VALTIOVARAINMINISTERIÖ

TURVALLINEN ETÄKÄYTTÖ TURVATTOMISTA VERKOISTA

2/2003

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

TURVALLINEN ETÄKÄYTTÖ TURVATTOMISTA VERKOISTA

Suositus turvallisen etäkäytön arkkitehtuurista

2/2003

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33 222

Sähköposti: vahtijulkaisut@vm.fi

ISSN 1455-2566
ISBN 951-804-395-7

Edita Prima Oy
HELSINKI 2003

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 24/01/2003

SUOSITUS
19.9.2003

Ministeriöille, virastoille ja laitoksille

SUOSITUS TURVALLISEN ETÄKÄYTÖN ARKKITEHTUURISTA

Valtiovarainministeriö antaa oheisen tietoturvallisuussuosituksen (jäljempänä suositus), joka on laadittu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Suositus täydentää laajaa olemassa olevaa valtiovarainministeriön antamaa valtionhallinnon tietoturvallisuusohjeistoa (www.vm.fi/vahti) ja erityisesti Valtionhallinnon etätyön tietoturvallisuusohjetta (VAHTI 3/2002) .

Suosituksessa käsitellään etäkäytön erityiskysymyksiä tietoturvallisuuden kannalta. Etäkäytöllä tarkoitetaan työpisteen ulkopuolelta etäyhteyden avulla tapahtuvaa tietoteknisten palvelujen käyttöä. Suosituksen lähestymistapa on tekninen.

Etäkäyttö lisääntyy ja saa uusia muotoja. Tässä tilanteessa korostuvat mm. jatkuvaluonteinen, ennakoiva ja ohjeistuksen mukainen tietotekninen tietoturvallisuustyö sekä organisaation henkilökunnan opastaminen ja ohjeistaminen etäkäyttöön. Turvallisen etäkäytön toteuttaminen edellyttää mm. johdon, tietohallinnon ja etäkäyttäjien toimenpiteitä.

Suosituksen yhdeksi lähtökohdaksi on otettu etäkäytettävien sovellusten luokittelu niissä käsiteltävien aineistojen luottamuksellisuuden mukaan. Kunkin organisaation tulee arvioida, mitkä sovellukset halutaan ja voidaan tarjota etäkäyttöön. Tässä suosituksessa ei ole pyritty luomaan uutta luokitusta, vaan tiedot ja aineistot luokitellaan annettujen ohjeiden mukaan (Valtion tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000 ja Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 5/01/2000).

Annetut suositukset on syytä ottaa huomioon myös asennettaessa langattomia verkkoja, joiden käytön riskit ovat monelta osin samantyyppisiä kuin etäkäytön riskit.

Asiakirja tulee Valtionhallinnon tietoturvallisuuden johtoryhmän Internet-sivuille, jotka ovat osoitteissa www.vm.fi/vahti ja www.vm.fi/tietoturvallisuus. Suositusta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi). Lisätietoja antavat projektipäällikkö Olli-Pekka Rissanen (Olli-Pekka.Rissanen@vm.fi) sekä neuvotteleva virkamies Mikael Kiviniemi (Mikael.Kiviniemi@vm.fi).

Ylijohtaja Jorma Karjalainen

Neuvotteleva virkamies Mikael Kiviniemi

Liite: Turvallinen etäkäyttö turvattomista verkoista: Suositus turvallisen etäkäytön arkkitehtuurista (VAHTI 2/2003)

SISÄLLYS

1 JOHDANTO

1.1 Tausta ja suosituksen valmistelu

Valtionhallinnon organisaatiot hyödyntävät nykyisin yhä laajemmin etätyön ja etäkäytön antamia mahdollisuuksia työtehtävien hoitamisessa. Etäkäyttömahdollisuudet valtionhallinnossa ovat laajoja ja edelleen kasvussa. Etäkäyttömahdollisuuksia on varsin laajasti myös operatiivisiin ja hallinnollisiin järjestelmiin sähköpostien laajan etäkäyttömahdollisuuden lisäksi.

VM on antanut syyskuussa 2002 uuden ohjeen etätyön tietoturvallisuudesta (VAHTI 3/2002). Ohjeessa käsitellään etätyön tietoturvallisuusriskejä ja tietoturvallisuusjärjestely- ja tietoturvallisuuden kahdeksan osa-alueen pohjalta. Ohjeessa on käsitelty yleisellä tasolla myös turvalliseen etätyöhön ja etäkäyttöön liittyviä teknisiä turvallisuusratkaisuja.

