOGRAFIAN PERIAATTEISTA

Kryptografia tarkoittaa oppia salakirjoituksen menetelmistä ja niihin perustuvista tiedon suojausmenetelmistä [VM00]. Kryptografiaa on käytetty vuosituhansia, mutta sen uuden tulemisen voidaan katsoa tapahtuneen toisen maailmansodan jälkeen transistorin ja mikroprosessorin kehittämisen ja myöhemmin 1970-luvulla löydettyjen epäsymmetristen salausmenetelmien myötä.

Kryptografiaa, erilaisia salakirjoitusmenetelmiä ja niiden perustana olevia matemaattisia teorioita on tutkittu runsaasti, ja niistä on kirjoitettu laajoja teoksia. Tässä luvussa kryptografiaa käydään läpi vain siinä laajuudessa kuin on tarpeellista myöhempien lukujen ymmärtämiselle. Erityisesti tarkastellaan symmetristä ja epäsymmetristä salausta, tiivistefunktioita sekä näiden soveltamista digitaaliseen allekirjoitukseen, haaste/vaste-todentamiseen ja symmetrisen istuntoavaimen johtamiseen.

Soveltajan näkökulmasta kryptografinen algoritmi voidaan useimmiten mallintaa "mustana laatikkona" (Kuva 9), joka saa tietyn syötteen (esimerkiksi salattava viesti ja salausavain) ja antaa tietyn tulosteen (esimerkiksi salaviesti). Soveltajan ei siis tarvitse välttämättä ymmärtää, kuinka esimerkiksi tietty salausalgoritmi yksityiskohtaisesti toimii. Käytännössä mustaa laatikkoa edustaa esimerkiksi soveltajan käytössä oleva valmis funktiokirjasto, kuten avoimeen lähdekoodiin perustuva OpenSSL [OPEN02] tai RSA Security -yhtiön tuottama kaupallinen RSA BSAFE [RSAB02].



Kuva 9. Soveltajan näkökulmasta kryptografinen algoritmi voidaan useimmiten mallintaa "mustana laatikkona".

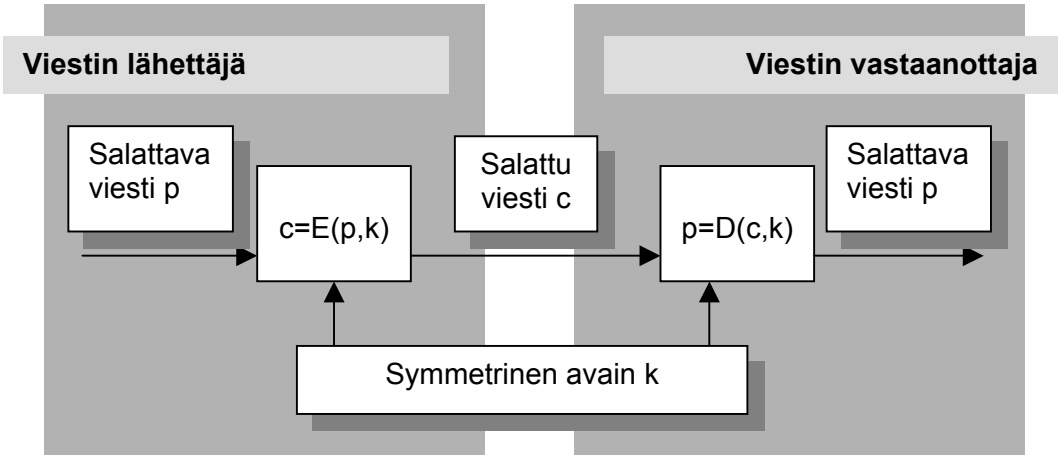
Soveltajan on kuitenkin tunnettava tietyt kryptografian perusperiaatteet, jotta hän osaa sovelluksia rakentaessaan välttää turvallisuutta vaarantavia ratkaisuja. Soveltajan on esimerkiksi syytä tietää, millaisia kryptografisia algoritmeja ja avaimia eri tarkoituksiin kannattaa käyttää, miten ja miksi avaimet on suojattava sekä kuinka usein avaimet on syytä uusia.

4.1. Symmetrinen salausmenetelmä

Kryptografian perusasetelma on tilanne, jossa joku haluaa lähettää suojaamatonta kanavaa pitkin jollekulle toiselle luottamuksellisen sanoman, jonka sisällön vain vastaanottaja pystyy lukemaan. Sen mahdollistamiseksi lähettäjällä ja vastaanottajalla on oltava käytettävissään jotain viestiin liittyvää lisätietoa, kuten salausavaimet, joiden avulla lähettäjä voi muuttaa viestin sellaiseen muotoon, että vain vastaanottaja pystyy purkamaan salauksen.

Niin sanotun Kerckhoffin suunnitteluperiaatteen mukaan salausmenetelmän turvallisuus ei kuitenkaan saa perustua siihen, että itse salausalgoritmin toiminta pidetään salaisuutena [MENE97, s. 14]. Käytetty salausalgoritmi on siis voitava huoletta julkistaa, kunhan salausavaimet pysyvät vain asiaankuuluvien tahojen tiedossa.

Salausmenetelmää, jossa samaa salausavainta käytetään sekä viestin salaamiseen että salauksen purkamiseen, kutsutaan symmetriseksi salausmenetelmäksi ja salausavainta symmetriseksi avaimeksi. Salauksen periaate on esitetty ohessa (Kuva 10). Salattava viesti p (plaintext) ja salausavain k (key) syötetään salausalgoritmille E (encrypt), jonka tuottama salattu viesti c (cryptotext) voidaan siirtää turvatonta kanavaa pitkin vastaanottajalle. Tämä antaa salatun viestin ja saman salausavaimen k salauksen purkualgoritmille D (decrypt), jolloin tulokseksi saadaan alkuperäinen salattava viesti p.



Kuva 10. Symmetrisen salausmenetelmän periaate.

Salausmenetelmän ydin on salausalgoritmi. Erilaisia symmetrisiä salausalgoritmeja on lukuisia, ja niistä vanhimmat ovat helposti murrettavissa vaatimattomillakin välineillä. Nykyään käytössä on salausalgoritmeja, joita ei pystytä murtamaan oleellisesti tehokkaammin kuin väsytysmenetelmällä (brute force attack). Siinä kaikkia mahdollisia avaimia kokeillaan järjestelmällisesti, kunnes oikea sattuu kohdalle. Väsytysmenetelmä on yhä helpompi tietokoneiden laskentatehon kasvaessa, mutta sitä voidaan vaikeuttaa käyttämällä pidempää salausavainta, jolloin kokeiltavien

avainten määrä kasvaa. Kun avaimen pituutta kasvatetaan yhdellä bitillä, kaksinkertaistuu kokeiltavien avainten määrä.

Yksi tunnetuimmista symmetrisistä salausalgoritmeista on DES (Data Encryption Standard), jonka yhdysvaltalainen National Bureau of Standards standardoi vuonna 1977 [FIPS46]. Edelleen laajassa käytössä oleva DES käyttää 56-bittistä salausavainta, mitä nykyään pidetään yleisesti riittämättömänä. Nykyisillä tietokoneilla 56-bittinen salaus on murrettavissa kohtuullisen pienessä ajassa kokeilemalla vuorotellen läpi kaikki 2^{56} (noin 72 057 594 miljardia) erilaista avainta, kunnes oikea löytyy. Vuonna 1999 suoritetussa kokeessa lähes 100 000 tavallisesta PC-työasemasta koostunut hajautettu supertietokone kykeni murtamaan DES-salauksen 22 tunnissa 15 minuutissa [RSA99].

DES-algoritmin lisäksi on kehitetty monia muita symmetrisiä salausalgoritmeja, kuten 3DES, Blowfish, CAST-128, RC5 ja RC2. Viimeaikoina huomiota on herättänyt erityisesti AES (Advanced Encryption Standard), jonka National Institute of Standards and Technology (entinen National Bureau of Standards) on standardoinut DES-algoritmin seuraajaksi [FIPS197]. AES-algoritmi tukee 128–256 bitin salausavaimia.

Matemaatikot ovat arvioineet symmetristen salausalgoritmien riittäviä avainpituuksia tietokoneiden laskentakapasiteetin ja sen hinnan historiallista kehitystä kuvaavan Mooren lain pohjalta. Riittäväksi symmetrisen avaimen pituudeksi vuonna 2002 arvioidaan 72 bittiä ja vuonna 2022 87 bittiä. Samalla kuitenkin muistutetaan, että yleensä avaimen pituudella ei ole ratkaisevaa merkitystä. Riittää, että avain on tarpeeksi pitkä, koska tavallisesti järjestelmän heikoin lenkki on kuitenkin jossain muualla: esimerkiksi tavassa, jolla salausavaimet on suojattu paljastumiselta. [LENS01]

Käytetystä salausalgoritmista riippumatta symmetrinen salausmenetelmä johtaa toiseen ongelmaan: salattujen viestien vaihtaminen edellyttää, että osapuolilla on sovittuna salausavain, jota molemmat osapuolet käyttävät. Jotta kukaan muu ei voisi avata viestejä, ei kyseinen avain saa olla sivullisten tiedossa.

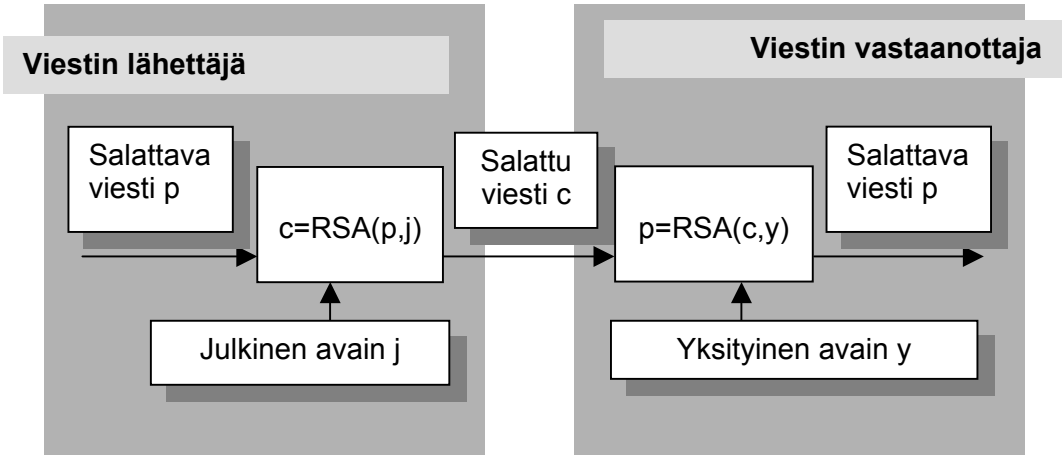
Koska keskenään kommunikoivien osapuolien määrä avoimessa tietoverkossa voi olla miljoonia, ei voida ajatella, että jokaisella osapuolella olisi valmiiksi sovittuna symmetrinen avain kaikkien muiden osapuolien kanssa. Niinpä käytännön ratkaisut toimivat yleensä niin, että osapuolet sopivat symmetrisestä avaimesta silloin, kun tahtovat aloittaa salattujen viestien lähettämisen toisilleen. Tämän jälkeen kaikki osapuolten väliset viestit salataan tällä niin sanotulla **istuntoavaimella** (session key), kunnes asia on saatu toimitetuksi loppuun ja suojattu yhteys voidaan purkaa.

Ongelmaksi muodostuu siis istuntoavaimesta sopiminen kutakin uutta yhteyttä luotaessa. Yleensä osapuolilla ei ole aikaa lähetin, kirjatun kirjeen tai muun luotettavana pidetyn fyysisen ratkaisun käyttämiseen. Ratkaisuksi on kehitetty protokollia, joissa istuntoavaimesta sovitaan tietoverkossa lähetettävien viestien avulla. Yksi tällainen protokolla on niinikään symmetriseen salausmenetelmään perustuva Kerberos [RFC1510]. Istuntoavaimen sopiminen voidaan toteuttaa myös käyttämällä epäsymmetristä salausmenetelmää, joka esitellään seuraavaksi.

4.2. Epäsymmetrinen salausmenetelmä

1970-luvulla symmetristen salausmenetelmien rinnalle kehitettiin epäsymmetrinen salausmenetelmä. Se eroaa symmetrisestä siten, että salausmenetelmässä käytetään yhden sijasta kahta eri avainta: julkista avainta (public key) ja yksityistä avainta (private key), jotka yhdessä muodostavat avainparin. Avainten välillä on matemaattinen yhteys, mutta yksityinen avain on ylivoimaisen vaikea päätellä, jos pelkkä julkinen avain tunnetaan. Julkinen avain voidaan siis huoletta julkistaa. Epäsymmetrinen salausmenetelmä tunnetaankin myös julkisen avaimen salausmenetelmänä.

Epäsymmetristä salausmenetelmää sovellettaessa jokaisella kommunikoivalla osapuolella on (ainakin yksi) avainpari. Kukin asettaa julkisen avaimensa muiden kommunikoivien osapuolien saataville. Avain voidaan tallettaa esimerkiksi julkiseen avainhakemistoon, josta kaikki halukkaat voivat noutaa sen. Yksityinen avain sen sijaan pidetään visusti tallessa, sillä se on tarkoitettu vain haltijansa käyttöön eikä missään tapauksessa saa päätyä vääriin käsiin.



Kuva 11. RSA-algoritmin käyttäminen viestin salaamiseen.

Epäsymmetrisiä salausalgoritmeja tunnetaan useita. Osa algoritmeista on yleiskäyttöisiä, osa soveltuu tiettyihin erityistarkoituksiin, kuten tuonnempana esiteltävään avaimen sopimiseen tai digitaaliseen allekirjoitukseen. Ehkä tunnetuin yleiskäyttöinen algoritmi on löytäjiensä mukaan nimetty RSA (Rivest-Shamir-Aldeman)

[RIVE78], jonka soveltamista salattujen viestien lähettämiseen on kuvattu ohessa (Kuva 11). Viestin lähettäjä hankkii itselleen viestin vastaanottajan julkisen avaimen ja salaa sillä lähetettävän viestin. Vastaanottaja purkaa saamansa salatun viestin yksityisellä avaimellaan.

Epäsymmetristen salausalgoritmien, esimerkiksi RSA:n, murtovahvuus perustuu diskreetin matematiikan hankalasti ratkaistaviin ongelmiin, jotka on valjastettu hyötykäyttöön. Esimerkiksi suuren kokonaisluvun jakaminen tekijöihinsä on matemaatikoiden käsityksen mukaan työlästä. Vastaava yleisesti käytetty ongelma on niin sanotun diskreetin logaritmin laskeminen suurelle kokonaisluvulle.

Kuten edellisessä luvussa todettiin, tapahtuu symmetrisen salauksen murtaminen yleensä kokeilemalla kaikkia mahdollisia salausavaimia, kunnes oikea löytyy. Epäsymmetrisen salauksen murtajat kohdistavat hyökkäyksensä sen sijaan yleensä algoritmin pohjana olevaan matemaattiseen ongelmaan, minkä johdosta epäsymmetrisissä salausmenetelmissä käytetään symmetrisiä salausmenetelmiä pidempiä salausavaimia. Edellä mainitun lähteen mukaan matemaatikot suosittelevat esimerkiksi vuonna 2002 käytettäväksi RSA-avainta, jonka moduulin pituus on vähintään 1028 bittiä, vuonna 2022 jo vähintään 1995 bittiä [LENS01].

Suurestakaan avainpituudesta ei ole hyötyä, jos osapuolten yksityinen avain ei ole varmassa tallessa. Työasemassa yksityinen avain on perinteisesti talletettu kiintolevylle, mahdollisesti salattuna käyttäjän antamasta salasanasta johdetulla symmetrisellä salausavaimella. Tällöin yksityinen avain saattaa altistua työasemaan tunkeutuneelle tuho-ohjelmalle, joka pääsee avaimeen käsiksi esimerkiksi käyttöjärjestelmän toteutusvirheiden kautta. Esimerkiksi Microsoftin käyttöjärjestelmien alttiutta tälle hyökkäystavalle on dokumentoitu lähteessä [GUTM02].

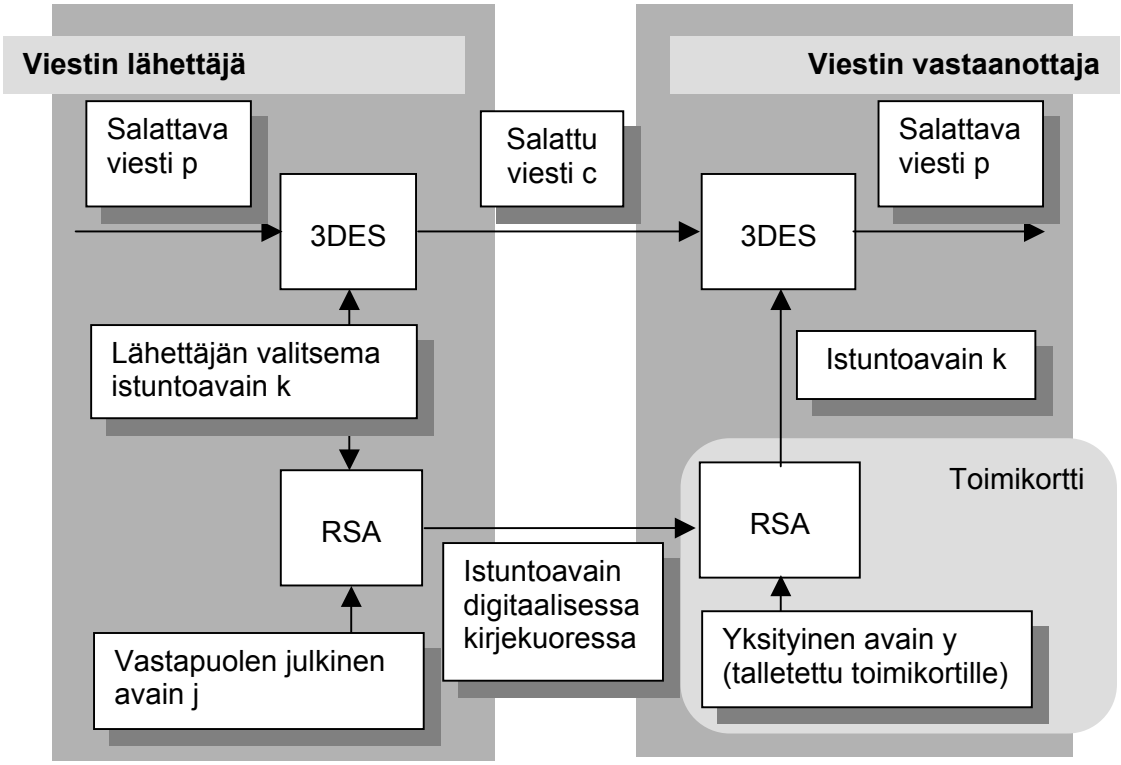
Lisäsuojaa yksityiselle avaimelle voidaan tavoitella esimerkiksi erottamalla se fyysisesti ympäristöstään, jossa se on alttiina vahingoille, huolimattomuudelle, Troijan hevosille yms. Yksi tapa tämän toteuttamiseen voisi olla yksityisen avaimen tallettaminen sellaisen työaseman kiintolevylle, joka ei olisi yhteydessä tietoverkkoon, jossa ajettaisiin vain luotettavia ohjelmia, ja jota säilytettäisiin lukitussa kassakaapissa.

Käyttäjän kannalta mukavampi ratkaisu on kuitenkin yksityisen avaimen tallettaminen esimerkiksi toimikortille, joka mahtuu lompakkoon ja joka tarjoaa hintaansa nähden varsin hyvän suojan yksityiselle avaimelle. Koska toimikortin suoritin kykenee laskutoimituksiin, voidaan yksityistä avainta paitsi säilyttää, myös käyttää toimikortin sisällä. Niinpä avainta ei tarvitse koskaan tuoda ulos kortilta edes laskutoimituksien suorittamista varten. Parhaassa tapauksessa avainpari on jopa luotu toimikortin sisällä, mikä lisää yksityisen avaimen ja siten koko järjestelmän turvallisuutta.

4.3. Istuntoavaimen johtaminen epäsymmetrisellä salausalgoritmilla

RSA:n kaltaista epäsymmetristä salausalgoritmia voidaan periaatteessa käyttää sellaisenaan viestien salaamiseen: viestin lähettäjä salaa viestin sen vastaanottajan julkisella avaimella, ja viestin vastaanottaja käyttää mahdollisesti toimikortilla olevaa yksityistä avaintaan salatun viestin avaamiseen. Epäsymmetristen salausmenetelmien käyttämät laskutoimitukset ovat kuitenkin oleellisesti symmetristen salausmenetelmien laskutoimituksia työläämpiä. Erityisesti vaatimattomalla laskentakapasiteetilla varustettu toimikortti ei selviytyisi niistä siedettävässä ajassa, jos niitä pitäisi soveltaa koko viestiin.

Luottamuksellisen tiedonsiirron mahdollistavat käytännön sovellukset, kuten myöhemmin käsiteltävät Secure shell-, TLS- ja S/MIME-protokollat, käyttävät symmetrisen ja epäsymmetrisen salauksen yhdistelmää. Varsinaiseen tiedonsiirtoon käytetään luvussa 4.1 esiteltyä symmetristä salausmenetelmää ja istuntoavainta, jonka osapuolet tässä tapauksessa johtavat epäsymmetrisen salausmenetelmän avulla. Istuntoavaimen johtamiseen käytettävät tietoturvaprotokollat voivat perustua joko avaimesta sopimiseen tai avaimen kuljettamiseen [HOUS01, s. 11–12].



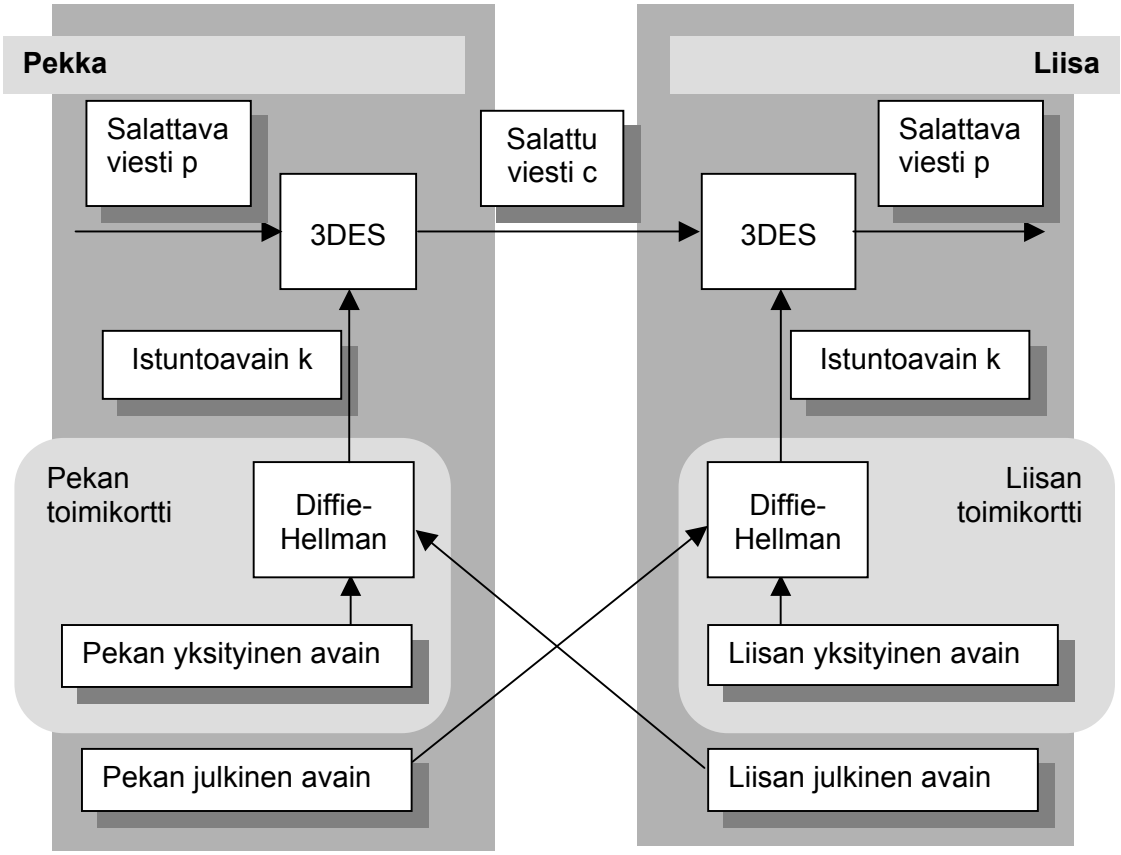
Kuva 12. Esimerkki istuntoavaimen kuljettamisesta digitaalisen kirjekuoren avulla, jossa käytetään 3DES- ja RSA-algoritmeja sekä toimikorttia.

Avaimen kuljetus (key transport) tarkoittaa, että toinen osapuoli valitsee istuntoavaimen ja välittää sen toiselle osapuolelle ”digitaalisesti suljetussa kirjekuoressa” salattuna vastapuolen julkisella avaimella (Kuva 12). Vain vastapuoli pystyy

avaamaan kirjekuoren yksityisen avaimensa avulla, ja siten istuntoavain on vain kommunikoivien osapuolien tiedossa. Tunnetuin avaimen kuljetukseen käytetty algoritmi on RSA.

Avaimen kuljetukseen liittyy ongelmia: avaimen vastaanottaja joutuu luottamaan lähettäjän kykyyn valita turvallinen symmetrinen avain. Vastaanottaja ei myöskään välttämättä voi varmistua avaimen tuoreudesta: kyseessä voi olla myös toistohyökkäys (replay attack), jolloin hyökkääjä pyrkii hämäämään vastaanottajaa lähettämällä uudelleen lähettäjän jonkin aikaisemman viestin.

Avaimesta sopiminen (key agreement) eroaa avaimen kuljetuksesta siten, että molemmat osapuolet osallistuvat istuntoavaimen valitsemiseen. Osapuolet muodostavat yhteisen istuntoavaimen laskutoimituksella, jossa tarvitaan oman yksityisen avaimen lisäksi vastapuolen julkista avainta (Kuva 13). Tällöin molemmilla osapuolilla on siis oltava oma avainpari sekä sovittuna joitain avaimiin liittyviä yhteisiä parametreja. Tunnetuin avaimen sopimiseen käytetty algoritmi on Diffie-Hellman [DIFF76].



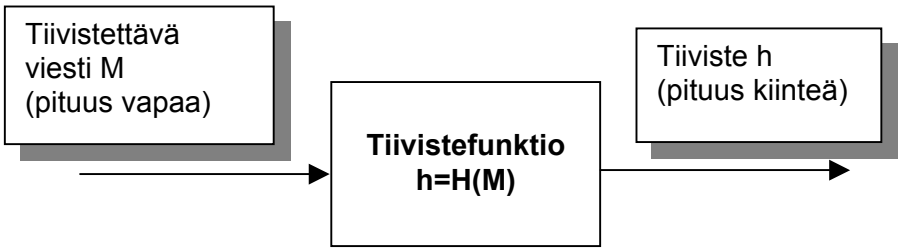
Kuva 13. Esimerkki istuntoavaimen sopimisesta Diffie-Hellmanin avaimensopimisprotokollan avulla.

Istuntoavain ja sen johtaminen epäsymmetrisen salausmenetelmän avulla yhdistää symmetrisen ja epäsymmetrisen salauksen hyvät puolet: symmetrisen salauksen nopeuden ja epäsymmetrisen salauksen joustavuuden. Toimikorttia ja epäsymmet-

ristä salausalgoritmia tarvitaan vain yhteyden muodostuksessa, jonka aikana johdettua istuntoavainta ja symmetristä salausalgoritmia voidaan käyttää siitä eteenpäin viestien salaamiseen. Istuntoavain on melko lyhyt, käytännössä muutamia satoja bittejä, joten raskassoutuista epäsymmetristä algoritmia ei tarvita kovin pitkän viestin työstämiseen. Symmetrisellä algoritmilla ja istuntoavaimella sen sijaan voidaan istunnon kuluessa salata helposti megatavujenkin suuruisia tietomääriä. Tällöin on eduksi, että käytössä on nopea algoritmi ja tehokas suoritin. Koska symmetrisessä salauksessa ei tarvita toimikorttia ja sille talletettua yksityistä avainta, voidaan algoritmin suorittaminen uskoa työaseman korttia tehokkaamman suorittimen tehtäväksi.

4.4. Tiivistealgoritmit

Tiivistealgoritmia ei voi käyttää salattujen viestien lähettämiseen samalla tavalla kuin symmetrisiä ja epäsymmetrisiä salausmenetelmiä, mutta se liittyy yhtenä rakennuspalasena moneen suurempaan kokonaisuuteen, esimerkiksi digitaaliseen allekirjoitukseen. Tiivistealgoritmi on kryptografinen algoritmi, jonka avulla vaihtelevan pituisesta viestistä voidaan laskea määrämittainen, esimerkiksi 160 bittiä pitkä merkkijono, jota kutsutaan tiivisteeksi (hash, digest). Periaate on esitetty oheisessa kuvassa (Kuva 14).



Kuva 14. Tiivistealgoritmin periaate.

Tiivistealgoritmille on ominaista, että tiivisteen h laskeminen viestistä M on laskennallisesti helppo toimenpide, mutta käänteinen toimenpide, jossa etsitään (jokin) tiivisteeseen h tiivistyvä viesti M, on kryptografisesti vahvaa tiivistealgoritmia käytettäessä ylivoimaisen työläs ratkaistavaksi [STAL99, s. 253]. Jos yksikin bitti viestissä M muuttuu, myös tiiviste h muuttuu. Koska tiivisteen h pituus on kiinteä, mutta viestissä M voi olla mikä vain määrä bittejä, on luonnollisesti olemassa lukuisia eri viestejä M_1 ja M_2, joille pätee $H(M_1)=H(M_2)=h$ – niiden löytäminen vain on hyvin vaikeaa.

Tiettyyn 160-bittiseen tiivisteeseen tiivistyvän (erään) viestin M etsiminen väsytysmenetelmällä vaatii keskimäärin 2^{159} eri viestin M' kokeilemista. Tiivisteiden riittäviä pituuksia arvioitaessa keskeisessä asemassa on kuitenkin syntymäpäiväpa-

radoksi: kahden samaan tiivisteeseen tiivistyvän viestin löytäminen onkin ehkä yllättäen paljon helpompaa. Voidaan todistaa, että kahden samaan n-bittiseen tiivisteeseen tiivistyvän eri viestin M_1 ja M_2 löytymiseen tarvitaan keskimäärin likimain $2^{n/2}$ viestin kokeilemista. Syntymäpäiväparadoksi on saanut nimensä todennäköisyysmatematiikan klassisesta esimerkistä, jonka mukaan luokkahuoneessa pitää olla vähintään 23 oppilasta (joka on likimain 365:n neliöjuuri), jotta todennäköisyys sille, että luokassa on kaksi samana päivänä syntymäpäivää viettävää opiskelijaa, on yli 50 prosenttia. Laskelmien todistus sivuutetaan tässä. [STAL99, s. 264-269]

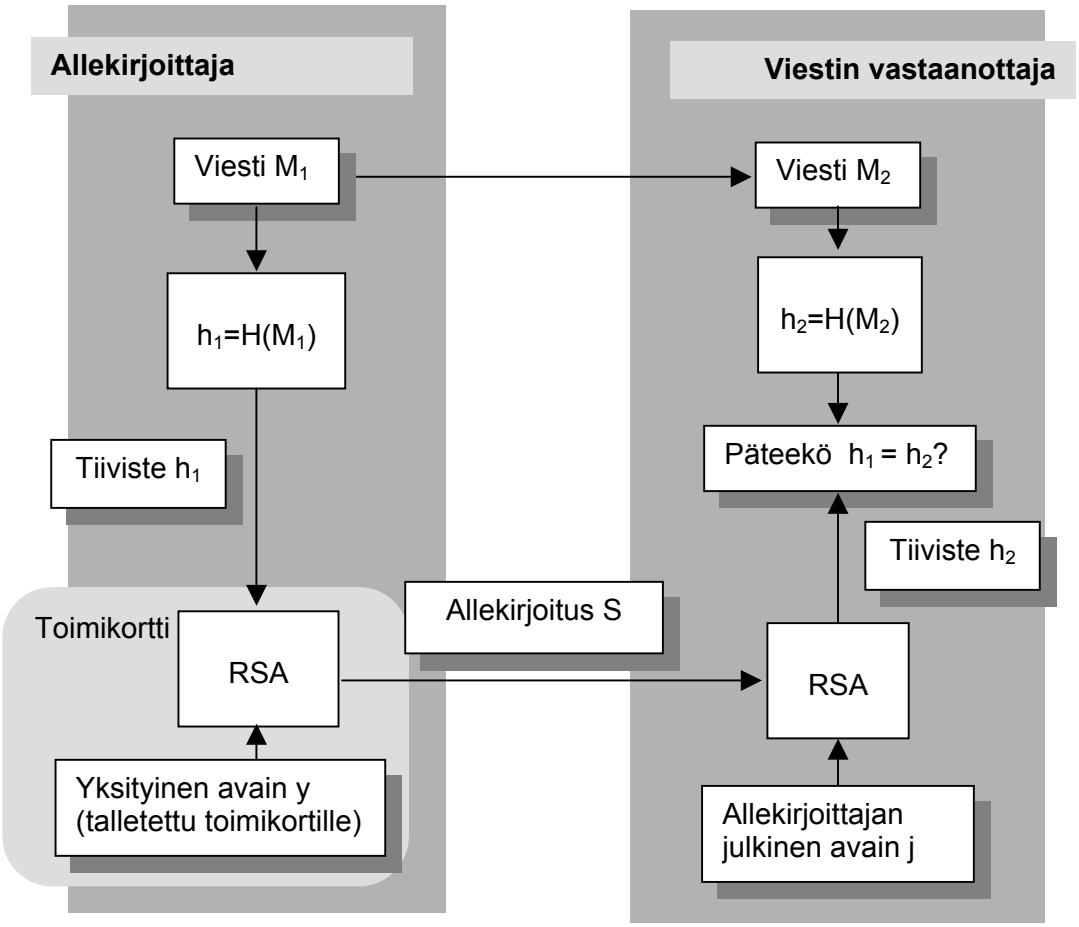
Yleisesti käytettyjä tiivistealgoritmeja ovat MD5 [RFC1321] ja SHA-1 [FIPS180]. MD5 tiivistää viestit 128 bittiin, joten syntymäpäiväparadoksin mukaan kahden samaan MD5-tiivisteeseen tiivistyvän eri viestin löytämiseen tarvitaan noin 2^{64} yritystä. MD5:stä ollaankin siirtymässä vähitellen uudempaan SHA-1-algoritmiin, jota pidetään turvallisempana muun muassa sen pidemmän 160-bittisen tiivisteen vuoksi. Tätäkin pidemmän tiivisteen laskevia algoritmeja on suunnitteilla, sillä tietokoneiden laskentatehon kasvaminen luo paineita myös tiivisteiden pituuden kasvattamiselle.

Tiivisteitä käytetään muun muassa seuraavassa alaluvussa esiteltävässä digitaalisessa allekirjoituksessa varmistamaan viestin alkuperäisyys. Tiivistealgoritmia voidaan käyttää myös salasanan tiivistämiseen, kun salasanaa ei haluta tallettaa tietojärjestelmään paljaaltaan. Kun käyttäjä valitsee salasanansa, laskee tietojärjestelmä salasanan tiivisteen, joka talletetaan. Kun käyttäjä myöhemmin todennetaan salasanan avulla, lasketaan hänen antamastaan salasanasta tiiviste, jota verrataan järjestelmään talletettuun salasanaan. Mikäli nämä täsmäävät, on käyttäjä tiennyt oikean salasanan. Järjestelyn etu on, että tiivistetyn salasanatietokannan haltuunsa saanut hakkeri ei pysty suoraan lukemaan tietokannasta yhdenkään käyttäjän salasanaa.

4.5. Digitaalinen allekirjoitus

Joitakin epäsymmetrisiä salausalgoritmeja, esimerkiksi RSA-algoritmia, voidaan käyttää normaaliin salausjärjestykseen verrattuna päinvastaisessa järjestyksessä. Selväkielinen viesti salataankin yksityisellä avaimella, ja salattu viesti lähetetään vastaanottajalle, joka purkaa salauksen vastaavalla julkisella avaimella. Tällainen järjestely ei takaa viestin luottamuksellisuutta. Jos julkinen avain on saatavilla esimerkiksi julkisesta hakemistosta, voi kuka tahansa noutaa avaimen ja avata viestin, joka on salattu vastaavalla yksityisellä avaimella. Sen sijaan järjestelyn avulla voidaan toteuttaa **digitaalinen allekirjoitus** (digital signature), joka on sähköinen allekirjoitus, joka on tehty asiakirjan tai viestin laatijan tai lähettäjän yksityisellä avaimella julkisen avaimen menetelmän mukaisesti [VM00].

Digitaalisen allekirjoituksen periaate on esitetty oheisessa kuvassa (Kuva 15). Allekirjoitettavasta viestistä M_1 lasketaan tiiviste h_1, joka salataan mahdollisesti toimikortille sijoitetulla yksityisellä avaimella y. Näin syntynyt allekirjoitus S siirretään yhdessä alkuperäisen viestin kanssa vastaanottajalle, joka purkaa allekirjoituksen lähettäjän julkisella avaimella j ja vertaa tulosta h_1 vastaanottamastaan viestistä M_2 laskettuun tiivisteeseen h_2. Mikäli tiivisteet h_1 ja h_2 ovat samat, on allekirjoitus laadittu lähettäjän yksityisellä avaimella y ja viesti allekirjoituksineen siirtynyt muuttumattomana lähettäjältä vastaanottajalle, toisin sanoen $M_1 = M_2$.



Kuva 15. Digitaalinen allekirjoitus käytännössä.

Digitaalisella allekirjoituksella on yhtäläisyyksiä ja eroavaisuuksia perinteiseen kynällä tehtyyn allekirjoitukseen. Sekä perinteinen että digitaalinen allekirjoitus voidaan ymmärtää tekijänsä sitoutumisena allekirjoitettavaan asiaan: jos voidaan olla varmoja, että tietty yksityinen avain on vain tietyn henkilön hallinnassa (mikä tosin ei ole itsestään selvää, kuten luvussa 6.4.2 tullaan toteamaan), ja jos vastaavan julkisen avaimen avulla todetaan, että viesti on allekirjoitettu nimenomaan kyseisen henkilön hallussa olevalla yksityisellä avaimella, ei henkilöllä ole mahdolli-

suutta jälkeenpäin kiistää, että hänen yksityistä avaintaan on käytetty viestin allekirjoittamiseen.

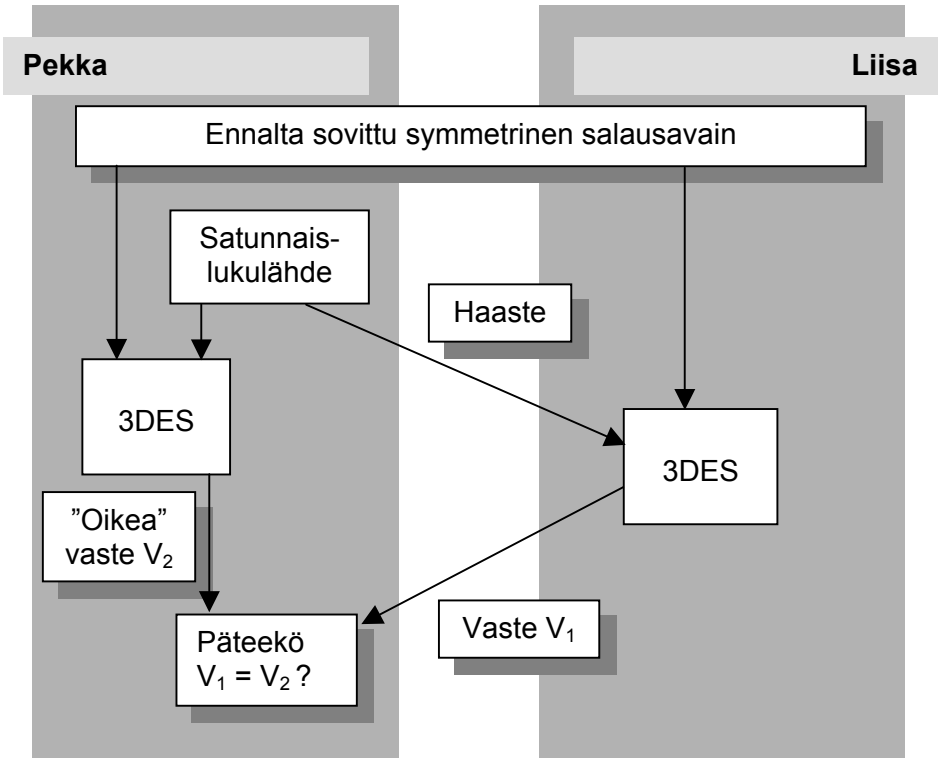
Digitaalinen allekirjoitus on kuitenkin perinteistä huomattavasti vaikeampi väärentää, ja myös yritys peukaloida dokumenttia allekirjoituksen jälkeen paljastuu. Digitaalisesti allekirjoitettua dokumenttia on helppo paitsi siirtää ja arkistoida, myös kopioida, mikä altistaa digitaalisen allekirjoituksen toistohyökkäykselle (replay attack). Digitaalisesti allekirjoitetun dokumentin käyttäminen tositteena esimerkiksi maksusuorituksesta on vaikeaa, koska tositetta voidaan kopioida rajattomasti, eikä alkuperäisellä tositteella ja sen kopioilla ole mitään eroa.