VAHTI-ryhmä asetti valmistelutyöryhmän, jonka tehtävänä on arvioida erilaisia turvallisen etäkäytön järjestelmäarkkitehtuurivaihtoehtoja ja soveltuvin osin laatia asiaan liittyviä suosituksia. Ryhmän muodostivat:

Olli-Pekka Rissanen, Valtionvarainministeriö, puheenjohtaja
Heikki Haukirauma, Työministeriö
Vesa Hongisto, Museovirasto
Jarmo Iiskola, Työministeriö
Kari Karlsson, Ilmatieteen laitos
Kyösti Kononen, Maa- ja metsätalousministeriö
Kaarlo Korvola, Sisäasiainministeriö
Sami Koskinen, Teknillinen korkeakoulu
Hannu Kukkonen, VTT
Petri Ollikainen, Ilmailulaitos
Seppo Riihimäki, Valtiovarainministeriö
Kari Tuominen, Maa- ja metsätalousministeriön tietokeskus

Konsulttityöstä vastasivat:

Juhani Jämiä, Fujitsu Invia
Kari Kyttälä, Fujitsu Invia, sihteeri.

Suositus on käsitelty valtionhallinnon tietoturvallisuuden johtoryhmässä kesäkuussa 2003.

1.2 Tarkoitus ja kohderyhmä

Ryhmän työn tuloksena syntynyt suositus on tarkoitettu valtionhallinnon yksiköiden tietohallinnolle ja tietoturvallisuusvastaaville. Sitä on tarkoitus käyttää virastotason tietoteknisten etäkäyttöjärjestelyjen tukena. Suositus määrittelee suunnan ja tavoitetilan, jota kohti virastojen suositellaan kehittävän etäkäyttöratkaisujaan.

Huomattakoon, että vaikka suosituksen aiheena on etäkäyttö, tässä annetut suositukset pätevät myös sellaiseen paikalliseen käyttöön, jossa käytetään langattomia WLAN- tai Bluetooth-verkkoja. Nämä ja niiden käyttö ovat riskeiltään yleisiin, avoimiin verkkoihin rinnastettavia.

1.3 Suosituksen rakenne

Suosituksesta on pyritty muodostamaan itsenäisesti toimiva kokonaisuus, jonka käytössä ei tarvitsisi turvautua lähde- ja viitemateriaaleihin. Suosituksessa on aluksi melko laajasti kuvailtu etäkäytön toimintaympäristöä (*luku 2*), tarpeita (*luku 3*) sekä etäkäyttöön liittyviä uhkia (*luvussa 4*). Luvussa 4 käydään läpi etäkäytön suojaamiseen liittyvät tekniikat ja ratkaisut. *Luvussa 5* esitetään metodologia ja konkreettiset suositukset turvallisen etäkäytön arkkitehtuurin rakentamiselle. Lopuksi *luvussa 6* esitellään esimerkki turvallisen etäkäyttöarkkitehtuurin soveltamista.

1.4 Käsitteet

Suosituksen lukijalle oletetaan tietotekniikan ja sen käyttöön liittyvien peruskäsitteiden ja –ratkaisujen olevan tuttuja. Suosituksessa esiintyvät aiheeseen liittyvät lyhenteet ja tekniset termit, joista osa on englanninkielisiä, on selitetty *liitteessä 1, lyhenteitä ja teknisiä termejä*. Kaikki suosituksen ymmärtämisen kannalta olennaiset etäkäyttöön liittyvät käsitteet on pyritty määrittelemään tekstissä sitä mukaa kuin ne tulevat esille. Seuraavaan on koottu keskeisimpien käsitteiden selitykset siinä muodossa kuin ne tekstissäkin esitetään.