Tietoverkkojen ja Internetin kaupallisen hyödyntämisen lisääntyessä on syntynyt tarve kehittää menetelmiä, joiden avulla toisilleen entuudestaan tuntemattomat osapuolet voivat tehdä sitovia sopimuksia verkon välityksellä ilman, että heidän tarvitsee tavata fyysisesti. Suomalainen lainsäädäntö on reagoimassa tilanteeseen eduskunnan käsittelyssä olevalla lailla sähköisestä allekirjoituksesta [HE01], jolla implementoidaan EU:n direktiivi digitaalisesta allekirjoituksesta [EP99]. Lakiesitys pyrkii takaamaan, että sähköinen allekirjoitus ja sen erikoistapauksena digitaalinen allekirjoitus tullaan tiettyjen ehtojen täyttyessä muotovaikutukseltaan rinnastamaan käsin tehtyyn allekirjoitukseen. Aiheeseen palataan tuonnempana luvussa 6.5.

4.6. Haaste/vaste-todentaminen

Sekä symmetrisen että epäsymmetrisen salausmenetelmän avulla voidaan toteuttaa osapuolten – esimerkiksi verkon palvelimen ja sen käyttäjän – henkilöllisyyden vahva todentaminen. Todentamiseen soveltuvia perusprotokollia on useita, ja ne nojaavat joko aikaleimoihin tai haaste/vaste-periaatteeseen [STAL99, s. 304]. Tässä syvennytään haaste/vaste-todentamiseen, joka on laajassa käytössä.

Haaste/vaste-protokollan avulla Pekka voi todentaa Liisan henkilöllisyyden lähettämällä hänelle haasteen, johon Liisan tulee vastata lähettämällä Pekalle haasteesta johdettu vastaus [STAL99 s. 304]. Pekalla on käytettävissään keino tarkistaa, että Liisa on johtanut vastauksen oikein.



Kuva 16. Esimerkki haaste/vaste-todentamisesta käyttämällä symmetristä salausmenetelmää.

Oheisessa esimerkissä (Kuva 16) Pekka ja Liisa ovat etukäteen sopineet symmetrisestä salausavaimesta. Pekka valitsee haasteen arpomalla pitkän satunnaisluvun, jonka hän lähettää Liisalle. Liisa ottaa vastaan Pekan haasteen, salaa sen salausavaimellaan ja lähettää salatun luvun V_1 Pekalle. Pekka salaa Liisalle esittämänsä haasteen samalla avaimella. Jos saatu tulos V_2 täsmää Liisan esittämän vasteen V_1 kanssa, Pekka on varma, että vastauksen on lähettänyt henkilö, jolla on tiedossaan haaste ja sama symmetrinen salausavain. Liisan henkilöllisyys on siis tullut todennetuksi.

Salasanatodentamiseen verrattuna haaste/vaste-todentamisessa huomionarvoista on se, että Liisan ja Pekan viestejä salakuunteleva hyökkääjä ei pääse käsiksi tietoon, joka mahdollistaisi Liisaksi tekeytymisen. Pekka pääsee itse valitsemaan lähetettävän haasteen, joka on jokaisella kerralla eri satunnaisluku, ja vastaukseksi hän kelpuuttaa vain haasteesta oikein johdetun vastauksen. Hyökkääjän on turha yrittää käyttää esimerkiksi Liisan edellisellä kerralla Pekalle esittämää vastausta. Se kelpaa vastaukseksi vain Pekan silloin esittämään haasteeseen, joka ei seuraavalla kerralla ole sama.

Edellinen esimerkki kuvastaa yksisuuntaista todentamista: Pekka varmistuu Liisan henkilöllisyydestä, mutta Liisa ei voi päätellä sen perusteella vielä mitään haasteen

esittäjän henkilöllisyydestä. Kaksisuuntainen todentaminen tapahtuu esimerkiksi silloin, kun myös Liisa esittää haasteen, johon Pekka vastaa.

Esimerkissä käytettiin symmetristä salausmenetelmää. Jos Pekalla on Liisan julkinen avain, hän voi todentaa Liisan henkilöllisyyden myös epäsymmetrisen salausmenetelmän ja digitaalisen allekirjoituksen avulla. Tällöin Pekka pyytää Liisaa allekirjoittamaan esitetyn haasteen yksityisellä avaimellaan, ja todentaa Liisan lähettämän vastauksen tämän julkisella avaimella. Näin Liisa ja Pekka eivät tarvitse etukäteen sovittua symmetristä avainta. Muun muassa luvussa 7.3 esiteltävä Secure shell -protokolla, joka mahdollistaa turvallisen pääteyhteyden ottamisen palvelimeen, käyttää tätä periaatetta molempien osapuolien – käyttäjän ja palvelimen – todentamisessa.

5. JULKISEN AVAIMEN JÄRJESTELMÄ (PKI)

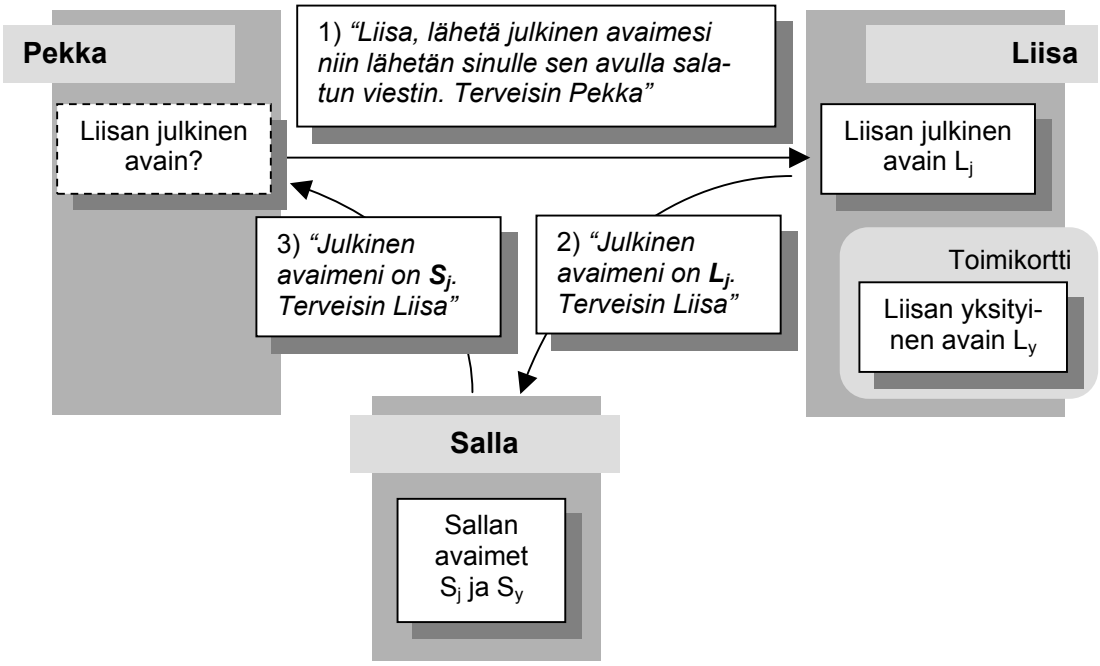
Tässä luvussa esitellään julkisen avaimen järjestelmä, sen käyttötarpeet ja -kohteet sekä keskeiset komponentit kuten varmenne, varmennearkkitehtuuri, -politiikka ja -käytäntö sekä luottamuksen rooli julkisen avaimen järjestelmässä. Tämän luvun roolihenkilöinä esiintyvät muun muassa kommunikoivat osapuolet Liisa ja Pekka, salakuuntelija Salla ja luotettu kolmas osapuoli Timo.

Tämän luvun alussa rajoitutaan käsittelemään nimenomaan henkilövarmenteita, jotka kytkevät julkisen avaimen ja henkilön nimen tai muun tunnistetiedon toisiinsa. Muita nimivarmenteita, kuten palvelinvarmenteita, ei käsitellä tässä erikseen, vaikka ne eivät toimintaperiaatteiltaan oleellisesti eroa henkilövarmenteista. Luvun lopussa luodaan katsaus myös rooli- ja attribuuttivarmenteisiin.

5.1. Mihin julkisen avaimen järjestelmää tarvitaan

Edellisessä luvussa esitettiin epäsymmetrisen salausmenetelmän toimintaperiaate: kuinka henkilö voi lähettää viestin toiselle henkilölle salaamalla sen hänen julkisella avaimellaan ja kuinka vastaanottaja pystyy avaamaan viestin käyttämällä mahdollisesti toimikortille talletettua yksityistä avaintaan. Tämä ei kuitenkaan vielä riitä, jos halutaan toteuttaa laajamittainen salattujen viestien lähettämisen infrastruktuuri avoimeen tietoverkkoon. Ratkaisematta on vielä kysymys, kuinka viestin lähettäjä saa käsiinsä julkisen avaimen ja varmuuden, että sitä vastaava yksityinen avain kuuluu viestin vastaanottajalle.

Ongelmaa on havainnollistettu ohessa (Kuva 17): Pekalla on sähköpostiyhteys Liisaan avoimen Internetin yli. Matkan varrella Sallalla on mahdollisuus Pekan ja Liisan tietämättä salakuunnella ja peukaloida heidän lähettämiään viestejä: Salla pystyy tekemään klassisen välimieshyökkäyksen (man-in-the-middle attack). Kuvan tilanteessa Pekka haluaa lähettää salaisen viestin Liisalle, mutta on tietoinen siitä, että hänen lähettämänsä sähköpostiviesti kulkee Liisalle täysin salaamattomana avoimen Internetin läpi. Pekka on kuullut epäsymmetrisestä salausmenetelmästä, ja lähettää ensin Liisalle viestin pyytäen häntä lähettämään oman julkisen avaimensa paluupostissa (viesti 1). Liisalla on avainpari L_j ja L_y, joista jälkimmäinen, yksityinen avain, sijaitsee Liisan omistamalla toimikortilla. Liisa vastaa Pekan viestiin ja liittää vastaukseensa julkisen avaimensa (viesti 2). Liisan ja Pekan välisiä sähköposteja salakuunteleva Salla onnistuu sieppaamaan Liisan lähettämän sähköpostin, korvaa viestin liitteenä olevan Liisan julkisen avaimen omalla julkisella avaimellaan S_j, ja lähettää sähköpostiviestin eteenpäin (viesti 3) Pekalle, joka kuvittelee viestin tulleen Liisalta. Näin Pekka saa haltuunsa Sallan julkisen avaimen, jonka hän kuvittelee kuuluvan Liisalle.



Kuva 17. Yksi tapa tehdä välimieshyökkäys.

Seuraavaksi Pekka todennäköisesti käyttää saamaansa julkista avainta ja edellisessä luvussa esitettyä digitaalista kirjekuorta lähettääkseen salaisen viestin Liisalle. Pekka kuvittelee, että yksinomaan Liisa pystyy avaamaan hänen lähettämänsä salatut viestit, mutta todellisuudessa viestit avaakin omalla yksityisellä avaimellaan Salla, joka edelleen salakuuntelee liikennettä ja jonka julkinen avain Pekalla on. Viestit eivät välttämättä koskaan edes saavu Liisan sähköpostilaatikkoon, ja vaikka saapuisivatkin, ei Liisalla olisi mahdollisuutta avata niitä, koska viestit voi avata vain Sallan hallussa olevalla yksityisellä avaimella.

Vaihtoehtoisesti voidaan tietysti ajatella ratkaisuja, joissa Pekka ei saisi Liisan julkista avainta sähköpostina häneltä itseltään, vaan noutaisi sen esimerkiksi julkisille avaimille varatusta hakemistopalvelimesta. Se ei kuitenkaan muuta asetelmaa: Salla voi matkan varrella väärentää myös Pekan hakemistosta noutaman avaimen. Hakemistoon on saatettu myös murtautua tai hakemiston ylläpitäjä voi olla epärehellinen.

Huomionarvoista on se, että vaikka Liisan yksityinen avain onkin talletettu luotettavasti toimikortille, ei toimikortti anna mitään suojaa esitetylle hyökkäykselle. Ongelmana ei ole Liisan yksityisen avaimen paljastuminen sivulliselle, vaan sen selvittäminen, kenen hallussa tiettyyn julkiseen avaimeen liittyvä yksityinen avain todellisuudessa on. Tavalla tai toisella Pekan tulisi varmistaa, että hänen saamansa julkisen avaimen yksityinen vastakappale todellakin on Liisalla.

Julkisen avaimen järjestelmällä (public key infrastructure, PKI) tarkoitetaan niitä toimenpiteitä ja käytäntöjä, joiden perusteella julkisen avaimen tietoverkossa

kohtaava voi varmistaa vastaavan yksityisen avaimen haltijan nimen (tai muun haltijaan liittyvän ominaisuuden, mihin syvennytään luvussa 5.10). Julkisen avaimen järjestelmän avulla voidaan suojautua edellä esitetyltä välimieshyökkäykseltä. Epäsymmetrisen salausmenetelmän käyttäminen edellyttää julkisen avaimen järjestelmän toteuttamista tavalla tai toisella.

Julkisen avaimen järjestelmä voidaan rakentaa eri tavoin. Luotettavin tapa Liisan julkisen avaimen saamiseksi lienee hakea se Liisalta henkilökohtaisesti. Jos Pekka tuntee Liisan äänestä, voi Liisa luetella avaimensa Pekalle myös puhelimessa. Vaihtoehtoisesti Liisa voi myös lähettää Pekalle avaimensa esimerkiksi sähköpostina, kuten edellä esitettiin, mutta avaimen saatuaan Pekan tulee soittaa Liisalle ja pyytää häntä luettelemaan julkisesta avaimestaan laskemansa tiivisteen (fingerprint eli "sormenjälki"). Jos Liisan luettelema tiiviste on sama kuin sähköpostina saadusta avaimesta laskettu tiiviste, ei sähköpostina tullutta avainta ole väärennetty matkan varrella.

5.2. Luotettu kolmas osapuoli

Julkisen avaimen järjestelmä ei ole kovin helppokäyttöinen, jos se perustuu yksityisen avaimen haltijalta henkilökohtaisesti haettuun julkiseen avaimeen. Osapuolet voivat sijaita kaukana toisistaan, eivätkä he välttämättä tunne toistensa ääntä puhelimessa tai ole edes koskaan tavanneet toisiaan.

Entäpä jos julkista avainta ei tarvitsisi hakea yksityisen avaimen haltijalta henkilökohtaisesti, vaan julkista avainta tarvitseva osapuoli voisi lähettää luottohenkilönsä toimittamaan asiansa? Eräänä aamuna Liisan ovelle kolkuttaisi Timo, joka toisi terveiset Pekalta ja pyytäisi Liisaa antamaan hänelle kopion julkisesta avaimestaan: ”Pekalla on tärkeä viesti, jonka hän haluaa lähettää salattuna.”

On selvää, että Pekan tulee luottaa lähettinä toimivaan Timoon voidakseen uskoa hänelle lähetin tärkeän tehtävän. Jos Timo ei ole luottamuksen arvoinen, hän voi lähettinä toimiessaan väärentää Liisan antaman julkisen avaimen kuten Salla edellä. Lähettäessään Timon matkaan Pekan tulee myös evästää häntä ja varmistaa, että hänellä on vastuullisesta tehtävästä selviytymiseen tarvittava osaaminen: jos Timo ei tunne Liisaa, tulee Timon tarkistaa esimerkiksi Liisan passista, että oven avannut henkilö todella on Pekan tavoittelema Liisa. Lisäksi Timon tulee paluumatkalla herkeämättä valvoa paperinpalaa tai levykettä, johon Liisan julkinen avain on kirjoitettu. Hyväksi olisi myös, jos Timo tavalla tai toisella varmistaisi, että Liisa todella kirjoittaa paperille oman julkisen avaimensa, eikä epähuomiossa jonkun muun avainta.

Liisan ei tarvitse luottaa Timoon, ja tuskinpa hän voisikaan: eihän Liisa välttämättä edes tunne ovelleen kolkuttanutta miestä. Timon tehtävä **luotettuna kolmantena osapuolena** on valvoa Pekan etua, ei Liisan etua. Jos Liisa haluaa varmistaa, että hänelle sähköpostia lähettänyt Pekka todellakin on väittämänsä henkilö, eikä esimerkiksi viestejä salakuunteleva Salla, on Liisan varustettava matkaan oma luottohenkilönsä, joka vastaavalla tavalla kuin Timo noutaa julkisen avaimen Pekalta.

5.3. Varmenne

Palattuaan Liisan luota Timo antaa saamansa julkisen avaimen Pekalle. Pekalla on nyt kädessään kallisarvoinen tieto: avain luottamuksellisen viestin lähettämiseen Liisalle. Pekka sulkee Liisan julkisen avaimen kassakaappiinsa.

Pekka ei suinkaan käytä kassakaappiaan sen takia, että Liisan julkinen avain pitäisi pitää muilta salassa – avainhan on nimensä mukaan julkinen, ja kuka vain voi mennä pyytämään sitä Liisalta. Sen sijaan Pekan täytyy huolehtia, että kukaan ei pääse peukaloimaan Liisan julkista avainta tai että avain ei pääse hukkumaan. Pekkaa kiinnostaa siis Liisan julkisen avaimen aitouden ja eheyden säilyttäminen. Siihen ei kuitenkaan välttämättä tarvita kassakaappia: digitaalinen allekirjoitus voi taata saman asian.

Seuraavalla kerralla, kun Timo lähetetään hakemaan Liisan tai jonkun muun Pekan ystävättären julkista avainta, Pekan ei tarvitse enää pyytää Timoa palaamaan luokseen Liisan julkinen avain mukanaan. Ennen lähtöään Timo antaa henkilökohtaisesti Pekalle oman julkisen avaimensa, ja noudettuaan Liisan julkisen avaimen hän allekirjoittaa sen ja Liisan henkilötiedot omalla yksityisellä avaimellaan. Timon allekirjoittamaa Liisan julkista avainta kutsutaan Liisan **varmenteeksi** eli **sertifikaatiksi** (certificate) ja varmenteen allekirjoittanutta Timoa **varmentajaksi** (certification authority, CA).

Timo voi lähettää Liisan varmenteen Pekalle esimerkiksi sähköpostina tai antaa varmenteen Liisalle itselleen, joka voi liittää sen seuraavaan Pekalle lähettämäänsä sähköpostiin. Koska varmenne on allekirjoitettu Timon yksityisellä avaimella, se voidaan siirtää myös turvatonta kanavaa pitkin. Pekka käyttää Timon julkista avainta varmenteen todentamiseen eli verifioimiseen: näin Pekka varmistuu, että turvatonta kanavaa pitkin siirretty varmenne on todellakin Timon allekirjoittama väärentämätön todiste siitä, että varmenteeseen sisältyvä julkinen avain kuuluu Liisalle. Pekan pitää vain huolehtia Timon julkisen avaimen aitoudesta – sen avulla hän voi todentaa kaikki Timon allekirjoittamat varmenteet.

Timon ei ole pakko toimittaa Liisan varmennetta Pekalle, vaan hän voi vaihtoehtoisesti tallettaa sen varmennehakemistoon, josta Pekka voi itse noutaa kopion sii-

tä. Tämä järjestely on hyödyllinen erityisesti silloin, jos muutkin kuin Pekka luottavat Timoon. Kaikki Timoon luottavat verkon käyttäjät, jotka haluavat lähettää luottamuksellisen viestin Liisalle, voivat noutaa Liisan varmenteen julkisesta varmennehakemistosta (edellyttäen että nimi Liisa tuo heille mieleen saman neidin kuin Timolle, mihin kysymykseen palataan luvussa 5.9). Tämä avaa Timolle mahdollisuuden kaupallistaa ammattitaitonsa: Timo voi ryhtyä ammattimaiseksi varmentajaksi, joka myy osaamistaan – luotettavuutta – henkilöille, jotka haluavat lähettää salattuja viestejä avoimen tietoverkon yli.

Pääosa olemassa olevista laajamittaisista julkisen avaimen järjestelmistä pohjautuu varmenteisiin. Varmenne kytkee tietyn julkisen avaimen tiettyyn henkilöön tai muuhun olioon. Käytännössä tämä tapahtuu sisällyttämällä varmenteen tietoihin henkilön julkisen avaimen lisäksi hänen nimensä, sähköpostiosoitteensa tai jokin muu hänet yksilöivä tai häneen liittyvä tieto. Lisäksi varmenteesta tyypillisesti ilmenee ainakin varmenteen myöntäjä eli varmentaja sekä voimassaoloaika. Internetissä yleisesti käytetty X.509-varmenne esitellään myöhemmin.

5.4. Varmennearkkitehtuurit

Timon ei välttämättä tarvitse itse suorittaa kaikkien varmennettavien henkilöiden julkisten avainten noutoa: hän voi myös delegoida tehtävän eteenpäin Alpolle, mikäli Timo ja hänen omat toimeksiantajansa luottavat Alpoon. Alposta tulee alivarmentaja, ja Timo allekirjoittaa hänen julkisen avaimensa omalla yksityisellä avaimellaan. Alpo käyttää omaa yksityistä avaintaan uusien varmenteiden allekirjoittamiseen.

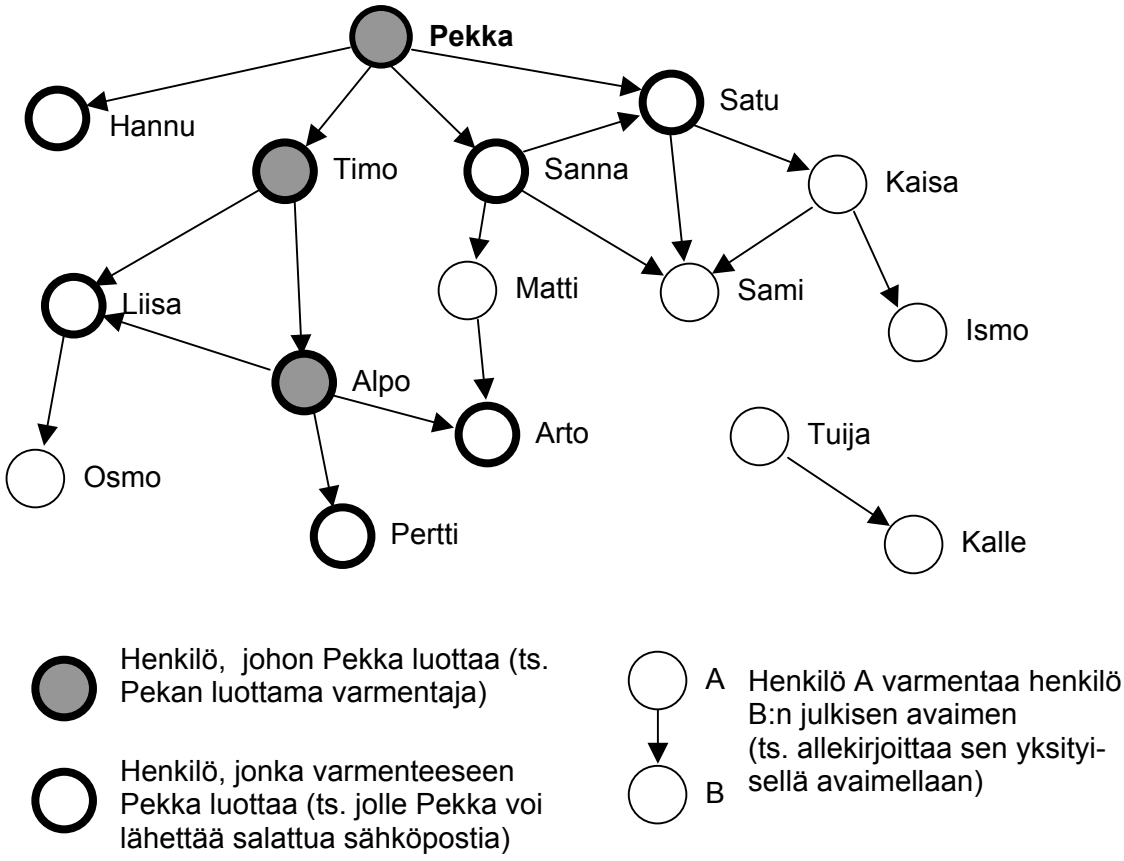
Näin syntyy useiden varmenteiden muodostamia ketjuja, joissa edellinen varmentaja varmentaa oman alivarmentajansa julkisen avaimen. Käytetyt varmennearkkitehtuurit on tässä jaettu varmenneketjujen topologian mukaan kahteen ryhmään: verkostomaisiin ja puumaisiin varmennearkkitehtuureihin. Laajemmin varmennearkkitehtuureja on käsitelty esimerkiksi lähteessä [PERL99].

5.4.1. Luottamusverkko

Luottamusverkon (web of trust) lähtökohtana on, että kaikki verkkoon kuuluvat henkilöt voivat toimia varmentajana, ja jokainen saa itse päättää, minkä varmentajan myöntämiin varmenteisiin hän luottaa. Luottamusverkko on "Internetin hengen" mukainen: siinä ei ole yksittäisiä solmupisteitä, joihin kaikki varmenteiden käyttäjät väistämättä joutuisivat luottamaan ja joiden mahdollinen haavoittuvuus näin muodostaisi riskitekijän. Luottamusverkon tunnettu sovellus on PGP (Pretty Good Privacy), joka on yhdysvaltalaisen Philip Zimmermannin luoma vapaalevit-

teinen, alkujaan sähköpostin ja muiden tiedostojen salaukseen ja allekirjoittamiseen tarkoitettu työkalu [PGP02].

PGP:n käyttämän varmennearkkitehtuurin periaatteita on selvennetty oheiseen kuvaan (Kuva 18) piirretyllä kuvitteellisella varmenneverkolla, jossa Pekkaa koskevat elementit on lisäksi korostettu. Jokaisella PGP:n käyttäjällä on (ainakin yksi) avainpari, jonka avulla hän voi paitsi vastaanottaa salattuja ja lähettää allekirjoitettuja sähköpostiviestejä, myös varmentaa eli allekirjoittaa toisten PGP:n käyttäjien julkisia avaimia. Kuvassa varmentamista on kuvattu nuolella; esimerkiksi Pekka on allekirjoittanut Hannun, Timon, Sannan ja Satun julkisen avaimen. Allekirjoituksellaan Pekka tuo julki, että nämä henkilöt hänen näkemyksensä mukaan ovat vastaavan yksityisen avaimen haltijoita. Vastaavasti Timo on allekirjoittanut Liisan ja Alpon julkiset avaimet, Liisa Osmon avaimen ja niin edelleen. Lopputuloksena on kuvan mukainen varmenteiden verkosto.



Kuva 18. Esimerkki luottamusverkosta.

On huomattava, että Pekka ei voi luottaa kaikkiin varmenneverkkoon kuuluviin henkilöihin, eikä edes heille myönnettyihin varmenteisiin. Pekan itse on valittava, kenen allekirjoittamiin varmenteisiin hän luottaa. Lähtökohtana on, että Pekka luottaa itseensä: koska Pekka on allekirjoittanut Hannun, Timon, Sannan ja Satun julkisen avaimen saatuaan ne henkilökohtaisesti heiltä itseltään, hän voi huoletta

käyttää syntyneitä varmenteita lähettääkseen heille sähköpostia. Lisäksi Pekka on päättänyt luottaa Timoon ja Alpoon: heidän rehellisyyteensä (etteivät he tieten tahtoen toimi vilpillisesti allekirjoittaessaan muiden julkisia avaimia) ja osaamiseensa (että heillä on riittävä osaaminen varmentajana toimimiseen). Kun Pekalla lisäksi on Timon varmennettu julkinen avain (jonka hän itse on allekirjoittanut) ja Alpon julkinen avain (jonka hänen luottamansa Timo on allekirjoittanut), voi Pekka luottaa paitsi itsensä, myös Timon ja Alpon allekirjoittamiin varmenteisiin. Niinpä Pekka voi lisäksi turvallisin mielin lähettää sähköpostia Liisalle, Alpolle, Artolle ja Pertille. Esimerkiksi Osmolle Pekka ei kuitenkaan voi lähettää salattua sähköpostia, koska Pekalla ei ole sellaista Osmolle kuuluvaa varmennetta, jonka hänen luottohenkilönsä olisi allekirjoittanut. Osmon varmenteen on allekirjoittanut Liisa, ja vaikka sekä Timo että Alpo ovat varmentaneet Liisan julkisen avaimen, se ei tarkoita, että Pekalla olisi syytä luottaa Liisaan ja hänen kykyynsä toimia varmentajana. Pekan luottamus Timoon ja Alpoon takaa pelkästään sen, että Liisan varmenteeseen sisältyvää julkista avainta vastaava yksityinen avain on Liisan hallussa.

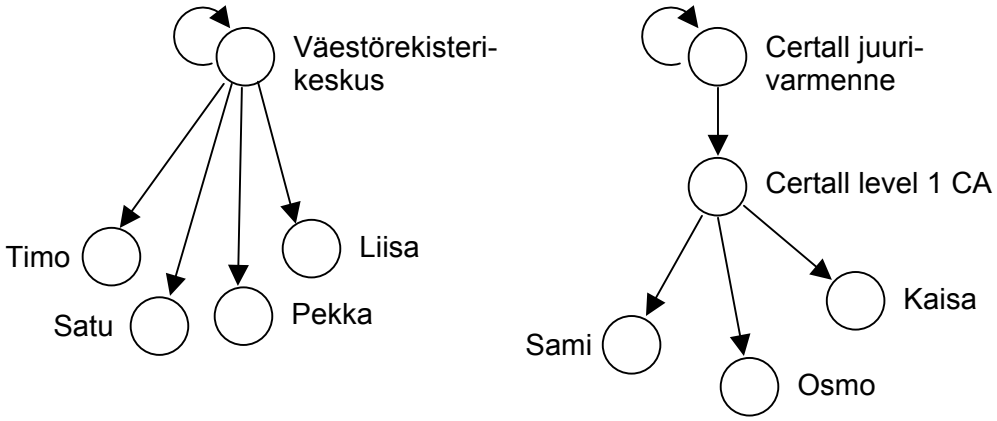
PGP tarjoaa monipuoliset työkalut varmenteiden ja luottamuksen hallintaan. Pekka voisi esimerkiksi määritellä luottavansa lisäksi osittain sekä Sannaan että Satuun, jonka seurauksena hän voisi pitää myös Samin varmennetta luotettavana. Kun vähintään kaksi osaksi luotettua henkilöä allekirjoittaa kolmannen henkilön julkisen avaimen, pidetään myös näin syntynyttä varmennetta luotettavana. Hienojakoisempiakin järjestelyjä voidaan ajatella: kuhunkin varmenteeseen voidaan esimerkiksi liittää lukuarvo, joka kuvaa Pekan luottamusta kyseiseen varmenteeseen. Samalla syntyvän luottamusverkon matematiikka kuitenkin monimutkaistuu. Yhden laskentamallin luottamuksen hallintaan on esittänyt Carroni [CARO00]. Audunin laskentamalli [AUDU99] huomioi lisäksi yhtenä laskennan parametrina Pekan epävarmuuden: Pekka on esimerkiksi vain 80-prosenttisen varma siitä, että Sanna ja Satu ovat osittain luotettavia.

Monipuolisuus tarkoittaa myös monimutkaisuutta. Nykyään Internetiä käyttää myös suuri joukko sellaisia henkilöitä, joiden ei voida olettaa olevan teknisesti riittävän valveutuneita käsittääkseen, mistä varmentamisessa ja luottamuksessa on kysymys. Niinpä varmentaminen tuntuu luontevalta jättää ammattilaisten tehtäväksi. Ammattimaisessa toiminnassa varmennearkkitehtuuri yleensä organisoituu verkoston sijaan puumaiseksi hierarkiaksi. Jatkossa tässä tutkimuksessa keskitytään lähinnä puumaisiin varmennearkkitehtuureihin.

5.4.2. Puumainen varmennearkkitehtuuri

Kaupallistuvassa Internetissä suuntaus on kohti laajamittaista ammattimaista varmentamistoimintaa ja sen myötä kohti puumaista varmennearkkitehtuuria. Tällöin varmentajana toimii esimerkiksi kaupallinen yritys, joka hankkii varmentamistoi-

mintaan tarvittavan erityisosaamisen ja -laitteiston ja myy varmennepalveluja asiakkailleen. On olemassa suuri määrä kaupallisia varmentajia kuten Verisign, Entrust ja Thawte. Tunnettuja kaupallisia suomalaisia varmentajia ovat Väestörekisterikeskus, Certall ja Sonera. Monet yritykset varmentavat itse sisäiseen käyttöön tarkoitettuja varmenteitaan.



Kuva 19. Puumaisen varmennearkkitehtuurin toteutusvaihtoehtoja

Puumaista varmennearkkitehtuuria on kuvattu ohessa (Kuva 19). Luottamuksen lähtökohta eli **juuri** (root) varmennehierarkiassa on varmentajan julkinen avain. Usein varmentaja allekirjoittaa julkisen avaimensa omalla yksityisellä avaimellaan, jolloin syntyy itseallekirjoitettu (self-signed) juurivarmenne. Tämä ei kuitenkaan ole välttämätöntä. Itseallekirjoitetun varmenteen tunnistaa siitä, että varmenteeseen sisältyvä varmentajan nimi ja varmenteen haltijan nimi ovat samat [HOUS01, s. 103].

Kaikki muut varmennehierarkiasta löytyvät varmenteet on allekirjoitettu joko varmentajan juureen liittyvällä yksityisellä avaimella (arkikielessä käytetään usein sinällään virheellistä ilmaisua "allekirjoitettu juurivarmenteella") tai tarkoitusta varten myönnettyyn alivarmentajan varmenteeseen liittyvällä yksityisellä avaimella. Esimerkiksi Väestörekisterikeskus allekirjoittaa Suomen kansalaisille myönnettävät kansalaisvarmenteet suoraan juurivarmenteeseensa liittyvällä yksityisellä avaimella, Certall puolestaan allekirjoittaa juurivarmenteeseen liittyvällä yksityisellä avaimella vain alivarmentajien varmenteita.

Varmenteisiin luottavan osapuolen tehtävä on varmennetta käyttäessään todentaa koko varmenteista muodostuva ketju juuresta alkaen. Ketjun jokaisen lenkin on oltava aito, voimassaoleva varmenne. Esimerkiksi kuvan Osmon varmenteeseen luottavan tulee ensiksi haalia käsiinsä Osmon varmenteen lisäksi myös molemmat Certallin varmenteet ja varmistaa Certallin juurivarmenteeseen liittyvän julkisen

avaimen avulla, että Certall Level 1 CA -varmenne on allekirjoitettu Certallin juurivarmenteeseen liittyvällä yksityisellä avaimella. Samalla periaatteella tarkistetaan, että Osmon varmenne on allekirjoitettu Certall Level 1 CA -varmenteeseen liittyvällä yksityisellä avaimella. Lisäksi tarkistetaan kaikkien varmenteiden voimassaolo.

Ongelmaksi muodostuu usein varmentajan juuri. Juuren mahdollinen itseallekirjoitus takaa vain, että allekirjoituksen tekijän hallussa on varmenteeseen liittyvä yksityinen avain, mutta ei, että allekirjoituksen on todella tehnyt kyseinen varmentaja. Kuka vain voi luoda avainparin, ja käyttää sen yksityistä avainta luodakseen itseallekirjoitetun varmenteen, jossa varmenteen väitetään vilpillisesti kuuluvan esimerkiksi Väestörekisterikeskukselle. Tämän jälkeen hän voi käyttää yksityistä avaintaan allekirjoittaakseen uusia varmenteita, jotka näyttävät Väestörekisterikeskuksen Suomen kansalaisille myöntämiltä varmenteilta. Petkutus onnistuu, jos varmenteeseen luottavalla osapuolella ei ole hallussaan Väestörekisterikeskuksen aitoa juurta, josta varmenneketjun todentaminen alkaa.

Varmenteeseen luottavan osapuolen tulee siis vielä käyttää jotain erityisjärjestelyä luotettavan juuren hankkimiseksi – hän voi esimerkiksi marssia levyke kädessä varmentajan toimipisteeseen pyytämään juurta kuten Timo edellä. Juuren saatuaan hän voi PGP:n antaman mallin mukaisesti halutessaan allekirjoittaa sen omalla yksityisellä avaimellaan, jolloin varmenneketju saa alkuunsa vielä yhden lenkin. Tällöin myös luottamusketjun ensimmäinen askel varmenteeseen luottavasta osapuolesta varmentajaan tulee ilmaistuksi eksplisiittisesti varmenteella, eikä juuren eheyden säilymisestä tarvitse enää olla huolissaan. Käytännössä harva käyttäjä kuitenkaan menettelee näin.

Monet kaupalliset varmentajat ovat tulleet kuluttajaa vastaan pyytämällä käyttöjärjestelmien valmistajia sisällyttämään juurensa käyttöjärjestelmän asennuslevykkeille – moni Windows-työaseman omistava peruskäyttäjä tuleekin todennäköisesti tietämättään luottaneeksi myös tässä asiassa Microsoftiin. Toimikortit tarjoavat varmentajien juurien luotettavaan jakeluun toisen vaihtoehdon, joka esitellään myöhemmin luvussa 6.1.

5.5. Julkisen avaimen järjestelmän osapuolet

Tähän mennessä on käsitelty lähinnä varmentajaa, varmenteita ja niistä muodostuvaa arkkitehtuuria. Tässä alaluvussa käydään läpi muutkin julkisen avaimen järjestelmän keskeiset komponentit. Esimerkkinä käytetään Suomen kansallista julkisen avaimen järjestelmää: Väestörekisterikeskuksen sähköistä henkilökorttia, sen yksityistä avainta varmentavaa kansalaisvarmennetta ja siihen kuuluvaa julkisen avaimen järjestelmää [VRK99]. Lähteenä on käytetty teosta [HOUS01 s. 43–52].

5.5.1. Varmentaja

Varmentajan tehtävä on allekirjoittaa varmenteet, joilla todistetaan tietyn yksityisen avaimen kuuluminen tietylle henkilölle. Varmenne sisältää haltijansa julkisen avaimen ja hänet yksilöivän tiedon, kuten nimen (jonka monikäsitteisyydestä aiheutuvaan ongelmaan palataan luvussa 5.9). Lisäksi varmenteeseen voidaan liittää myös koko joukko muuta tietoa. Varmentaja menee takuuseen myös muiden varmenteeseen sisältyvien tietojen oikeellisuudesta, esimerkiksi varmenteeseen liitetyn sähköpostiosoitteen kuulumisesta samalle henkilölle.

Yksi varmenteeseen sisältyvä tieto kertoo varmenteen voimassaoloajan. Esimerkiksi Väestörekisterikeskuksen kansalaisvarmenteet ovat tällä hetkellä voimassa kolme vuotta, jonka jälkeen varmenteen haltijan on haettava uusi sähköinen henkilökortti. Voi kuitenkin syntyä tilanteita, joissa varmenteen käyttö on estettävä jo ennen varmenteeseen kirjatun voimassaoloajan päättymistä. Yksityinen avain voi hukkua, paljastua, joutua vääriin käsiin, varmenteen tiedot voivat muuttua tai koko varmenne vain käydä tarpeettomaksi. Tällainen varmenne asetetaan **sulkulistalle** (certificate revocation list, CRL), joka on varmentajan digitaalisesti allekirjoittama ja julkaisema luettelo varmenteista, jotka on mitätöity ennen voimassaoloajan päättymistä. Uusi sulkulista julkaistaan säännöllisesti, esimerkiksi Väestörekisterikeskuksen sulkulista on voimassa kaksi tuntia kerrallaan.

Varmenteeseen luottava osapuoli – esimerkiksi Liisalle tämän varmenteella salatun viestin lähettävä Pekka – on velvollinen tarkistamaan aina ennen varmenteen käyttämistä, ettei kyseinen varmenne ole sulkulistalla. Tarkistaminen tapahtuu noutamalla sulkulista, todentamalla sen allekirjoitus ja varmistamalla, että mainittu varmenne ei löydy listalta. Myös vaihtoehtoisia menettelytapoja varmenteen voimassaolon tarkistamiselle on kehitetty: varmenteeseen luottava osapuoli voi esimerkiksi lähettää varmenteen erityiselle luotetulle OCSP (Open Certificate Status Protocol) -palvelimelle, joka tarkistaa kysyjän puolesta sulkulistan ja ilmoittaa varmenteen kelpoisuudesta [RFC2560].

Koska varmentajan yksityisiä avaimia käytetään muiden varmenteiden ja sulkulistojen allekirjoitukseen, muodostaa varmentajan yksityisen avaimen paljastuminen järjestelmän yhden keskeisen riskitekijän. Niinpä saattaa olla syytä esimerkiksi säilyttää varmentajan yksityistä avainta toimikortilla kassakaapissa, joka sijaitsee kallion sisään louhitussa luolassa. Yksityisen avaimen käyttäminen saattaa edellyttää esimerkiksi kahden valtuutetun henkilön läsnäoloa.

Varmentaja on kokonaisvastuussa varmentamistoiminnasta, mutta voi kuitenkin delegoida osan tehtävistään alihankkijoilleen. Esimerkiksi Väestörekisterikeskus ei itse ole järjestänyt ympärivuorokautista palvelunumeroa, joka ottaa vastaan pyyntöjä varmenteiden asettamisesta sulkulistalle, vaan sulkulistapalvelun toteuttaa

Luottokunta. Väestörekisterikeskus ei myöskään itse valmista eikä yksilöi sähköisiä henkilökortteja, vaan nämä tehtävät hoitaa sekä kortin sähköisen että muovisen osan osalta Setec. Näiden tehtävien lisäksi varmentajan keskeisiä alihankkijoita on rekisteröijä.

5.5.2. Rekisteröijä

Rekisteröijän (registration authority, RA) tehtävänä on varmistaa, että varmenteen tiedot pitävät paikkansa: että yksityinen avain on varmenteen haltijan hallussa ja että muutkin tiedot tulevat kirjatuksi varmenteeseen oikein. Rekisteröinti voi tapahtua verkon välityksellä, niin kuin monen sähköpostiosoitteen ja julkisen avaimen kytkevän varmentajan kohdalla toimitaankin. Varmennetta hakeva henkilö tilaa ja saa varmenteensa WWW:n kautta, ja varmennetta myönnettäessä sähköpostiosoitteen oikeellisuus tarkastetaan pyytämällä henkilöä vastaamaan lähetettyyn sähköpostiviestiin.