Käsite	Selitys
etäkäytettävä sisältö	**Etäkäyttöpalveluun** liittyvät tiedot ja aineistot • joita syötetään palveluun / käsitellään palvelussa • jotka ovat palvelun avulla tavalla tai toisella saatavilla • joita tarvitaan muuten palvelua käytettäessä.
etäkäyttö	Tietotekniikkapalvelujen käyttö **viraston verkon** ulkopuolelta.
etäkäyttöluokittelu	Etäkäytettävien sovelluspalvelujen ryhmittely luokkiin sen mukaan miten hyvin suojattu **etäkäyttöratkaisu** tarvitaan.
etäkäyttöpalvelu	**Viraston palvelujärjestelmän** sovellus, jonka käyttö viraston verkon ulkopuolelta on mahdollistettu.
etäkäyttöpolitiikka	Asiakirja, jossa määritellään toimintapoliittiset linjaukset viraston tietojärjestelmäpalvelujen **etäkäytölle**.
etäkäyttöratkaisu	Tekniset järjestelyt tietojärjestelmäpalvelujen **etäkäyttöön**. Etäkäyttöratkaisun muodostavat **päätelaite**, **päätteen verkkoliitäntä**, **verkkoyhteys** sekä **palvelun verkkoliitäntä**.
etäkäyttöympäristö	Paikka ja tilanne, jossa **etäkäyttö** tapahtuu.
etätyö	Etätyö on työtä, joka tehdään muualla kuin varsinaisella työpaikalla. Työ tehdään käyttäen **etäkäyttöympäristöä.**
käyttäjän identiteetti	Käyttäjän tunnistetiedot ja niihin liittyvä rooli, joka on **tunnistettavissa** ja **todennettavissa.**
käyttötilanne	Tilanne, jossa yksittäinen **etäkäyttö**tapaus tapahtuu. Siihen liittyy tietty paikka, käyttäjä ja **etäkäyttöratkaisu**.
palvelun verkkoliitäntä	Tekniset ja hallinnolliset järjestelyt, jotka määrittelevät ja toteuttavat sen, miten jokin **etäkäyttöpalvelu** on käyttäjien saatavilla ja käytettävissä.
pääsynvalvonta	Menettelyt, joilla käyttäjät **tunnistetaan** ja **todennetaan** sekä valvotaan että he pääsevät käyttämään vain palveluja, joihin heillä on käyttöoikeus.
päätelaite	Laite, jonka avulla käyttäjä käyttää **etäkäyttöpalvelua.**
päätteen verkkoliitäntä	Tekniikka, jolla etäkäyttäjän **päätelaite** kytketään **verkkoon.**

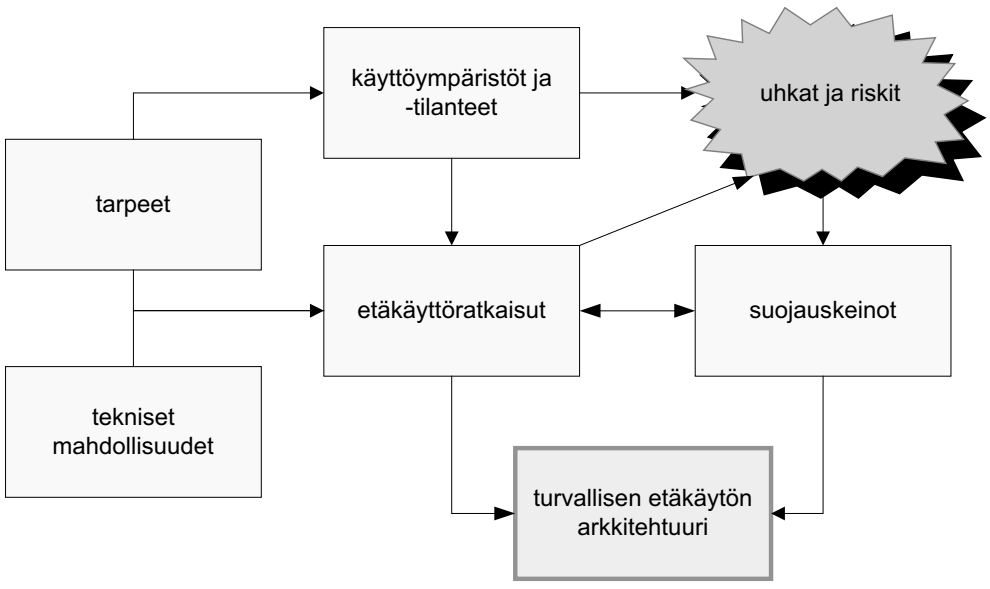
todennusmenetelmä	Menettely ja siihen mahdollisesti liittyvät välineet, joita käyttäen varmistaudutaan **käyttäjän identiteetistä**.
todennusväline	Väline, jota **todennusmenetelmä** edellyttää. Välineen oletetaan olevan käyttäjän hallussa ja joskus se edellyttää erityisvalmiuksia myös käyttäjän **päätelaitteelta**.
todentaminen	Varmistautuminen **käyttäjän identiteetistä.**
tunnistaminen	**Käyttäjän identiteetin** selvittäminen. Palvelujen käytössä useimmiten halutaan käyttäjän vahvaa tunnistamista jotain **todentamismenetelmää** käyttäen.
ulkoinen verkko	Verkko, jolla on liittymäpisteitä **viraston verkon** ulkopuolella
verkkoyhteys	Tietoliikennelaitteita ja -verkkoja sekä niiden palveluja hyödyntämällä toteutettu tiedonsiirtotie, joka **etäkäytössä** etäkäyttäjän ja palvelujärjestelmän, välisen kommunikoinnin.
viraston palvelujärjestelmä	**Viraston verkkoon** kytketty tietotekninen palvelujärjestelmä.
viraston verkko	Viraston toimitiloihin ja toimitilojen välille rakennettu suljettu verkko, johon viraston paikalliskäyttäjien **päätelaitteet** ja **viraston palvelujärjestelmät** on kytketty.