Sähköpostin avulla tai muuten verkon välityksellä tapahtuvaa rekisteröintiä ei tietenkään voi pitää kovin luotettavana. Varmenteen luotettavuutta parantaa henkilökohtaisesti kasvotusten tapahtuva rekisteröinti. Tällöin rekisteröijä todentaa varmenteen hakijan henkilöllisyyden jonkin luotettavana pidetyn asiakirjan, esimerkiksi passin tai muun henkilöllisyystodistuksen, avulla ja tarkistaa luotettavalla tavalla myös muut varmenteeseen liittyvät tiedot, kuten työnantajan nimen tai sähköpostiosoitteen.

Varmentajan toimintaperiaatteista riippuen varmenteen hakija voi joko itse luoda varmenteeseen tarvittavan avainparin ja tuoda siihen liittyvän julkisen avaimen varmennettavaksi tai avainparin luomisesta (esimerkiksi toimikortille) voi huolehtia varmentaja. Jos avainpari on varmenteen hakijan itsensä tekemä, rekisteröijä varmistaa, että varmenteen hakijalla todella on hallussaan esitettyyn julkiseen avaimeen liittyvä yksityinen avain. Jos avainpari on luotu varmentajan toimesta, rekisteröijän tehtävä on luovuttaa yksityisen avaimen sisältävä laite, kuten toimikortti, varmenteen hakijalle.

Varmentajan kannalta on luontevaa uskoa rekisteröijän tehtävät tarkoituksenmukaiselle taholle. Esimerkiksi Väestörekisterikeskus ei odota kansalaisvarmenteen hakijoiden pistäytyvän Helsingin Pasilassa sijaitsevassa toimistossaan, vaan sähköistä henkilökorttia voi hakea poliisilaitokselta, josta muutkin viranomaisen myöntämät tunnistamisasiakirjat jaetaan. Yrityksissä rekisteröijänä voi toimia esimerkiksi henkilöstöhallinto, joka on muutenkin tekemisissä työsuhdettaan aloittavien työntekijöiden kanssa.

5.5.3. Varmennehakemisto

Myönnetyt varmenteet ovat noudettavissa varmennehakemistosta. Liisalle viestin lähettävä Pekka voi noutaa Liisan varmenteen hakemistosta, jos tietää Liisan käyttämän varmentajan hakemiston sijainnin. Vaihtoehtoisesti hakemisto voidaan hajauttaa sälyttämällä varmenteiden jakaminen niiden haltijoiden kontolle. Tällöin Pekan tulee ensin pyytää Liisan varmennetta häneltä itseltään. Hakemistoa käytetään usein varmenteiden lisäksi myös sulkulistan jakamiseen.

Varmennehakemiston ylläpitäjän ei tarvitse olla rekisteröijän tavoin luotettu osapuoli. Koska varmenteet sisältävät jo itsessään digitaalisen allekirjoituksen, ei hakemiston epäluotettavakaan ylläpitäjä pysty kajoamaan niihin. Varmennehakemistoon liittyvät vaatimukset painottuvatkin palvelun saatavuuteen: varmentajan allekirjoittamien varmenteiden ja tuoreimman sulkulistan tulee olla varmenteisiin luottavan osapuolen saatavilla.

Varmennehakemisto voi olla joko kaikkien tai vain valtuutettujen henkilöiden saatavilla. Esimerkiksi Väestörekisterikeskuksen myöntämät kansalaisvarmenteet ovat yleisesti saatavilla `ldap.fineid.fi`-nimiseltä palvelimelta. Organisaation sisäiseen käyttöön tarkoitetun varmennehakemiston pääsyä voidaan rajoittaa sijoittamalla se organisaation palomuurin taakse ja asettamalla hakemistopalvelin vaatimaan käyttäjän henkilöllisyyden todentamista. Varmennehakemiston kanssa asioidaan tyypillisesti LDAP-protokollan välityksellä, joka esitellään myöhemmin.

5.5.4. Varmennearkisto

Varmenne, jonka voimassaoloaika päättyy, poistetaan varmennehakemistosta. Myös sulkulista poistuu hakemistosta, kun se syrjäytetään uudella, tuoreemmalla sulkulistalla. Sulkulistalle asetettu varmenne puolestaan poistuu sulkulistalta, kun varmenteeseen kirjattu voimassaoloaika päättyy.

Joskus voi syntyä tilanne, jossa varmenteen voimassaolon jo päätyttyä on pystyttävä selvittämään, oliko varmenne todellakin aito, voimassaoleva varmenne tiettynä ajan hetkenä (vai onko se ehkä tekaistu myöhemmin, kun esimerkiksi varmentajan yksityinen avain paljastui). Varmennearkiston tehtävä on varastoida myönnetyt varmenteet ja sulkulistat. Varmennearkistossa varmenteet ja sulkulistat suojataan fyysisillä toimenpiteillä niin, että niiden aitouteen ja eheyteen voidaan luottaa vielä varmenteiden voimassaolon päätyttyäkin.

5.5.5. Varmenteen haltija

On helppo unohtaa, että myös varmenteen haltija on yksi julkisen avaimen järjestelmän osa – hänen henkilöllisyytensä todentamista vartenhan koko järjestelmä lopulta on rakennettu. Varmenteen haltija on se henkilö tai muu toimija, jonka nimi on kirjattu varmenteessa varmenteen kohteeksi. Samalla varmenteen haltija on varmenteeseen liittyvän yksityisen avaimen hallussapitäjä.

Varmenteen haltijallakin on vastuita. Hänen tehtävänsä on parhaan kykynsä mukaan suojata yksityistä avaintaan hukkumiselta tai paljastumiselta. Jos näin kuitenkin pääsee tapahtumaan, tulee hänen heti ilmoittaa asiasta varmentajalle, joka asettaa varmenteen sulkulistalle. Varmenteen haltijan vastuu hukkuneen yksityisen avaimen väärinkäytöstä lakkaa tyypillisesti silloin, kun pyyntö varmenteen peruuttamisesta saapuu varmentajalle.

5.5.6. Varmenteeseen luottava osapuoli

Varmenteisiin luottavan osapuolen tulee aluksi tavalla tai toisella hankkia varmentajan juuri, josta varmenneketjun todentaminen voi alkaa. Varmenteeseen luottava osapuoli rakentaa varmenneketjun ja todentaa sen jokaisen lenkin aina varmenteen haltijan varmenteeseen saakka. Hän tarkistaa, että varmenteen allekirjoitukset on todellakin tehty ketjun edelliseen varmenteeseen liittyvällä yksityisellä avaimella ja että varmenne on voimassa eikä sitä ole asetettu sulkulistalle.

Varmenteisiin luottava osapuoli – Liisalle sähköpostia lähettävää Pekkaa tai Liisan käyttämän verkkokaupan ylläpitäjää – voi julkisen avaimen järjestelmän avulla varmistua, kenen kanssa hän on asioimassa turvattoman tietoverkon yli. Julkisen avaimen järjestelmä on siis olemassa nimenomaan varmenteisiin luottavaa osapuolta varten.

Toisaalta juuri tässä perusasetelmassa tiivistyy myös laajempi kysymys järjestelmän rakentamiskustannusten jakamisesta: normaalissa taloudellisessa toiminnassa rahalliseen panostukseen on yleensä halukas se taho, joka arvioi panostuksen kautta saavansa taloudellista hyötyä kuten kustannussäästöä. Väestörekisterikeskuksen sähköinen henkilökortti on yleistynyt hitaammin kuin valtionhallinnossa olisi toivottu, ja julkisuudessa on tuotu toistuvasti esiin, että kansalaisilla ei ole riittäviä kannustimia 29 euron hintaisen kortin hankkimiseen. Sähköisestä henkilökortista hyötyy lähinnä sähköisiä palvelujaan automatisoiva julkishallinto, jolle kansalaisvarmenteen käyttäjät tuovat kustannussäästöä. Työntekijöilleen varmennekortit hankkivassa yrityksessä kustannukset ja kortista saatava hyöty sen sijaan osuvat yksiin: työnantaja vastaa kortin käyttöönoton koulutuksesta, tuesta ja kustannuksis-

ta, mutta odottaa myös saavansa investoinnille vastinetta esimerkiksi kasvavan tietoturvallisuuden myötä.

5.6. Varmennepolitiikka

Edellä esitetyssä esimerkissä Pekan luottamus Timoon perustui siihen, että Pekka tunsi Timon henkilökohtaisesti ja sen perusteella koki hänet luotettavaksi. Timo saattoi olla esimerkiksi Pekan lapsuudenystävä, jonka kanssa hän oli aina jakanut ilot ja surut. Lisäksi Pekka ehkä tiesi Timon olevan riittävän terävä ja valveutunut myös varmenteisiin liittyvissä asioissa selviytyäkseen luotetun kolmannen osapuolen tehtävistä. Luottamus ammattimaisiin varmentajiin ei kuitenkaan voi perustua lapsuudenkokemuksiin, vaan sen takaaminen tapahtuu lainsäädäntötasolla tai sopimusteitse. Luottamuksen välikappaleena käytetään yleisesti kahta dokumenttia: varmennepolitiikkaa ja varmennekäytäntölausumaa, joiden merkitykselle ja roolijaolle on käytössä erilaisia tulkintoja. Tässä esitetyn lähteenä on käytetty teosta [HOUS01, s. 184–185].

Varmentajan tehtävänä on julkaista **varmennepolitiikka** (certificate policy, CP), joka esittelee varmentajan keskeiset toimintaperiaatteet, joihin varmentaja toiminnassaan sitoutuu. Varmennepolitiikka kuvaa varmentajan toimintaperiaatteita melko yleisellä tasolla menemättä yksityiskohtiin. Tällä pyritään siihen, että varmennepolitiikka olisi hyvin staattinen asiakirja, jonka muuttamiseen on tarvetta harvoin. Varmenteeseen luottava osapuoli arvioi varmentajan myöntämien varmenteiden luotettavuutta juuri varmennepolitiikan perusteella.

Varmennekäytäntölausuma (certificate practices statement, CPS) on varmennepolitiikan toteutussuunnitelma, joka konkretisoi varmennepolitiikan määrittelemät toteutusperiaatteet yksityiskohtaisiksi käytännöiksi ja toimintatavoiksi. Varmennekäytäntölausuma menee tarkastelussaan yksityiskohtiin, joten se on alttiimpi muutoksille kuin varmennepolitiikka. Varmennekäytäntölausuma ei välttämättä ole julkinen, koska yksityiskohtien – esimerkiksi tietystä tehtävistä vastaavan henkilön nimen – julkisuus saattaisi tarjota pahantahtoisille tahoille otollisen pisteen, johon varmentajaa vastaan tehtävä hyökkäys voitaisiin kohdistaa.

Jotta eri varmentajien varmennepolitiikat ja -käytännöt olisivat helpommin vertailtavissa, määrittelee RFC2527 [RFC2527] puitteet Internetissä käytettäville varmennepolitiikoille ja -käytäntölausumille. RFC2527 määrittelee kahdeksan pääluvun alle jakaantuvan asiakirjapohjan, jota sovelletaan sekä varmennepolitiikkaan että -käytäntöön. Tässä esitetyn lähteenä on käytetty teoksia [HOUS01] ja [RFC2527] ja suomennoksien osalta [VRK99].

Varmennepolitiikan ja -käytäntölausuman ensimmäinen luku on **johdanto**, joka luo yleiskatsauksen kyseisen varmentajan myöntämiin varmenteisiin, niiden haltijoihin ja käyttötarkoituksiin sekä varmennearkkitehtuuriin. **Yleiset ehdot** -luku käsittelee muun muassa eri osapuolten velvollisuuksia, vastuita ja heidän maksettavakseen lankeavia maksuja sekä tietojen, kuten varmenteiden, julkistamista. Lisäksi luku käsittelee varmentajan toiminnan auditoinnin järjestämistä. Auditoinnilla pyritään varmistamaan, että varmennepolitiikka on pantu asianmukaisesti täytäntöön. Nämä tiedot ovat tärkeitä muun muassa ristiinvarmentamisen kannalta.

Kolmas luku käsittelee **varmenteen hakijan tunnistamista**. Kuten edellä todettiin, varmenteen luotettavuus riippuu pitkälti tavasta, jolla varmenteen hakija on tunnistettu ja hänen henkilöllisyytensä todennettu – kasvotusten tapahtuva todentaminen tekee varmenteesta luotettavamman kuin esimerkiksi sähköpostitse suoritettu todentaminen. Luvussa esitetään myös toimintaperiaate varmenteen uusimiseksi ja asettamiseksi sulkulistalle. **Toiminnalliset vaatimukset** -luku käsittelee muun muassa varmenteen myöntämiseen ja varmentajan toimintaan liittyviä muita vaatimuksia, kuten varmenteen myöntämisen ja sulkulistalle asettamisen perusteita, arkistoinnin periaatteita ja käytäntöjä sekä toimintaa varmentajan toiminnan päättyessä tai varmentajan yksityisen avaimen paljastuessa.

Varmentajan toiminta on paljon muutakin kuin tekniikkaa. **Fyysiset, toiminnalliset ja henkilöstöä koskevat turvatoimet** -luvussa käsitellään muun muassa varmentajan toimitilan suojausta vesivahingoilta ja murtomiehiltä, varmentajan sisäistä valvontaa, kuten kriittisten työtehtävien eriyttämistä useamman työntekijän harteille, ja varmentajan palkkaaman henkilökunnan luotettavuuden arvioimista esimerkiksi Suojelupoliisin antaman luotettavuuslausunnon avulla. **Tekniset turvatoimet** kuvaavat tietojärjestelmien, erityisesti varmentajan ja varmenteen haltijan yksityisen avaimen, suojausta. Luvussa muun muassa kerrotaan, tallennetaanko yksityinen avain esimerkiksi toimikortille, otetaanko siitä varmuuskopioita ja voidaanko avaimen varmuuskopio vaadittaessa pakkoluovuttaa esimerkiksi viranomaisille (key recovery, government access to keys).

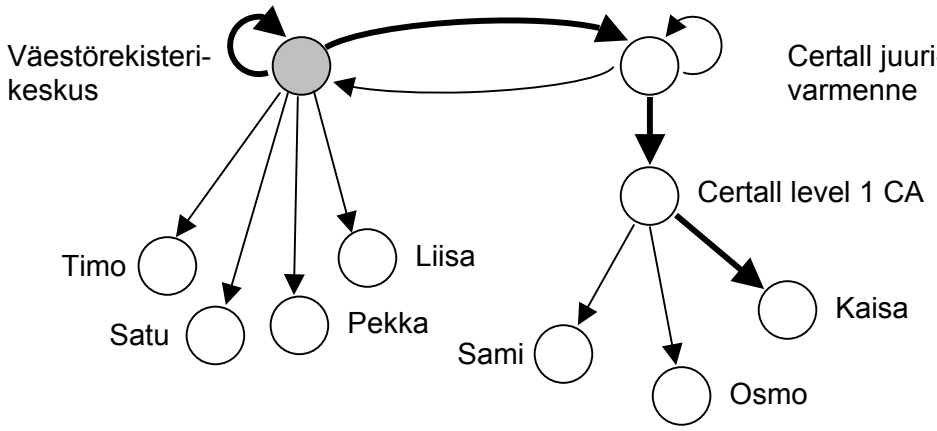
Seitsemännessä luvussa määritellään kyseisen varmentajan käyttämä **varmenne- ja sulkulistaprofiili**, jossa esitellään varmenteiden ja sulkulistan kenttien rakenne ja merkitys. Viimeisessä luvussa esitetään **varmennepolitiikan hallinnointi**, jossa kuvataan menettelytapa kyseisen varmennepolitiikan tai -käytäntölausuman muuttamiseksi.

5.7. Ristiinvarmennus

Ei näytä kovinkaan todennäköiseltä, että kaikki Internetin käyttäjät koskaan päätyisivät yhden tai edes muutaman varmentajan asiakkaiksi. Kaupallisten varmenta-

jien lisäksi monet yritykset ja organisaatiot ovat itse asettaneet oman varmentajansa, joka myöntää varmenteita yrityksen työntekijöille tai asiakkaille. Verkon käyttäjillä on kuitenkin tarve viestiä myös sellaisten henkilöiden kanssa, joiden varmenteen on antanut joku muu varmentaja kuin hänen itse käyttämänsä. Tällöin henkilöt kuuluvat eri varmennehierarkiaan.

Palataan esimerkkiin puumaisista varmennehierarkioista (Kuva 19 sivulla 50) ja oletetaan, että Pekka haluaa lähettää salaisen viestin Kaisalle. Voidaan tietysti ajatella, että Pekka tavalla tai toisella hankkisi Certallin aidon juurivarmenteen, josta alkavan varmenneketjun avulla hän pystyisi todentamaan myös Samin, Osmon ja Kaisan varmenteet ja lähettämään heille salattuja viestejä. Jos varmentajia on kuitenkin lukuisia, tehtävä tulisi ennen pitkää ylivoimaiseksi Pekalle; varsinkin, kun pelkkä juurivarmenteen hankkiminen ei riitä, vaan Pekan pitäisi myös tutustua varmentajan varmennepolitiikkaan.



Kuva 20. Kuvitteellinen tilanne: Väestörekisterikeskus ja Certall ovat ristiinvarmentaneet toistensa juurivarmenteet.

Onneksi varmentaja voi hoitaa asian Pekan ja kaikkien muidenkin varmenteenhaltijoiden puolesta. Väestörekisterikeskus voi hankkia Certallin juurivarmenteen ja allekirjoittaa sen julkisen avaimen omalla allekirjoitusavaimellaan. Jos Certall menettelee samalla tavalla Väestörekisterikeskuksen juurivarmenteen kanssa, ovat Väestörekisterikeskus ja Certall ristiinvarmentaneet toistensa juurivarmenteet (Kuva 20). Nyt Pekka voi rakentaa varmenneketjun (lihavoitu kuvassa), joka alkaa hänen luottamastaan Väestörekisterikeskuksen juurivarmenteesta (varjostettu kuvassa) ja päätyy Certallin juurivarmenteen kautta Kaisaan.

Kuvan esimerkki on kuvitteellinen, ja sen toteutumisen tiellä eivät niinkään ole tekniset ongelmat. Juurivarmenteita ristiinvarmennettaessa tullaan ottaneeksi kantaa paitsi varmentajan juuren aitouteen, myös varmentajien varmennepolitiikkojen yhteismitallisuuteen. Jos esimerkiksi Väestörekisterikeskuksen varmennepolitiikka edellyttää, että varmenteen haltija käy hakemassa toimikorttinsa henkilökohtaisesti

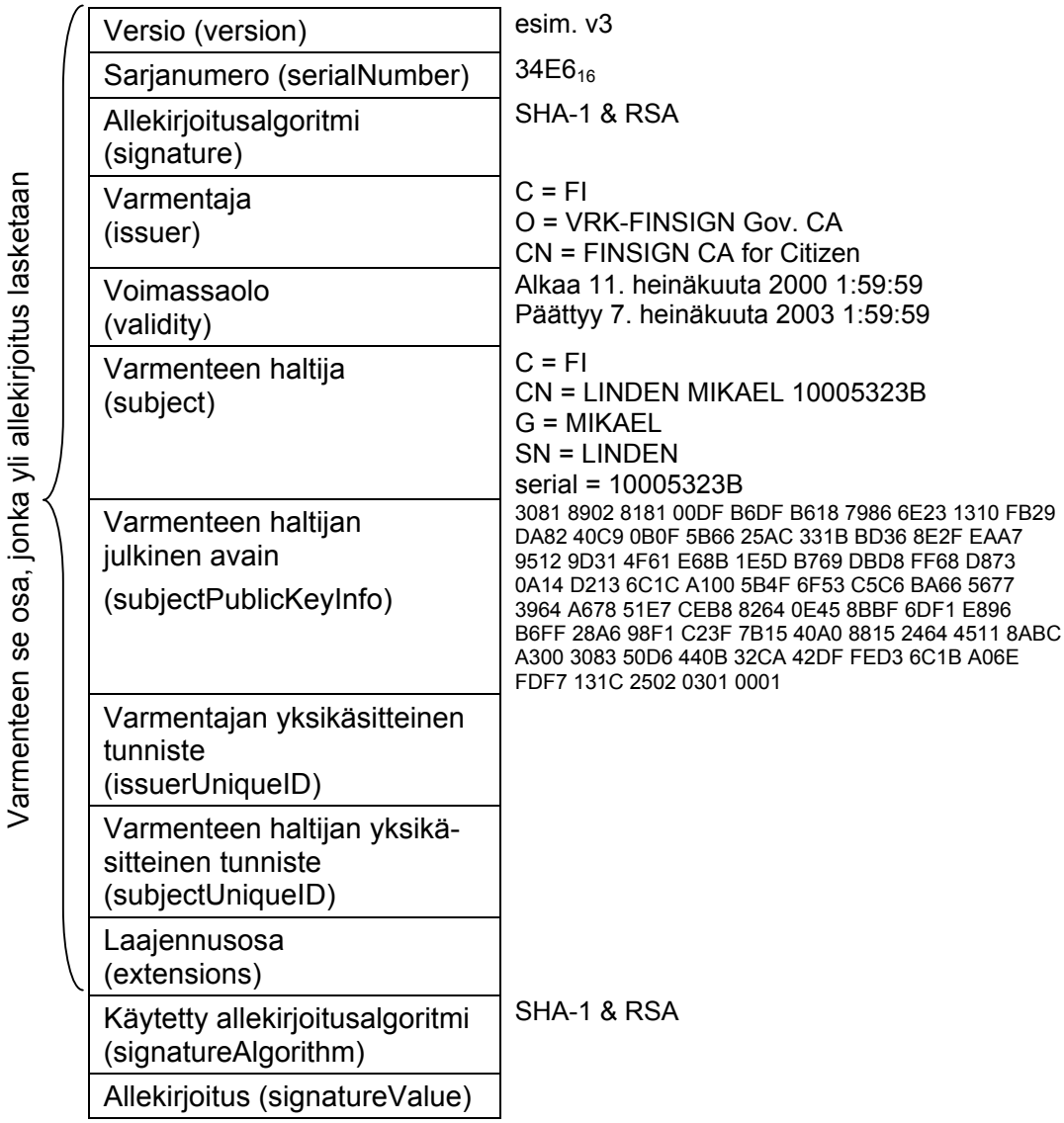
poliisilaitokselta, mutta Certallin varmennepolitiikka sallii myös muut ratkaisut, voi Väestörekisterikeskus katsoa, että Certallin myöntämät varmenteet eivät ole yhtä luotettavia kuin heidän omansa. Niinpä ristiinvarmentamisessa huomio kiinnittyykin osapuolien toimintatapojen ja sitä kautta varmennepolitiikkojen vertailemiseen.

Ristiinvarmenteiden lisääntyessä varmenneketjun rakentaminen vaikeutuu. Vaikka Pekan luottamasta Väestörekisterikeskuksen juurivarmenteesta olisikin olemassa varmenneketju Outin varmenteeseen, sen löytäminen voi olla vaikeaa: Väestörekisterikeskus on esimerkiksi voinut ristiinvarmentaa varmentajan X, joka on ristiinvarmentanut varmentajan Y, joka on allekirjoittanut Outin varmenteen. Pekalla saattaa olla suuri työ löytää kyseinen varmenneketju ja haalia siihen kuuluvat varmenteet – ristiinvarmenteista muodostuu luvussa 5.4.1 esitetyn kaltainen luottamusverkko. Yksi väline ristiinvarmentamistilanteiden hallitsemiseen on siltavarmentaja (bridge CA), jota on esitelty muun muassa lähteessä [HOUS01, s. 64–66].

5.8. X.509v3-varmenteet

Varmenne on varmentajan digitaalisesti allekirjoittama todiste, joka sitoo tietyn julkisen avaimen tietyn henkilön nimeen. Jotta varmenteesta olisi hyötyä, on eri osapuolten pystyttävä lukemaan ja ymmärtämään sen sisältämät tiedot: varmenteen muoto täytyy standardoida. ITU-T:n (International Telecommunication Union) standardoiman X.500-hakemiston yhteydessä on myös määritelty varmenteen esitystapa, joka tunnetaan nimellä X.509 [X50900]. Suurin osa Internetissä nykyisin käytetyistä ammattimaisten varmentajien myöntämistä varmenteista on standardin kolmannen version mukaisia X.509v3-varmenteita. RFC2459 [RFC2459] täsmentää X.509v3-standardia rajaamalla niitä periaatteita, joiden mukaisesti X.509v3-varmenteita voidaan käyttää myös Internetissä.

X.509-varmenteeseen sisältyviä tietoja kutsutaan kentiksi, ja niitä on määritelty lähes kolmekymmentä. Osa kentistä on pakollisia (esimerkiksi varmenteen haltijan nimi), osa vapaaehtoisia (esimerkiksi varmennetta myönnettäessä käytetyn varmennepolitiikan tunnus). X.509-varmenteen tietosisältö esitetään toimikorteissa ja tietoliikenteessä laajemminkin käytetyn ASN.1-notaation ja DER-koodauksen avulla. X.509v3-varmenteen sisältö on esitetty ohessa (Kuva 21), laajempi esimerkki varmenteesta on liitteenä. Tässä yhteydessä käydään läpi lähinnä varmenteen peruskentät, laajennukset käydään läpi vain ryhmittäin. Lähteenä on käytetty [HOUS01].



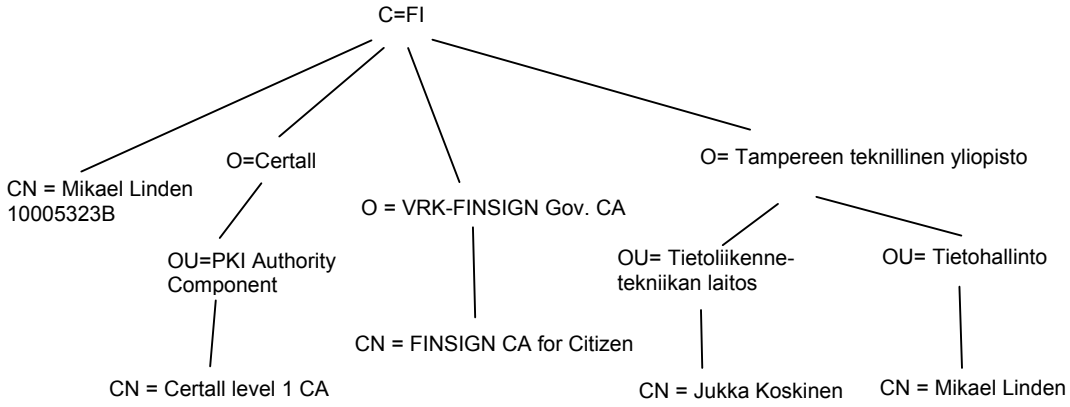
Kuva 21. X.509v3-varmenteen rakenne ja esimerkki.

Versio-kenttä ilmaisee yksinkertaisesti, mistä varmenteen versiosta on kyse. Tällä hetkellä käytössä ovat versiot v1, v2, v3 ja v4. Varmenteen **sarjanumero** on varmentajan kyseiselle varmenteelle antama yksikäsitteinen juokseva numero. Jokaisella yhden varmentajan myöntämällä varmenteella tulee olla eri sarjanumero. **Allekirjoitusalgoritmi**-kenttä ilmaisee, mitä tiiviste- ja salausalgoritmia varmentaja on käyttänyt allekirjoittaessaan varmennetta. Sama kenttä löytyy myös varmenteen lopusta.

Varmentaja-kenttä yksilöi kyseessä olevan varmenteen myöntäjän. Varmenne on allekirjoitettu varmentajan yksityisellä avaimella. **Varmenteen haltija** on kyseisen varmenteen kohde – joko alivarmentaja tai loppukäyttäjä. Varmenteen oleellinen tehtävä on sitoa varmenteen haltija -kenttä **varmenteen haltijan julkinen avain** -kenttään, joka sisältää itse julkisen avaimen lisäksi myös tunnisteen salausalgorit-

mille (esim. RSA), johon kyseinen avain sopii. Varmentajalle ja varmenteen haltijalle voidaan lisäksi antaa vaihtoehtoisia nimiä varmenteen laajennuskentissä.

Varmentaja ja varmenteen haltija – oli kyseessä sitten organisaatio tai luonnollinen henkilö – yksilöidään X.500-standardin käyttämän DN (distinguished name) -nimeämiskäytännön mukaisesti. DN koostuu hierarkkisista osista; ajatus on, että hierarkian jokainen taso hallinnoi itse omaa nimiavaruuttaan. Tavallisesti käytettyjä hierarkian tasoja ovat maatunnus C (country), organisaatiotunnus O (organization), organisaatioyksikkö OU (organizational unit) ja nimi CN (common name). Tuloksena on oheisen kuvan kaltainen hierarkia (Kuva 22).



Kuva 22. Distinguished name muodostuu hierarkkisista osista.

X.500-hakemiston filosofia perustuu siihen, että maailmassa olisi yksi suuri X.500-hakemisto, josta jokainen olio (esim. henkilö, organisaatio tai palvelin) löytäisi oman paikkansa. Koska yhtä suurta X.500-hakemistoa ei ainakaan vielä ole saatu rakennetuksi, vaihtoehtoisena nimeämiskäytäntönä on esitetty myös Internetin domain-nimiin perustuvaa hierarkiaa (esimerkiksi DC=fi, DC=tut, CN=Mikael Linden), joka on laajassa käytössä ja siten luonnollinen tapa hallita Internetin nimiavaruutta.

Voimassaolo-kenttä ilmaisee varmenteen voimassaoloajan: milloin varmenteen voimassaolo alkaa ja koska se päättyy. Ajan esityksessä suositellaan käytettävän UTC-aikaa. **Varmentajan yksikäsitteinen tunniste** ja **varmenteen haltijan yksikäsitteinen tunniste** ovat kenttiä, joita ei suositella käytettävän enää X.509:n version 3 varmenteissa.

Ryhmä	Sisältö muun muassa
Varmenteen haltijan tyyppi	Onko varmenteen haltija alivarmentaja vai loppukäyttäjä?
Vaihtoehtoiset nimet	Millä muulla nimellä varmentaja tai varmenteen haltija tunnetaan?
Avaimeen liittyvät attribuutit	Mihin tarkoituksiin varmennettua julkista avainta voidaan käyttää? Miten erottaa avaimet toisistaan?
Varmennepolitiikka	Minkä varmennepolitiikan puitteissa varmenne on myönnetty?
Muut tiedot	Mistä sulkulista on noudettavissa?

Taulukko 1. X.509v3-varmenteen laajennuskenttien jaottelu.

X.509-standardin kolmas versio toi mukanaan joukon laajennuksia, jotka voidaan jaotella viiteen ryhmään (Taulukko 1) [HOUS01]. Ensimmäiseen ryhmään kuuluvat kentät, joiden avulla varmenteesta voidaan päätellä, onko sen haltija varmentaja vai loppukäyttäjä. Tämän kentän avulla varmentaja voi estää loppukäyttäjää ryhtymästä alivarmentajaksi tämän varmenteen turvin. Toiseen ryhmään kuuluvat muun muassa kentät, joiden avulla varmentajalle tai varmenteen haltijalle voidaan esittää peruskenttiin nähden vaihtoehtoisia nimiä. On hyvin yleistä, että esimerkiksi varmenteen haltijan sähköpostiosoite esitetään tässä kentässä, ja luvussa 7.4 tullaan toteamaan, että itse asiassa monet sähköpostiasiakasohjelmat jopa vaativat sitä. Windows 2000 -käyttöjärjestelmän sisäänkirjautuminen puolestaan edellyttää, että tähän kenttään on talletettu varmenteen haltijan käyttäjätunnus (username@domain).

Kolmanteen ryhmään on koottu tietoa varmenteeseen sisältyvän julkisen avaimen ominaisuuksista, kuten sen käyttötarkoituksista. On tavallista ja turvallisuuskysymysten varjolla perusteltua, että tiettyä avainparia saa käyttää vain tiettyyn tarkoitukseen. Esimerkiksi Väestörekisterikeskuksen sähköinen henkilökortti sisältää itse asiassa kaksi yksityistä avainta ja varmennetta, joista toiselle käyttötarkoitukseksi on asetettu kiistämättömyys (non-repudiation) ja toiselle muu digitaalinen allekirjoitus, avaimen kuljetus ja tiedoston salaaminen. Kiistämättömyysvarmennetta käytetään, kun varmenteen haltija haluaa ilmaista sitoutumisensa esimerkiksi sopimukseen. Muuta digitaalista allekirjoitusta puolestaan sovelletaan esimerkiksi haaste/vaste-todentamisessa, kun varmenteen haltijan tulee allekirjoittaa esitetty haaste yksityisellä avaimellaan. Jos kiistämättömyysavainta käytettäisiin myös haasteen allekirjoittamiseen, voisi haasteen esittäjä valita satunnaisluvun sijaan haasteeksi esimerkiksi tiivisteen sopivasta viestistä, johon hän haluaisi todennettavalta sitoutumisen. Lisäksi avainparien pyhittäminen eri käyttötarkoituksiin mahdollistaa niiden erilaisen hallinnoinnin. Esimerkiksi salatun sähköpostin avaamisen tarkoitetusta yksityisestä avaimesta voidaan haluta ottaa varmuuskopio, jotta sähköpostit olisivat avattavissa yksityisen avaimen hukkumisesta huolimatta. Kiistä-

mättömyyteen käytettävästä yksityisestä avainparista ei sen sijaan tulisi ottaa varmuuskopioita.

Neljänteen ryhmään on koottu tietoa varmennepolitiikoista, joiden puitteissa kyseinen varmenne on myönnetty. Jos varmenne ristiinvarmentaa toisen varmentajan, voidaan eri varmentajien käyttämien varmennepolitiikkojen vastaavuuksia osoittaa näiden kenttien avulla. Viidenteen ryhmään kuuluvat kentät tarjoavat tietoa muun muassa sulkulistan sijainnista.

5.9. Nimiavaruuksien ongelma

Normaalissa elämässä ihmiset ovat oppineet käyttämään toisistaan nimiä, mutta julkisen avaimen järjestelmässä tietoverkkoa käyttävän ihmisen henkilöllisyyttä edustaa teknisessä mielessä julkinen avain. Tätä taustaa vasten on luontevaa, että tietoverkossa käytetään normaalisti henkilövarmenteita, jotka sitovat julkisen avaimen henkilön nimeen. *Ihmiset* ajattelevat tietävänsä, kenestä verkon käyttäjästä on kyse, kun he tietävät hänen nimensä.

Kun siirrytään yksittäisen ihmisen tuttavapiiristä laajempiin yhteisöihin (kuten Internet), on ihmisiä kuitenkin niin paljon, että henkilön nimi ei enää kelpaa henkilön tunnisteeksi. Nimet eivät ole yksikäsitteisiä, vaan käyttäjillä voi olla lukuisia täyskaimoja – pelkästään Tampereen puhelinluettelon kotinumerohakemistosta löytyy 18 Matti Virtasta [SOON01]. Yksikäsitteisiä tunnisteita tarvitaan kuitenkin eri tilanteissa, ja esimerkiksi Suomen valtio on antanut henkilötunnuksen Suomen kansalaisten ja Suomessa pysyvästi asuvien ulkomaalaisten tunnisteeksi, jota hyödyntävät julkishallinnon lisäksi myös muun muassa pankit (Kuva 2 sivulla 7).

Jokainen tunniste voi olla on yksikäsitteinen vain antajansa vallassa olevassa nimiavaruudessa, joskin laajempaan ja jopa maailmanlaajuiseen yksikäsitteisyyteen voidaan pyrkiä tuomalla nimiavaruuksiin hierarkiaa. Puhelinnumero on yksikäsitteinen yhden telealueen sisällä, mutta telealueesta toiseen voidaan soittaa liittämällä numeroon suuntanumero. Sähköpostinimi mikael.linden on yksikäsitteinen vain Tampereen teknillisen yliopiston piirissä, mutta postinimi mikael.linden@tut.fi koko Internetin SMTP-protokollaa käyttävässä postijärjestelmässä. Koko maailman kattava X.500-hakemisto, johon edellisessä luvussa viitattiin, tarjoaisi myös yksikäsitteisen DN-nimeämiskäytännön, mutta hakemisto näyttää kaatuvan omaan mahdottomuuteensa.

Omat ongelmansa syntyvät tilanteissa, joissa yksikäsitteiset tunnisteet muuttuvat. Henkilö, hänen sitoumuksensa ja valtuutensa säilyvät yleensä samana, vaikka hänen nimensä, käyttäjätunnuksensa tai sähköpostiosoitteensa vaihtuisikin. Vapautuneita tunnisteita voidaan antaa uudelleen eri henkilöille, mistä seuraa ongelmia:

esimerkiksi matkapuhelinliittymän avaaja voi (tämän tutkimuksen tekijän tavoin) yllättyä ikävästi huomatessaan, että puhelinnumeron edellinen haltija on ollut runsaasti asiakaskontakteja omistanut myyntimies.

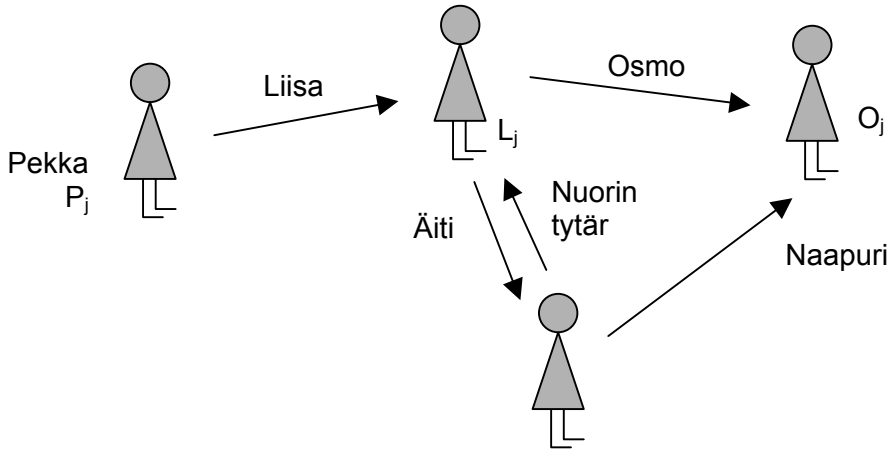
Myös julkisen avaimen järjestelmän rakentajat ovat joutuneet ottamaan kantaa täyskaimojen muodostamaan ongelmaan, ja eri tavoin on koitettu varmistaa, että kaksi eri varmenteen haltijaa voidaan luotettavasti erottaa toisistaan. Väestörekisterikeskuksen ratkaisu nojaa väestötietojärjestelmään, johon jokaiselle Suomen kansalaiselle tai Suomessa vakinaisesti asuvalle ulkomaalaiselle voidaan kirjata yksikäsitteinen sähköinen asiointitunnus (SATU). Sähköinen asiointitunnus liitetään varmenteen haltijan CN-kenttään (esimerkiksi ”Mikael Linden 10005323B”). Vaikka Väestörekisterikeskus myöntäisi varmenteen haltijalle uuden varmenteen tai varmenteen haltijan nimi vaihtuisi, voidaan sähköisen asiointitunnuksen avulla päätellä kysymyksessä olevan sama henkilö. Jotkut varmentajat käyttävät yksilöivänä tunnisteena sähköpostiosoitetta, organisaation sisäiseen käyttöön tarkoitetuissa varmenteissa luonteva yksilöivä tieto voi olla esimerkiksi organisaation sisäinen henkilönumero.

Yksikäsitteisten tunnisteiden hallinnointi on joka tapauksessa hankalaa ja monen mielestä myös tarpeetonta. On tehty aloitteita, että yksikäsitteisistä tunnisteista luovuttaisiin, ja julkisen avaimen järjestelmä ja sitä hyödyntävät järjestelmät rakennettaisiin paikallisten tunnisteiden varaan. Tunnettuja paikallisten nimiavaruuksien puolestapuhujia ja hyödyntäjiä ovat SDSI (Simple Distributed Security Infrastructure) [RIVE96] ja SPKI (Simple Public Key Infrastructure) [RFC2693].

Paikallisessa nimiavaruudessa lähtökohdaksi otetaan, että tietyllä nimellä on tietty merkitys vain nimen antajalle: Luvun 5.2 esimerkissä nimi 'Liisa' tuo Pekalle mieleen sen neidin, jolle hän halusi lähettää salaisen viestin, mutta muille nimi 'Liisa' tarkoittaa todennäköisesti aivan eri henkilöä. Jos halutaan ilmaista, että kysymys on nimenomaan siitä Liisasta, jonka kanssa Pekalla on kirjeenvaihtoa, voidaan Liisa nimetä 'Pekan tuntema Liisa'. Liisa puolestaan tuntee Osmon, joka voidaan nimetä 'Pekan tunteman Liisan tuntema Osmo', ja näin paikallisista nimiavaruuksista voidaan muodostaa ketjuja, jotka ovat aina suhteellisia ensimmäiseen lenkkiinsä. Yhtä nimiavaruutta hallinnoivaa tahoa ei tarvita.

Jos epäsymmetrisiä avainpareja generoiva algoritmi on laadukas, on todennäköisyys sille, että kahdella verkon oliolla olisi sama avainpari, olematon. Niinpä julkisen avaimen järjestelmässä jokaisella oliolla on automaattisesti ainakin yksi yksikäsitteinen tunniste: hänen julkinen avaimensa, johon paikalliset nimiavaruudet voidaan ripustaa. Nyt Pekka voi allekirjoittaa yksityisellä avaimellaan väitteen "tuntemaani Liisaa edustaa julkinen avain L_j" ja Liisa voi menetellä samoin Osmon

kanssa. Lopputuloksena on paikallisia nimiavaruuksia hyödyntävä varmenneverkko, jota muun muassa roolivarmenteet hyödyntävät.



Kuva 23. Esimerkki paikallisista nimiavaruuksista.

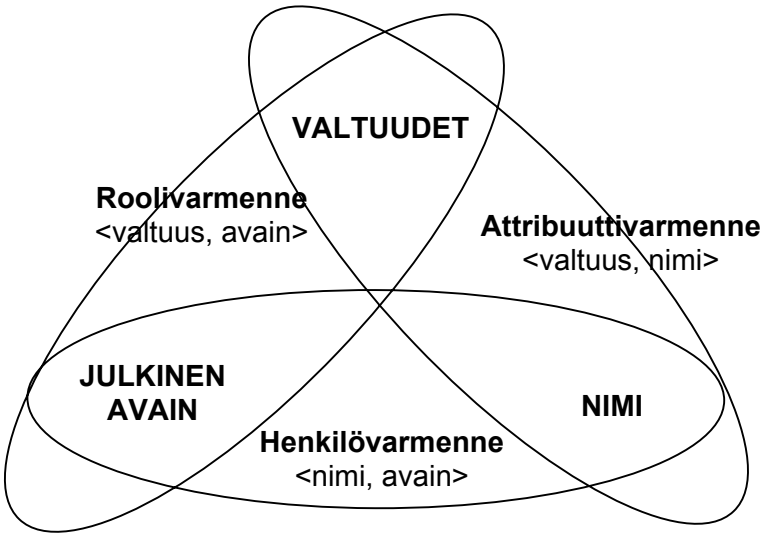
Esimerkiksi oheisessa kuvassa (Kuva 23) on esitetty tilanne, jossa 'Pekan tunteman Liisan tuntema Osmo' on itse asiassa 'Pekan tunteman Liisan äidin naapuri'. Jos Liisan äidillä on useita naapureita, viittaa nimi 'Liisan äidin naapuri' itse asiassa ryhmään. Liisa (tai muu asiasta kiinnostunut) voi vertailla Liisan äidin naapurien ja Osmon julkisia avaimia todetakseen, onko Liisan tuntema Osmo tosiaan hänen äitinsä naapuri.

5.10. Rooli- ja attribuuttivarmenteet

Henkilövarmenne sitoo julkisen avaimen haltijansa nimeen, mitä tarkastelukulmaa tässäkin tutkimuksessa pääosin sovelletaan. Tietoverkossa pääsynvalvontaa suorittavaa verkkolaitetta ei kuitenkaan viime kädessä kiinnosta varmenteen haltijan nimi vaan se, tuleeko kyseiselle käyttäjälle sallia pääsy verkon resurssiin. Kuten luvussa 2.2.3 todettiin, tämä hoidetaan perinteisesti todentamalla ensin käyttäjän henkilöllisyys (esimerkiksi julkisen avaimen ja sopivan haaste/vaste-protokollan avulla) ja sen jälkeen selvittämällä esimerkiksi käyttöoikeudet sisältävän pääsylistan avulla, mihin resursseihin kyseinen käyttäjä on valtuutettu pääsemään käsiksi. Pääsynvalvonta suorittaa siis seuraavanlaisen päättelyketjun:

Julkinen avain –> käyttäjän nimi –> valtuudet

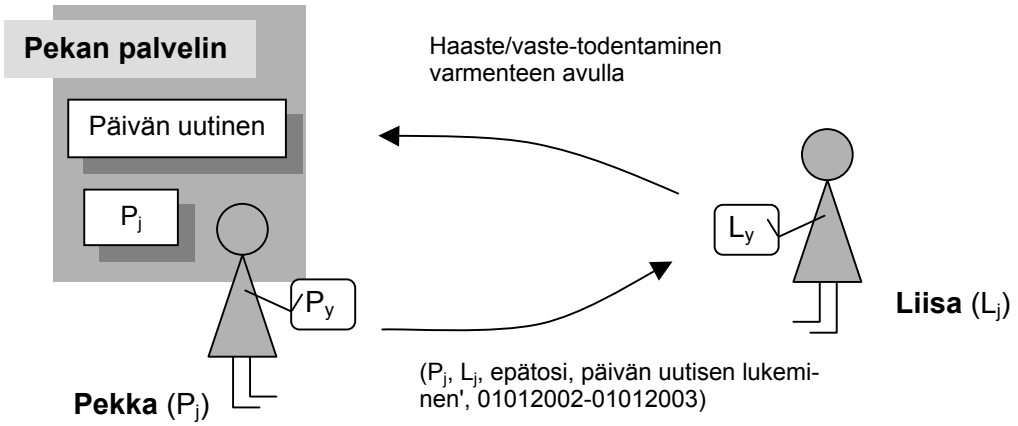
SPKI ja SDSI tuovat julkisen avaimen nimeen sitovan henkilövarmenteen vaihtoehdoksi kaksi muuta varmennetta: roolivarmenteet (authorization certificate) ja attribuuttivarmenteet (attribute certificate), joiden keskinäistä suhdetta hahmotetaan ohessa (Kuva 24). Tässä esitetty perustuu lähteisiin [RFC2693], [RIVE96] ja [LEHT98].



Kuva 24. Henkilövarmenne, attribuuttivarmenne ja roolivarmenne.

SPKI/SDSI esittää, että kahdesta osasta koostuvaa päättelyketjua yksinkertaistettaisiin siirtymällä henkilövarmenteista roolivarmenteisiin. Julkista avainta ei sidottaisikaan tiettyyn henkilöön, vaan kyseisen avaimen haltijalle kuuluviin valtuuksiin. Tällöin koko nimiavaruuksien ongelma saadaan sivuutetuksi – järjestelmässä on pelkästään julkisia avaimia ja niihin kytkettyjä valtuuksia. Päättelyketju on lyhyt:

Julkinen avain –> valtuudet

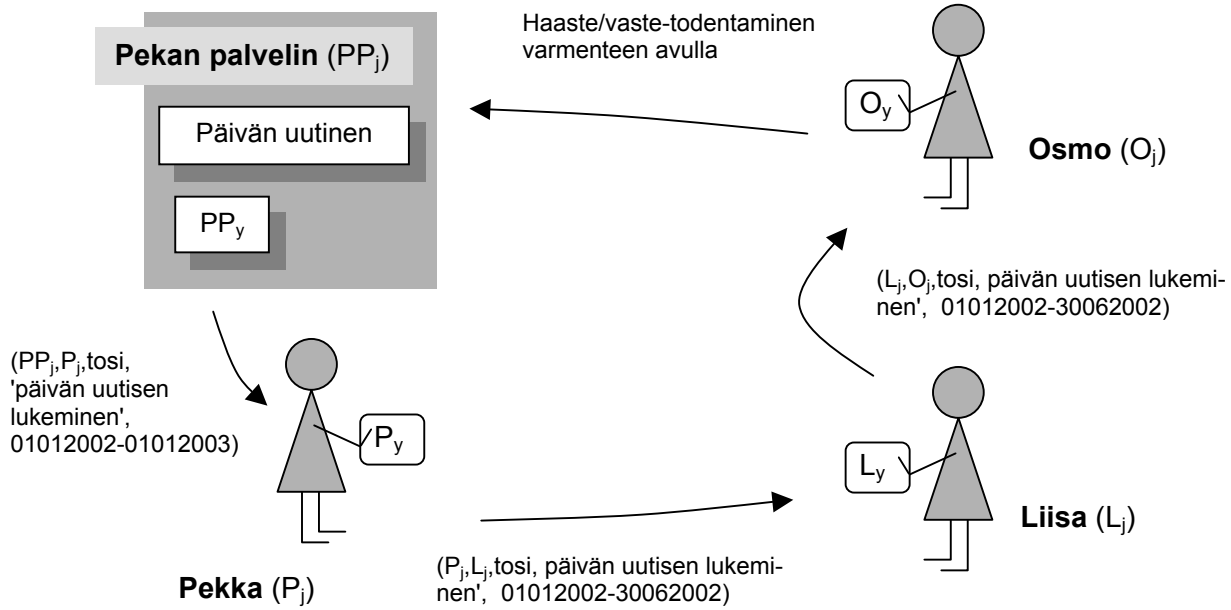


Kuva 25. Esimerkki roolivarmenteen käytöstä.

Esimerkiksi oheisessa kuvassa (Kuva 25) Pekka valtuuttaa Liisan lukemaan päivän uutisen Pekan ylläpitämältä palvelimelta allekirjoittamalla roolivarmenteen, jossa Liisan julkiseen avaimeen kytketään lukuoikeutta tarkoittava rooli. Pekka on määritellyt palvelimensa pääsynvalvonnan hyväksymään vain sellaiset roolivarmen-

teet, jotka hän on allekirjoittanut. Roolivarmenteen keskeiset kentät on esitetty SPKI:ssa viisikkona (I,S,D,A,V), jossa I (issuer) on varmenteen myöntäjä (Pekan julkinen avain), S (subject) varmenteen haltija (Liisan julkinen avain), D (delegation) mahdollinen lupa delegointiin, A (authorization) annettu valtuus ja V (validity) varmenteen voimassaoloaika. Varmenteissa osapuolia edustavat siis heidän julkiset avaimensa. Jos osapuolille halutaan antaa ihmiselle helpommin luettava nimi esimerkiksi käyttöliittymää varten, se voidaan sisällyttää varmenteeseen hyödyntämällä paikallista nimiavaruutta.

Roolivarmenteet mahdollistavat valtuuksien sulavan delegoinnin (Kuva 26). Ellei Pekka ole kieltänyt delegointia, voi Liisa allekirjoittaa uuden roolivarmenteen, jolla myös Osmo valtuutetaan lukemaan mainittu tiedosto. Jos Pekka haluaa, että hänen lisäkseen myös Timo voi delegoida valtuuksia päivän uutisen lukemiseen, hän luo Pekan palvelimelle toisen avainparin, ja allekirjoittaa sillä Timolle ja itselleen roolivarmenteen, joka sallii delegoimisen. Näin roolivarmenteista syntyy ketjuja, ja Pekan palvelin sallii varmenteen esittäjälle pääsyn tiedostoon, jos Pekan palvelimen julkisesta avaimesta (PP_j) voidaan rakentaa varmenneketju esitettyyn varmenteeseen. Esimerkissä Pekan palvelin on antanut Pekalle luvan tiedoston lukemiseen vuoden loppuun saakka, mutta Pekka on päättänyt delegoida valtuuden Liisalle vain alkuvuoden osalta.



Pekan varmenne: (PP_j, P_j, tosi, 'päivän uutisen lukeminen', 01012002-01012003)
Liisan varmenne: (P_j, L_j, tosi, 'päivän uutisen lukeminen', 01012002-30062002)
Osmon varmenne: (L_j, O_j, tosi, 'päivän uutisen lukeminen', 01012002-30062002)

Kuva 26. Esimerkki roolivarmenteiden käytöstä delegoinnissa.

Osmon todentaminen Pekan palvelimelle sulkee varmenneketjun silmukaksi. Varmenneketjun juurena toimiva Pekan palvelin on siis samalla itse myös varmentei-

siin luottava osapuoli. Niinpä A-kentän sisällön määrittäminen jää yksin Pekan palvelimen tehtäväksi, eikä erilaisten valtuuksien syntaksia ja semantiikkaa tarvitse sen laajemmin standardoida. Myöskään luotettavan juuren hankkiminen ei aiheuta ongelmia: varmenneketjun todentaminen alkaa Pekan palvelimen omasta julkisesta avaimesta PP_j. Käytännössä roolivarmenne voidaan toteuttaa esimerkiksi SPKI:n määrittämällä S-listana (S-expression) tai X.509v3-varmenteen laajennuskenttien avulla.

SPKI tunnustaa, että useimmat nykyään käytössä olevat varmenteet ovat henkilövarmenteita, ja ehdottaa siirtymäajan ratkaisuksi attribuuttivarmennetta, joka kytkee henkilön nimen hänelle kuuluviin oikeuksiin. Tällöin pääsynvalvonta suorittaisi kaksiosaisen päättelyketjun

Julkinen avain –> käyttäjän nimi –> valtuudet,

jonka ensimmäinen osa tapahtuisi henkilövarmenteen avulla ja jälkimmäinen attribuuttivarmenteen avulla. Internet Engineering Task Force (IETF) onkin määritellyt X.509-varmenteisiin nojaavan profiilin attribuuttivarmenteille Internetissä [RFC3281].

Periaatteessa henkilövarmenteen tietosisältöön voisi sisällyttää myös rooli- ja valtuustietoja, mutta erillisen attribuuttivarmenteen käytössä on joitain etuja. Henkilövarmenteen voimassaoloaika on tyypillisesti pidempi kuin attribuuttivarmenteiden. Jos attribuuttivarmenne varmentaa esimerkiksi haltijansa aseman yrityksessä, saattaa tämä asema muuttua monta kertaa henkilövarmenteen muutaman vuoden voimassaoloajan kuluessa. Tällöin koko henkilövarmenne jouduttaisiin asettamaan sulkulistalle vanhentuneen roolitiedon vuoksi. Lisäksi henkilövarmennetta myöntävän rekisteröijän voi olla hankala mennä takuuseen varmenteen haltijan valtuuksista – valtuuksia hallinnoi tyypillisesti eri organisaatio tai saman organisaation toinen osa. [HOUS01 s. 274–277]

6. PKI JA TOIMIKORTIT

Yksi julkisen avaimen järjestelmän kulmakivistä on yksityinen avain, joka tulee suojata huolellisesti paljastumista ja katoamista vastaan. Perinteisesti käyttäjän tiedot varastoidaan mikrotietokoneissa kiintolevylle tai levykkeelle, mutta yksityiselle avaimelle tätä parempi suoja on saavutettavissa tallettamalla se ympäristöstään eristettyyn, peukalointia sietävään laitteeseen, kuten toimikortille. Tässä luvussa tarkastellaan toimikortteja hyödyntävän julkisen avaimen järjestelmän luonteenpiirteitä ja sen muotoutumassa olevia standardeja. Lisäksi luodaan katsaus järjestelmän turvallisuuteen, minkä antamaa taustaa vasten luvun lopussa tutustutaan eduskuntakäsittelyssä olevaan esitykseen laiksi sähköisestä allekirjoituksesta.

6.1. Perusperiaatteet

Toimikortteja hyödyntävässä julkisen avaimen järjestelmässä keskeinen periaate on, että varmenteeseen liittyvä yksityinen avain on talletettu toimikortille. Yksityinen avain on suojattu siten, että se ei tule koskaan ulos toimikortilta. Käytännössä yksityinen avain on tallennettu toimikortin tiedostoon, jonka lukeminen ja kirjoittaminen on avaimen luomisen jälkeen estetty kokonaan, mutta jonka *käyttäminen* salatun viestin purkamiseen tai viestin allekirjoittamiseen on mahdollista, kun toimikortti on todentanut käyttäjänsä esimerkiksi PIN-koodin avulla. Toimikortti omaa riittävän laskentakapasiteetin yksityistä avainta käyttävän epäsymmetrisen salausalgoritmin suorittamiseksi toimikortin suorittimessa.

Avainpari voidaan luoda toimikortille eri tavoilla. Jos avainpari on luotu toimikortin sisällä, voidaan olla varmoja, että yksityisestä avaimesta ei luontivaiheessakaan ole jäänyt kopiota kortin ulkopuolelle. Avainparin luomiseen tarvittava satunnaisuus voidaan tuottaa esimerkiksi kohinasta toimikortin sisällä, tai satunnaisuus voidaan tuoda kortille ulkoapäin, jolloin kortti joutuu luottamaan käytettävissä olevien satunnaislukujen laatuun. Toinen vaihtoehto on luoda avainpari kortin ulkopuolella ja tallettaa valmis avainpari kortille, jolloin yksityisestä avaimesta voi jäädä kopio kortin ulkopuolelle.

Varmenteen haltijan näkökulmasta luotettavin tapa hankkia avainpari on luoda se itse: tällöin varmenteen haltijan ei tarvitse luottaa kehenkään muuhun. Peruskäyttäjän – toisin kuin varmentajan – ei kuitenkaan voi olettaa ymmärtävän kryptografiaa ja siihen liittyvää tekniikkaa kovin syvällisesti. Niinpä varmentaja tyypillisesti huolehtii avainparin luomisesta toimikortille voidakseen luottaa siihen, että toimikortin avainpari on luotu luotettavalla tavalla ja että esimerkiksi yksityisestä avaimesta ei ole jäänyt kopiota mihinkään. Avainparin luomisen jälkeen varmentaja personoi ja varmentaa toimikortin eli allekirjoittaa luodun julkisen avaimen ja

varmennettavan henkilön henkilötiedot omalla yksityisellä avaimellaan. Syntynyt varmenne talletetaan varmennehakemiston lisäksi tyypillisesti myös itse toimikortille. Tällä järjestelyllä ei niinkään pyritä lisäämään turvallisuutta vaan varmenteen saatavuutta. Omaa varmennettaan tarvitessaan käyttäjän ei tarvitse välttämättä lähteä noutamaan sitä varmennehakemistosta, vaan hän saa sen kätevästi toimikortiltaan.

Lopuksi varmentajan tulee huolehtia, että yksityisen avaimen sisältävä toimikortti ja siihen mahdollisesti sisältyvä PIN-koodi toimitetaan varmennetulle henkilölle luotettavalla tavalla. Rekisteröijän tehtäväksi jää korttien jakaminen käytännössä, ja se voidaan toteuttaa luotettavasti esimerkiksi kasvokkain tapahtuvan tunnistamisen perusteella. Turvallisuuden lisäämiseksi kortin käyttöön tarvittava PIN-koodi voidaan toimittaa kortinhaltijalle toista reittiä pitkin, esimerkiksi postittamalla se hänelle kotiin kirjeenä.

Kuten edellisessä luvussa todettiin, on luotettavan juuren hankkiminen yksi asia, josta varmenteisiin luottavan osapuolen on huolehdittava. Yksityisen avaimen ja siihen liittyvän varmenteen lisäksi toimikorttia käytetäänkin usein myös varmentajan juurivarmenteen tallettamiseen, jotta varmenteen haltija voisi käyttää toimikorttia varmentajan todentamiseen. Palveluja rakentava henkilö voi luottaa esimerkiksi Väestörekisterikeskuksen juurivarmenteen aitouteen, koska hän on aikanaan hakenut oman toimikorttinsa poliisilta, jolle Väestörekisterikeskus on uskonut rekisteröijän tehtävät.

Julkisen avaimen järjestelmään kuuluvaa toimikorttia, joka sisältää haltijansa varmenteeseen liittyvän yksityisen avaimen, kutsutaan jäljempänä PKI-toimikortiksi. Puhekielessä käytetään runsaasti ilmaisua "toimikortilla oleva varmenne" sen sijaan, että sanottaisiin "toimikortilla oleva yksityinen avain, johon liittyvä julkinen avain on varmennettu", esimerkiksi "Väestörekisterikeskuksen HST-tekniikassa varmenne sijaitsee toimikortilla". Ilmaisu ei ole suorastaan virheellinen mutta harhaanjohtava. Kuten edellä todettiin, on toimikortilla kyllä varmenne (lisäksi sama varmenne on myös varmennehakemistossa ja mahdollisesti myös eri puolilla tietoverkkoa, jonne syystä tai toisesta on taltioitunut siitä kopio). Keskeistä kuitenkin on, että toimikortilla sijaitsee varmenteen lisäksi siihen liittyvä yksityinen avain. Puhekielen ilmaisua käytetään ehkä siksi, että se mahdollisesti avautuu paremmin peruskäyttäjälle: varmenne käsitteenä lienee konkreettisempi kuin yksityinen avain, jota kortin haltija ei koskaan ole nähnyt.

Vaikka tässä luvussa keskitytäänkin pitkälti toimikortteihin, voidaan yksityisen avaimen turvallisempi säilytyspaikka toteuttaa myös muilla vastaavilla, peukalointia sietävillä toimiavaimilla. Viime aikoina huomiota on herättänyt suoraan työaseman USB-väylään kiinnitettävä avaimenperän kokoinen, USB tokeniksi kutsut-

tu laite, joka poistaa tarpeen työasemaan liitettävän toimikortinlukijan hankkimiselle. Lisäksi laite pystyy kommunikoimaan työaseman kanssa huomattavasti toimikorttia nopeammin. Myös PCMCIA-korttipaikkaan työnnettävät laitteet muodostavat vaihtoehdon toimikortille.

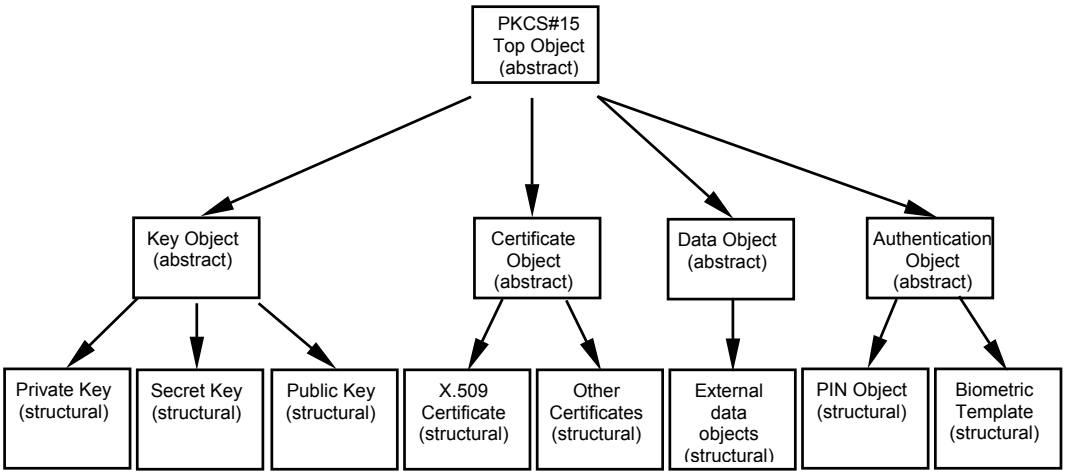
6.2. PKI-toimikortti ja PKCS#15-standardi

PKI-toimikortin käyttämiseen tarvitaan kortin lisäksi kortinlukija, joka on yhteydessä tarvittavan ohjelmiston sisältävään tietokoneeseen. Kuten aikaisemmin todettiin, ovat toimikortin tiedostorakenne sekä toimikortin ja kortinlukijan välinen kommunikointi pitkälti standardoitua. Tämä ei kuitenkaan vielä riitä PKI-toimikorttien hyödyntämiseen sovelluksissa. Toimikorttia käyttävän tietokoneohjelmiston on lisäksi tiedettävä, mikä toimikortin tiedosto tarkkaan ottaen sisältää muun muassa yksityisen avaimen, siihen liittyvän varmenteen ja varmentajan juurivarmenteen sekä missä muodossa näiden käyttöön liittyvät parametrit on esitetty.

Alkujaan tämä kysymys oli ratkaistu siten, että sama toimittaja, joka loi PKI-toimikortin tiedostorakenteen, toteutti myös toimikortin käyttöön tarvittavat tietokoneohjelmistot. Näin syntyi tilanne, jossa eri valmistajien tekniikalla toteutetut PKI-toimikortit ja niitä käyttävät tietokoneohjelmistot eivät olleet keskenään yhteensopivia. Tietotekniikassa yleinen suuntaus on kuitenkin pois valmistajakohtaisista ratkaisuista kohti avoimia standardeja, mikä usein on ollut edellytys uuden teknologian käytön yleistymiselle.

Yhdysvaltalainen RSA Laboratories on julkaisemansa PKCS-määritysten (Public Key Cryptography Standard) sarjan avulla pyrkinyt vauhdittamaan epäsymmetrisen salausmenetelmän ja julkisen avaimen järjestelmän yleistymistä. PKCS-määritykset pyrkivät olemaan teollisuusstandardeja, joiden varaan valmistajat voivat rakentaa yhteensopivia järjestelmiä. PKCS-määritysten viidestoista osa, PKCS#15 ”Cryptographic Token Information Syntax Standard”, ottaa kantaa PKI-toimikortin tai muun laitetason turvallisuutta tarjoavan välineen tiedostorakenteeseen, päämääränään eri valmistajien eri alustoihin, kuten käyttöjärjestelmiin, perustuvien PKI-toimikorttien ja tietokoneohjelmien keskinäinen yhteensopivuus [PKCS15, s. 4].

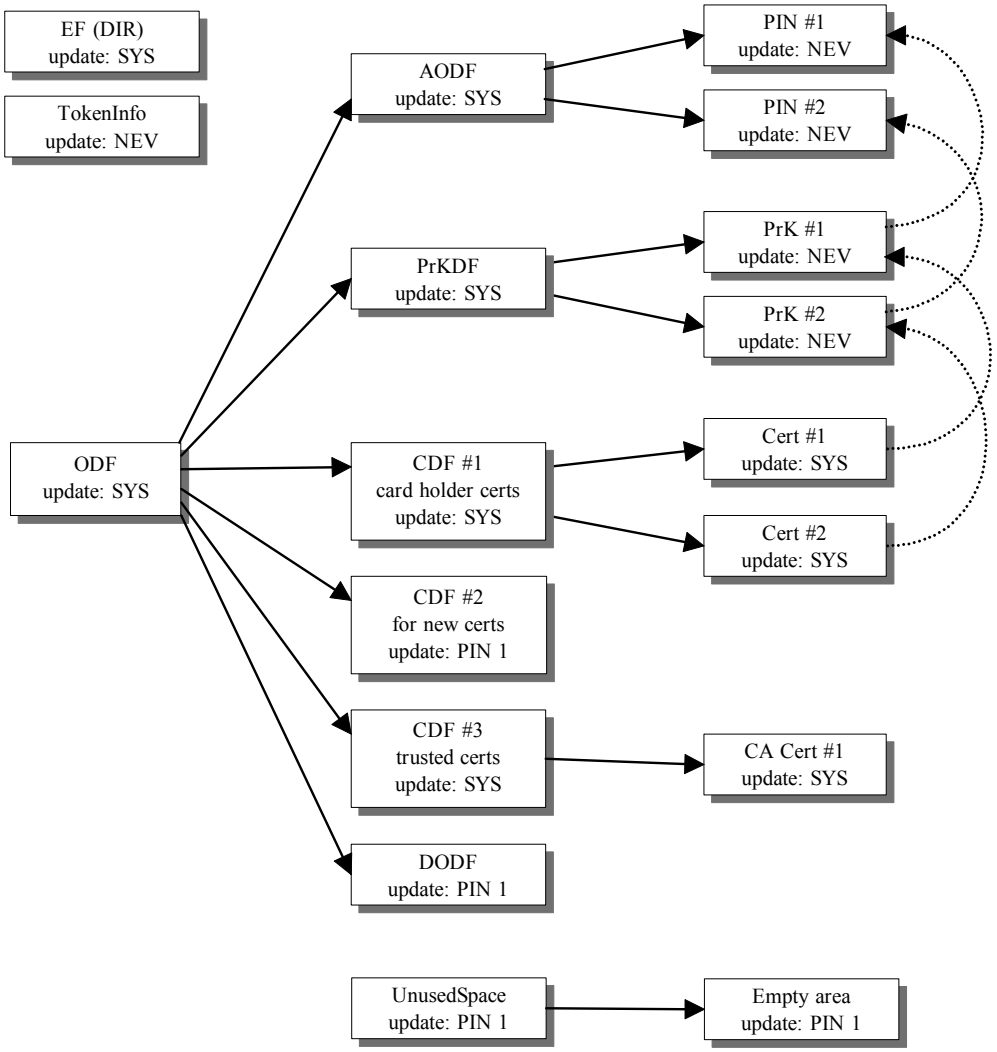
PKCS#15-spesifikaatio määrittelee, kuinka toimikortille voidaan tallettaa symmetrisiä avaimia tai epäsymmetrisiä avainpareja, varmenteita ja muuta dataa sekä toimikortin käyttäjän henkilöllisyyden todentamiseen käytettävää tietoa, kuten PIN-koodeja (Kuva 27). PKCS#15 ohjeistaa, kuinka kyseiset tiedostot tulee sijoitella ja nimetä sekä mikä niiden sisältämien tietojen rakenne ja merkitys on. Tietojen esitystapana käytetään ASN.1-notaatiota.



Kuva 27. PKCS#15-standardin määrittelemät tietotyypit [PKCS15, s.8].

PKCS#15 ei kuitenkaan ota kantaa yksittäisten PKCS#15-toteutuksien ominaisuuksiin, kuten toimikortilla olevien avainten ja varmenteiden lukumäärään, vaan jättää nämä tiedot toimikortin PKI-sovelluksen toteuttajan päätettäväksi. PKI-sovelluksen toteuttaja määrittelee toimikortin PKCS#15-profiilin, jossa nämä ominaisuudet kiinnitetään.

Esimerkiksi Väestörekisterikeskus on julkaissut varmennepolitiikkaansa perustuvan sähköisen henkilökortin PKCS#15 -profiilin [VRK99b]. Dokumentissa muun muassa määritellään, että sähköisellä henkilökortilla on kaksi avainparia, joista toinen on tarkoitettu kiistämättömyyden osoittamiseen (”allekirjoitusavain”) ja toinen salaukseen sekä todentamiseen. Varmenteita sähköisellä henkilökortilla on kolme: haltijansa kahden kansalaisvarmenteen lisäksi toimikortilla on myös Väestörekisterikeskuksen juurivarmenne. Lisäksi profiili mahdollistaa omien lisävarmenteiden tallettamisen kortille. Dokumentissa sähköisen henkilökortin PKCS#15-tiedostorakennetta havainnollistetaan oheisella kuvalla (Kuva 28). Esitetty tiedostorakenne on looginen ja kertoo siihen kuuluvien tiedostojen keskinäisestä hierarkiasta. Todellisuudessa kaikki tiedostot sijaitsevat omassa alihakemistossaan (DF, dedicated file).



Kuva 28. Sähköisen henkilökortin PKCS#15-profiilin määrittelemä toimikortin looginen tiedostorakenne [VRK99b, s. 4]

PKCS#15-määrityksen mukaisesti sähköisen henkilökortin PKI-sovelluksesta löytyy ODF-tiedosto (object definition file), joka sisältää viittauksen muihin keskeisiin tiedostoihin. Näitä ovat yksityiset avaimet määrittelevä PrKDF-tiedosto (private key definition file), varmenteet määrittelevät CDF-tiedostot (certificate definition file), kortinhaltijan todentamiseen tarvittavat PIN-koodit määrittelevä AODF-tiedosto (authentication object definition file) sekä mahdollisen muun datan määrittelevä DODF-tiedosto (data object definition file). Nämä tiedostot puolestaan viittaavat itse PKI:n kannalta keskeisiin tietoihin, kuten toimikortin yksityisiin avaimiin (PrK#1 ja #2) sekä määrittelevät niihin liittyvää tietoa, kuten yksityisen avaimen nimen, esimerkiksi ”Todentamis- ja salausavain” ja ”allekirjoitusavain”. Varmenteet viittaavat niitä vastaaviin yksityisiin avaimiin (kuvan katkoviiva), nämä puolestaan PIN-koodeihin, jotka tulee antaa kortille ennen yksityisen avaimen

sisältävän tiedoston käyttämistä. Todentamis- ja salausavaimen käyttö edellyttää PIN1-koodin antamista ja allekirjoitusavaimen käyttö PIN2-koodin antamista. Turvallisuuden lisäämiseksi sähköisen henkilökortin profiilissa määritellään, että PIN2-koodi on annettava uudelleen joka kerta, kun allekirjoitusavainta halutaan käyttää.

Sähköisellä henkilökortilla on lisäksi tyhjää tilaa, johon voidaan tallettaa käyttäjän haluamaa tietoa, kuten lisävarmenteita. PKCS#15-profiilin Empty area -tiedosto sisältää toteutuksesta riippuen muutaman kilotavun verran tyhjää tilaa, jota käyttäjä voi kirjoittaa annettuaan ensin PIN1-koodin. CDF#2-tiedostoa päivittämällä käyttäjä voi linkittää Empty Area -tiedostoon kirjoittamansa lisävarmenteen osaksi PKCS#15-tiedostorakennetta, jolloin lisävarmenne on myös työaseman sovellusohjelmien käytössä. Lisävarmenne voi sisältää saman julkisen avaimen kuin toinen henkilövarmenteista Cert#1 ja Cert#2 sekä viittauksen vastaavaan yksityiseen avaimeen.

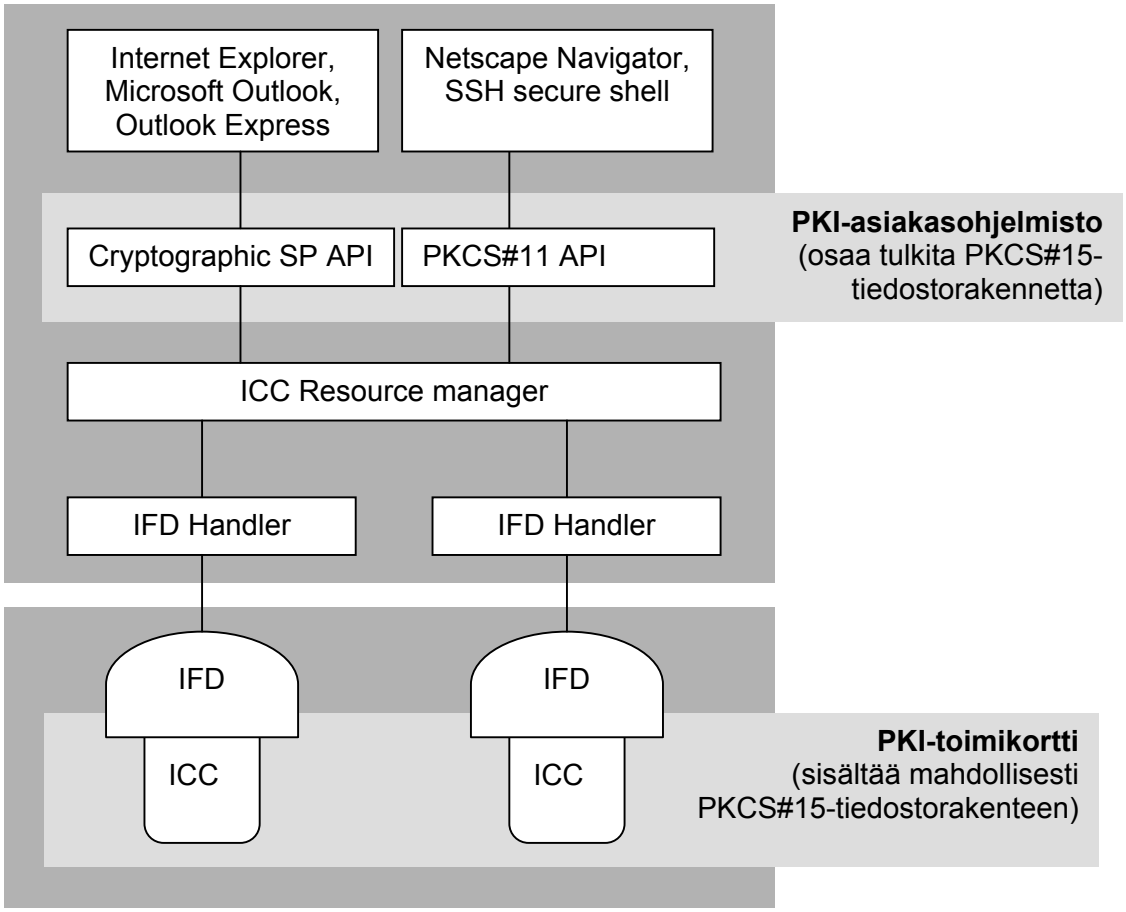
Lisävarmenteen avulla voidaan muun muassa toteuttaa kirjautuminen Windows 2000 -toimialueeseen. Windows 2000:n toimikorttikirjautuminen edellyttää, että kirjautumiseen käytettävä varmenne ilmaisee, millä käyttäjätunnuksella (username) ja mihin toimialueeseen (domain) varmenteen haltijalla on valtuudet kirjautua. Kun sähköinen henkilökortti aktivoidaan toimikorttikirjautumiseen, toimialueen käyttäjätunnusten ylläpitäjä allekirjoittaa tunnistautumisvarmenteen julkinen avaimen yhdessä varmenteen haltijan käyttäjätunnuksen ja toimialueen kanssa, ja syntynyt varmenne talletetaan kortille lisävarmenteeksi. Kysymys on siis eräänlaisesta roolivarmenteesta: sähköisen henkilökortin yksityisen avaimen haltijalle myönnetään valtuus kirjautua toimialueeseen käyttämällä tiettyä käyttäjätunnusta.

6.3. Työaseman ohjelmistoarkkitehtuuri ja PKI-asiakasohjelmisto

Kuten luvussa 3.3 kerrottiin, tapahtuu toimikortin ja kortinlukijan välinen kommunikointi käyttämällä ISO 7816 -standardissa määriteltyä protokollaa, joka matalan abstraktionsa vuoksi on epämiellyttävä työasemaan sovelluksia toteuttavalle ohjelmoijalle. Luvussa 3.9.2 esiteltiin PC/SC-arkkitehtuuri, joka tarjoaakin ohjelmoijalle jo korkeamman abstraktion rajapinnan. Yksi PC/SC-arkkitehtuurin määrittämä palveluntarjoaja on cryptographic service provider (CSP), joka tarjoaa sovellusohjelmoijalle rajapinnan (API, application programming interface) toimikortin käyttämiseen.

Microsoft, jonka käyttöjärjestelmät itsessään sisältävät nykyisin PC/SC-arkkitehtuurin perusosat, käyttää toimikortteja tukevissa tuotteissaan CSP-rajapintaa. Muiden ohjelmistovalmistajien PKI-toimikorttia hyödyntävissä ratkaisuissa nojataan sen sijaan usein PKCS#11-rajapintaan, joka on RSA Laboratories -

yhtiön niinikään kehittämä ”Cryptographic Token Interface Standard” -niminen määritys, jota usein kutsutaan nimellä Cryptoki [PKCS11]. PKCS#11 ei rajoitu pelkästään toimikortteihin, vaan määrittelee API:n ylipäätään kryptografisiin laitteisiin, joiden toteutus voi perustua esimerkiksi toimikorttiin, PCMCIA-korttiin tai työasemassa olevaan ohjelmistoon.



Kuva 29. PKI-asiakasohjelmisto toteuttaa korkean abstraktiotason ohjelmointirajapinnan, joka helpottaa PKI-toimikortin käyttöä sovelluksissa.

PKI-asiakasohjelmistoksi (PKI client) kutsutaan työasemassa tai muussa päätelaitteessa käytettävää ohjelmistoa, joka toteuttaa sovellusohjelmoijan käyttämän korkean abstraktion rajapinnan kryptografisen laitteen käyttämistä varten. Windows-ympäristössä käytetyt PKI-asiakasohjelmistotuotteet usein toteuttavat molemmat edellä esitetyt rajapinnat, jolloin syntyy oheisen kuvan mukainen arkkitehtuuri (Kuva 29). PKI-asiakasohjelmiston tehtävä on muun muassa tulkita ja hyödyntää toimikortin PKCS#15-standardin mukaisen tiedostorakenteen sisältöä.

Valmistaja	Tuote	Käyttöjärjestelmä
Sonera SmartTrust	Personal	Windows 95, 98, ME, NT4 ja 2000
Setec	Web and email security	Windows 95, 98, ME, NT4 ja 2000
SSH Communications	Accession	Red Hat Linux 6.2, 7.1, 7.2 Windows 98, ME, NT4, 2000 ja XP
Gemplus	GemSAFE	Windows 95, 98, NT4, 2000
Teknillinen korkeakoulu	Smart Card IDentification Infrastructure (SCIDI)	Debian, FreeBSD, Solaris

Taulukko 2. Joitain saatavilla olevia PKI-asiakasohjelmistoja.

Markkinoilla on kaupallisia ja ei-kaupallisia PKI-asiakasohjelmistoja, joista muutamia on koottu oheiseen taulukkoon (Taulukko 2). Varsinkin Unix- ja Linux-ympäristöihin PKI-asiakasohjelmia on saatavilla vielä melko vähän. Eräänä PKI-toimikorttien käytön yleistymisen jarruna pidetään nykyisin nimenomaan PKI-asiakasohjelmistojen huonoa saatavuutta ja suhteellisen korkeaa hintaa.

6.4. Työasemaan kytketyn PKI-toimikortin turvallisuus

Toimikortin turvallisuutta käsiteltiin luvussa 3.8 ja työasemaan kytketyn toimikortin turvallisuutta luvussa 3.9.3. Tässä luvussa tarkastellaan nimenomaan PKI-toimikortin turvallisuutta yleensä ja tilanteessa, jossa sitä käytetään työasemaan kytketyn kortinlukijan välityksellä.

6.4.1. PKI-toimikortin turvallisuus

Luvussa 3.8 esiteltiin erilaisia tapoja päästä väkivalloin tai muuten käsiksi toimikortin sisältämään tietoon. Samalla todettiin, että erilaisia uhkakuvia analysoitaessa tulee miettiä, kenen intressiä toimikortti itse asiassa suojelee ja kuka on potentiaalinen hyökkääjä. Lisäksi huomautettiin, että toimikorttiin nojaavia järjestelmiä suunniteltaessa on tarpeen rakentaa puolustuksellista syvyyttä: yhden suojamuurin sortuminen ei saa vaarantaa koko linnoitusta.

PKI-toimikortti sisältää kaksi tietoa, joita sen on määrä varjella: varmenteen haltijan PIN-koodin ja hänen yksityisen avaimensa. Toimikortti ei suojele näitä tietoja varmenteen haltijan itse suorittamilta hyökkäyksiltä: varmenteen haltijalla ei ole intressiä saada tietoonsa omaa yksityistä avaintaan (riittää että hänellä on mahdollisuus käyttää sitä) ja oman PIN-koodinsa hän tietää muutenkin (tai jos hän on unohtanut sen, hän ottaa yhteyden varmentajaan, joka on järjestänyt lukittuneiden korttien avaamisen esimerkiksi PUK-koodin avulla). Ei siis haittaa, että varmenteen haltijalla on aikaa peukaloida omaa korttiaan luvussa 3.8 esitetyillä tavoilla aina varmenteen voimassaolon päättymiseen asti.

Kuviteltavissa oleva hyökkäys PKI-toimikorttia vastaan tulee sivulliselta, joka haluaisi päästä käsiksi varmenteen haltijan yksityiseen avaimeen voidakseen käyttää sitä väärin. Tällöin PKI-toimikortti tukeutuu puolustukselliseen syvyyteen: hyökkääjän pitää päästä toimikorttiin käsiksi, jotta hän voisi pyrkiä murtamaan kortin suojaukset laboratoriossaan. Varmenteen haltijan oma etu ja varmennepolitiikka puolestaan edellyttävät, että varmenteen haltija ilmoittaa kortin hukkumisesta, jotta varmentaja asettaa kortin sulkulistalle. Hyökkääjällä on aikaa murtaa ja väärinkäyttää korttia vain siihen saakka, kun varmenne asetetaan sulkulistalle tai se vanhenee. Vaikka hyökkääjä saisikin murrettua yksittäisen toimikortin ja paljastettua sen yksityisen avaimen, ei tapahtunut kuitenkaan horjuta koko julkisen avaimen järjestelmää: yksittäisen varmenteen haltijan yksityisen avaimen paljastuminen ei vaikuta varmentajan yksityisen avaimen turvallisuuteen.