2 ETÄKÄYTTÖ JA SIIHEN VAIKUTTAVAT TEKIJÄT

2.1 Etäkäytön toteutukseen vaikuttavat tekijät

Tietojärjestelmien etäkäyttöön vaikuttavia tekijöitä on havainnollistettu *kuvassa 1*.

Kuva 1 Etäkäytön tarpeista ratkaisuihin

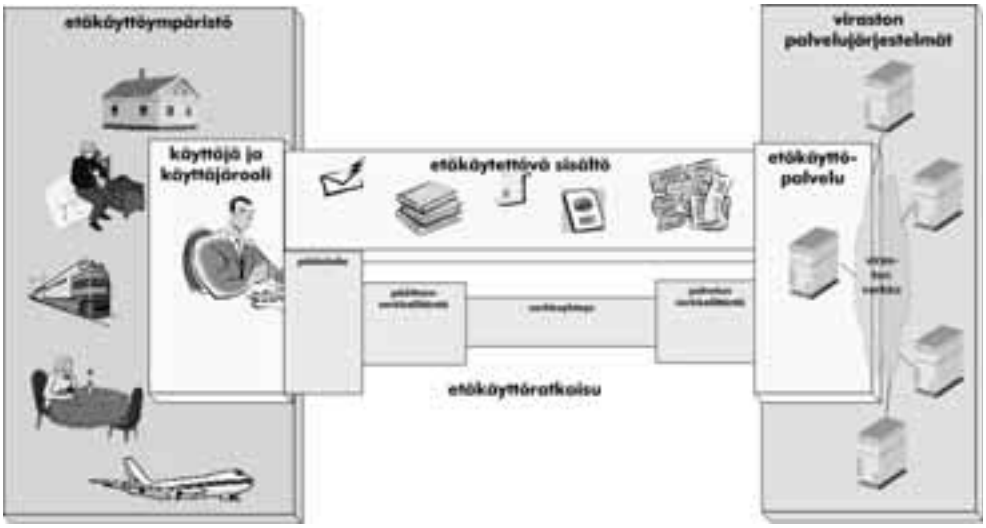


Lähtökohtana ovat organisaatioissa esiintyvät **tarpeet** organisaation tietojärjestelmien käyttöön myös muualta kuin työntekijän omasta työpisteestä ja muulloinkin kuin normaalina työaikana. Tarpeet määrittävät joukon **käyttöympäristöjä ja -tilanteita**, joissa etäkäyttömahdollisuus pitäisi olla tarjolla. Näistä voidaan johtaa – tekniikan tarjoamien mahdollisuuksien puitteissa – eri tilanteissa tarvittavat **etäkäytön tekniset ratkaisut**. Käyttöympäristöt ja -tilanteet toisaalta sanelevat millaisille tietoturvallisuuden **uhkille ja riskeille** etäkäyttäjä ja käytettävät järjestelmät altistuvat. Tarvitaan **suojauskeinoja**, jotka jossakin määrin ovat riippuvaisia käytössä olevasta etäkäyttöratkaisusta. Etäkäyttöratkaisujen ja niiden yhteydessä sovellettavien suojauskeinojen kokonaisuudesta syntyy **turvallisen etäkäytön arkkitehtuuri**, jonka määrittely on tämän hankkeen tavoitteena.

2.2 Etäkäytön toimintaympäristö

Kuva 2 esittää tietojärjestelmien etäkäytön toimintaympäristöä ja sen toiminnallisia komponentteja, jotka ovat lähtökohtana myöhempien lukujen tarkasteluille.

Kuva 2 Etäkäytön toimintaympäristö



Etäkäytön toimintaympäristö voidaan jakaa kahteen osaan: **teknisestä ratkaisusta riippumattomiin komponentteihin** ja teknisten ratkaisujen, **etäkäyttöratkaisujen komponentteihin**. Tässä keskitytään jälkimmäisiin unohtamatta kuitenkaan edellisiä, sillä turvallisen etäkäytön toteuttaminen ei ole pelkästään tekninen ongelma vaan myös toimintapolitiikkaa, ohjeita, valvontaa ja riskien hallintaa.