Tilanne on paljon pahempi, jos hyökkääjä pystyy paljastamaan toimikortilla olevan yksityisen avaimen ilman, että varmenteen haltija tulee tietoiseksi tapahtuneesta. Tämä voisi tapahtua esimerkiksi tavalliseksi toimikortinlukijaksi naamioidulla laitteella, johon varmenteen haltija pahaa aavistamatta työntää korttinsa. Anderson ja Kuhn ovat esittäneet, kuinka kesken RSA-laskutoimituksen toimikorttiin kohdistettu transientti (luku 3.8) saattaa aiheuttaa laskuvirheen, jonka tuloksena yksityinen avain on helppo laskea allekirjoituksesta [ANDE97].

6.4.2. PKI-toimikortti ja työaseman turvallisuus

PKI-asiakasohjelmisto tarjoaa sovellusohjelmalle korkean abstraktiotason sovellusrajapinnan toimikortin käyttämistä varten. Esimerkiksi PKCS#11-rajapinta tarjoaa funktion C_SignInit(), jonka kutsuminen käynnistää digitaalisen allekirjoituksen laskemisen esimerkiksi toimikortilla olevan yksityisen avaimen avulla [PKCS11]. PKI-asiakasohjelmisto muuttaa funktiokutsun APDU-komentosarjaksi, joka lähetetään resurssinhallinnan, kortinlukijan ajurin ja kortinlukijan kautta toimikortille käsiteltäväksi. Työaseman arkkitehtuuri ei kuitenkaan takaa PKI-asiakasohjelman ja kortinlukijan välisen viestinvaihdon aitoutta ja eheyttä.

Työaseman ohjelmisto- tai laitteistoarkkitehtuuriin mahdollisesti pesiytyneet tuho-ohjelmat ovat vakava uhka PKI-toimikortin turvallisuudelle. Tuho-ohjelmat voivat tehdä monenlaisia hyökkäyksiä toimikortin ja PKI-asiakasohjelmiston väliseen kommunikointiin. Yksinkertaisimpiin hyökkäyksiin kuuluu palvelunestohyökkäyksen toteuttaminen: havaitessaan kortinlukijaan työnnetyn toimikortin tuho-ohjelma alkaa välittömästi syöttää sille satunnaisesti valittuja PIN-koodeja, kunnes kortti lukittuu (esimerkiksi sähköinen henkilökortti lukittuu kolmen yrityksen jälkeen).

Kiistämättömyyden vaarantava hyökkäys on ehkä vielä vahingollisempi: tuho-ohjelma saattaa vaihtaa PKI-asiakasohjelmiston lähettämän, allekirjoitettavaksi tarkoitetun tiivisteen omaansa, jolloin kortti tekee kuuliaisesti digitaalisen allekirjoituksen vilpilliseen viestiin. Vaihtoehtoisesti tuho-ohjelma voi poimia talteen PKI-asiakasohjelmiston toimikortille lähettämän allekirjoitus-PIN-koodin, ja käyttää sitä hankkiakseen varmenteenhaltijan tietämättä allekirjoituksia myös muihin tiivisteisiin.

Kuten luvussa 3.9.3 todettiin, on tuho-ohjelmilta suojautuminen hankalaa. Toimikortin tarjoama melko hyvä turvallisuus valuu hukkaan, koska kokonaisuus on suojaton toimikortin ja käyttäjän väliseen kommunikaatioon kohdistuvalle vilpille. Markkinoilla on kyllä PIN-koodin syöttämistä varten erillisen PIN-näppäimistön sisältäviä kortinlukijoita, jotta työasemaan pesiytynyt tuho-ohjelma ei pääsisi kaappaamaan ja peukaloimaan PIN-koodeja. PIN-näppäimistökin ratkaisee vain osan ongelmasta: tuho-ohjelma pääsee edelleen peukaloimaan PKI-asiakasohjelmiston toimikortille lähettämiä tiivisteitä ja muita viestejä.

Ongelma olisi ratkaistavissa siirtämällä toimikortin ja varmenteenhaltijan väliseen kommunikointiin liittyvä TCB kokonaan pois turvattomasta työasemasta. Tämä voisi olla mahdollista korvaamalla toimikortinlukija luotetulla päätelaitteella, jossa olisi oma näyttö ja näppäimistö ja jossa suoritettaisiin vain luotettuja ohjelmia. Päätelaite esittäisi varmenteenhaltijalle allekirjoitettavan dokumentin luotetun näytön välityksellä, ja pyytäisi häntä hyväksymään dokumentin antamalla PIN-koodin luotetun näppäimistön kautta.

Esimerkiksi lähteessä [HELM97] on hahmoteltu työasema-arkkitehtuuri, jossa TCB sisältää näytön, näppäimistön ja kortinlukijan lisäksi turvamoduulin, jonka tehtävä on kontrolloida allekirjoituksen tuottamista toimikortin avulla. Lisäksi turvamoduuli todentaa allekirjoituksia ja varmenneketjuja sekä pitää lokitiedoston avulla kirjaa allekirjoitetuista dokumenteista, joihin edellytetään myös toisen sopimusosapuolen allekirjoitusta. Normaalisti kokonaisuus toimii kuten tavallinen työasema, mutta kun käyttäjä haluaa allekirjoittaa dokumentin, hän aktivoi turvamoduulin fyysisestä kytkimestä. Työaseman näyttö ja näppäimistö oletetaan luotettaviksi, joten kytkin katkaisee niiden yhteyden turvattomaan työasemaan ja liittää ne turvamoduuliin. Luettuaan allekirjoitettavan sopimuksen näytöltä käyttäjä painaa turvamoduuliin kytkettyä fyysistä 'hyväksyn'-nappia, jonka jälkeen hän voi syöttää PIN-koodin toimikortille.

Luotetusta päätelaitteesta syntyy kuitenkin lisäkustannuksia, ja jos päätelaitteen tulee kyetä esittämään varmenteenhaltijalle monimutkaisestikin koodattuja dokumentteja, kasvavat päätelaitteessa olevien ohjelmistovirheiden aiheuttamat tietoturvariskit.

6.5. Digitaalista allekirjoitusta koskevaa lainsäädäntöä

Euroopan Unioni on halunnut edistää digitaalisen allekirjoituksen käyttöä ja sen oikeudellista tunnustamista edellyttämällä yhteisen lainsäädännön luomista digitaalisesta allekirjoituksesta ja varmentajille asetettavista vähimmäisvaatimuksista. Euroopan parlamentin ja neuvoston direktiivi sähköisten allekirjoitusten yhteisestä kehyksestä [EP99] annettiin 30. marraskuuta 1999. Suomessa hallitus on 26. lokakuuta 2001 antanut eduskunnalle esityksen HE 197/2001 laiksi sähköisestä allekirjoituksesta [HE01], johon lähteeseen tässä esitetty perustuu.

Lain soveltamisalaan kuuluvat sähköiset allekirjoitukset sekä palveluntarjoajat, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä tuotteita tai palveluja yleisölle. Lain perusteluissa yleisö täsmennetään käyttäjäryhmäksi, jota ei ole ennalta rajattu esimerkiksi työ-, virka- tai asiakassuhteen perusteella: niinpä laki ei koskisi tilannetta, jossa esimerkiksi työnantaja hankkii varmenteen työntekijöilleen ulkoiselta varmentajalta. Lain piirissä olisivat ainakin sellaiset kansalaisvarmenteen kaltaiset tapaukset, joissa varmenteeseen luottava osapuoli ei ole minkäänlaisessa sopimussuhteessa varmentajaan eikä allekirjoittajaan.

Sähköinen allekirjoitus
Sähköisessä muodossa oleva tieto,
- joka on liitetty tai loogisesti liittyy allekirjoitettavaan tietoon
- jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä

Kehittynyt sähköinen allekirjoitus
Sähköinen allekirjoitus, joka
- liittyy yksiselitteisesti allekirjoittajaan
- yksilöi allekirjoittajan
- on luotu menetelmällä, jota allekirjoittaja voi pitää yksinomaisessa valvonnassaan
- paljastaa allekirjoitetun tiedon rämettymisen

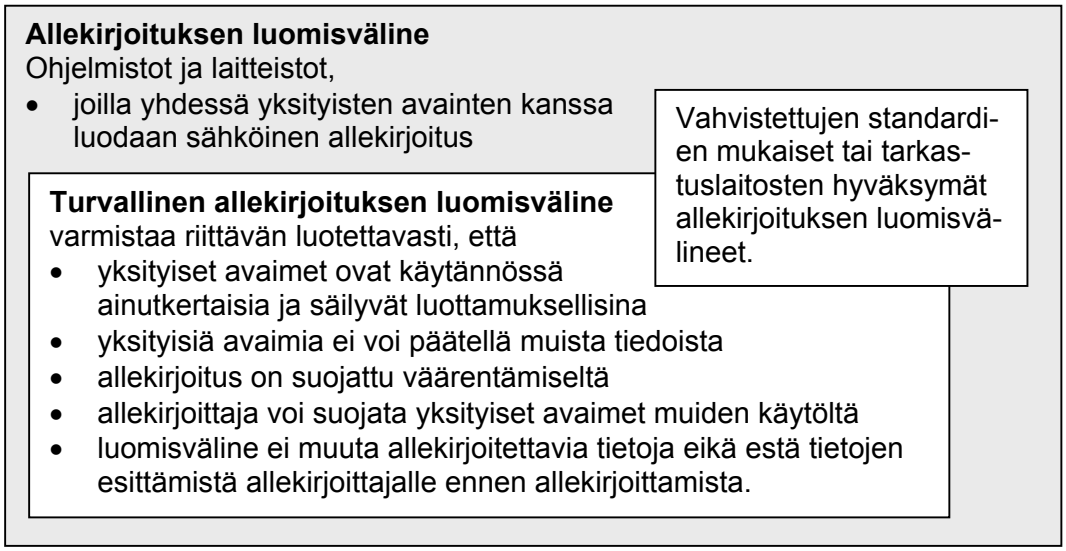
Kuva 30. Sähköisen allekirjoituksen ja kehittyneen sähköisen allekirjoituksen määritelmät havainnollistettuna.

Lakiesitys määrittelee **sähköisen allekirjoituksen** sähköisessä muodossa olevaksi tiedoksi, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä. **Kehittynyt sähköinen allekirjoitus** lisää edelliseen neljä vaatimusta: allekirjoituksen tulee liittyä yksiselitteisesti allekirjoittajaan; allekirjoituksen avulla tulee voida yksilöidä allekirjoittaja; allekirjoitus tulee olla luotu menetelmällä, jota allekirjoittaja voi pitää yksinomaisessa valvonnassaan; ja allekirjoituksen tulee liittyä muuhun sähköi-

seen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita. Käsitteiden eroa havainnollistetaan oheisessa kuvassa (Kuva 30).

Lakiesityksessä **allekirjoittaja** tarkoittaa luonnollista henkilöä, jolla on laillisesti hallussaan allekirjoituksen luomistiedot ja joka toimii itsensä tai edustamansa luonnollisen tai oikeushenkilön puolesta. Allekirjoittaja on siis aina luonnollinen henkilö, mikä ei muuta tilannetta nykyiseen verrattuna: esimerkiksi osakeyhtiössä yhtiöjärjestys voi nimetä yhtiön nimenkirjoittajaksi vaikkapa toimitusjohtajan, joka allekirjoittaa yhtiön sitoumukset. **Allekirjoituksen luomistiedoilla** tarkoitetaan allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämää ainutkertaista tietokokonaisuutta (kuten yksityisiä avaimia). **Allekirjoituksen todentamistieto** on sähköisen allekirjoituksen todentamisessa käytettävä tietokokonaisuus (kuten julkinen avain).

Allekirjoituksen luomisväline on ohjelmisto ja laite (kuten toimikortti), joilla yhdessä allekirjoituksen luomistietojen kanssa luodaan sähköinen allekirjoitus. **Turvallisen allekirjoituksen luomisvälineen** on lisäksi *riittävän luotettavasti* varmistettava, että allekirjoituksen luomistiedot ovat käytännössä ainutkertaisia ja ne säilyvät luottamuksellisina; allekirjoituksen luomistietoja ei voida päätellä muista tiedoista; allekirjoitus on suojattu väärentämiseltä; allekirjoittaja voi suojata allekirjoituksen luomistiedot muiden käytöltä; sekä luomisväline ei muuta allekirjoitettavia tietoja eikä estä tietojen esittämistä allekirjoittajalle ennen allekirjoittamista. Allekirjoituksen luomisväline on kuitenkin aina turvallinen, jos se on komission vahvistamien yleisesti tunnustettujen standardien mukainen tai jos tehtävään nimetty tarkastuslaitos on hyväksynyt sen. Käsitteitä on koottu oheiseen kuvaan (Kuva 31).



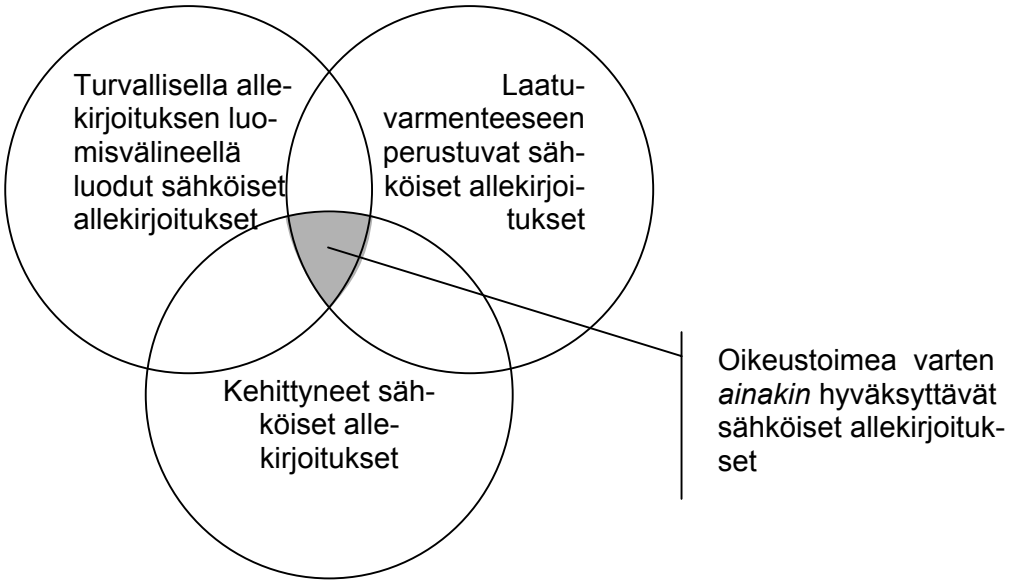
Kuva 31. Allekirjoituksen luomisvälineen ja turvallisen allekirjoituksen luomisvälineen määritelmät havainnollistettuna.

Kun digitaalisen allekirjoituksen luomiseen käytetään toimikorttia, PKI-asiakasohjelmisto laskee allekirjoitettavasta dokumentista tiivisteen ja pyytää käyttäjää antamaan tarvittavan PIN-koodin. Niinpä määritelmää voidaan tulkita niin, että PKI-toimikortin lisäksi myös toimikortinlukija, PKI-asiakasohjelmisto ja kaikki muu työasemassa allekirjoituksen luomiseen osallistuva ohjelmisto käyttöjärjestelmä mukaan lukien ovat allekirjoituksen luomisvälineitä. Lain perustelujen mukaan turvallisen allekirjoituksen luomisvälineen yhteydessä 'riittävän luotettavasti' tarkoittaa mahdollisimman suurta luotettavuutta, joka voidaan saavuttaa käyttämällä hyväksi parhaimpia mahdollisia teknisiä ratkaisuja. Erikseen on kuitenkin määritelty vielä **sähköisiin allekirjoituksiin liittyvä tuote**, joka tarkoittaa laitteistoa tai ohjelmistoa tai niiden merkityksellistä osaa, jotka on tarkoitettu palveluntarjoajan käyttöön tämän tarjotessa sähköiseen allekirjoitukseen liittyviä palveluja tai käytettäväksi sähköisten allekirjoitusten luomiseen tai todentamiseen.

Lakiesitys määrittelee **varmenteen** sähköiseksi todistukseksi, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa hänen henkilöllisyytensä. Varmenteet tarjoaa **varmentaja**, joka on luonnollinen henkilö tai oikeushenkilö. **Laatuvarmenne** puolestaan on varmenne, joka sisältää lakiesityksessä määritellyt tiedot (kuten varmentajan nimen ja sijaintivaltion sekä varmenteen haltijan nimen tai peitenimen) ja jonka antaa laissa säädetyt vaatimukset täyttävä varmentaja.
Laatuvarmentajan tulee muun muassa huolehtia henkilöstönsä asiantuntemuksesta, kokemuksesta ja pätevyydestä sekä turvata yksityisten avaintensa luottamuksellisuudesta. Varmenteen haltijalle luovutettujen allekirjoitusavainten kopioiminen on erityisesti kiellettyä. Laatuvarmentajan tulee huolehtia käyttämiensä laitteiden ja ohjelmistojen turvallisuudesta ja luotettavuudesta. Varmentajan on huolellisesti ja luotettavalla tavalla tarkistettava varmenteen hakijan henkilöllisyys ja todennettava hänet henkilökohtaisesti. Lisäksi laatuvarmentajan tulee ylläpitää sulkulistaa, johon peruutetut laatuvarmenteet asetetaan välittömästi.

Lakiesityksen 17. pykälän mukaan vastuu yksityisten avainten oikeudettomasta käytöstä siirtyy varmenteen haltijalta varmentajalle sillä hetkellä kun varmenteen peruutuspyyntö saapuu varmentajalle. Kuluttaja on vastuussa yksityisen avaimen oikeudettomasta käytöstä vain, jos hän on luovuttanut yksityiset avaimet toiselle; jos yksityisten avainten joutuminen niiden käyttöön oikeudettomalle on aiheutunut hänen lievää suuremmasta huolimattomuudestaan; tai jos hän menetettyään luomistietojen hallinnan muulla kuin edellisessä kohdassa mainitulla tavalla on laiminlyönyt varmenteen peruutuspyynnön. Varmenteen haltija saa siis syyllistyä lievään huolimattomuuteen joutumatta vahingonkorvausvastuuseen, kunhan muistaa peruuttaa varmenteen välittömästi sen jälkeen kun havaitsee yksityisten avainten kadonneen.

Jo nykyisin suurin osa yksityisoikeudellisista oikeustoimista on muotovapaita, ja sopimusvapaus ja vapaa todistusharkinta tarjoavat jo nyt hyvän mahdollisuuden käyttää sähköisiä allekirjoituksia. Jos oikeustoimeen vaaditaan kuitenkin lain mukaan allekirjoitus, täyttää vaatimuksen lakiesityksen 18. pykälän mukaan *ainakin* sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä (Kuva 32). Lakiesitys ei siis edellytä, että laatuvarmenteeseen perustuvan allekirjoituksen tekemiseen käytettäisiin aina turvallista allekirjoituksen luomisvälinettä tai että laatuvarmenteeseen perustuva sähköinen allekirjoitus olisi aina kehittynyt sähköinen allekirjoitus. Oikeustoimen edellyttämä allekirjoitus voidaan tehdä ainakin silloin kun kaikki mainitut piirteet täyttyvät, mutta joissain tapauksissa myös ilman.



Kuva 32. Oikeustoimessa käsin tehtyyn allekirjoitukseen rinnastuva sähköinen allekirjoitus.

Turvallista allekirjoituksen luomisvälinettä ja kehittynyttä sähköistä allekirjoitusta kohtaan on esitetty kritiikkiä [BOHM00]. Kriitikoiden näkemyksen mukaan tällä hetkellä ei ole vielä olemassa teknologiaa, joka täyttäisi kehittyneen sähköisen allekirjoituksen vaatimukset. Esimerkiksi allekirjoituksen luominen PKI-toimikortilla ei ole menetelmä, jota allekirjoittaja kykenisi pitämään yksinomaisessa valvonnassaan (luku 6.4.2). Kriitikot eivät myöskään tunne ohjelmistoja ja laitteistoja, jotka täyttäisivät turvallisen allekirjoituksen luomisvälineen vaatimukset. Turvalliseksi katsottavia allekirjoituksen luomisvälineitä voi syntyä siis vain sitä kautta, että välineet täyttävät komission vahvistamat yleisesti tunnetut standardit tai että tehtävään nimetty tarkastuslaitos hyväksyy välineet. Allekirjoituksen luontivälineen muuttaminen turvalliseksi hallinnollisella päätöksellä vaikuttaa kuitenkin erikoiselta.

Direktiivistä ja siihen pohjautuvasta lakiesityksestä kuitenkin näkee, että myös viranomaiset ovat lakia säätäessään tienneet yksityisten avainten suojaamiseen ja väärinkäytön estämiseen liittyvät ongelmat. Komissio tai tarkastuslaitos voi katsoa laitteen ja ohjelmiston turvalliseksi allekirjoituksen luomisvälineeksi, vaikka lakiin kirjatut kriteerit eivät täytykään. Oikeustointa varten voidaan hyväksyä myös muut kuin kehittyneet sähköiset allekirjoitukset. Toisaalta oikeusvaikutukseltaan sähköinen allekirjoitus rinnastetaan vain käsin tehtyyn allekirjoitukseen – myös käsin tehtyjä allekirjoituksia voidaan väärentää ja kiistää. Lakiesityksessä on siis huomioitu, että myös digitaalisia allekirjoituksia voidaan ja tullaan kiistämään. Perusasetelma ei siis muutu, kun siirrytään käsin tehdyistä allekirjoituksista digitaalisiin allekirjoituksiin – vain välineet ja menetelmät muuttuvat. [BOHM00]

7. PKI:A HYÖDYNTÄVIÄ PROTOKOLLIA

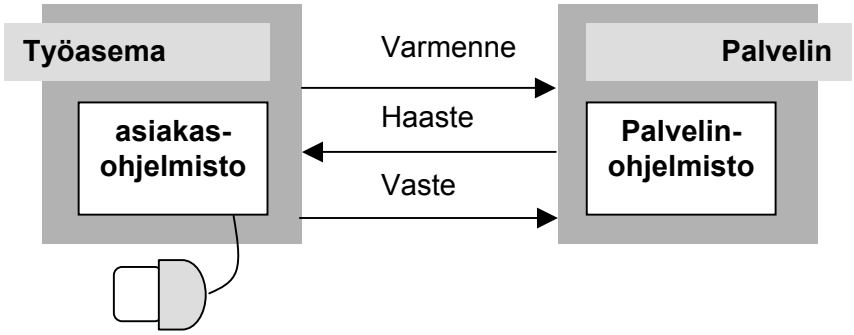
Aikaisemmissa luvuissa kerrottiin, kuinka epäsymmetristä salausmenetelmää, julkisen avaimen järjestelmää ja toimikortteja voidaan käyttää salattujen viestien vaihtamiseen. Tässä luvussa syvennytään muutamaan keskeiseen tietoliikenneprotokollaan, jotka hyödyntävät julkisen avaimen järjestelmää erityisesti käyttäjän henkilöllisyyden todentamisessa henkilövarmenteen avulla. Tässä luvussa käyttäjään viitataan pääasiassa käyttämällä asiakas/palvelin-arkkitehtuurin yleisesti käytettyä termiä asiakas (client).

7.1. Yhteisiä piirteitä

Useimmat julkisen avaimen järjestelmää hyödyntävistä protokollista, kuten TLS ja Secure shell, ovat sellaisenaan jo yleisessä käytössä ja julkisen avaimen järjestelmää käytetään asiakas/palvelin-arkkitehtuurissa nykyisin yleisesti palvelimen todentamisessa (server authentication). Asiakkaan todentamisessa (client authentication) käytetään nykyisellään tavallisesti salasanaa. Itse protokollien määrittelyssä on kyllä otettu huomioon julkisen avaimen järjestelmän hyödyntäminen myös asiakkaan todentamisessa, mutta näitä piirteitä ei juurikaan ole käytetty. Keskeinen syy tähän on se, että tähän mennessä varsin harvalla käyttäjällä on ollut henkilökohtainen varmenne, jota on voinut käyttää asiakkaan todentamisessa. Tässä yhteydessä syvennytään erityisesti asiakkaan todentamiseen varmenteen avulla.

Asiakas/palvelin-arkkitehtuurin ajatellaan suppeassa merkityksessään tavallisesti koostuvan asiakastietokoneesta, palvelintietokoneesta ja näiden käyttämään protokollaan perustuvasta viestien vaihdosta. Todentamista tutkittaessa laajempi näkemys on tarpeen: asiakkaalla ei niinkään ymmärretä sitä tietokonelaitteistoa, jossa palvelimelle lähetettävät viestit tuotetaan (esimerkiksi mikrotietokoneessa käytettävä WWW-selain, joka lähettää kyselyjä WWW-palvelimelle HTTP-protokollan avulla) vaan palvelun tiettyä käyttäjää – ihmistä, joka tietokonelaitteiston välityksellä asioi esimerkiksi pankin verkkopalveluissa. Pankkiahan ei niinkään kiinnosta se, miltä tietokoneelta tai päätelaitteelta pankin asiakas on yhteydessä pankin palvelimeen. Sen sijaan pankki haluaa tietää, kuka pankin asiakkaista on kysymyksessä: kenen tililtä asiakkaan antamat maksumääräykset tulee veloittaa. Asiakkaan todentamisessa toki käytetään apuna tietokonelaitteita, kuten esimerkiksi WWW-selaimen sisältävää mikrotietokonetta ja siihen kytkettyä PKI-toimikorttia. Käytännössä tällöin syntyy ketju, jossa pankin palvelin todentaa varmenteen avulla asiakkaan PKI-toimikortin (vahva todentaminen), ja PKI-toimikortti todentaa PIN-koodin avulla haltijansa (heikko todentaminen).

Vastaavalla tavalla palvelimella ei niinkään tarkoiteta palvelua toteuttavaa tietokonelaitteistoa, kuten WWW-palvelinta: palvelin tarkoittaa itse asiassa palvelua ja siitä vastaavaa yritystä. Eihän esimerkiksi verkkopankkia käyttävää asiakasta niinkään kiinnosta, millä tietokonelaitteistolla pankki on palvelunsa toteuttanut ja onko rikkoontunut tietokonelaite kenties edellisenä yönä vaihdettu uuteen vastaavaan. Sen sijaan pankin valveutunutta asiakasta kiinnostaa, että palvelin, jonka kanssa hän verkon välityksellä asioi, todella kuuluu sille pankille, jonka asiakas hän on, eikä esimerkiksi huijarille, joka toivoo pankin asiakkaiden hyväuskoisuuttaan paljastavan salasanansa pystytetylle valepalvelulle. Palvelimen todentamisella pyritään varmistamaan, että tietokonelaitteisto, johon asiakas on yhteydessä, todella kuuluu sille palveluntarjoajalle, jolle asiakas sen olettaa kuuluvan.



Kuva 33. Varmenteeseen perustuva asiakkaan todentaminen palvelimelle.

Varmenteen avulla tapahtuvan todentamisen yleinen periaate on esitetty ohessa (Kuva 33). Asiakkaalla on varmenne, johon liittyvä yksityinen avain sijaitsee vaikkapa toimikortilla. Asiakas tunnistautuu palvelimelle esittämällä varmenteensa. Todentaakseen asiakkaan palvelin lähettää haasteen (luku 4.6.), johon asiakas johtaa yksityisen avaimensa avulla vastauksen. Palvelin purkaa vastauksen varmenteesta poimitun julkisen avaimen avulla. Jos tulos ja esitetty haaste täsmäävät, voi palvelin olla varma, että asiakkaalla on hallussaan varmenteeseen liittyvä yksityinen avain.

Tyypillistä useimmille julkisen avaimen järjestelmää hyödyntäville tietoliikenneprotokollille on, että protokolla ja siihen sisältyvä asiakkaan todentaminen eivät välitä siitä, miten yksityinen avain on suojattu; onko se talletettu esimerkiksi kiintolevylle vai toimikortille. Yksityistä avainta käyttäessään tietoliikenneprotokollan asiakaspään toteutus pelkästään hyödyntää kappaleessa 6.3. esitetyn PKI-asiakasohjelmiston tarjoamaa ohjelmointirajapintaa murehtimatta asiaa sen enempää. Niinpä varmenteeseen perustuvassa asiakkaan todentamisessa ainoa tieto, joka näkyy palvelimelle, on asiakkaan esittämä varmenne. Tietoliikenneprotokollat eivät yleensä tarjoa palvelimelle eksplisiittisesti tietoa siitä, onko varmenteeseen liittyvä yksityinen avain talletettu esimerkiksi toimikortille. Palvelimella on kuitenkin mahdollisuus hankkia kyseinen tieto muuta kautta. Asiakkaan esittämässä

X.509v3-varmenteessa voidaan viitata varmennepolitiikkaan, jonka puitteissa varmenne on myönnetty. Kuten aikaisemmin todettiin, varmennepolitiikka ottaa kantaa muun muassa yksityisen avaimen sijoituspaikkaan ja suojaamiseen.

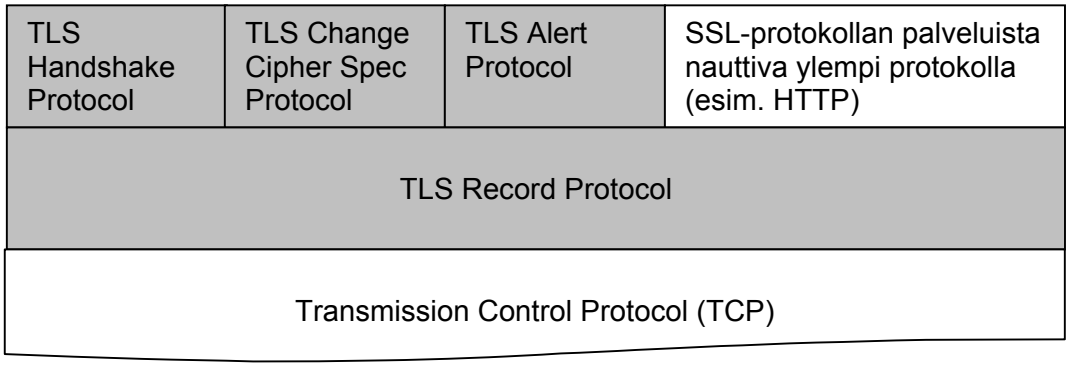
7.2. Transport Layer Security (TLS)

WWW-selaimen ja -palvelimen välisen tiedonsiirron luottamuksellisuus, eheys ja osapuolten todentaminen voidaan varmistaa IETF:n määrittelemällä Transport Layer Security -protokollalla [RFC2246]. TLS on hyvin lähellä yhdysvaltalaisen Netscape Commucations -yhtiön alun perin määrittelemää Secure Sockets Layer (SSL) -protokollaa, jonka nykyisin käytössä oleva versio on 3.0 [FRIE96]. WWW-palvelimet ovat vähitellen siirtymässä SSL-protokollasta TLS-protokollan käyttöön.

TLS-protokolla mahdollistaa varmenteen käytön sekä asiakkaan että palvelimen todentamisessa. Koska varmenteita on nykyisin käytössä lähinnä vain palvelimilla, on asiakkaan todentaminen toteutettu muilla tavoin, esimerkiksi TLS-protokollan päällä ajettavan HTTP-protokollan tarjoamalla Basic authentication -palvelulla, joka perustuu käyttäjätunnukseen ja salasanaan. Asiakkaan varmenteen avulla tapahtuva todentaminen, johon tässä lähinnä keskitytään, on TLS-protokollassa vapaaehtoinen ominaisuus. Tässä esitetyn lähteenä on käytetty [STAL99].

7.2.1. TLS-protokollan rakenne

TLS-protokolla koostuu itse asiassa neljästä eri protokollasta, jotka on esitetty ohessa (Kuva 34). TLS Record Protocol tarjoaa ylemmän tason protokollille luottamuksellisen kuljetuspalvelun, joka perustuu palvelimen ja asiakkaan sopimaan symmetriseen salausavaimeen. Salausavain sovitaan yhteydenmuodostusvaiheessa. Valittavana on joukko vaihtoehtoisia symmetrisiä algoritmeja, kuten DES, 3DES, RC4 ja IDEA.



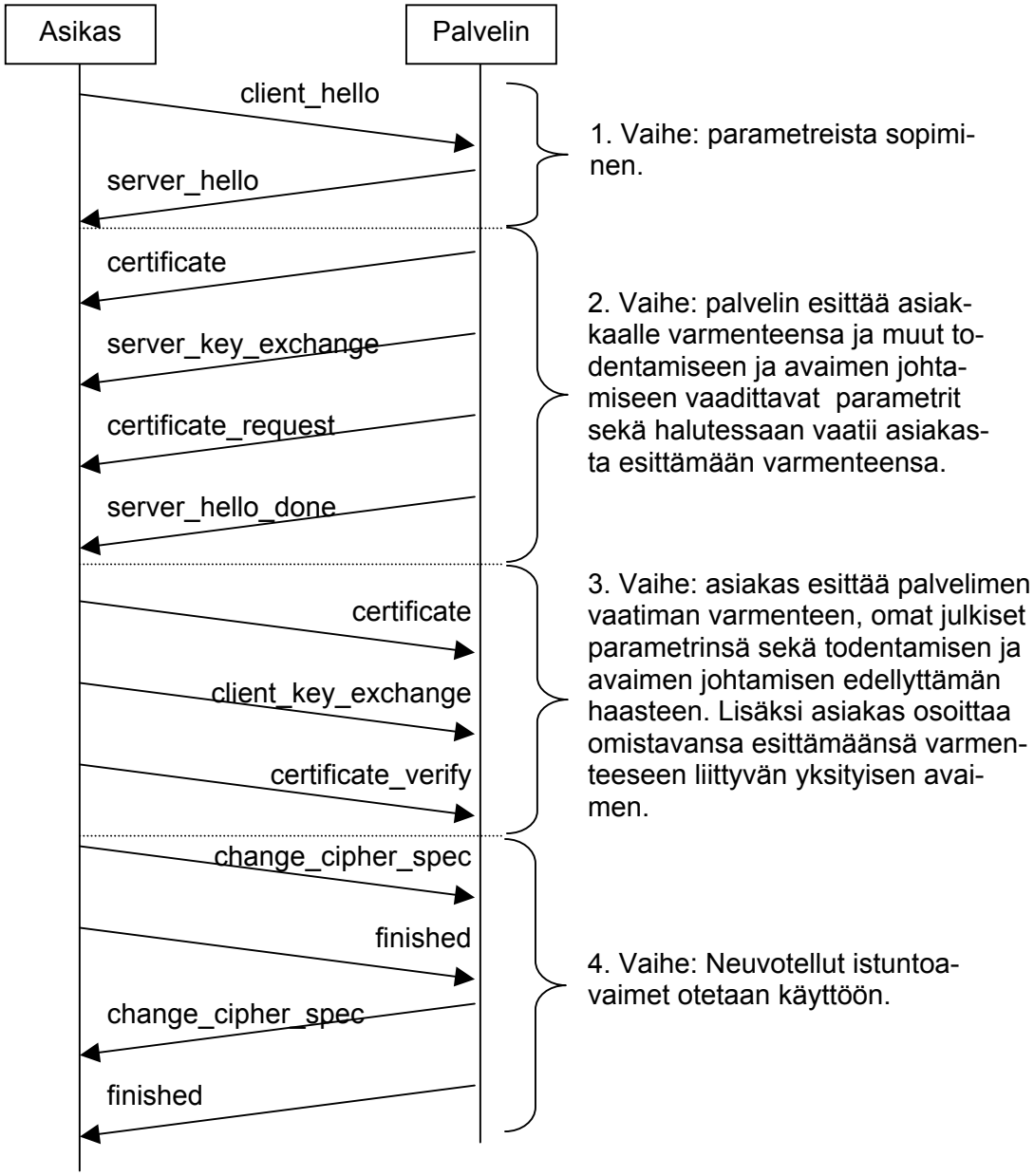
Kuva 34. TLS-protokolla koostuu neljästä protokollasta.

TLS Record Protocol huolehtii myös kuljetettavan protokollan eheystarkistuksesta. Jos kuormaa havaitaan siirron aikana peukaloidun, on TLS-protokollan tehtävänä suorittaa hälytys sekä asiakas- että palvelinpäähän. Vastapuolelle hälytyksen toimittaa TLS Alert Protocol, joka vie asiakkaan ja palvelimen välisiä viestejä paitsi eheysrikoista, myös muista havaituista ongelmista. Tällaisia voivat olla esimerkiksi vastapuolen vanhentuneet, vialliset, rämettyneet tai sulkulistalle asetetut varmenteet, joita hän on koettanut käyttää yhteydenmuodostusvaiheessa.

7.2.2. Yhteydenmuodostus

TLS-protokollan monimutkaisin osa on yhteydenmuodostus, jonka avulla osapuolet todentavat toisensa ja sopivat käytettävistä salausalgoritmeista ja -avaimista. Yhteydenmuodostus suoritetaan ennen kuin ylemmän tason protokollalle annetaan lupa aloittaa tiedonsiirto TLS-yhteyden yli. Yhteydenmuodostuksen toteuttavat TLS Handshake Protocol ja TLS Change Cipher Spec Protocol. Leijonanosan toiminnallisuudesta toteuttaa Handshake Protocol.

Yhteydenmuodostukseen liittyvät viestit on esitetty ohessa (Kuva 35). Yhteydenmuodostus voidaan jakaa neljään osaan. Ensimmäisessä osassa osapuolet vaihtavat tietoja tukemistaan ominaisuuksista, kuten salaus- ja tiivistealgoritmeista (client_hello, server_hello). Samassa yhteydessä vaihdetaan myös satunnaislukuja ja aikaleimoja, joita myöhemmin käytetään apuna istuntoavaimia ja todentamiseen tarvittavia haasteita johdettaessa.



Kuva 35. Viestisekvenssikaavio TLS-yhteydenmuodostuksesta.

Toisessa vaiheessa palvelin lähettää asiakkaalle palvelimen todentamiseen ja symmetrisen salausavaimen vaihtoon tarvittavia tietoja. Palvelin lähettää asiakkaalle oman varmenteensa ja kaikki muutkin varmenteet, joita tarvitaan varmenneketjun todentamisessa (certificate). Käytetystä avaimenjohtamismenetelmästä riippuen palvelin saattaa lähettää asiakkaille varmenteiden lisäksi myös muita avaimen johtamiseen tarvittavia julkisia parametreja (server_key_exchange).

Toisen vaiheen lopuksi palvelin voi vastavuoroisesti pyytää myös asiakasta todennettavaksi (certificate_request). Tässä yhteydessä palvelin luettelee asiakkaalle tukemansa epäsymmetriset salausalgoritmit ja ilmoittaa varmentajat, joiden myöntämät varmenteet se hyväksyy tunnistamisvälineenä. Tämän jälkeen palvelin antaa puheenvuoron asiakkaalle (server_hello_done).

Kolmas vaihe käsittää asiakkaan todentamisen ja vie loppuun symmetrisen salausavaimen vaihdon. Asiakas lähettää palvelimelle tämän pyytämän varmenteen (certificate) sekä käytetystä avaimenjohtamismenetelmästä riippuen omat julkiset parametrinsa tai haasteen, jonka avulla asiakas myöhemmin varmistaa, että palvelimella on hallussaan esittämäänsä varmenteeseen liittyvä yksityinen avain (client_key_exchange). Lisäksi asiakas itse osoittaa omistavansa edellä esittämäänsä varmenteeseen liittyvän yksityisen avaimen. Asiakas allekirjoittaa yksityisellä avaimellaan haasteen, joka on johdettu asiakkaan ja palvelimen aikaisempien viestien pohjalta (certificate_verify).

Nyt asiakas ja palvelin ovat sopineet tarvittavista parametreista ja vaihtaneet kaiken tarvittavan tiedon, joiden pohjalta osapuolet voivat laskea symmetrisen salausavaimen. Neljännessä vaiheessa asiakas ilmoittaa TLS Change Cipher Spec -protokollan avulla palvelimelle, että TLS Record Protocol voi nyt ottaa käyttöön uuden istunnon ja siihen liittyvän istuntoavaimen (change_cipher_spec). Mikäli palvelin pystyy tämän jälkeen lukemaan asiakkaan sille lähettämän viimeisen TLS Handshake -protokollan viestin (finished), joka sisältää aikaisempien viestien avulla lasketun tiivisteen ja jonka TLS Record Protocol on siirtänyt uuden istuntoavaimen avulla salattuna, on istuntoavaimen johtaminen onnistunut. Vastaavat viestit (change_cipher_suite ja finished) lähetetään vielä palvelimelta asiakkaalle. Jos asiakas pystyy avaamaan viestit, on palvelimellakin käytössä sama istuntoavain, mikä puolestaan edellyttää, että palvelin on laskenut oikean vasteen asiakkaan aiemmin esittämään haasteeseen. Näin myös palvelin on saatu todennetuksi.

Kun TLS-yhteydenmuodostus ja siihen kuuluva varmenteeseen perustuva asiakkaan todentaminen on saatu päätökseen, on palvelin varmistanut, että asiakkaalla on hallussaan esitettyyn varmenteeseen sisältyvää julkista avainta vastaava yksityinen avain. Pääsynvalvonnan tehtävä on kyseisen varmenteen ja käyttäjille annettujen valtuuksien perusteella päätellä, mihin asioihin asiakkaalla on valtuudet – esimerkiksi, mitä WWW-sivuja asiakkaalla on oikeus selata TLS-yhteyden yli.