2.2.1 Etäkäytön teknisestä ratkaisusta riippumattomat komponentit

ETÄKÄYTTÖYMPÄRISTÖ

Etäkäyttöympäristö määräytyy paikasta ja tilanteesta, jossa etäkäyttöä harjoitetaan. Käyttö voi tapahtua etäkäyttäjän kotoa tai toisen organisaation sisäverkosta, matkoilla ollessa jostain julkisesta tilasta, hotellihuoneesta tai kulkuvälineestä kotimaassa tai ulkomailla. Ympäristö vaikuttaa siihen, minkälaista etäkäyttöratkaisua voidaan ja on tarkoituksenmukaista käyttää. Käyttöympäristön yksityisyys vaikuttaa siihen, mitä palveluja on järkevää käyttää tai olla käyttämättä. Tämän arviointi jää viime kädessä aina etäkäyttäjän harkittavaksi.

KÄYTTÄJÄT JA KÄYTTÄJÄROOLIT

Etäkäyttöpalvelujen käyttäjät ovat viraston omia tai yhteistyökumppanien työntekijöitä tai toisen organisaation tietojärjestelmiä. Asiakkaille tarjottavat palvelut on rajattu pois tässä tarkastelussa. Käyttäjä voi eri etäkäyttötilanteissa toimia eri rooleissa. Roolit voivat joissain tapauksissa olla samat kuin palvelujen paikallisessa käytössä. Käyttäjällä on identiteetti, joka todennetaan palveluun kytkeydyttäessä. Käyttäjän identiteetti määrää hänen roolinsa ja sitä kautta lopulta palvelut, joita hän voi käyttää ja etäkäytettävän sisällön, johon hän pääsee käsiksi.

ETÄKÄYTETTÄVÄ SISÄLTÖ

Etäkäytettävällä sisällöllä tarkoitetaan etäkäyttöpalveluun liittyviä tietoja ja aineistoja,

- joita syötetään palveluun / käsitellään palvelussa
- jotka ovat palvelun avulla tavalla tai toisella saatavilla
- joita tarvitaan muuten palvelua käytettäessä.

Sisältöjä on monentyyppisiä: rakenteista ja rakenteetonta dataa, dokumentteja ja multimediaa. Myös niiden luottamuksellisuus vaihtelee sovelluksesta toiseen. Etäkäytettävän sisällön turvaaminen on yksi turvallisen etäkäytön päätavoite. Turvaamisessa käytetään yksikön käyttämiä asiapapereiden turvaluokituksia.

ETÄKÄYTTÖPALVELU JA VIRASTON PALVELUJÄRJESTELMÄT

Etäkäyttöpalvelu on **viraston palvelujärjestelmässä** toteutettu sovellus, jonka etäkäyttö viraston sisäverkon ulkopuolelta on mahdollistettu. Mitkä tahansa sovellukset, joita viraston paikalliskäyttäjätkin käyttävät, voivat olla tarjolla myös etäkäyttäjille. Usein etäkäyttö rajataan vain osaan viraston järjestelmistä.

Teknisesti viraston palvelujärjestelmällä tarkoitetaan palvelinta tai palvelinryhmää, jossa ajetaan viraston työntekijöille, yhteistyökumppaneille tai asiakkaille tarkoitettuja sovelluspalveluja. Järjestelmät toimivat **viraston verkossa**, johon myös viraston paikalliset käyttäjät on kytketty. Viraston verkko on kokonaisuus, joka tavallisesti muodostuu useista fyysisistä verkkosegmenteistä sekä loogisista aliverkoista, joiden välillä voi olla eri tasoisia liikennöintirajoituksia.

2.2.2 Etäkäyttöratkaisujen komponentit

Etäkäyttöratkaisulla tarkoitetaan teknisiä järjestelyjä, jotka mahdollistavat tietojärjestelmäpalvelun etäkäytön. *Kuva 3* on tarkennettu kuva komponenteista. Etäkäyttöratkaisujen komponentit ovat **päätelaite**, joka tarjoaa etäkäyttöpalvelun käyttäjälle näkyvän käyttöliittymän, sekä **verkkoyhteys**, joka mahdollistaa päätelaitteen ja etäkäyttöpalvelun välisen kommunikoinnin. Verkkoyhteys useimmiten ainakin osittain kulkee riskialttiissa yleisissä verkoissa. Etäkäytön käyttömukavuuteen mutta myös turvallisuuteen vaikuttaa olennaisesti se, miten etäkäyttäjän päätelaite (**päätteen verkkoliitäntä**) ja etäkäyttöpalvelu (**palvelun verkkoliitäntä**) on kytketty. Etäkäyttöratkaisun kaikkiin komponentteihin liittyy turvauhkia, joiden torjunta on otettava huomioon ratkaisua rakennettaessa. Uhkilta suojautumista kuvataan *luvussa 4*.

PÄÄTELAITE

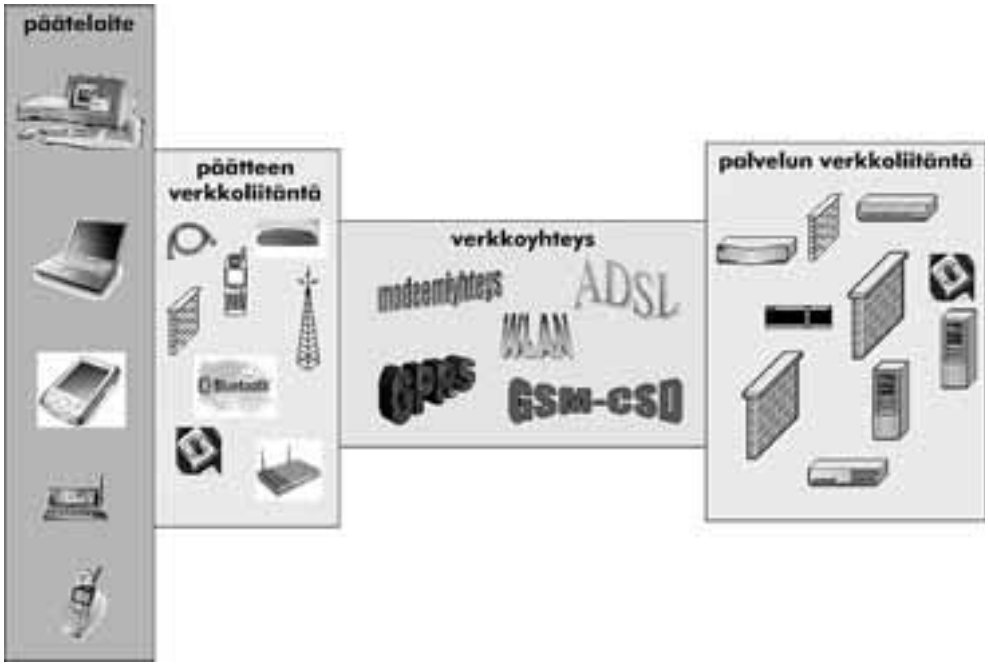
Päätelaitteen avulla käyttäjä käyttää etäkäyttöpalveluja. Käytännössä päätelaite voi olla lähes mitä tahansa yksinkertaisesta matkapuhelimesta kiinteään työasemaan tai itsenäiseen tietojärjestelmään. Viimemainitussa toisen organisaation tietojärjestelmä käyttää etäkäyttöpalvelua tarjoavan organisaation järjestelmää. Päätelaitteessa on useimmiten myös paikallisia sovellusohjelmia. Etäkäyttöön soveltuvien päätelaitteiden valikoima on koko ajan laajentumassa.

Matkapuhelimet

Matkapuhelinmallien lukumäärä kasvaa ja puhelinten käyttöominaisuudet monipuolistuvat jatkuvasti. Yksinkertaisimmissa laitteissa on hyvin rajoittuneet datakäyttöominaisuudet (tekstiviestit) sekä pieni näyttö, joka rajoittaa etäkäyttömahdollisuuksia. WAP on uusimmissa malleissa vakiovaruste ja yhä useammin myös GPRS. Kehittyneemmissä puhelimissa voi olla multimediaviestien (MMS) tuki, kalenteri ja mahdol-

lisuus sähköpostin käyttöön, näyttö voi olla isompi, ja laitteeseen voi ladata lisäsovelluksia. Kaapeli- ja infrapunaliitännän ohella Bluetooth on tulossa ammattikäyttöön tarkoitettujen matkapuhelimien vakiovarusteeksi.

Kuva 3 Etäkäyttöratkaisujen komponentit



Älypuhelimet ja PDA-laitteet

Älypuhelimilla ja PDA-laitteilla on etäkäytön näkökulmasta paljon samantyyppisiä ominaisuuksia. Peruserona näillä on se, että älypuhelimet ovat nimensä mukaisesti lähtökohtaisesti puhelimia, jotka tarjoavat lisäksi henkilökohtaisen ajanhallinnan, viestinnän ja viihdekäytön sovelluksia. PDA-laitteet taas ovat kehittyneet PC-maailman lähtökohdista tarjoten alun perin elektronisen kalenterin, osoitekirjan ja muistilehtiön. Vähitellen on lisätty viihde- ja kommunikointitoimintoja.