WWW-palvelimien kohdalla asia on käytännössä ratkaistu niin, että TLS-yhteydenmuodostuksen yhteydessä palvelimen asettamat ympäristömuuttujat tarjoavat tietoa asiakkaan esittämästä varmenteesta CGI- tai muille sovelluksille. Esimerkiksi Apache-palvelimessa, jossa TLS-protokollan toteuttaa avoimeen lähdekoodiin perustuva mod_ssl-moduli, suoritettava CGI-sovellus voi lukea varmenteenhaltijan distinguished name (DN) -kentän ympäristömuuttujasta, jonka nimi on SSL_CLIENT_S_DN [MODS02]. CGI-sovellus voi luottaa siihen, että WWW-palvelin on todentanut asiakkaan ja että vastapuolella on varmasti kyseiseen varmenteeseen liittyvä yksityinen avain.

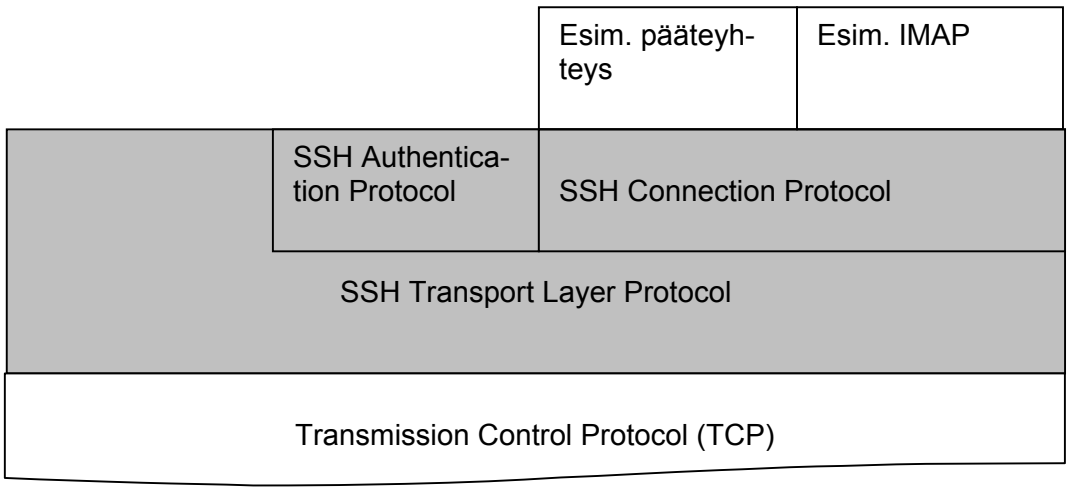
7.3. Secure shell (SSH)

TLS-protokollan tavoin myös Secure shell -protokolla tarjoaa kuljetuspalvelua, johon sisältyy symmetrisellä istuntoavaimella toteutettu luottamuksellinen yhteys asiakkaan ja palvelimen välille, eheystarkistus sekä molempien osapuolien todentaminen. Alkujaan Teknillisessä korkeakoulussa kehitetyn protokollan versiota 2.0 ollaan parhaillaan työstämässä IETF:ssä, jossa julkaistuihin Internet-drafteihin [YLON02a, YLON02b, YLON02c, YLON02d] tässä esitetty perustuu.

Alkujaan Secure shell kehitettiin Unix-palvelinten pääteyhteyksiä (terminal) varten turvattoman Telnet-protokollan korvaajaksi. Vaikka Secure shell mahdollistaa myös muun liikenteen tunneloinnin asiakkaan ja palvelimen välillä, on sen käyttö pitkälti keskittynyt pääteyhteyksiin, eikä sitä juurikaan käytetä esimerkiksi TLS-protokollan korvaajana WWW-yhteyksien salauksessa.

7.3.1. Secure shell -protokollan rakenne

Secure shell -protokolla koostuu kolmesta protokollasta, joiden asemaa on selvennetty ohessa (Kuva 36). SSH Transport Layer Protocol tarjoaa muille protokollille luottamuksellisen kuljetuspalvelun, johon liittyy eheystarkistus ja siirrettävän tiedon pakkaaminen. Protokolla huolehtii myös käytettävien algoritmien ja salausavainten neuvottelusta asiakkaan ja palvelimen kesken yhteyttä muodostettaessa. Symmetrisen istuntoavaimen sopiminen tapahtuu luvussa 4.3 esitellyn Diffie-Hellmanin avaimensopimisprotokollan avulla. Protokollaan sisältyvä palvelimen tekemä allekirjoitus suojaa yhteyttä välimieshyökkäykseltä ja lisäksi todentaa palvelimen asiakkaalle.



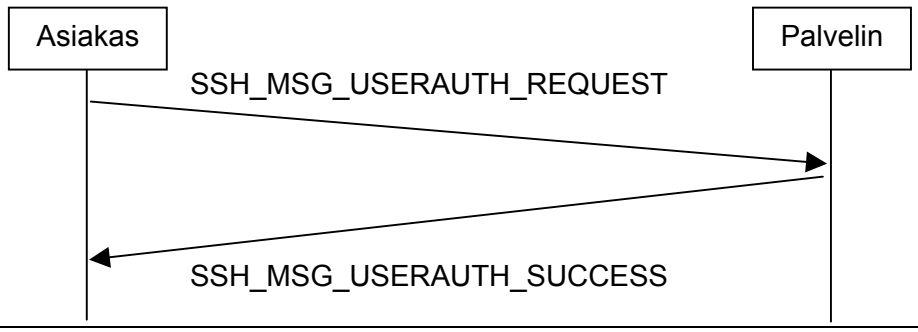
Kuva 36. Secure shell -protokolla koostuu kolmesta protokollasta.

SSH Connection Protocol mahdollistaa usean toisistaan riippumattoman kanavan avaamisen SSH Transport Layer -protokollan tarjoaman kuljetuspalvelun varaan. Kanavien avulla asiakas voi avata pääteyhteyksiä palvelimelle tai suorittaa siellä yksittäisiä komentoja. Lisäksi asiakkaan ja palvelimen välillä voidaan tunneloida X11-yhteyksiä tai yksittäisiä TCP-portteja, jolloin sinällään turvattomien, TCP:tä käyttävien protokollien, kuten sähköpostin noutamiseen käytettävän IMAP-protokollan, turvallisuutta saadaan kohennettua.

7.3.2. Asiakkaan todentaminen

Asiakkaan todentaminen on suunniteltu suoritettavaksi SSH Transport Layer -protokollan suorittaman yhteydenmuodostuksen jälkeen, ennen kuin SSH Connection Protocol avaa ensimmäisen kanavan asiakkaan ja palvelimen välille. SSH Authentication Protocol määrittelee kolme vaihtoehtoista todentamistapaa, joista salasanaan ja julkiseen avaimeen perustuvia menetelmiä esitellään alla. Kolmannessa vaihtoehdossa palvelin todentaa käyttäjänsä sijaan sen järjestelmän, josta tämä on avaamassa yhteyttä, ja luottaa kyseisen järjestelmän suorittamaan asiakkaan todentamiseen. Kyseinen menettely soveltuu luontevasti esimerkiksi silloin, kun käyttäjä on avaamassa Secure shell -istuntoa saman organisaation ylläpitämältä Unix-palvelimelta käsin.

SSH Authentication -protokollan toiminta on yksinkertainen, kun todentaminen perustuu salasanaan (Kuva 37): asiakas lähettää SSH Transport Layer -protokollan tarjoamaa salattua kuljetuspalvelua käyttäen palvelimelle viestin ssh_msg_userauth_request, jonka parametrit on esitetty ohessa. Mikäli salasana on oikea, palvelin vastaa todentamisen onnistuneen lähettämällä viestin ssh_msg_userauth_success. Jos käyttäjätunnus tai salasana ovat väärin tai salasanaan perustuva todentaminen on kytketty pois käytöstä, lähetetään vastaus ssh_msg_userauth_failure, johon liitetään luettelo palvelimen hyväksymistä todentamismenetelmistä. Voi myös olla, että käyttäjätunnus ja salasana on kyllä annettu oikein, mutta palvelin edellyttää varmuuden vuoksi vielä toista onnistunutta todentamista esimerkiksi julkisen avaimen avulla. Tällöin vastausviestin parametrina tulee tieto todentamisen osittaisesta onnistumisesta.



SSH_MSG_USERAUTH_REQUEST -viestin parametrit	
user name	Käyttäjätunnus, jonka haltijaa ollaan todentamassa ts. jota käyttäen palvelimelle kirjaudutaan.
service	Palvelu, joka käynnistetään onnistuneen todentamisen jälkeen. Esim. "ssh-connection", joka aktivoi SSH Connection -protokollan palvelut.
"password"	Ilmaisee todentamisen tapahtuvan salasanalla
"true"/"false"	Vaihdetaanko samalla salasanaa
password	Salasana selkokielisenä
new password	Uusi salasana, jos salasana halutaan samalla vaihtaa

Kuva 37. Asiakkaan onnistunut todentaminen salasanaa käyttämällä.

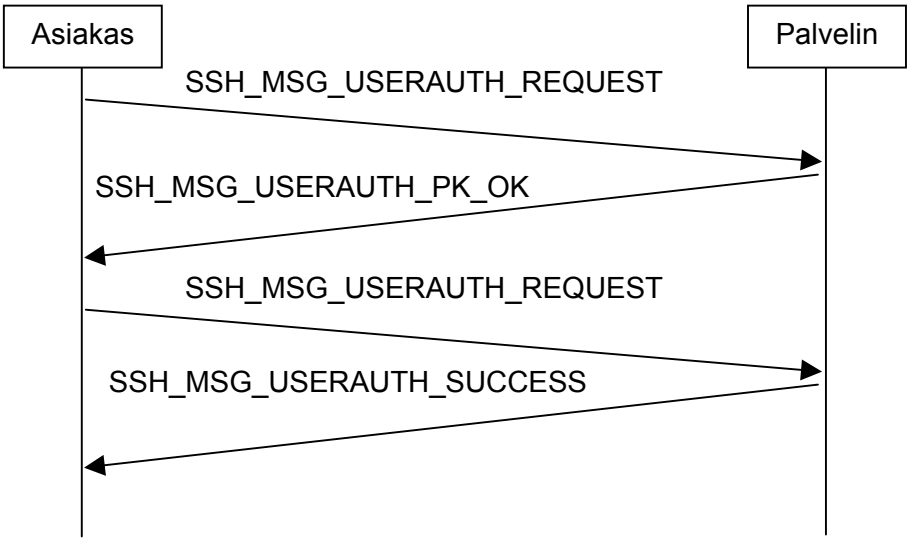
Vaikka salasana lieneekin yleisin tapa todentaa käyttäjän henkilöllisyys, ainoa toteutuksilta standardin mukaan edellytettävä todentamismenetelmä on julkiseen avaimeen perustuva todentaminen. Tällöin lähtökohtana on, että palvelimella on hallussaan käyttäjälle kuuluva julkinen avain, ja palvelin selvittää haaste/vastemenetelmällä, onko käyttäjällä hallussaan vastaava yksityinen avain.

Kuten aikaisemmin todettiin, epäsymmetristä salausta käytettäessä on aina tavalla tai toisella toteutettava julkisen avaimen järjestelmä. Yksinkertaisimmassa (ja nykyisissä toteutuksissa myös yleisimmässä) järjestelmässä asiakas luo itselleen avainparin tai hankkii PKI-toimikortin ja käy sen jälkeen itse viemässä julkisen avaimensa Secure Shell -palvelimelle. Tämä tapahtuu esimerkiksi avaamalla Secure Shell -pääteistunto, jossa todentaminen tapahtuu salasanalla, ja siirtämällä julkinen avain pääteistunnon välityksellä palvelimelle, tyypillisesti käyttäjän omaan kotihakemistoon. Esitetty järjestely on helppo toteuttaa, mutta haittapuolena on, että se ei lisää ratkaisevasti todentamisen luotettavuutta. Julkista avainta palvelimelle kopioitaessa tarvitaan edelleen salasanaa ja jokaisen käyttäjän tulee voida kirjautua palvelimelle salasanan avulla ainakin yhden kerran.

SSH Authentication Protocol mahdollistaa myös varmenteisiin perustuvan julkisen avaimen järjestelmän käytön, jolloin edellä esitetty "ketjun heikko lenkki" on vältettävissä. Tällöin Secure Shell -palvelimen ylläpitäjä määrittelee luotettavana pitämänsä varmentajat sekä toteuttaa järjestelyt, joiden avulla palvelin pystyy päättelemään, mihin käyttäjätunnukseen varmenteen haltijalla on oikeus. Palvelimen ylläpitäjä saattaa esimerkiksi määritellä, että Väestörekisterikeskuksen myöntämä

kansalaisvarmenne, jonka kohteen common name (CN) on "MIKAEL LINDEN 10005323B", oikeuttaa kirjautumaan palvelimelle käyttäjätunnuksella *linden*.

Julkiseen avaimeen perustuva todentaminen käyttää salasanatodentamisen kanssa pitkälti samoja viestejä, jotka on esitetty oheisessa viestisekvenssikaaviossa (Kuva 38). Salasanatodentamisesta poiketen viestejä vaihdetaan tyypillisesti kaksi paria. Ensimmäisen ssh_msg_userauth_request-viestin tarkoitus on selvittää, salliiko palvelin ylipäätään kyseisen käyttäjän todentamisen esitetyn julkisen avaimen avulla. Mikäli esitetty julkinen avain palvelimen käsityksen mukaan kuuluu kyseiselle käyttäjälle, vastaa palvelin viestillä ssh_msg_userauth_pk_ok. Vasta tämän jälkeen asiakasohjelmisto laskee käyttäjän yksityisen avaimen avulla allekirjoituksen, joka sisältyy palvelimelle lähetettävään jälkimmäiseen ssh_msg_userauth_request-viestiin. Allekirjoitus lasketaan tiivisteestä, joka sisältää SSH Transport Layer -protokollan kyseiselle istunnolle antaman osaksi satunnaisen tunnistenumeron sekä kyseessä olevan ssh_msg_userauth_request-viestin muut parametrit.



Ensimmäisen SSH_MSG_USERAUTH_REQUEST -viestin parametrit	
user name	Käyttäjätunnus, jonka haltijaa ollaan todentamassa.
service	Palvelu, joka käynnistetään onnistuneen todentamisen jälkeen.
"publickey"	Ilmaisee todentamisen tapahtuvan julkisella avaimella
"false"	
public key algorithm name	Käytettävän epäsymmetrisen salausalgoritmin nimi
public key blob	Käyttäjän julkinen avain tai varmenteet

Toisen SSH_MSG_USERAUTH_REQUEST -viestin parametrit	
user name	ks. yllä
service	ks. yllä
"publickey"	ks. yllä
"true"	
public key algorithm name	ks. yllä
public key blob	ks. yllä
signature	Allekirjoitus, joka on laskettu yli istunnon tunnistenumeron ja koko muun viestin

Kuva 38. Asiakkaan onnistunut todennus SSH Authentication -protokollan avulla käyttämällä julkista avainta.

Kahteen viestiin jaetun todentamisen taustalla on käyttömukavuus. Julkiseen avaimeen perustuva todentaminen edellyttää raskasta laskentaa ja myös käyttäjän toimenpiteitä, kuten PIN-koodin tai salasanan syöttämistä. Käyttäjää ei haluta vaivata näillä toimenpiteillä, jos etukäteen on jo tiedossa, että palvelin ei missään tapauksessa tule hyväksymään esitettyä julkista avainta kyseisen käyttäjän tunnistamisvälineenä.

7.4. S/MIME

Yksi vanhimmista Internetin tarjoamista palveluista on sähköposti, joka sellaisenaan tarjoaa kuitenkin hyvin niukan tietoturvatason. Lähettäjältä vastaanottajalle liikkuvaa sähköpostia voi lukea ja peukaloida kuka vain, jolla on pääsy sähköpostiviestiä sen matkan varrella käsitteleviin verkkolaitteisiin tai joka voi kuunnella niiden välistä tietoliikennettä. Tässä mielessä sähköposti rinnastuu perinteisen postikortin lähettämiseen. Postikorttia käytetään yleensä lähinnä lomamatkaterveisten lähettämiseen, mutta sähköpostia käytetään yhä enemmän esimerkiksi liiketoiminnan apuvälineenä, jolloin sen turvallisuuteen on kohdistettava erityistä huomiota.

MIME-määritys (Multipurpose Internet Mail Extensions, RFC 2045–2049) mahdollistaa mitä tahansa binäärimuotoista dataa sisältävän tiedon lähettämisen sähköpostiviestinä. Viestin sisällön tyyppi kerrotaan sähköpostin otsakeosassa Content-Type-otsakkeen avulla. Esimerkiksi tavallisen tekstin sisällön tyyppi on text/plain, HTML-sivun text/HTML. Siirtoa varten viesti koodataan niin, että myös erikoismerkit välittyvät muuttumattomina lähettäjältä toiselle. MIME-määrityksen mukainen viesti voi koostua useasta itsenäisestä kokonaisuudesta, mikä mahdollistaa esimerkiksi tekstinkäsittelyohjelmalla tuotettujen asiakirjojen liittämiseen sähköpostiviestiin.

Luvussa 5.4.1. todettiin, että PGP-salausohjelmistoa voidaan soveltaa muun muassa sähköpostin turvalliseen käyttöön. Toinen tunnettu sähköpostien salaamiseen ja allekirjoittamiseen soveltuva protokolla on S/MIME (Secure/Multipurpose Internet Mail Extensions), joka laajentaa MIME-määritystä. S/MIME käyttää X.509v3-varmenteita ja pohjautuu PKCS#7-määritykseen ”Cryptographic Message Syntax Standard” [PKCS7] salattujen viestien rakenteen ja merkityksen esitystavassa. S/MIME on IETF:n standardoima, ja sen version 3 ytimen muodostavat RFC 2630–2634. Tässä esitetyn lähde on [STAL99] ja [HOUS01].

7.4.1. Sähköpostiviestin salaaminen

S/MIME käyttää digitaalista kirjekuorta (luku 4.3.) salatun sähköpostiviestin lähettämisessä. Viestin lähettäjällä on oltava käytettävissään viestin vastaanottajan varmenne. Viestin lähettäjä valitsee käytettävän symmetrisen salausmenetelmän ja symmetrisen istuntoavaimen sekä salaa viestin vastaanottajan varmenteesta saadulla julkisella avaimella. Itse viesti salataan symmetrisellä istuntoavaimella, ja salattu viesti ja vastaanottajan julkisella avaimella salattu istuntoavain Base64-koodataan siirtoa varten, jotta viesti siirtyisi muuttumattomana vastaanottajalle asti. Viestin sisällön tyypiksi asetetaan application/pkcs7-mime lisämääreenään enveloped-data (Kuva 39). Viestin vastaanottaja käyttää yksityistä avaintaan päästäk-

seen käsiksi julkisella avaimellaan salattuun istuntoavaimeen. Itse viestin salaus puretaan istuntoavaimella.

Viestin otsakkeet

Julkisella avaimella salattu istuntoavain ja istuntoavaimella salattu viesti

Kuva 39. Esimerkki salatusta S/MIME-viestistä.

Mikäli viestillä on monta vastaanottajaa, täytyy istuntoavain salata erikseen kunkin vastaanottajan julkisella avaimella. Jos vastaanottajia on lukuisia, voidaan istuntoavaimen salaaminen vastaanottajien julkisella avaimella jättää myös luotetun sähköpostilista-agentin (mail list agent, MLA) tehtäväksi. On myös syytä huomata, että vaikka viestin lähettäjä arkistoisikin lähettämänsä viestit, ei hän itse pysty enää lukemaan lähettämäänsä digitaaliseen kirjekuoreen suljettua viestiä sen jälkeen, kun istuntoavain on tuhottu viestin lähettäneen laitteen muistista.

7.4.2. Sähköpostiviestin allekirjoittaminen

Lähettäjä, joka haluaa allekirjoittaa sähköpostiviestinsä, valitsee käytettävän tiiviste- ja allekirjoitusalgoritmin, laskee viestistä tiivisteen ja salaa sen yksityisellä avaimellaan. Syntynyt allekirjoitus ja sen todentamiseen tarvittavat varmenteet liitetään lähetettävään viestiin. Viestin vastaanottaja todentaa allekirjoituksen ja siihen käytetyn varmenteen varmenneketjun.

Viesti voidaan lähettää käyttämällä edellisen kohdan esimerkin tapaan sisältötyyppiä application/pkcs7-mime tällä kertaa lisämääreenään signed-data. Koska kaikki sähköpostiasiakasohjelmat eivät tue S/MIME:ä, viesti ja allekirjoitus voidaan vaihtoehtoisesti lähettää myös kahdesta osasta koostuvana kokonaisuutena (Kuva 40). Toisen osan muodostaa allekirjoitettava viesti ja toisen allekirjoitus. Tällöin myös S/MIME:ä hallitsematon sähköpostiasiakasohjelma pystyy näyttämään käyttäjälleen allekirjoitetun viestin, vaikka ei osaakaan käsitellä allekirjoitusta. Kahdesta osasta koostuvan viestin sisältötyyppi on multipart/signed, ja allekirjoituksen sisältävä osa on tyypiltään application/pkcs7-signature.

Kuva 40. Esimerkki S/MIME-viestistä, jossa on allekirjoitus.

7.4.3. S/MIME:n käytöstä

Sama S/MIME-viesti voidaan sekä salata että allekirjoittaa – salaukseen käytetään istuntoavainta ja vastaanottajan julkista avainta ja allekirjoitukseen lähettäjän yksityistä avainta. S/MIME-määrityksen versio 3 mahdollistaa myös allekirjoitetut vastaanottokuittaukset. Lähettäjä, joka haluaa varmistua viestin perillemenosta, voi pyytää vastaanottajaa lähettämään ilmoituksen viestin saapumisesta.

Myös S/MIME-määrityksen kehittäjät ovat joutuneet ottamaan kantaa samannimisistä henkilöistä syntyvään ongelmaan. Jos viestin lähettäjä haluaa lähettää sähköpostia tuttavalleen Matti Virtaselle, ja hänen käytettävissään on kahdelle eri Matti Virtaselle kuuluva varmenne, kuinka lähettäjä voi tietää, kummalla varmenteella sähköposti tulee salata? S/MIME-määritys ratkaisee ongelman suosittelemalla sähköpostiosoitteen sisällyttämistä varmenteen lisäkenttiin (luku 5.8). Viestin vastaanottajan sähköpostiosoite on joka tapauksessa yksikäsitteinen ja useimmiten myös lähettäjällä tiedossa. Viestin lähettäjän tai hänen sähköpostiasiakasohjelmansa tehtävä on siis etsiä käsiinsä sellainen varmenne, jonka lisäkentässä on hänen tarkoittamansa Matti Virtasen sähköpostiosoite.

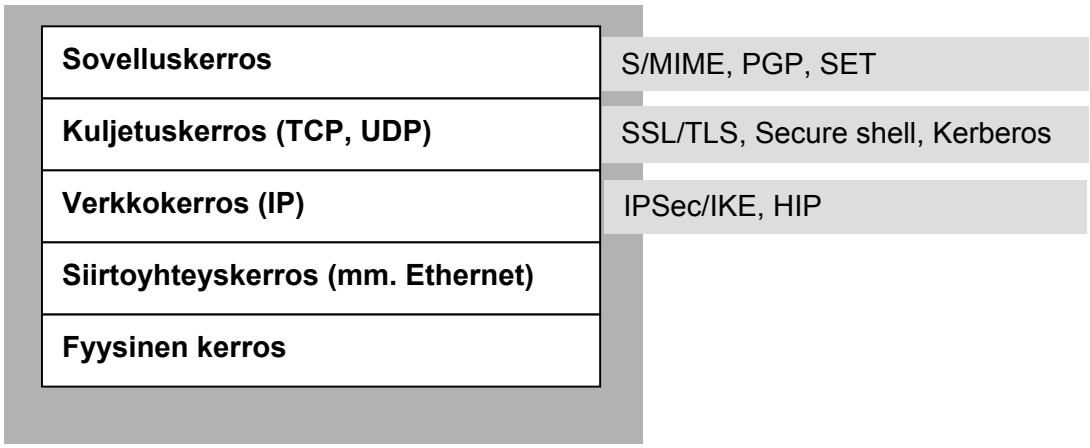
Suomalaisia S/MIME:n ja sähköisen henkilökortin käyttäjiä vaatimus sähköpostiosoitteesta on harmittanut. Koska Suomen kansalaisilla ei ole valtion järjestämää sähköpostiosoitetta, ei sitä ole myöskään voitu sisällyttää sähköisen henkilökortin kansalaisvarmenteeseen. Niinpä salatun ja allekirjoitetun sähköpostin käyttäminen oli pitkään sähköisen henkilökortin käyttäjien ulottumattomissa, kunnes S/MIME-standardin version 3 myötä vaatimusta löysennettiin ja sähköpostiosoite muutettiin pakollisesta suositeltavaksi [RFC2632].

S/MIME-toiminnallisuuksilla varustettuja sähköpostiasiakasohjelmia on melko hyvin saatavilla toimistokäyttöön, ja ne pystyvät hyödyntämään myös toimikortille talletettua yksityistä avainta. Sähköpostiasiakasohjelmat hyödyntävät luvussa 6.3. esiteltyjä PKI-asiakasohjelmiston tarjoamia rajapintoja viestin salaamisessa ja allekirjoittamisessa.

Vaikka S/MIME onkin luotu nimenomaan sähköpostin allekirjoittamista varten, voidaan samaa tekniikkaa käyttää myös laajemmin tilanteissa, joissa on tarpeen salata tai allekirjoittaa dokumentteja. Jotkin tuotteet esimerkiksi käyttävät S/MIME:n pohjana olevaa PKCS#7-määritystä WWW:n avulla toteutettavien sähköisesti allekirjoitettavien lomakkeiden toteutustekniikkana. Tällöin WWW-sivun kautta käynnistetään WWW-selaimeen asennettu lisäohjelma, joka huolehtii työasemaan asennetun PKI-asiakasohjelmiston avulla PKCS#7-allekirjoituksen tuottamisesta WWW-sivulla esitettyyn tietoon.

7.5. Muut protokollat

Edellä esiteltyjen kolmen protokollan lisäksi olemassa on lukuisia muita tietoliikenneprotokollia, jotka hyödyntävät varmenteita ja julkisen avaimen järjestelmää. Suuri joukko protokollista (kuten edellä esitetyt TLS ja Secure shell) tulee toimeen myös ilman varmenteita, mutta jotkut protokollat (kuten S/MIME) perustuvat nimenomaan epäsymmetrisen salausmenetelmän käyttöön. Osa protokollista hyödyntää X.509-varmenteita (kuten TLS ja S/MIME), mutta joillain protokollilla on omat erityisvarmenteensa (kuten PGP ja SET). Joidenkin tunnettujen varmenteita hyödyntävien tietoliikenneprotokollien sijoittumista Internetissä käytetyn protokollapinon eri tasoille on kuvattu ohessa (Kuva 41).



Kuva 41. Joitain julkisen avaimen järjestelmää hyödyntäviä protokollia sijoitettuna Internetin protokollapinon eri tasoille.

Sovelluskerrokselle protokollat tarjoavat konkreettisimmin käyttäjälle näkyviä, usein tiettyyn rajattuun käyttötarkoitukseen soveltuvia palveluja, kuten mahdollisuuden sähköpostin allekirjoittamiseen tai luottokorttiostosten turvalliseen maksamiseen SET-protokollan (Secure Electronic Transaction) avulla. Sovelluskerroksen protokollat tarjoavat päästä päähän (end-to-end) -tyyppistä turvallisuutta. Esimerkiksi S/MIME-protokollan avulla salattu sähköposti säilyy salattuna mikron kiintolevyllä vielä senkin jälkeen, kun sähköpostiasiakasohjelmisto on noutanut viestin sähköpostipalvelimelta työasemalle.

Kuljetuskerroksen ja verkkokerroksen protokollat tarjoavat tyypillisesti salatun yhteyden verkon kahden todennetun toimilaitteen, esimerkiksi työaseman ja palvelimen, välille. SSL-, TLS- ja Secure shell -protokollat tarjoavat TCP-protokollan päälle asettuvan turvallisen kuljetuspalvelun, Kerberos-protokolla ja sen epäsymmetristä salausmenetelmää hyödyntävä PKINIT-laajennus puolestaan käyttävät UDP-protokollaa. IPSec-protokolla ja siihen liittyvä IKE-avaimenjohtamisprotokolla mahdollistavat IP-protokollan pakettien salaamisen ja todentamisen verkkokerroksen tarjoamana palveluna. IKE-protokollan syrjäyttäjäksi ehdotettu HIP (Host Identity Payload [MOSK01]), joka irrottaa verkkolaitteen tunnisteen sen Internet-osoitteesta, hyödyntää myös julkisen avaimen järjestelmää.

Sovelluskerroksen protokollista poiketen kuljetus- ja verkkokerroksen protokollat tarjoavat vain turvallisen siirtokanavan viesteille, ja siirron päätyttyä viestien suojaaminen tulee hoitaa muilla tavoin. Jos esimerkiksi verkkokaupassa käytetään maksutapana luottokorttinumeroa, jonka asiakas välittää kauppiaan WWW-palvelimelle TLS-protokollalla suojatun yhteyden yli, saattaa asiakkaan luottokorttinumero paljastua kauppiaan WWW-palvelimeen murtautuneille hakkereille. TLS-salauksella ei voida suojata sitä tietokantaa, johon asiakkaiden luottokorttinumerot verkkokaupan tilausjärjestelmässä talletetaan.

8. PKI JA KÄYTTÄJÄHALLINTO ORGANISAATIOSSA

Edellisessä luvussa kerrottiin, kuinka yleisesti käytetyt tietoliikenneprotokollat hyödyntävät varmenteita käyttäjän henkilöllisyyden todentamisessa. Todentamisen ja valtuuksien perusteella suoritetaan pääsynvalvontaa; pääsy resursseihin sallitaan vain valtuutetuille henkilöille.

Käyttäjän henkilöllisyyden todentamisen tuloksena palvelimella on käyttäjän esittämä varmenne sekä varmuus siitä, että käyttäjällä on hallussaan varmenteeseen liittyvä yksityinen avain. Palvelimen on tämän jälkeen tavalla tai toisella pääteltävä varmenteesta, mihin palveluihin kyseisellä käyttäjällä on käyttöoikeus. Mikäli käytössä ovat roolivarmenteet, päättely on yksinkertaista: pääsynvalvontaa voidaan suorittaa pelkästään tarkastelemalla varmenteen tietosisältöä. Henkilövarmenne sitoo kuitenkin julkisen avaimen nimeen, eikä ota kantaa siihen, mihin resursseihin kullakin henkilöllä on pääsy.

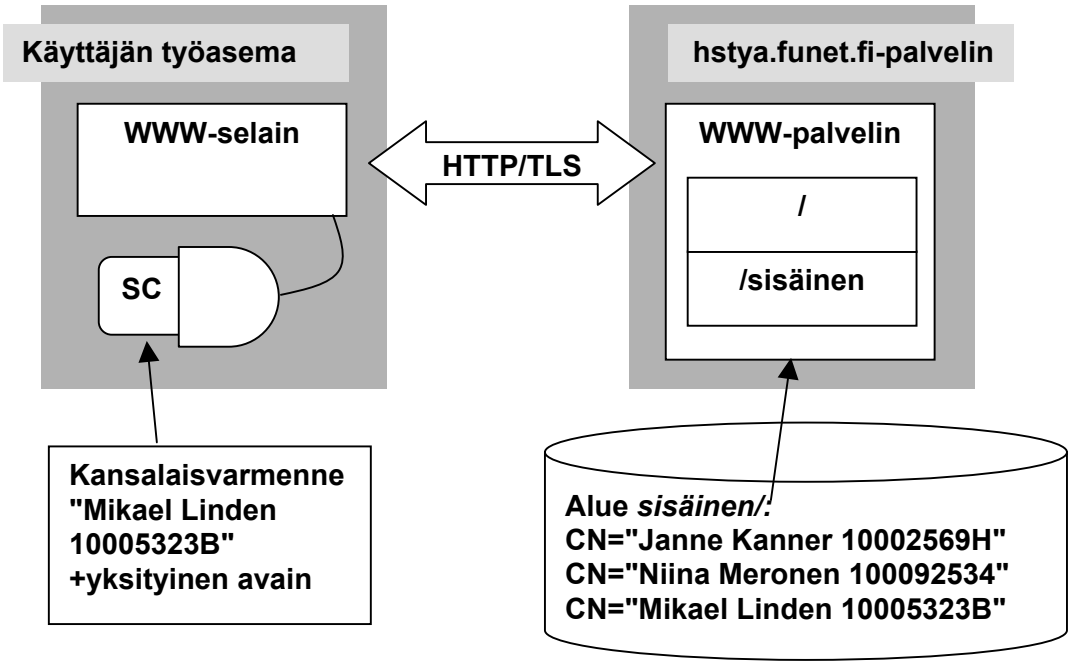
Tässä luvussa tarkastellaan organisaation käyttäjähallintoa, jonka tehtävänä on pitää kirjaa tietojärjestelmien käyttäjistä ja heidän valtuuksistaan. Erityisesti paneudutaan kysymyksiin, jotka liittyvät todentamisessa käytettäviin henkilövarmenteisiin. Käyttäjien valtuuksien hallinnointia sivutaan lähinnä käyttäjän henkilöllisyyden todentamisen näkökulmasta. Eräänä käyttäjähallinnon välineenä käsitellään lyhyesti LDAP-protokollaa ja -hakemistoja.

8.1. Esimerkki: yksinkertainen käyttäjähallinto

Tarkastellaan aluksi oheisen kuvan mukaista yksinkertaista asetelmaa, jossa *hstya.funet.fi*-nimisessä verkkolaitteessa sijaitsee WWW-palvelin (Kuva 42). Kuka tahansa verkon käyttäjä on oikeutettu lukemaan WWW-palvelimen juuressa olevia sivustoja, mutta palvelimen polussa *sisäinen* olevaa, organisaation sisäiseen käyttöön tarkoitettua sivustoa voivat lukea vain valtuutetut käyttäjät.

WWW-palvelimen ylläpitäjä on konfiguroinut palvelimen siten, että se käyttää TLS-protokollaa kaikessa käyttäjän kanssa HTTP-protokollan välityksellä tapahtuvassa tiedonsiirrossa. Koska kuka tahansa verkon käyttäjä voi lukea WWW-palvelimen juuren sivustoja, ei tämä alue edellytä käyttäjän henkilöllisyyden todentamista. Mikäli käyttäjä haluaa siirtyä lukemaan polussa *sisäinen* olevaa sivustoa, palvelin edellyttää uutta TLS-yhteydenmuodostusta, jolloin palvelin vaatii käyttäjän henkilöllisyyttä todennettavaksi varmenteen avulla. Palvelinta ylläpitävän organisaation politiikan mukaisesti käyttäjän tunnistamisessa hyväksytään vain Väestörekisterikeskuksen myöntämät kansalaisvarmenteet, joten TLS-yhteydenmuodostuksessa palvelin ilmoittaa käyttäjän selaimelle hyväksyvänsä

pelkästään varmenteet, joiden myöntäjä on "VRK-FINSIGN CA for citizen". Käyttäjä esittää palvelimelle kansalaisvarmenteensa, ja yhteydenmuodostuksen ja siihen sisältyvän haaste/vaste-todentamisen (luku 7.2.2.) tuloksena WWW-palvelin on saavuttanut varmuuden, että käyttäjällä on hallinnassaan varmenteeseen liittyvä yksityinen avain. Käyttäjän henkilöllisyys on siis todennettu onnistuneesti.



Kuva 42. Esimerkki palvelimesta ja sen yksinkertaisesta käyttäjähallinnosta.

WWW-palvelin suorittaa pääsynvalvontaa henkilöllisyyden todentamisen ja aikaisemmin suoritetun valtuutuksen perusteella. Valtuuden on myöntänyt WWW-palvelimen ylläpitäjä yksilöimällä kaikki sellaiset kansalaisvarmenteet, joiden haltijoilla on oikeus sivuston lukemiseen. Todellisuudessa valtuuden myöntämisen peruste ei kuitenkaan luultavasti ole pelkkä ylläpitäjän mielijohde, vaan jokin tapahtuma – esimerkiksi työtehtävien muutos – joka on palvelinta ylläpitävän organisaation käsityksen mukaan luonut kyseiselle käyttäjälle tarpeen ja oikeuden palvelimen käyttöön. Käytännössä valtuuttaminen tapahtuu luettelemalla WWW-palvelimen konfiguraatiotiedostossa varmenteen haltijan common name (CN) -kentät sellaisista varmenteista, jotka oikeuttavat sisäänpääsyyn. Käyttäjän pääsy *sisäinen*-osioon evätään, ellei hänen esittämänsä kansalaisvarmenne kuulu näiden varmenteiden joukkoon.

Esimerkin mukainen järjestely on sinällään toimiva, mutta skaalautuu huonosti. Ylläpitäjän työtaakka käy pian kohtuuttomaksi, jos palvelimen valtuutettuja käyttäjiä on kymmeniä tai satoja. Samoin käy, jos palvelimelle sijoitetaan *sisäinen*-osion lisäksi runsaasti muita osioita, joiden käyttöoikeudet asetetaan eri tavalla tai jos organisaatiossa on lukuisa joukko vastaavia palvelimia ja palveluita, jotka edellyttävät henkilöllisyyden todentamista, valtuuttamista ja pääsynvalvontaa. Tällöin

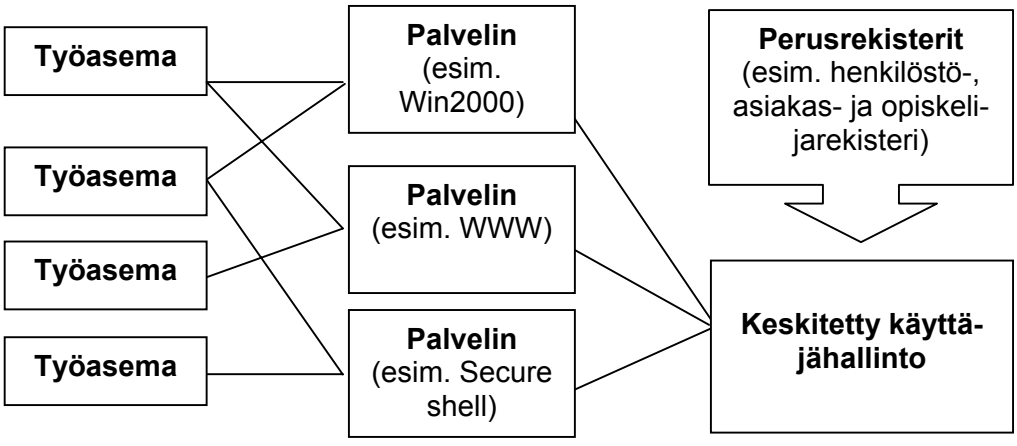
syntyy tarve minimoida käsityönä tehtävän käyttäjähallinnon määrä siirtämällä valtuuksien myöntäminen ja hallinnointi suoritettavaksi automaattisesti.

8.2. Käyttäjähallinto laajassa organisaatiossa

Henkilön valtuus tietoverkon eri resurssien käyttöön perustuu usein hänen rooliinsa ja toimenkuvaansa kyseisessä organisaatiossa ja on siten johdettavissa asianomaisten tietokantojen, kuten henkilöstö-, asiakas- tai opiskelijarekisterin, tiedoista. On luontevaa rakentaa järjestelmä niin, että tietojärjestelmien käyttäjähallinto kytkeytyy suoraan näihin perusrekistereihin ilman käsin tehtävää päivitystyötä.

Esimerkiksi yrityksen tietojärjestelmien käyttäjähallinto voi olla kytketty yrityksen henkilöstöhallinnon järjestelmiin siten, että uuden työntekijän kirjaaminen henkilöstörekisteriin käynnistää prosessin, jossa hänelle luodaan myös käyttäjätunnus ja salasana kaikkien työntekijöiden käyttämiin perusjärjestelmiin. Työsuhteessa tapahtuvat muutokset, kuten toisiin tehtäviin siirtyminen, saattavat aiheuttaa muutoksia myös työntekijöiden valtuuksiin, jotka ovat niinikään automaattisesti päivitettävissä. Kun työntekijän työsuhde kirjataan henkilöstörekisterissä päättyneeksi, sulkeutuvat myös hänen käyttäjätunnuksensa, eikä järjestelmiin jää unohtuneita, potentiaalisen tietoturvariskin muodostavia käyttäjätunnuksia.

Kun edellä kuvattu käyttöoikeuksien automaattinen ylläpito on toteutettu, on mielekästä liittää ainakin kaikki keskeisimmät, laajan käyttäjäkunnan sisältävät tietojärjestelmät hyödyntämään sitä. Tällöin voidaan puhua keskitetystä käyttäjähallinnosta (Kuva 43): organisaation käyttäjähallintoon liittyviä tietoja pidetään yllä keskitetysti yhdessä paikassa.

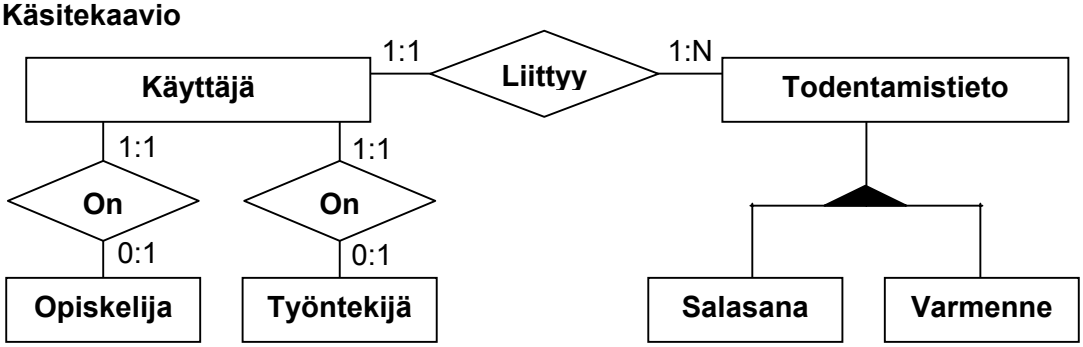


Kuva 43. Keskitetty käyttäjähallinto.