Rajanveto näiden laiteluokkien välillä on päivä päivältä hankalampaa – ja tarpeettomampaa. Älypuhelimissa ja PDA-laitteissa on monipuolisempien toimintojen lisäksi isommat näytöt ja kehittyneemmät tietojen syöttömahdollisuudet kuin matkapuhelimissa. Uusimmissa PDA-laitteissa on usein WLAN- ja Bluetooth-liitännät vakiovarusteena, älypuhelimissa Bluetooth.

Henkilökohtaiset taulutietokoneet

Nämä ovat pelkistettyjä kannettavia henkilökohtaisia tietokoneita, joiden kanssa käyttäjä kommunikoi samaan tapaan kuin PDA-laitteilla. Laitteissa on kehittyneet multimediaominaisuudet ja verkko-ominaisuudet kuten kannettavilla tietokoneillakin. Yhtenä erityispiirteenä näissä näyttäisi olevan varautuminen langattomaan käyttöön (WLAN ja/tai Bluetooth).

Kannettavat tietokoneet ja pöytäkoneet

Nämä ovat täysiverisiä henkilökohtaisia tietokoneita, jotka pystyvät kommunikoimaan tietoverkkopalvelujen kanssa kiinteän verkkoliittymän, modeemin tai langattoman yhteyden avulla, tai käyttäen hyväksi matkapuhelinta, johon laite kytketään kaapeli-, infrapuna- tai Bluetooth-yhteydellä. Yhä useammin käytetään kannettavia tietokoneita pöytäkoneen sijasta myös kiinteissä työpisteissä sijoitettuna telakkaan, johon on kytketty täyskokoinen näyttö ja näppäimistö, kiinteä verkkoliittymä sekä muut mahdolliset paikalliset oheislaitteet. Telakoituna kannettava on kuin pöytäkone ja esimerkiksi automaattisen ylläpidon piirissä.

PÄÄTTEEN VERKKOLIITÄNTÄ

Päätteen verkkoliitännällä tarkoitetaan tekniikkaa, jolla etäkäyttäjän päätelaite kytketään verkkoon. Verkkoliitännän toteutustekniikkaan vaikuttavat käytetyn verkkoyhteyden ja päätelaitteen tyyppi, etäkäyttöympäristö sekä halutut ominaisuudet.

Verkkoliitännän toteuttamisessa langattomien liitäntätekniikoiden (WLAN ja Bluetooth) käyttö on vahvasti lisääntymässä sekä toimisto- että matkakäytössä. Langattoman verkkoliitännän etuna on kannettavien tietokoneiden ja muiden helposti liikuteltavien päätelaitteiden käyttäjien vapaa liikkuvuus langattoman lähiverkon toiminta-alueella sekä pääsy eroon hankalista kaapeleista. Myös matkakäyttäjille Bluetooth-yhteyden avulla matkapuhelimen kautta kommunikoiva kevyt päätelaite tarjoaa entistä parempaa käyttömukavuutta ja käytön joustavuutta. Langattomien liitäntätekniikoiden kääntöpuolena ovat suuremmat tietoturvariskit sekä itse liitäntätekniikasta että sen mahdollistamasta etäkäytöstä lähes mistä ja milloin vain. Käyttäjälle voi tulla houkutus etäkäyttöön paikoissa ja tilanteissa, joissa luottamuksellista tietoa saattaa vuotaa ulkopuolisille.

Kuvassa 4 on esimerkki kahdesta jatkossa yleisestä tavasta hyödyntää langatonta verkkoliitäntätekniikkaa:

- Kytketään PDA tai muu päätelaite Bluetoothilla matkapuhelimeen ja sen avulla edelleen Internetiin (ja viraston palveluihin)
- Kytketään päätelaite WLANin välityksellä viraston sisäverkkoon tai esim. matkalla ollessa Internetiin jonkin WLAN-operaattorin välityksellä.

Kuva 4 Esimerkkejä langattoman verkkoliitännän käytöstä

VERKKOYHTEYS

Verkkoyhteydellä tarkoitetaan tässä tietoliikennelaitteita ja –verkkoja sekä niillä toteutettua tiedonsiirtotietä, joka mahdollistaa etäkäyttäjän päätelaitteen ja etäkäytettävän sovelluksen välisen kommunikoinnin. Verkkoyhteys voi olla kiinteä- tai valintayhteys. Se voi olla kokonaan yhtä verkkotekniikkaa tai se voi kulkea usean yhdysliikenneverkon kautta (vrt. *kuva 5*). Verkot voivat olla avoimia kuten yleinen puhelinverkko, matkapuhelinverkko ja Internet tai suljettuja, tietylle käyttäjäryhmälle yksinomaan varattuja.