Käyttäjähallinnossa kuhunkin käyttäjään voidaan yhdistää todentamistietoja, kuten salasanatiivisteitä. Salasanaa luotettavampana todentamistietona voidaan käyttää varmennetta, joka kytkeytyy salasanan tavoin tiettyyn käyttäjään. Organisaation

käytännöistä riippuen yhdellä käyttäjällä voi olla yksi tai useita varmenteita, jotka käyttäjähallinto kytkee häneen ja hänen käyttäjätunnukseensa.

Käsitekaavio



Taulu: Käyttäjät

Henkilönro	Nimi	Käyttäjä-tunnus	Opiskelijanro (jos opiskelija)	Työntekijänro (jos työntekijä)
10684	Teemu Teekkari	tteekkar	167804	
4562	Mikael Linden	linden	136854	8386
…				

Taulu: Todentamistiedot

Henkilönro	Tyyppi	Sisältö
4562	X.509v3	Varmentaja: VRK Finsign for Citizen Varmenteen haltija: Mikael Linden 10005323B jne…
10684	Salasanatiiviste	fH6D3tjhWjG4TH
10684	WTLS-varmenne	Varmentaja: Sonera CA Varmenteen haltija: Teekkari Teemu jne…
4562	X.509v3	Varmentaja: Certall level 1 CA Varmenteen haltija: Mikael Linden, mikael.linden@tut.fi jne…
…		

Kuva 44. Esimerkki käyttäjähallinnosta, jossa kullakin käyttäjällä on kaksi mahdollista perusroolia ja yksi tai useampia todentamistietoja.

Oheisessa esimerkissä (Kuva 44) on esitetty käsitekaavion ja käyttäjähallinnon tietokannan taulujen avulla suuntaviivoja eräästä käyttäjähallinnon toteutustavasta. Esimerkki on korkeakouluympäristöstä, jossa järjestelmien käyttäjä voi olla joko opiskelija tai korkeakoulun työntekijä tai kuulua samanaikaisesti molempiin ryhmiin. Korkeakouluympäristössä on luontevaa, että käyttäjähallinnon tietoja päivitetään opiskelijarekisterin ja henkilökuntarekisterin tietojen pohjalta.

Esimerkkitietokanta koostuu kahdesta taulusta. Käyttäjät-taulu sisältää tasan yhden tietueen jokaisesta tietojärjestelmän käyttäjästä, Todentamistiedot-taulu puolestaan sisältää yhden tai useamman tietueen jokaista Käyttäjät-taulussa olevaa käyttäjää kohti. Mikäli käyttäjä on kirjattu opiskelijarekisteriin, talletetaan hänen opiskelija-

numeronsa hänestä Käyttäjät-taulussa olevan tietueen asianomaiseen kenttään ja henkilökuntarekisterin osalta menetellään vastaavalla tavalla. Näin Käyttäjät-taulu luo pohjan perusroolien ja -valtuuksien hyödyntämiselle. Jos Käyttäjät-taulusta löytyy opiskelijanumero, kysymyksessä on opiskelija, ja esimerkiksi tenttiilmoittautumisista huolehtiva palvelin voi sallia kyseisen käyttäjän tenttiilmoittautumisen.

Todentamistiedot-taulu sisältää tiedot niistä välineistä, joita käyttäjähallinnossa on käytettävissä kyseisen henkilön henkilöllisyyden todentamiseksi. Kuhunkin käyttäjään voidaan kytkeä vaihteleva määrä eri tekniikkaa hyödyntäviä ja luotettavuudeltaan erilaisia todentamistietoja, kuten salasanatiivisteitä ja varmenteita. Keskitettyä käyttäjähallintoa todentamisessa hyödyntävä palvelin tukeutuu tähän tauluun. Käyttäjätunnusta ja salasanaa käytettäessä taulusta tarkastetaan käyttäjän henkilöllisyys ja hänen antamansa salasanan oikeellisuus. Pelkän varmenteen avulla todennettaessa taulun avulla selvitetään, kenelle tietojärjestelmän käyttäjistä kyseinen varmenne kuuluu.

Esimerkin ratkaisu on vain yksi mahdollinen, ja monia muitakin voidaan toteuttaa organisaation tarpeiden mukaan. Yhdellä käyttäjällä voi esimerkiksi olla monta eri käyttäjätunnusta, tai käyttäjätunnus voidaan kytkeä hänen rooliinsa. Käyttäjät, jotka ovat sekä opiskelijoita että henkilökuntaa, käyttävät yhtä käyttäjätunnusta työtehtävissään ja toista opiskeluunsa liittyvissä asioissa. Todentamistiedot voidaan kytkeä tiettyyn käyttäjätunnukseen, salasanojen määrä rajoittaa yhteen ja niin edelleen.

Esimerkin mukaista keskitettyä käyttäjähallintoa hyödyntävän palvelimen ratkaistavaksi jää, mitä todentamistapaa se pitää tarjottava palvelu huomioon ottaen riittävän luotettavana. Voi olla, että tenttiin ilmoittautuvan opiskelijan henkilöllisyyden todentamisessa salasanakin katsotaan riittävän luotettavaksi todentamismenetelmäksi. Opintosuoritusrekisteriin suoritusmerkintöjä kirjaavalta opettajalta voidaan sen sijaan edellyttää varmennetodentamista ja luotettavana pidetyn varmentajan käyttämistä. Olisihan ikävää, jos opettajan salasanan arvannut opiskelija pääsisi peukaloimaan opintosuorituksiaan itse.

Todentamistiedon kytkeminen käyttäjään keskitetyn käyttäjähallinnon tietokannassa tarjoaa joustavan tavan palvella organisaation eri palveluiden tarpeita. Kun käyttäjä haluaa vaihtaa salasanansa, on uusi salasana käytettävissä kaikissa palvelimissa ilman, että käyttäjän tarvitsee vaihtaa salasana joka palvelimeen erikseen. Luotettavampi henkilöllisyyden todentaminen voidaan toteuttaa jonkun käyttäjään liitetyn varmenteen avulla. Edellisessä esimerkissä (Kuva 44) Teemu Teekkari voidaan tunnistaa korkeakoulun WAP-palvelimelle salasanan lisäksi myös WTLS-

varmenteella, johon liittyvä yksityinen avain on sijoitettu Teemun WAP-puhelimen sisällä olevalle WIM-toimikortille (luku 3.5.).

Luvussa 5 todettiin, että varmenne voidaan asettaa sulkulistalle, jos siihen liittyvän yksityisen avaimen pelätään joutuneen vääriin käsiin. Käyttäjähallinto tuo organisaatiolle vaihtoehtoisen tavan epäkelvoiksi tulleiden varmenteiden poissulkemiseen. Kun varmenteen ja käyttäjän kytkentä käyttäjähallinnossa puretaan, ei käyttäjän henkilöllisyyttä voida enää todentaa kyseisellä varmenteella. Tämän järjestelyn avulla voidaan toteuttaa esimerkiksi vierailijakortti, jonka avulla vierailijat tai toimikorttinsa aamulla kotiin unohtaneet työntekijät pääsevät väliaikaisesti käsiksi organisaation tietojärjestelmään. Toimikortti kuitataan aamulla organisaation ATK-järjestelmätuesta, joka liittää toimikortin yksityiseen avaimeen liittyvän varmenteen kyseisen käyttäjän tietoihin käyttäjähallinnossa sen päivän ajaksi. Toimikortti palautetaan illalla, jolloin varmenteen ja käyttäjän välinen yhteys poistetaan käyttäjähallinnosta, ja seuraavana aamuna kortti voidaan antaa jo seuraavalle henkilölle. Koska toimikorttia käytetään vain käyttäjän henkilöllisyyden todentamiseen ja koska jokaisen todentamistapahtuman yhteydessä käyttäjähallinnon avulla selvitetään, kenen käyttäjän hallussa varmenteeseen liittyvä yksityinen avain juuri sillä hetkellä on, voidaan järjestelyä pitää turvallisena. Sen sijaan digitaalista allekirjoitusta tai tiedon salausta esitetyllä järjestelyllä ei ole syytä sallia. Digitaalisen allekirjoituksen tarkkaa luomishetkeä tai salatun viestin avaushetkeä on hankala todentaa, jolloin on myös vaikea tietää, kenen käyttäjän hallussa yksityinen avain sillä hetkellä on.

Monessa organisaatiossa käytetään edelleen perinteistä hajautettua käyttäjähallintotapaa, jossa kunkin järjestelmän käyttäjätunnuskantaa ylläpidetään toisistaan riippumattomasti ja henkilölle luodaan kuhunkin palveluun ja palvelinympäristöön käyttäjätunnus ja salasana erikseen. Varmenteiden tuominen salasanan rinnalle tai korvaajaksi monimutkaistaa järjestelmän käyttäjähallintoa, koska järjestelmäylläpidon pitää rakentaa mekanismit ja toimintatavat varmenteiden yhdistämiseksi järjestelmän oikeaan käyttäjään, ja myös toimintamallit edellä mainittujen tilapäisten vierailijakorttien käyttöönottoon on toteutettava. Päällekkäisten järjestelmien rakentaminen ja ylläpitäminen on tarpeetonta. Niinpä on resurssien tehokkaan käytön kannalta mielekästä keskittää käyttäjähallinto organisaatiossa yhteen pisteeseen, vaikka keskittäminen aiheuttaakin uusien järjestelmien rakentamis- ja ylläpitotyötä. Varmenteiden käyttöönotto käyttäjien henkilöllisyyden todentamisessa kulkee siis käsi kädessä käyttäjähallinnon keskittämisen kanssa.

8.3. Henkilövarmenteen yhdistäminen käyttäjään

Tietoturvallisuus on kuin ketju: ketju on kokonaisuudessaan yhtä heikko kuin sen heikoin lenkki. Ennen kuin käyttäjä voi alkaa käyttää hankkimaansa varmennetta

todentamisvälineenä organisaation tietojärjestelmissä, on varmenne tavalla tai toisella kytkettävä hänen henkilöllisyyteensä organisaation käyttäjähallinnossa. Käytetystä kytkentätavasta ei saa muodostua heikkoa kohtaa.

Helppo mutta turvaton tapa uuden varmenteen liittämiseksi tietoverkon käyttäjään on käyttäjän olemassa olevan todentamistiedon käyttäminen uuden, luotettavamman todentamistiedon aktivoimiseksi. Käyttäjä voisi esimerkiksi tunnistautua tarkoitusta varten asetetulle WWW-palvelimelle ensin salasanalla ja sen jälkeen käyttämällä uutta varmennettaan. Käyttäjähallinto pystyy tämän perusteella kytkemään esitetyn varmenteen jatkossa kyseiseen salasanan perusteella todennettuun käyttäjään. Tällöin on kuitenkin syntynyt järjestely, joka on varmenteesta huolimatta turvatasoltaan yhtä heikko kuin salasanatodentaminen. Hyökkääjä, joka on pystynyt sieppaamaan tai arvaamaan jonkun käyttäjän salasanan, pystyisi näin menetellen kytkemään hänen tietoihinsa omassa hallussaan olevan varmenteen.

Jos varmenteessa oleva varmenteen haltijan nimi olisi yksikäsitteinen, olisi varmenteen yhdistäminen tietoverkon käyttäjään suoraviivaista. Täyskaimoista aiheutuvan monikäsitteisyyden lisäksi pitäisi kuitenkin pystyä käsittelemään myös tilanteet, joissa varmenteen haltijan nimi vaihtuu avioliiton tai muun tapahtuman seurauksena. Vaikka nimi vaihtuu, henkilö ja hänen valtuutensa ovat edelleen samat. Tässä luvussa esitetään kolme tapaa yhdistää varmenne tiettyyn käyttäjään.

8.3.1. Varmenteen tietosisältö

Perustapauksessa organisaatiolla on mahdollisuus vaikuttaa varmenteen tietosisältöön. Käytännössä tämä tarkoittaa, että varmenne myönnetään haltijalleen organisaation toimesta: organisaatio joko toimii itse varmentajana tai alihankkii varmennepalvelun kaupalliselta varmentajalta. Näin toimitaan tyypillisesti esimerkiksi silloin, kun työnantaja hankkii työntekijälleen toimikortin työtehtävien hoitamista varten. Jatkossa tällaista varmennetta kutsutaan **organisaatiovarmenteeksi**.

Organisaatio voi huolehtia, että organisaatiovarmenteiden "varmenteen haltija" -kenttään sijoitetaan varmenteen haltijan yksilöivä tieto, jolla on suora merkitys organisaation käyttäjähallinnossa. Tällainen tieto voi olla esimerkiksi henkilönumero, joka pysyy käyttäjähallinnossa samana siitäkin huolimatta, että henkilön nimi, sähköpostiosoite tai käyttäjätunnus saattavat esimerkiksi sukunimen vaihtuessa muuttua. Organisaatiovarmenteeseen sisällytettävää yksilöivää tietoa valittaessa tulee kuitenkin huolehtia varmenteen haltijan yksityisyyden suojan säilymisestä. Varmenteet ovat aina jossain määrin yleisesti saatavilla ainakin organisaation sisällä, joten erityisesti henkilötunnuksen käyttöä varmenteessa tulee välttää.

Kun käyttäjä tunnistautuu saamallaan organisaatiovarmenteella ensimmäisen kerran organisaation palvelimelle, toteaa palvelin varmenteessa olevien "varmentaja"

ja "varmenteen haltija" -kenttien perusteella, että kysymys on organisaation omasta varmenteesta, ja käy varmenteessa olevan yksilöivän tiedon perusteella kirjaamassa varmenteen käyttäjähallinnon tietokantaan. Tässä voidaan tosin oikaista, jos varmentaja toimittaa myöntämänsä varmenteet organisaatiolle suoraan eräajona.

Henkilöllisyyden todentamisen kannalta organisaatiovarmenteiden kirjaamista käyttäjähallinnon tietokantaan voidaan pitää turhana – pystyyhän palvelin päättelemään jo varmenteen yksilöivän tunnuksen perusteella, mistä organisaation käyttäjästä on kyse. Jos samaista tietokantaa käytetään henkilöllisyyden todentamisen lisäksi myös esimerkiksi sähköpostin salaukseen käytettävien varmenteiden varastointiin ja jakamiseen, kuten luvussa 8.4 tullaan esittämään, on varmenteen lisääminen tietokantaan tarpeellista. Muuten varmenteen haltijalle salattua postia lähettävä henkilö ei pysty hakemaan salaukseen käytettävää varmennetta organisaation käyttäjähallinnosta.

8.3.2. Varmentaja tarjoaa palvelun

Vaihtoehdon organisaatiovarmenteille muodostavat varmenteet, joiden myöntämiseen tarkasteltavalla organisaatiolla ei ole osuutta. Esimerkiksi Väestörekisterikeskuksen kansalaisvarmenne on Suomen kansalaiselle tai Suomessa vakinaisesti asuvalle ulkomaalaiselle myönnettävä varmenne, jonka myöntämiseen tai tietosisältöön työnantaja ei voi vaikuttaa. Sama tilanne syntyy, kun pankki myöntää asiakkaalleen varmenteen, johon liittyvä yksityinen avain sijoitetaan pankkikortille. Itse asiassa molemmat esimerkit ovat nekin eräänlaisia organisaatiovarmenteita – toisessa organisaatio on Suomen valtio ja toisessa pankki.
Jos tällaiset varmenteet ovat teknisesti yhteensopivia ja julkisen avaimen järjestelmään kuuluvat muut elementit, kuten varmennepolitiikka ja sulkulista, ovat myös organisaation saatavilla, ei tällaisten varmenteiden käytölle organisaation sisäisenä todentamisvälineenä liene estettä. Tällöin organisaatio voi varmennepolitiikan pohjalta arvioida kyseisten varmenteiden luotettavuutta. Koska varmenteen tietosisällössä ei kuitenkaan todennäköisesti ole sellaista tietoa, joka mahdollistaisi varmenteen suoran yhdistämisen oikeaan käyttäjähallinnon tuntemaan käyttäjään, on varmenteen kytkeminen käyttäjään suoritettava muulla tavalla.

Usein varmentaja huolehtii, että varmenteen haltijasta kirjataan varmenteeseen jokin sellainen yksilöivä tieto, joka säilyy muuttumattomana, vaikka henkilön nimi tai sähköpostiosoite vaihtuisivat. Yksilöivän tiedon avulla henkilö voidaan luotettavasti erottaa kaimoistaan ja muista henkilöistä, ja se säilyy muuttumattomana, vaikka varmenne vanhenisikin. Varmentajan samalle henkilölle myöhemmin antamassa uudessa varmenteessa yksilöivä tieto on sama.

Kuten luvussa 8.3.1. todettiin, on varmenteen haltijan yksilöivää tietoa valittaessa kunnioitettava yksityisyyden suojaa. Erityisesti henkilötunnuksen käyttöä on vältettävä, ja esityksessä laiksi sähköisestä allekirjoituksesta [HE01] se onkin kielletty. Sähköisen henkilökortin haltijoiden yksilöintiin käytetään sähköistä asiointitunnusta, jonka Väestörekisterikeskus on luonut ja kirjannut väestötietojärjestelmään jokaisen kansalaisvarmenteen saaneen henkilön tietoihin. Varmenteita hyödyntävien osapuolien kannalta olisi helppoa, jos muutkin suomalaiset varmentajat voisivat käyttää Väestörekisterikeskuksen luomaa sähköistä asiointitunnusta varmenteidensa yksilöivänä tietona, mutta tätäkin järjestelyä on pidetty yksityisyyden suojan kannalta vahingoittavana. Sähköisestä asiointitunnuksesta muodostuisi pian uusi "henkilötunnus", jonka avulla erilaisten henkilörekisterien yhdistäminen tulisi liian helpoksi. Näyttää siis siltä, että samalla henkilöllä on eri varmentajien järjestelmissä ja varmenteissa käytössään erilaiset yksilöivät tiedot.

Yksityisyyden suojelusta huolimatta varmenteeseen luottavalla osapuolella on kuitenkin usein tarve saada varmenteen haltijasta muitakin tietoja kuin mitä sinällään mitäänsanomaton yksilöivä tieto on. Julkishallinnon palveluissa viranomainen tarvitsee yleensä varmenteen haltijan henkilötunnuksen pystyäkseen yhdistämään vireille pannun asian oikeaan kansalaiseen. Myös organisaation sisällä henkilötunnuksen kirjaamiselle henkilörekistereihin on usein henkilötietolain mukaiset perusteet [HETI99]. Niinpä varmenteisiin luottavat osapuolet tarvitsevat palvelua, joka yhdistää varmentajan käyttämän yksilöivän tiedon hänen henkilötunnukseensa.

Väestörekisterikeskus on vastannut kysyntään toteuttamalla palvelun, jossa sopimuksen tehneille osapuolille annetaan oikeus saada tiettyä sähköistä asiointitunnusta vastaava henkilötunnus väestötietojärjestelmästä julkisoikeudellisena suoritteena [VRK02]. Organisaatio voi toteuttaa palveluun nojaavan järjestelyn, jossa käyttäjähallinto käy uuden sähköisen asiointitunnuksen kohdatessaan automaattisesti selvittämässä, mille tietojärjestelmän käyttäjälle kyseinen asiointitunnus kuuluu. Järjestely on käyttäjän kannalta huomaamaton. Poliisilaitokselta sähköinen henkilökortti taskussaan tuleva käyttäjä voi alkaa muitta mutkitta käyttää kortillaan organisaation tietojärjestelmiä.

8.3.3. Varmenteen haltija esittää varmenteensa organisaatiolle

Kaikki varmentajat eivät kuitenkaan tarjoa palvelua yksilöivän tiedon ja henkilötunnuksen yhdistämiseksi Väestörekisterikeskuksen tavoin. Kolmas tapa varmenteen liittämiseksi käyttäjähallinnossa tiettyyn käyttäjään edellyttää aktiivisuutta varmenteen haltijalta itseltään: varmenteen haltija itse esittää varmenteensa organisaatiolle, joka kytkee varmenteen oikeaan tietoverkon käyttäjään. Tällöin toiminta-

tapa, jonka avulla varmenne todetaan tietylle käyttäjälle kuuluvaksi kelvoksi todentamistiedoksi, pitää suunnitella huolellisesti. Periaatteessa menettely voi olla joko fyysinen tai tapahtua tietoverkon välityksellä.

Fyysisessä menettelytavassa varmenteen haltija tulee henkilökohtaisesti käymään organisaation palvelupisteessä, jossa organisaation edustaja vastaanottaa käyttäjän esittämän varmenteen. Palvelupisteessä varmistetaan, että käyttäjällä on hallinnassaan varmenteeseensa liittyvä yksityinen avain. Tämä voi tapahtua esimerkiksi pyytämällä käyttäjää allekirjoittamaan annettu haaste yksityisen avaimen avulla. Lopuksi selvitetään esimerkiksi henkilökortin tai henkilöllisyystodistuksen avulla, kenestä organisaation käyttäjästä on kysymys: kehen tietoverkon käyttäjään esitetty varmenne tulee yhdistää.

Henkilökohtaista käyntiä edellyttävä menettelytapa sitoo organisaation palvelupisteen resursseja ja pakottaa varmenteen haltijan matkustamaan organisaation toimipisteeseen pitkienkin matkojen takaa. Olisi luontevaa, että varmenteen haltija voisi aktivoida varmenteensa myös tietoverkon välityksellä. Tämä tapahtuisi siten, että käyttäjän henkilöllisyys ensin todennettaisiin organisaation palvelimelle, jonka jälkeen käyttäjä esittäisi organisaatiolle varmenteensa ja osoittaisi, että myös varmenteeseen liittyvä yksityinen avain on hänen hallussaan. Esitetty järjestely on mahdollinen, kun otetaan huomioon, että käyttäjän henkilöllisyys on ensin todennettava vähintään yhtä luotettavalla todentamisvälineellä kuin mitä käyttöön otettava uusi varmenne luotettavuudeltaan edustaa.

Esimerkiksi Teemu Teekkarilla on hallussaan kolme todentamistietoa, joita hän haluaa käyttää korkeakoulunsa tietoverkkoon tunnistautumiseen: asettamansa salasanan lisäksi Teemulla on kansalaisvarmenne, johon liittyvän yksityisen avaimen sisältävä sähköinen henkilökortti on noudettu henkilökohtaisesti poliisilta. Lisäksi Teemu on hankkinut varmentaja X:ltä niin sanotun softavarmenteen, johon liittyvä yksityinen avain sijaitsee salattuna hänen työasemansa kiintolevyllä. Korkeakoulu katsoo, että varmentajan X softavarmenteet ovat salasanaa luotettavampia todentamisvälineitä. Kansalaisvarmenne on kuitenkin kolmikon luotettavin: yksityinen avain sijaitsee toimikortilla, jonka saaminen edellyttää henkilökohtaista käyntiä poliisilaitoksella.

Jos korkeakoulu on jo ottanut käyttöön Teemun kansalaisvarmenteen hänelle kuuluvana todentamistapana, Teemun henkilöllisyys voidaan ensin todentaa korkeakoulun WWW-palvelimelle kansalaisvarmenteella, ja tämän jälkeen Teemu voi joko vaihtaa salasanansa tai ilmoittaa korkeakoululle, että myös hänen softavarmenteensa on jatkossa käytettävissä hänen henkilöllisyyttään todennettaessa. Jos Teemun henkilöllisyys on todennettu WWW-palvelimelle kansalaisvarmenteen sijaan salasanalla, ei hänen ilmoitustaan softavarmenteen käyttöönotosta pidä

hyväksyä, sillä muuten Teemun softavarmenteen luotettavuus laskisi samalle tasolle salasanatodentamisen luotettavuuden kanssa.

8.4. LDAP-hakemistot

Luvussa 8.2 esiteltiin keskitetty käyttäjähallinto: arkkitehtuuri, joka kokoaa tiedot organisaation tietojärjestelmien käyttäjistä ja heidän valtuuksistaan yhteen paikkaan. Organisaation muut palvelut hyödyntävät keskitettyä käyttäjähallintoa käyttäjien henkilöllisyyden todentamisessa ja heidän valtuuksiensa tarkistamisessa. Tähän mennessä ei kuitenkaan ole otettu kantaa tapaan, jolla organisaation palvelimet pystyvät hyödyntämään käyttäjähallinnon tietokantaa. Perinteisesti toteutukset käyttäisivät ehkä RADIUS-protokollaa [RFC2865] tai suoria SQL-kielisiä kyselyitä asianomaisista relaatiotietokannoista.

Hakemistot ovat yleistymässä hierarkkisesti jäsentyvän tiedon tallennustapana. ITU-T on määritellyt arkkitehtuurin X.500-hakemistolle, joka on tietokanta, joka pystyy taltioimaan tietoa ihmisistä ja olioista eri puolille verkkoa sijoitettuihin palvelimiin [TEBB95]. X.500-hakemistoa suunniteltaessa päämääränä oli, että kaikki maailman hakemistopalvelimet muodostaisivat kokonaisuuden, joka näkyisi käyttäjälle yhtenä suurena Hakemistona. Käyttäjän ei tarvitsisi tietää, mihin yksittäiseen hakemistopalvelimeen hänen kysymänsä tieto olisi talletettu, vaan Hakemisto huolehtisi, että käyttäjän kysymä tieto tulee noudetuksi oikeasta palvelimesta ja toimitetuksi kysyjälle.

X.500-hakemistot eivät ole yleistyneet odotetulla tavalla. Internetissä suuntaus onkin kohti yksinkertaisemman LDAP-protokollan (Lightweight Directory Access Protocol [RFC 2251]) ja -hakemistojen käyttöä. Alun perin LDAP kehitettiin, jotta X.500-hakemistoa voitaisiin käyttää myös Internetin yli. Vähitellen LDAP itsenäistyi omaksi protokollakseen, eikä sillä enää nykyisin juurikaan asioida X.500-hakemiston edustakoneeksi asetetun LDAP-palvelimen kanssa, vaan usein LDAP-hakemisto muodostaa oman, itsenäinen tietokantansa.

LDAP-protokolla määrittelee paitsi itse tietoliikenneprotokollan, myös tavan, jolla tiedot esitetään hierarkkisena rakenteena niihin kohdistuvien hakujen mahdollistamiseksi. Tällöin hakemistoon talletetun olion (entry) hakuavaimena toimii varmenteista tuttu X.500 distinguished name (DN), joka kertoo olion sijainnin hakemiston puumaisessa hierarkiassa (Kuva 22, sivu 61).

LDAP-hakemistot ovat parhaimmillaan sellaisen tiedon varastoinnissa, jota käytetään vilkkaasti eri paikoista Internetin yli, mutta jota pitää päivittää suhteellisen harvoin. Henkilötietojen lisäksi LDAP-hakemistoon voidaan tallentaa esimerkiksi todentamistietoja ja roolitietoja, jotka ymmärretään kyseiseen henkilöön liittyviksi

attribuuteiksi. Henkilön attribuutteja voivat olla esimerkiksi hänen puhelinnumeronsa, sähköpostiosoitteensa, henkilötunnuksensa, salasanatiivisteensä, varmenteensa ja asemansa organisaatiossa. Osa attribuuteista, kuten sähköpostiosoite, voidaan asettaa hakemistoon kaikkien saataville. Esimerkiksi monet sähköpostiasiakasohjelmistot osaavat jo nykyisellään hyödyntää LDAP-hakemistoja vastaanottajan sähköpostiosoitteen noutamisessa. Osaan attribuuteista lukuoikeus annetaan vain valtuutetuille käyttäjille. Tällöin LDAP-hakemisto todentaa käyttäjänsä henkilöllisyyden esimerkiksi salasanalla tai varmenteella.

LDAP-hakemistoon asetettujen käyttäjätietojen hyödyntäminen tapahtuisi käytännössä esimerkiksi siten, että todennettuaan käyttäjän henkilöllisyyden ensin TLS-protokollan ja varmenteen avulla organisaation WWW-palvelin suorittaisi organisaation LDAP-palvelimelle kyselyn, jossa se tiedustelisi, kenelle käyttäjistä kyseinen varmenne kuuluu. Vastauksessaan LDAP-palvelin kertoisi kyseisestä käyttäjästä myös WWW-palvelimen pyytämät muut attribuutit, kuten käyttäjän nimen, henkilönumeron ja aseman kyseisessä organisaatiossa. LDAP-palvelimen kanssa tapahtuvan asioinnin luottamuksellisuus, eheys ja aitous voidaan turvata esimerkiksi ajamalla LDAP-protokollaa TLS-protokollan yli.

Jotta WWW-palvelin ja LDAP-palvelin voisivat ymmärtää toisiaan, on organisaation määriteltävä käyttämänsä LDAP-skeema. Skeema on kokoelma käytetyistä olioluokka- ja attribuuttimäärityksistä, jonka avulla määritellään, mitä olioita ja attribuutteja LDAP-hakemistoon talletetaan. Osalle olioluokista ja attribuuteista on jo sovittu määritelmät, esimerkiksi olioluokkaan inetOrgPerson kuuluva olio voi sisältää attribuutin userCertificate, joka on kyseiselle henkilölle kuuluva henkilövarmenne [RFC2798]. Organisaatio voi lisäksi määritellä omia olioluokkia ja attribuuttejaan omien tarpeidensa pohjalta.

9. PKI:N HYÖDYNTÄMINEN ORGANISAATIOSSA

Aikaisemmissa luvuissa on käyty läpi julkisen avaimen järjestelmän toimintaperiaatteet, esitelty muutamia sitä hyödyntäviä tietoliikenneprotokollia ja osoitettu sen yhtymäkohtia organisaation käyttäjähallintoon. Tässä luvussa esitetään näkökulma siihen, millaisia peruspalveluja julkisen avaimen järjestelmän varaan voidaan rakentaa eli mikä on organisaation motivaatio ottaa käyttöön julkisen avaimen järjestelmä.

Teknisessä mielessä julkisen avaimen järjestelmän käyttökohteet voidaan kiteyttää kolmeen perustapaukseen: henkilövarmenteita voidaan käyttää henkilöllisyyden todentamiseen, digitaaliseen allekirjoitukseen ja sähköpostin tai muiden tiedostojen salaamiseen. Näistä varmenteiden käyttäminen henkilöllisyyden todentamiseen tuo vaihtoehdon perinteisille todentamismenetelmille. Digitaalinen allekirjoitus ja muille lähetettävien tiedostojen salaus sen sijaan ovat asioita, joita ei aikaisemmin juurikaan ole voitu toteuttaa luotettavalla ja joustavalla tavalla. Tosin myös eksoottisempiakin käyttökohteita löytyy kuin nämä, vaikka niitä tässä ei käsitelläkään. Julkisen avaimen järjestelmän ja sopivien tietoturvaprotokollien avulla voidaan myös toteuttaa esimerkiksi vaalit tai huutokauppa.

9.1. Luotettavampi todentaminen ja keskitetty käyttäjähallinto

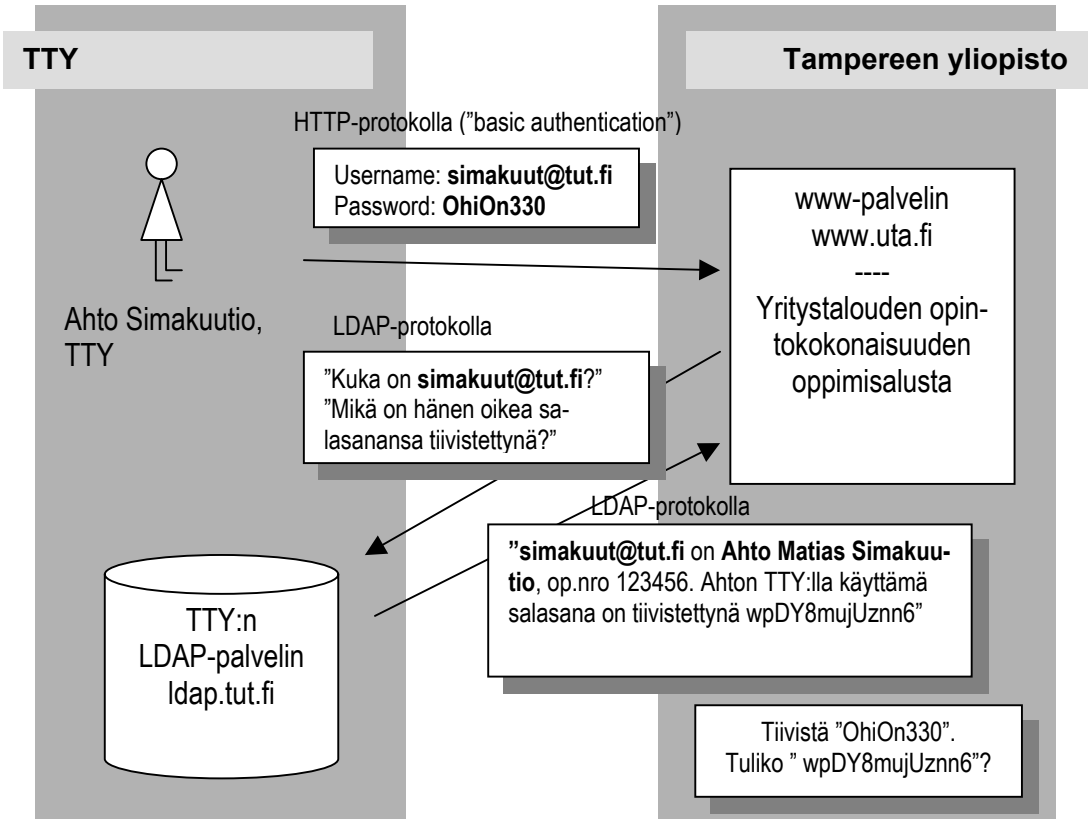
Edellisessä pääluvussa syvennyttiin keskitettyyn käyttäjähallintoon, jonka johtoajatuksena oli, että kullakin käyttäjällä on organisaation tietoverkossa yksi ainoa henkilöllisyys, jonka todentamisen avulla hän saa kaikki tarvitsemansa verkkopalvelut. Tällöin käyttäjän ei tarvitse muistaa useita salasanoja, vaan hänen henkilöllisyytensä voidaan todentaa samalla salasanalla kaikkiin tietojärjestelmiin. Yhden salasanan liian laaja käyttö aiheuttaa kuitenkin riskien kasautumista. Mitä laajempaan joukkoon resursseja käyttäjä pääsee käsiksi yhdellä salasanalla, sitä suurempi vahinko syntyy, jos salasana tavalla tai toisella paljastuu.

Seuraava yliopistomaailmaan liittyvä kuvitteellinen esimerkki havainnollistaa tilannetta. Tampereen teknillinen yliopisto (TTY) ja Tampereen yliopisto (TaY) olkoot kumpikin toteuttaneet keskitetyn käyttäjähallinnon. Tähän liittyen molemmat yliopistot ovat asettaneet käyttäjiensä tiedot sisältävän LDAP-hakemiston, johon myös naapuriyliopistolla on pääsy. Yksi käyttäjään liittyvä attribuutti on hänen käyttämänsä salasanan tiiviste.

TTY:lla opiskeleva Ahto Simakuutio on kiinnostunut TaY:n tarjoamasta yritystalouden opintokokonaisuudesta, johon hän on anonut ja saanut opinto-oikeuden. Osa yritystalouden opinnoista tapahtuu yliopiston WWW-pohjaisessa oppimisym-

päristössä, joka edellyttää käyttäjän henkilöllisyyden todentamista. Perinteisen toimintatavan mukaan Ahtolle luotaisiin käyttäjätunnus ja salasana TaY:n palvelimelle. Kustannussäästön ja käyttäjän mukavuuden vuoksi TTY ja TaY ovat kuitenkin sopineet, ettei tunnuksia luoda, vaan niiden sijaan käytetään opiskelijoiden kotiyliopistossa käytössä olevia käyttäjätunnuksia ja salasanoja. TTY ja TaY ovat siis menneet koko organisaation kattavasta käyttäjähallinnosta vielä askeleen pidemmälle ja ottaneet käyttöön organisaatiorajat ylittävän käyttäjähallinnon.

Tampereen yliopiston palvelimelle kirjautuessaan Ahto antaa käyttäjätunnukseksi *simakuut@tut.fi*, jolla siis ilmaistaan hänen käyttäjätunnuksensa sijaitsevan TTY:n käyttäjätunnusavaruudessa. Salasanaksi Ahto antaa TTY:lla käyttämänsä salasanan *OhiOn330*. Näiden tietojen perusteella TaY:n palvelin käyttää Ahtosta TTY:n LDAP-hakemistoon talletettuja tietoja hänen henkilöllisyytensä todentamiseen (Kuva 45).



Kuva 45. Esimerkki LDAP-hakemiston avulla tapahtuvasta organisaatioiden välisestä käyttäjän henkilöllisyyden todentamisesta.

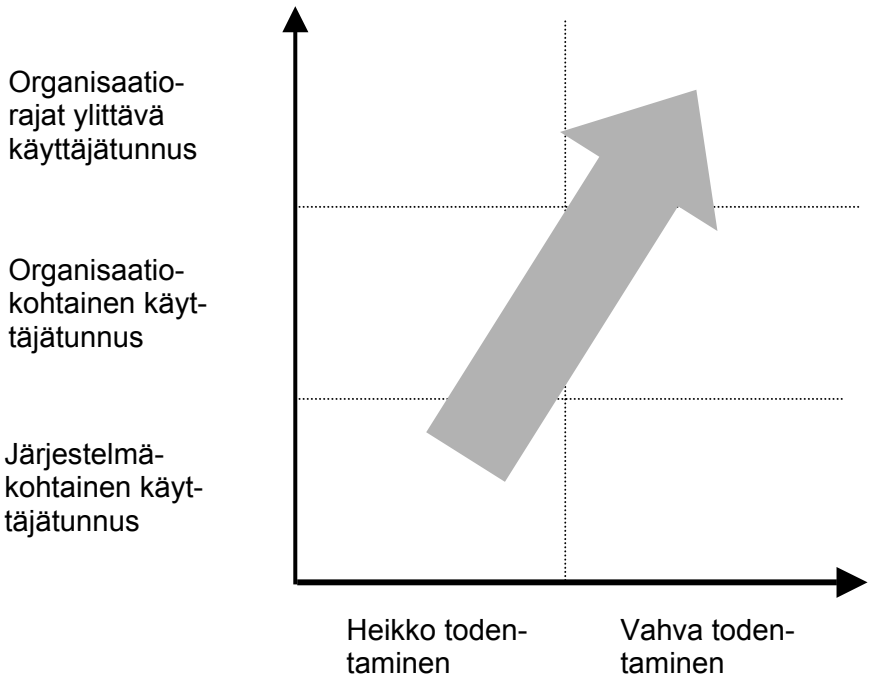
Esimerkin toimintatapa on sinällään toimiva, mutta siihen sisältyy riski. Mitä suurempaan joukkoon palveluita Ahto pääsee salasanallaan, sitä suurempi vahinko on vaarassa syntyä, jos salasana on niin helppo, että se arvataan. Vaikeasti arvattavan salasanan käyttökään ei auta, jos tietoturvataso jossain Ahton käyttämässä palvelimessa on muita alempi – esimerkiksi, jos jokin WWW-palvelimista ei vaadi TLS-

protokollaa käyttäjätunnuksen ja salasanan siirtämiseen selaimen ja palvelimen välillä, jolloin salasana on helposti siepattavissa tietoverkosta.

Yliopistojen verkostoituessa yhdeksi suureksi virtuaaliyliopistoksi Ahto saattaa yhtä aikaa käyttää verkon välityksellä puolenkymmenen eri yliopiston tarjoamia resursseja. Tietoturvallisuuskulttuuri vaihtelee eri organisaatioissa, ja kokonaisuuden turvataso määräytyy ketjun heikoimman lenkin mukaan. Jos Ahton salasana jotain kautta (esimerkiksi naapuriyliopiston palvelimelta) paljastuu, suurin kärsijä on todennäköisesti Ahto ja hänen kotiyliopistonsa, jossa hänen käyttäjätunnuksellaan voidaan tehdä todennäköisesti eniten hallaa.

Salasanojen käytön turvallisuutta voidaan kuitenkin kohentaa esimerkiksi rakentamalla Kerberosta muistuttava järjestely, jossa Ahton henkilöllisyyden todentaa aina hänen kotiyliopistonsa TTY:n palvelin riippumatta siitä, missä yliopistossa sijaitsevia verkkopalveluja hän on käyttämässä. Tällaisista protokollista on olemassa erilaisia kaupallisia ja ei-kaupallisia toteutuksia WWW-ympäristöön, kuten käyttäjän henkilöllisyyden todentamiseen organisaation sisällä tarkoitetut Siteminder [NETE02] ja Pubcookie [UWAS02] sekä organisaatiorajat ylittävään verkkoresurssien käyttöön suunniteltu Shibboleth [INTE02]. Nekään eivät kuitenkaan suojaa salasanojen perusongelmilta, kuten helpolta arvattavuudelta.

Jos salasanan sijaan henkilöllisyyden todentaminen suoritetaan varmenteen ja haaste/vaste-protokollan avulla, ei vastaavaa riskiä synny. Salasanatiivisteen sijaan TaY:n palvelin käy kysymässä TTY:n LDAP-hakemistosta, onko Ahton TLS-protokollan välityksellä esittämä varmenne TTY:n käyttäjähallinnon näkemyksen mukaan käypä todentamisväline henkilölle nimeltä Ahto Simakuutio.



Kuva 46. Käyttäjähallinnon keskittäminen luo paineen siirtyä kohti käyttäjän henkilöllisyyden vahvempaa todentamista [GNOM01].

Siirtyminen keskitettyyn käyttäjähallintoon lisää osaltaan tarvetta siirtyä kohti salasanaa luotettavampaa henkilöllisyyden todentamista (Kuva 46). Perinteisessä toimintatavassa, jossa käyttäjätunnus on annettu jokaiseen tietojärjestelmään erikseen, ei salasanan käyttöön liittyvä riski ole yhtä suuri. Salasanalla pääsee vain yhteen järjestelmään, ja toisaalta hermopisteitä, josta salasana saattaa paljastua, on vähemmän. Mitä laajempaan joukkoon palveluja salasanalla pääsee, sitä suurempi uhka salasanan paljastumiseen liittyy. Vahvalla, esimerkiksi varmenteeseen perustuvalla henkilöllisyyden todentamisella paljastuneen salasanan riski on kuitenkin väistettävissä.

9.2. Luotettavampi todentaminen ja arkaluontoiset palvelut

Käyttäjän henkilöllisyyden luotettavampi todentaminen helpottaa entistä arkaluontoisempien palveluiden tuomista avoimeen tietoverkkoon. Kotiin asti ylettyvät laajakaistayhteydet mahdollistavat esimerkiksi etätyön tekemisen, mutta samalla organisaatio joutuu avaamaan pääsyn tietojärjestelmiinsä ja niissä talletettuna olevaan luottamukselliseen tietoon myös sisäverkkonsa ulkopuolelle, mikä muodostaa turvallisuusriskin. Riskiä voidaan hallita tarjoamalla työntekijälle luottamuksellinen, todennettu virtuaalinen yksityisverkko (virtual private network, VPN) IPSec-protokollan avulla, joka hyödyntää käyttäjän henkilöllisyyden todentamisessa esimerkiksi varmennetta.

WWW-ympäristöön toteutetut palvelut ovat yleistyneet organisaatioiden intranet- ja extranet-ympäristöissä, ja entistä arkaluontoisempia palveluita on mahdollista

käyttää WWW-selaimella. Verkkopankkien käyttäminen WWW-selaimella on tavallista Suomessa: pankki antaa asiakkaalleen kertakäyttösalasanoja, joiden avulla henkilöllisyyden todentaminen voidaan suorittaa pysyvää salasanaa luotettavammin. Suomalaiset pankit ovatkin tuotteistaneet kertakäyttösalasanoihin perustuvan autentikointipalvelun. Pankkien yhteisen Tupas-protokollan (Tunnistepalvelu asiointipalvelujen tuottajille) avulla myös muut kuin pankit itse voivat todentaa tietoverkon käyttäjän henkilöllisyyden pankin antamien kertakäyttösalasanojen perusteella [PANK01].

Näyttää siltä, että vastaisuudessa tietojärjestelmien rakentajilla on käytettävissä useita eri vahvuisia välineitä käyttäjän henkilöllisyyden todentamiseksi. Turvallisuudeltaan heikoin todentamistapa on ehkä salasana, joka säilyy samana tai tulee vaihtaa esimerkiksi kolmen kuukauden välein. Turvallisemmin käyttäjän henkilöllisyys voidaan todentaa kertakäyttösalasanalla, jolloin kutakin salasanaa käytetään vain kerran. Tätäkin turvallisempi todentaminen tapahtuu varmenteen avulla, jolloin jaettua salaisuutta ei tarvita. Varmennetodentamisen turvallisuutta voidaan kasvattaa esimerkiksi sijoittamalla yksityinen avain toimikortille.

Äärimmilleen viety turvallisuus ei ole kustannustehokasta eikä tarpeellistakaan. Käytettävää todentamismenetelmää valittaessa pitää ensin arvioida tarjottavalta palvelulta vaadittava tietoturvallisuustaso, ja sen perusteella päättää, mitä pidetään riittävän luotettavana todentamismenetelmänä.

Ohessa (Taulukko 3) on kuvitteellinen esimerkki yliopistosta, jossa on käytössä kolme vaihtoehtoista henkilöllisyyden todentamistapaa: varmennetodentamisen lisäksi käytössä ovat salasanatodentaminen ja tätä turvallisempana pidetyt kertakäyttösalasanat. Yliopisto on arvioinut tietoverkossa tarjoamiaan palveluita ja niiltä vaadittavaa turvallisuustasoa eri käyttäjäryhmien kannalta.

Käytetty palvelu	**Palvelun käyttäjä**	**Hyväksytyt todentamistavat**		
		Varmenne	**Kertakäyttö-salasana**	**Salasana**
Palvelimelle kirjautuminen	Opiskelija	X	X	X
Palvelimelle kirjautuminen kampusverkon ulkopuolelta	Opiskelija	X	X	
Palvelimelle kirjautuminen	Ylläpitäjä	X		
Omien opintosuoritusten selaus opiskelijarekisterissä	Opiskelija	X	X	X
Opiskelijoiden opintosuoritusten selaus	Henkilökunta	X	X	
Opintosuoritusten kirjaus	Henkilökunta	X		

Taulukko 3. Esimerkki henkilöllisyyden todentamisen turvallisuustason asettamisesta.

Esimerkissä yliopisto on lähtenyt siitä, että koska ylläpitäjillä on laajimmat valtuudet tietojärjestelmässä, heidän henkilöllisyytensä todennetaan vain varmenteella.

Myös opintosuoritusten kirjaaminen opiskelijarekisteriin on katsottu varmennetodentamista edellyttäväksi tapahtumaksi. Opiskelijoiden osalta salasanankin on arvioitu riittävän. Opiskelijoiden valtuudet tietojärjestelmissä on katsottu siinä määrin rajoitetuiksi, että varmennetodentamisen edellyttämistä ei kustannukset huomioon ottaen ole pidetty järkevänä. Kampusverkon ulkopuolelta tulevia yhteydenottoja pidetään kuitenkin siinä määrin epäilyttävinä, että todentamiseen vaaditaan vähintään kertakäyttösalasana.

9.3. Luotettavampi todentaminen ja käytettävyys

Korkeakouluopiskelijoiden keskuudessa tehty tutkimus [CONS01] osoittaa, että kasvanut turvallisuus on huono argumentti, kun PKI-toimikorttien käyttöä salasanat korvaavana henkilöllisyyden todentamiskeinona halutaan perustella käyttäjille. Peruskäyttäjä ei miellä salasanan käyttämistä turvattomaksi eikä salasanan paljastumista kovin vaaralliseksi: "Eihän minulla nyt ole mitään niin salaista siellä verkossa." Kimmokkeen toimikortin käyttöön on tultava muuta kautta.

Tietoturvallisuutta kehitettäessä järjestelmän turvallisuus ja käytettävyys muodostavat helposti vastakohdan toisilleen. Jos järjestelmän turvallisuutta halutaan kasvattaa, se on vaarassa tapahtua käytön helppouden kustannuksella. Uusien, tietoturvallisuutta kohentavien toimenpiteiden käyttöönotto kohtaa vastarintaa, jos ne vähentävät järjestelmän käyttömukavuutta. Tämä näkökulma koskee myös PKI-toimikorttien käyttöönottoa varsinkin, jos se edellyttää käyttäjältä itseltään investointeja esimerkiksi toimikortinlukijaan.

Ihannetilanteessa käyttäjä mieluummin käyttäisi toimikorttiaan kuin vanhaa toimintatapaa. Esimerkiksi tietojärjestelmään kirjautuminen suoritettaisiin mieluummin toimikortilla kuin salasanalla, koska toimikorttitodentaminen koettaisiin salasanaa helpommaksi ja mukavammaksi. Tällöin siirtyminen toimikortin käyttöön tapahtuisi luonnollista tietä, eikä organisaation tarvitsisi käyttää pakkokeinoja, kuten salasanan käytön estämistä.

Toimikorttitodentamisen tekeminen salasanatodentamista helpommaksi on haasteellista. PKI-toimikorttien käytettävyyttä korkeakouluopiskelijoiden keskuudessa selvittänyt tutkimus [ULAB02] osoittaa, että monen mielestä työaseman ääreen istuttaessa on helpompaa antaa käyttäjätunnus ja salasana kuin ottaa lompakko taskusta ja toimikortti lompakosta, asettaa kortti kortinlukijaan ja antaa PIN-koodi. Vasta kun jokainen mikro on varustettu toimikortinlukijalla ja kaikki palvelut hallitsevat myös varmennetodentamisen, voidaan salasanatodentamisesta luopua, jolloin muistettavien salasanojen ja PIN-koodien määrä vähenee. Sisäänkirjoittautuminen toimikortin avulla ei saisi myöskään kestää salasanatodentamista pidempään.

Toimikortin käyttämisestä tulee koitua käyttäjälle sellaista etua, että hän kokee sen käyttämisen vanhaa toimintatapaa mukavammaksi. Käyttäjän henkilöllisyyttä todennettaessa tämä tarkoittaa, että käyttäjän tarvitsee työasemalle saapuessaan asettaa toimikortti kortinlukijaan ja antaa PIN-koodi kerran, jonka jälkeen hänen henkilöllisyytensä todennetaan kaikkiin tarvittaviin tietojärjestelmiin automaattisesti. Näin toimikortin käytöstä saatetaan kokea saatavan etua, vaikka kortti pitääkin ensin ottaa esiin lompakosta.

9.4. Uudet palvelut

Vaikka salasanan korvaaminen toimikortilla ei antaisikaan käyttäjälle riittävää kimmoketta toimikortin käyttämiseen, saattaa kimmoke tulla toista kautta, jos käyttäjä pystyy toimikortin ansiosta selviytymään helpommin jostain muusta askareesta, jota aikaisemmin ei ole lainkaan voinut tehdä tietoverkon avulla tai joka on ollut vaivalloista. Tällöin kysymykseen tulevat toimikortin ja julkisen avaimen järjestelmän mahdollistamat uudet palvelut: käsin tehtyyn allekirjoitukseen rinnastettava digitaalinen allekirjoitus sekä varmenteen käyttäminen tiedon salaukseen.

Eduskuntakäsittelyssä oleva laki sähköisestä allekirjoituksesta rinnastaa digitaalisen allekirjoituksen tiettyjen ehtojen (luku 6.5) täyttyessä käsin tehtyyn. Näin viimeisetkin juridiset esteet digitaalisen allekirjoituksen käyttöön väistyvät. Organisaatiot voivat käyttää digitaalista allekirjoitusta toisaalta sisäisessä hallinnossaan, esimerkiksi matkalaskuissa ja kirjanpidossa, ja toisaalta myös ulkoisessa asioinnissa, kuten asiakkaiden tekemissä tilauksissa ja muissa sopimuksissa. Digitaalisen allekirjoituksen oletetaan synnyttävän kustannussäästöjä, kun perinteisesti allekirjoitettujen asiakirjojen käsittelyyn tarvittava rutiinityö vähenee. Käyttäjäkin on tyytyväinen, jos digitaalinen allekirjoitus muuttaa asioiden hoitoa joustavammaksi hänen näkökulmastaan.

Toisaalta digitaalisen allekirjoituksen liittäminen asian hallinnolliseen käsittelyyn on haastavaa ja edellyttää usein suunnitteluvaiheessa kyseessä olevan asian käsittelyprosessin huolellista läpikäymistä: mitä vaiheita asian käsittelyyn liittyy, kenellä on valtuudet niiden suorittamiseen ja mitä asioita kussakin käsittelyvaiheessa on otettava huomioon. Usein jo pelkkä asian käsittelyprosessin virtaviivaistaminen ilman digitaalista allekirjoitusta voi tuoda huomattavia säästöjä. Asian hallinnollisesta käsittelymallista ja digitaalisesta allekirjoituksesta on laadittu viitearkkitehtuureja, muun muassa Valtiovarainministeriö on laatinut viranomaisasiointia kuvaavan viitekehyksen [VM01a].

Sähköposti on Internetin käytetyimpiä palveluita, jonka turvataso nykyisellään on kuitenkin postikorttiluokkaa. Toisaalta sähköpostia käytetään organisaatiossa hyvin yleisesti toisinaan luottamuksellistenkin asiakirjojen välittämiseen. Sähköpos-

tin turvallisuutta voidaan kohentaa todentamalla viestin lähettäjän henkilöllisyys digitaalisella allekirjoituksella ja huolehtimalla viestin luottamuksellisuudesta salaamalla se vastaanottajan varmenteen julkisella avaimella. Sähköpostin salaukseen yleisesti käytettävää S/MIME-protokollaa käsiteltiin luvussa 7.4, ja sitä tukevia sähköpostiasiakasohjelmia on yleisesti saatavilla. Asiakasohjelmat osaavat hyödyntää organisaation mahdollisesti asettamaa käyttäjähakemistoa ja LDAP-protokollaa noutaakseen vastaanottajan varmenteen, jolla lähetettävä viesti voidaan salata. Sähköpostin salaaminen ja allekirjoittaminen onkin yksi PKI-toimikortin ilmeisistä käyttökohteista, kun tietoisuus sähköpostin tietoturvan heikosta nykytasosta leviää myös peruskäyttäjien joukossa.

10. YHTEENVETO

Tässä tutkimuksessa on esitelty julkisen avaimen järjestelmän (public key infrastructure) toteutusperiaatteita, keskeisiä käsitteitä ja välineitä. Erityistä huomiota on kiinnitetty toimikortteihin, joiden tarjoama laitteistotason toteutus tuo lisäturvallisuutta yksityisen salausavaimen tallettamiseen. Julkisen avaimen järjestelmää ja sitä hyödyntäviä tietoliikenneprotokollia on tarkasteltu erityisesti Internetissä käytettyjen protokollien näkökulmasta.

Lisäksi tutkimuksessa on kytketty julkisen avaimen järjestelmä osaksi laajempaa kokonaisuutta, joka käsittää käyttäjän henkilöllisyyden todentamisen (autentikointi), hänelle kuuluvien käyttöoikeuksien myöntämisen ja hallinnoinnin (auktorisointi) ja tämän pohjalta tapahtuvan pääsynvalvonnan tietoverkossa oleviin resursseihin. Organisaatiossa käyttäjän henkilöllisyyden todentamiseen ja käyttäjän valtuuttamiseen liittyvät järjestelyt ovat osa tietojärjestelmien käyttäjähallintoa, johon on niinikään luotu silmäys erityisesti käyttäjän henkilöllisyyden todentamisen näkökulmasta.

Peruskäyttäjälle julkisen avaimen järjestelmä konkretisoituu ehkä toimikorttiin, joka ”sisältää” varmenteen. Julkisen avaimen järjestelmä on kuitenkin paljon muutakin kuin pelkkä toimikortti. Se on ennen kaikkea joukko sovittuja toimintatapoja, joihin järjestelmän eri osapuolet ovat sitoutuneet. Järjestelmästä kokonaisvastuussa on varmentaja, joka muun muassa huolehtii, että käyttäjän varmenteen ja yksityisen avaimen sisältämä toimikortti luovutetaan käyttäjälle henkilökohtaisesti. Järjestelmää hyödyntävä osapuoli on velvollinen esimerkiksi varmistamaan, että käyttäjän varmennetta ei ole asetettu sulkulistalle. Käyttäjä, jonka henkilöllisyyden järjestelmä varmentaa, puolestaan on velvollinen muun muassa huolehtimaan, ettei hänen toimikorttinsa pääse hukkumaan.

Epäsymmetrisen salausmenetelmän ja siihen liittyvän julkisen avaimen järjestelmän avulla on mahdollista toteuttaa kolme tietoverkon peruspalvelua. Käyttäjän henkilöllisyys voidaan todentaa, hän voi ilmaista sitoutumisensa tiettyyn viestiin tekemällä digitaalisen allekirjoituksen ja hän voi salata tietoverkon käyttäjille lähetettäviä viestejä. Näistä erityisesti henkilöllisyyden todentaminen salasanoja luotettavammalla tavalla on houkutteleva mahdollisuus. Monet olemassaolevat tietoliikenneprotokollat tukevat jo nykyään käyttäjän henkilöllisyyden todentamista julkisen avaimen järjestelmän avulla, mutta sen mahdollisuuksia ei ole hyödynnetty kovin laajasti. Salasanan käyttämiseen liittyy riskejä, ja muistettavien salasanojen määrä on rasite myös käyttäjille. Kehitys kulkee kohti tulevaisuutta, jossa verkossa on saatavilla entistä suurempi joukko mahdollisesti eri organisaatioiden

tuottamia henkilökohtaisia palveluja, jotka edellyttävät käyttäjän henkilöllisyyden todentamista.

Peruskäyttäjä saattaa kokea, että palvelut ”sijaitsevat” itse toimikortilla. Kun julkisen avaimen järjestelmää käytetään käyttäjän henkilöllisyyden todentamiseen, tilanne on kuitenkin juuri päinvastainen. Toimikorttia käytetään pelkästään avaimena palveluihin, jotka todellisuudessa sijaitsevat verkossa. Jos palveluja tai niihin liittyviä käyttöoikeuksia muutetaan, ei toimikorttia tarvitse päivittää, vaan riittää, että muutokset tehdään palvelut tuottavassa tietojärjestelmässä ja siihen kytkeytyvässä käyttäjähallinnossa.

Julkisen avaimen järjestelmän avulla toteutettu digitaalinen allekirjoitus mahdollistaa paitsi sähköpostiviestien lähettäjän ja eheyden varmistamisen, myös perinteisen kirjallisesti tapahtuneen asiankäsittelyn ja kynällä tehdyn allekirjoituksen siirtämisen tietoverkkoon. Erilaiset organisaation sisäiset asiat, kuten kirjanpito ja muu taloushallinto, ja organisaation ja asiakkaan väliset asiat, kuten tilaukset tai hakemukset, ovat siirrettävissä paperilta sähköiseen muotoon. Käyttäjä voi allekirjoittaa matkalaskunsa tai pankkisiirtonsa esimerkiksi toimikortin avulla WWW-selaimen välityksellä. Organisaation odotetaan hyötyvän näin saatavista kustannussäästöistä, asiakkaan puolestaan aikaan ja paikkaan sitomattomasta asiointimahdollisuudesta. Sähköisen allekirjoituksen toteuttaminen on kuitenkin työlästä ja edellyttää myös kyseisen asian hallinnollisen käsittelyprosessin analysointia ja mallintamista.

Internetin lähtökohtaisesti tarjoama turvallisuustaso on vaatimaton, ja esimerkiksi sähköposti kulkee verkossa täysin salaamattomana, jolloin jokainen viesteihin käsiksi pääsevä voi halutessaan lukea ne. Julkisen avaimen järjestelmä mahdollistaa sähköpostin ja muiden tiedostojen salaamisen, ja yksi sen varteenotettava käyttökohde on sähköpostin luottamuksellisuustason nostaminen. Julkisen avaimen järjestelmän avulla sähköpostina voi lähettää luottamuksellisiakin dokumentteja, jotka vain vastaanottaja pystyy lukemaan.

Valitettavasti toimikortit eivät kuitenkaan ratkaise lopullisesti edes kaikkia käyttäjän henkilöllisyyden todentamiseen liittyviä ongelmia. Käytetyt toimikortit ovat kompromisseja turvallisuuden ja tuotantokustannusten välillä ja ovat murrettavissa riittävän asiantuntemuksen ja työvälineiden avulla. Akuutimman riskin muodostaa kuitenkin työasema, johon mahdollisesti pesiytynyt tuho-ohjelma voi väärinkäyttää toimikorttia. Työaseman turvallisuuteen liittyvissä kysymyksissä on syytä olla varpaillaan.

Tässä tutkimuksessa ei ole keskitytty organisaation käyttövaltuuksien myöntämiseen ja hallinnointiin, vaan niitä on lähinnä sivuttu sikäli, kun ne liittyvät julkisen avaimen järjestelmään. On kuitenkin ilmeistä, että julkisen avaimen järjestelmän käyttöönottaminen käyttäjän henkilöllisyyden todentamisessa luo tarpeen myös

näiden järjestelmien kehittämiselle. On jossain määrin työlästä rakentaa järjestely, jonka avulla voidaan päätellä, kenen henkilöllisyydellä tietyn varmenteen esittänyt käyttäjä on oikeutettu kirjautumaan sisälle palvelimelle, ja niinpä on luontevaa toteuttaa järjestely kussakin organisaatiossa keskitetysti. Näin julkisen avaimen järjestelmän käyttöönottaminen osaltaan kasvattaa painetta siirtyä kohti keskitettyä käyttäjähallintoa.

LÄHTEET

ANDE97 Anderson, R., Kuhn, M. Low Cost Attacks on Tamper Resistant Devices. Proceedings of Security Protocols, 5th International Workshop, Paris, France, 7–9 huhtikuuta 1997. LNCS 1361, s. 125–136.

ANDE01 Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons, Inc. 2001. 612 s.

AUDU99 Audun, J., An Algebra for Assessing Trust in Certification Chains. Proceedings of NDSS'99, Network and Distributed Systems Security Symposium, The Internet Society, San Diego, CA USA, 1999.

AVAN02 Automatia rahakortit. Avant-korttiraha. http://www.avant.fi/ Viitattu 11.2.2002.

BOHM00 Bohm, N., Brown, I., Gladman, B. Electronic Commerce: Who carries the Risk of Fraud? The Journal of Information, Law and Technology (JILT), no. 3, 2000.

CARO00 Caronni G. Walking the Web of trust. IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprices, Gaithersburg, MD USA, 14–16 kesäkuuta 2000. s. 153–158.

CCID01 Universal Serial Bus. Device Class Specification for USB Chip/Smart Card Interface Devices, 2001. 135 s.

CONS01 Topi Jurvanen. Korttikonseptin vastaanotto. Helsinki: Consumer Compass – Kuluttajatieto Oy, 2001. 42 s.

DIFF76 Diffie, W., Hellman, M. New Directions in Cryptography. IEEE Transactions on Information Theory. Vol IT-22, no. 6, 1976, s. 644–654.

EMV00 EMV-määrittelyprojekti 1999–2000. EMV yleiskuvaus versio 1.2, 2000. 39 s. Saatavilla myös http://www.luottokunta.fi/download/emv_1.pdf

EP99 1999/93/EY Euroopan parlamentin ja neuvoston direktiivi, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puitteista.

ETSI00 TS 100 977. Digital cellular telecommunications system (Phase 2+) (GSM);Specification of the Subscriber Identity Module – Mobile Equipment (SIM - ME) interface(GSM 11.11 version 8.3.0 Release 1999). Sophia

Antipolis: European Telecommunications Standards Institute, 2000.

FIPS46 FIPS PUB 46-3. Data Encryption Standard (DES). Federal Information Processing Standards Publication 46-3. National Institute of Standards and Technology, 1999. 26 s. Saatavilla myös http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

FIPS180 FIPS PUB 180-1. Secure Hash Standard. Federal Information Processing Standards Publication 180-1. National Institute of Standards and Technology, 1995. 24 s. Saatavilla myös http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf

FIPS197 FIPS PUB 197. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. National Institute of Standards and Technology, 2001. 51 s. Saatavilla myös http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FRIE96 A. Frier, P. Karlton, P. Kocher. The SSL 3.0 Protocol. Netscape communications, 1996. Saatavilla myös http://home.netscape.com/eng/ssl3/ssl-toc.html

GNOM01 Global Nordic Middleware Symposium. http://www.uninett.no/info/seminar/gnomis/ Viitattu 9.1.2002.

GOBI96 Gobioff, H., Smith, S., Tygar, J., Yee, B. Smart Cards in Hostile Environments. Proceedings of the Second USENIX Workshop on Electronic Commerce, Oakland, CA USA, Marraskuu 1996.

GUTM02 Gutman, P. How to recover private keys for Microsoft Internet Explorer, Internet Information Server, Outlook Express, and many others – or – Where do your encryption keys want to fo today? http://www.cs.auckland.ac.nz/~pgut001/pubs/breakms.txt Viitattu 30.9.2002.

HE01 HE 197/2001 Hallituksen esitys eduskunnalle laeiksi sähköisistä allekirjoituksista ja viestintähallinnosta annetun lain 2 §:n muuttamisesta.

HELM97 Helm, A., Mullender, S. What You See is What Gets Signed. Huygens Report 97-01. Universisteit Twente, Enschede. Maaliskuu, 1997.

HETI99 523/1999 Henkilötietolaki.

HOUS01 Housley, R., Polk, T. Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure. New York: John Wiley & Sons, Inc. 2001. 352 s.

INTE02 Internet2/MACE. Shibboleth Project. http://middleware.internet2.edu/shibboleth Viitattu 7.10.2002.

IS7816 ISO/IEC 7816. Identification cards -- Integrated circuit(s) cards with contacts. Osat 1–10. Geneve: International Organization for Standardization.

IS8824 ISO/IEC 8824:1990 Information technology -- Open Systems Interconnection -- Specification of Abstract Syntax Notation One (ASN.1). Geneve: International Organization for Standardization, 1990.

ISO01 Bennett, F. Information technology : Refining personal identification techniques using biometric data. ISO Bulletin, September 2001, s. 3–5. Saatavilla myös http://www.iso.ch/iso/en/commcentre/isobulletin/articles/2001/pdf/identification0109.pdf,

KÖMM99 Kömmerling, O., Kuhn, M. Design Principles for Tamper-Resistant Smartcard Processors. Proceedings of the USENIX Workshop on Smartcard Technology, Chigago, IL USA, 10–11 toukokuuta 1999. s. 9–20.

LEHT98 Lehti, I., Nikander, P. Certifying Trust. Proceedings of Public Key Cryptography – First International Workshop on the Practice and Theory of Public Key Cryptography PKC'98, Yokohama, Japan, helmikuu 1998. s. 83-98.

LENS01 Lenstra A.K., Verheul E.R. Selecting cryptographic Key Sizes. Journal of Cryptography, vol. 14, no. 7, 2001. s. 255–293.

MENE97 Menezes, A., van Oorschot P., Vanstone, S. Handbook of Applied Cryptography. Boca Raton: CRC Press, Inc, 1997. 780 s.

MODS02 Ralf S. Engelschall. Mod_ssl: The Apache Interface to OpenSSL. User Manual. http://www.modssl.org/docs/2.8/ Viitattu 7.2.2002.

MOSK01 Moskowitz, R. Host Identity Payload and Protocol. Internet Engineering Task Force. Work in progress, 2001.

MUSC02 MUSCLE - Movement for the Use of Smart Cards in a Linux Environment. http://www.linuxnet.com Viitattu 11.2.2002.

NETE02 Netegrity , Inc. Netegrity SiteMinder. http://www.netegrity.com/ Viitattu 7.10.2002.

NICH99 Nichols R. ICSA Guide to Cryptography. New York: The McGraw-Hill Companies, Inc, 1999. 832 s.

OPEN02 The OpenSSL Project. http://www.openssl.org/ Viitattu 8.2.2002.

PANK01 Suomen pankkiyhdistys. Tunnistepalvelu asiointipalvelun tuottajille. Palvelun kuvaus ja palveluntuottajan ohje. Versio 1.1. 2001. 18 s. Saatavilla myös http://www.pankkiyhdistys.fi/sisalto/upload/pdf/tupasasia.pdf

PCSC97 PC/SC Workgroup. Interoperability Specification for ICCs and Personal Computer Systems. Part 1. Introduction and Architecture Overview. 1997. 29 s. Saatavilla myös http://www.pcscworkgroup.com/Specifications/p1v10doc.zip

PCSC99 PC/SC Working group. White Paper: Introducing the PC/SC Specifications 2.0. 1999. 18 s.

PERU99 731/1999 Suomen perustuslaki.

PERL99 Perlman, R. An Overview of PKI Trust Models. IEEE Network, marras/joulukuu 1999. s. 38–43.

PGP02 The International PGP Home Page. http://www.pgpi.org/ Viitattu 8.2.2002.

PKCS7 RSA Laboratories. PKCS #7: Cryptographic Message Syntax Standard, versio 1.5. 1993. 28 s. Saatavilla myös ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.pdf

PKCS11 RSA Laboratories. PKCS#11: Cryptographic Token Interface Standard, versio 2.11. 2001. 360 s. Saatavilla myös ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v211/pkcs-11v2-11r1.pdf

PKCS15 RSA Laboratories. PKCS #15: Cryptographic Token Information Format Standard, versio 1.1. 2000. 81 s. Saatavilla myös ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf

RFC1321 RFC 1321. The MD5 Message-Digest Algorithm. Internet Engineering Task Force. 1992. 21 s.

RFC1510 RFC 1510. The Kerberos Network Authentication Service (V5). Internet Engineering Task Force. 1993. 112 s.

RFC2246 RFC 2246. The TLS Protocol. Internet Engineering Task Force. 1999. 80 s.

RFC2251 RFC 2251. Lightweight Directory Access Protocol (v3). Internet Engineering Task Force. 1997. 50 s.

RFC2289 RFC 2289. A One-Time Password System. Internet Engineering Task Force. 1998. 25 s.

RFC2459 RFC 2459. Internet X.509 Public Key Infrastructure, Certificate and CRL Profile. Internet Engineering Task Force. 1999. 129 s.

RFC2527 RFC 2527. Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework. Internet Engineering Task Force. 1999. 45 s.

RFC2560 RFC 2560. X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP. Internet Engineering Task Force. 1999. 23 s.

RFC2632 RFC 2632. S/MIME Version 3 Certificate Handling. Internet Engineering Task Force. 1999. 13 s.

RFC2693 RFC 2693. SPKI Certificate Theory. Internet Engineering Task Force. 1999. 43 s.

RFC2798 RFC 2798. Definition of the inetOrgPerson LDAP Object Class. Internet Engineering Task Force. 2000. 20 s.

RFC2865 RFC 2865. Remote Authentication Dial In User Service (RADIUS). Internet Engineering Task Force. 2000. 76 s.

RFC3281 RFC 3281. An Internet Attribute Certificate Profile for Authorization. Internet Engineering Task Force. 2002. 40 s.

RIVE78 Rivest, R., Shamir, A., Adleman, L. A Method for Obtaining DigitalSignatures and Public-key cryptosystems. Communications of the ACM, vol 21, no. 2, 1978, s. 120–126.

RIVE96 Rivest, R., Lampson, B. SDSI – A Simple Distributed Security Infrastructure. 1996

RSA99 RSA Security Inc. DES Challenge III Broken in Record 22 Hours. RSA Lehdistötiedote 19.1.1999. Saatavilla myös http://WWW.rsasecurity.com/news/pr/990119-1.html

RSAB02 RSA Security Inc. RSA BSAFE. http://www.rsasecurity.com/products/bsafe/index.html Viitattu 8.2.2002.

RSAS02 RSA Security Inc. RSA SecurID Tokens. http://www.rsasecurity.com/products/securid/tokens.html Viitattu 11.2.2002.

SOON01 Soon Communications Oyj. Pirkanmaan puhelinluettelo, 2001.

STAL99 Stallings, W. Cryptography and Network Security. Toinen painos. New Jersey: Prentice-Hill Inc., 1999. 569 s.

TEBB95 Tebbut, J. Guidelines for Evaluation of X.500 Directory Products. Gaithersburg, MD: National Institute of Standards and Technology, 1995. NIST Special Publication; 500–228.

ULAB02 Tampereen yliopisto, Tietojenkäsittelytieteen laitos, käytettävyyslaboratorio. Käytettävyyden arviointi HSTYA-projektissa, loppuraportti. Tampere, 2002. 92 s.

UWAS University of Washington. Pubcookie. http://www.washington.edu/pubcookie. Viitattu 7.10.2002

VISA02 Visa International Service Association. Visa Cash. http://corporate.visa.com/mc/facts/visacash.shtml Viitattu 11.2.2002.

VM00 Valtiovarainministeriö, Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtionhallinnon tietoturvakäsitteistö. Helsinki, 2000. 51 s. Saatavilla myös http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/sanasto/sisallys.htm

VM01 Valtiovarainministeriö, Hallinnon kehittämisosasto. Hallinnon sähköisen asiointipalvelun viitearkkitehtuuri. Helsinki: Valtiovarainministeriön työryhmämuistioita 34/2001. 42 s. Saatavilla myös http://www.vn.fi/vm/julkaisut/tyoryhmamuistiot/pdf/tr34_2001.pdf

VM01b Valtiovarainministeriö, Hallinnon kehittämisosasto. Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje. Helsinki: Valtionhallinnon tietoturvallisuuden johtoryhmä 4/2001. 31 s. Saatavilla myös http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/vahti42001.pdf

VRK99 Väestörekisterikeskus. HST-varmennepolitiikka: Sähköisellä henkilökortilla olevia hallinnon sähköisen asioinnin henkilövarmenteita varten. Helsinki, 1999. 30 s. Saatavilla myös http://www.fineid.fi/download/shksf.pdf

VRK99b Väestörekisterikeskus. FINEID – 4-1 Implementation Profile 1, versio 1.1. Helsinki, 1999. 35 s. Saatavilla myös http://www.fineid.fi/download/S4-1v100.doc

VRK02 Väestörekisterikeskus. Sähköinen henkilökortti. http://www.fineid.fi/ Viitattu 11.2.2002.

WAPF01 WAP-260-WIM-20010712-a. Wireless Application Protocol; Wireless Identity Module. Wireless Application Protocol Forum Ltd., 2001. 105 s.

YLON02a Ylönen, T., Kivinen, T., Saarinen, M., Rinne, T. Lehtinen, S. SSH Protocol Architecture. Internet Engineering Task Force.Work in progress, 2002.

YLON02b Ylönen, T., Kivinen, T., Saarinen, M., Rinne, T. Lehtinen, S. SSH Connection Protocol. Internet Engineering Task Force.Work in progress, 2002.

YLON02c Ylönen, T., Kivinen, T., Saarinen, M., Rinne, T. Lehtinen, S. SSH Transport Layer Protocol. Internet Engineering Task Force.Work in progress, 2002.

YLON02d Ylönen, T., Kivinen, T., Saarinen, M., Rinne, T. Lehtinen, S. SSH Authentication Protocol. Internet Engineering Task Force.Work in progress, 2002.

X50900 ITU-T X.509 (03/00). Information technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks. Geneve: International Telecommunication Union, 2000.

LIITE A: ESIMERKKI X.509V3-VARMENTEESTA

Erään X509v3-varmenteen tietosisältö, jonka ASN.1-rakenne on purettu auki mukavammin luettavaan muotoon OpenSSL-työkalulla [OPEN02].

```
Data:
    Version: 3 (0x2)
    Serial Number: 13542 (0x34e6)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=FI, O=VRK-FINSIGN Gov. CA, CN=FINSIGN CA for Citizen
    Validity
        Not Before: Jul 10 23:59:59 2000 GMT
        Not After : Jul  6 23:59:59 2003 GMT
    Subject: C=FI, S=LINDEN, G=MIKAEL,
             CN=LINDEN MIKAEL 10005323B, SN=10005323B
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:df:b6:df:b6:18:79:86:6e:23:13:10:fb:29:da:
                82:40:c9:0b:0f:5b:66:25:ac:33:1b:bd:36:8e:2f:
                ea:a7:95:12:9d:31:4f:61:e6:8b:1e:5d:b7:69:db:
                d8:ff:68:d8:73:0a:14:d2:13:6c:1c:a1:00:5b:4f:
                6f:53:c5:c6:ba:66:56:77:39:64:a6:78:51:e7:ce:
                b8:82:64:0e:45:8b:bf:6d:f1:e8:96:b6:ff:28:a6:
                98:f1:c2:3f:7b:15:40:a0:88:15:24:64:45:11:8a:
                bc:a3:00:30:83:50:d6:44:0b:32:ca:42:df:fe:d3:
                6c:1b:a0:6e:fd:f7:13:1c:25
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Certificate Policies:
            Policy: 1.2.246.517.1.1
        X509v3 Subject Key Identifier:
            4A:6F:F7:AB:68:AC:4B:6C
        X509v3 CRL Distribution Points:
            URI:ldap://193.229.0.210:389/
            cn=finsign%20ca%20for%20citizen,o=vrk-finsign%20gov.%20ca,
            dmdname=fineid,c=FI?certificaterevocationlist
        X509v3 Authority Key Identifier:
            keyid:46:49:4E:43:41:4B:30:31
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment, Data Encipherment
Signature Algorithm: sha1WithRSAEncryption
    af:ff:30:81:e5:c5:70:eb:44:2a:5b:8f:2e:07:44:95:63:a1:
    8b:83:53:e8:64:13:9c:63:0e:53:ec:39:7e:f1:59:83:db:d2:
    1d:0b:dc:4c:fc:d3:43:2a:e6:7a:d3:92:36:f0:6e:ac:f8:99:
    45:b9:4b:d1:14:69:25:dd:22:d0:07:06:fc:3b:67:3b:5f:99:
    b0:bb:5b:ee:df:21:a2:2a:c9:cc:60:56:19:bc:24:80:28:04:
    35:33:59:2e:59:9d:c0:aa:71:e6:18:41:01:5e:3d:60:0c:03:
    b6:99:a3:62:41:53:81:7d:9f:dc:ca:5f:e5:7b:07:1f:ee:d4:
    83:d8:ed:6a:60:03:b8:44:a2:c3:fd:7d:15:b0:ad:ad:c6:70:
    30:4f:02:92:a2:af:dc:1a:ca:1e:db:09:06:a6:6b:54:94:f6:
    fd:e0:2d:d3:63:64:e7:1d:a4:d1:f4:fa:be:bf:79:ef:3b:7e:
    d8:2c:49:b6:ed:3a:94:4e:f7:b3:51:6b:ac:09:bd:16:3a:3f:
    b7:52:2a:15:27:6e:c7:96:b6:3d:42:f3:15:3e:47:6e:85:25:
    65:93:2b:df:a5:28:6b:d9:9f:13:6e:56:18:dc:c9:8a:35:91:
    8a:cb:b1:c4:a7:1b:04:64:81:51:f0:21:c8:f5:76:c0:51:0c:
    45:e6:e8:cb
```

Edellisen sivun X.509v3-varmenne DER- ja Base 64 -koodatussa muodossa, kehystettynä varmenteen alkua ja loppua osoittavilla merkinnöillä.


```
-----BEGIN CERTIFICATE-----
MIIDlTCCAn2gAwIBAgICNOYwDQYJKoZIhvcNAQEFBQAwTDELMAkGA1UEBhMCRkkx
HDAaBgNVBAoUE1ZSSy1GSU5TSUdOIEdvdi4gQ0ExHzAdBgNVBAMUFkZJTlNJR04g
Q0EgZm9yIENpdGl6ZW4wHhcNMDAwNzEwMjM1OTU5WhcNMDMwNzA2MjM1OTU5WjBl
MQswCQYDVQQGEwJGSTEPMA0GA1UEBBQGTElOREVOMQ8wDQYDVQQqFAZNSUtBRUwx
IDAeBgNVBAMUF0xJTkRFTiBNSUtBRUwgMTAwMDUzMjNCMRIwEAYDVQQFEwkxMDAw
NTMyM0IwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN+237YYeYZuIxMQ+yna
gkDJCw9bZiWsMxu9No4v6qeVEp0xT2Hmix5dt2nb2P9o2HMKFNITbByhAFtPb1PF
xrpmVnc5ZKZ4UefOuIJkDkWLv23x6Ja2/yimmPHCP3sVQKCIFSRkRRGKvKMAMINQ
1kQLMspC3/7TbBugbv33ExwlAgMBAAGjgeswgegwFAYDVR0gBA0wCzAJBgcqgXaE
BQEBMBEGA1UdDgQKBAhKb/eraKxLbDCBlwYDVR0fBIGPMIGMMIGJoIGGoIGDhoGA
bGRhcDovLzE5My4yMjkuMC4yMTA6Mzg5L2NuPWZpbnNpZ24lMjBjYSUyMGZvciUy
MGNpdGl6ZW4sbz12cmstZmluc2lnbiUyMGdvdi4lMjBjYSxkbWRuYW1lPWZpbmVp
ZCxjPUZJP2NlcnRpZmljYXRlcmV2b2NhdGlvbmxpc3QwEwYDVR0jBAwwCoAIRklO
Q0FLMDEwDgYDVR0PAQH/BAQDAgSwMA0GCSqGSIb3DQEBBQUAA4IBAQCv/zCB5cVw
60QqW48uB0SVY6GLg1PoZBOcYw5T7Dl+8VmD29IdC9xM/NNDKuZ605I28G6s+JlF
uUvRFGkl3SLQBwb8O2c7X5mwu1vu3yGiKsnMYFYZvCSAKAQ1M1kuWZ3AqnHmGEEB
Xj1gDAO2maNiQVOBfZ/cyl/lewcf7tSD2O1qYAO4RKLD/X0VsK2txnAwTwKSoq/c
Gsoe2wkGpmtUlPb94C3TY2TnHaTR9Pq+v3nvO37YLEm27TqUTvezUWusCb0WOj+3
UioVJ27HlrY9QvMVPkduhSVlkyvfpShr2Z8TblYY3MmKNZGKy7HEpxsEZIFR8CHI
9XbAUQxF5ujL
-----END CERTIFICATE-----
```

LIITE B: LYHENTEET

AES	advanced encryption standard
AODF	authentication object definition file
APDU	application protocol data unit
API	application programming interface
ASN.1	abstract syntax notation one
C	country
CA	certification authority
CCID	USB chip/smart card interface devices
CDF	certificate definition file
CP	certificate policy
CPS	certification practices statement
CRL	certificate revocation list
CSP	cryptographic service provider
DER	distinguished encoding rule
DES	data encryption standard
DF	dedicated file
DN	distinguished name
DODF	data object definition file
EEPROM	electronically erasable programmable read-only memory
EF	elementary file
EMV	europay-mastercard-visa
FIB	Focused ion beam
GSM	global system for mobile communications
HSM	hardware security module
HST	henkilön sähköinen tunnistaminen
HTTP	hypertext transfer protocol

ICC	integrated circuit card
IETF	internet engineering task force
IFD	interface device
IP	internet protocol
IPSec	internet protocol security
ISO	international organization for standardization
ITU-T	international telecommunication union
LDAP	lightweight directory access protocol
MF	master file
MIME	multipurpose internet mail extensions
MLA	mail list agent
MUSCLE	movement for the use of smart cards in a linux environment
PCMCIA	personal computer memory card international association
PC/SC	personal computer / smart card
PGP	pretty goof privacy
PIN	personal identification code
PKI	public key infrastructure
O	organization
OCSP	open certificate status protocol
ODF	object definition file
OU	organizational unit
PKCS	public key cryptography standard
PKINIT	public key cryptography for initial authentication in kerberos
PrDF	private key definition file
PrK	private key
RA	registration authority
RAM	random access memory
RFC	request for comments

ROM	read-only memory
RSA	rivest-shamir-adleman
SATU	sähköinen asiointitunnus
SET	secure electronic transaction
SIM	subscriber identification module
SPKI	simple public key infrastructure
SQL	structured query language
SSH	secure shell
SSL	secure sockets layer
TaY	Tampereen yliopisto
TCB	trusted computing base
TCP	transmission control protocol
TLS	transfer layer security
TPDU	transmission protocol data unit
TTY	Tampereen teknillinen yliopisto
USB	universal serial bus
VPN	virtual private network
WAP	wireless application protocol
WIM	wireless identity module
WTLS	wireless transfer layer security