Yhteystyypeillä on erilaisia ominaisuuksia kuten tiedonsiirtonopeus, luotettavuus, käyttömukavuus, kustannukset ja alttius tietoturvauhkille.

Kiinteät yhteydet

Kahden pisteen välille voidaan muodostaa monia eri tekniikoita käyttäen suljettu, kiinteä, aina käytettävissä oleva fyysinen tai virtuaaliyhteys. Mahdollisia tekniikoita ovat esimerkiksi erillinen kupari- tai valokaapeliyhteys, DSL, ATM, Frame Relay, ja MPLS. Toteutustekniikkojen määrä lisääntyy jatkuvasti. Yhteys rakennetaan jonkin teleoperaattorin palveluna.

Kiinteä suljettu yhteys on erittäin luotettava ja turvallinen sekä käyttäjän kannalta mukava tapa toteuttaa verkkoyhteyksiä. Sen varjopuolia ovat korkea hinta sekä soveltumattomuus liikkuvaan ja satunnaiskäyttöön.

Valintayhteydet

Valintayhteydet ovat yleisten televerkkojen datayhteyksiä. Ne soveltuvat hyvin satunnaiseen ja liikkuvaan käyttöön. Koska valintayhteydet toteutetaan avoimissa verkoissa, niihin liittyy kiinteitä yhteyksiä suurempia turvariskejä. Ominaisuudet vaihtelevat yhteystyypeittäin.

- **Piirikytkentäinen datayhteys yleisessä puhelinverkossa**
  Perinteinen tietoliikenneratkaisu, joka on suhteellisen luotettavasti käytettävissä missä tahansa. Tarvittava modeemi voi olla päätelaitteeseen sisäänrakennettu. Käyttömukavuutta alentaa pitkä kytkentäviive. Käyttökustannukset riippuvat käytetystä yhteysajasta ja etäkäyttäjän sijainnista. Etäkäytössä voi muodostaa yhteyden viraston omaan soittosarjaan. Nykyään käytetään useimmiten Internet-palveluntarjoajaa. Yhteyden siirtokapasiteetti muutamia kymmeniä kbit/s. Sopii parhaiten lyhytkestoiseen satunnaiskäyttöön.
- **ISDN-yhteys yleisessä televerkossa**
  Piirikytkentäinen datasiirtotekniikka, joka tarjoaa laadukkaan siirtotien, nopeammat kytkentäajat ja suuremman kapasiteetin kuin perinteinen modeemiyhteys. Käytetään lähinnä kiinteiden yhteyksien korvaajana. Poistuva teknologia. Ei sovellu matkakäyttöön.
- **Piirikytkentäinen datayhteys matkapuhelinverkossa (CSD)**
  Vastaa ominaisuuksiltaan lähinnä puhelinverkon modeemiyhteyttä, paitsi että siirtokapasiteetti on vain 9.6 kbit/s ja yhteys voi olla tukiasemien reuna-alueilla tai liikkuvan käyttäjän tapauksessa epäluotettava. Käyttökustannukset ovat korkeammat kuin puhelinverkon modeemiyhteyksillä. Käyttäjä ei ole sidottu televerkon kiinteisiin liityntäpisteisiin.
- **Nopea piirikytkentäinen datayhteys matkapuhelinverkossa (HSCD)**
  Kuten edellinen, mutta maksimisiirtonopeus jopa 43.5 kbit/s. Kaikki matkapuhelinoperaattorit eivät tarjoa tätä palvelua.
- **GPRS-datayhteys matkapuhelinverkossa**
  Pakettivälitteinen yhteys, joka voidaan pitää jatkuvasti päällä ja joka tarjoaa pääsyn suoraan teleoperaattorin verkosta myös Internet-palveluihin. Kaikki verkot eivät vielä tue GPRS-verkkovierailua. Maksimisiirtonopeus teoriassa yli 100 kbit/s, käytännössä joitain kymmeniä kbit/s. Käyttökustannukset riippuvat siirretystä tietomäärästä. Piirikytkentäisten yhteyksien käyttömukavuutta alentavat kytkentäviiveet puuttuvat. Yhteyksien laadussa ja todellisessa siirtokapasiteetissa on toistaiseksi melkoisesti vaihtelua.
- **3G- (UMTS-) matkapuhelinverkkojen datayhteydet**
  Verkot ja sitä hyväksikäyttävät laitteet ovat vasta tulossa. Teoriassa megabittejä sekunnissa luokkaa oleva maksimikapasiteetti, mikä mahdollis-

taisi yhä laajemman Internet-palvelujen käytön. Käyttökustannukset tullevat riippumaan siirretyn datan määrästä.

- **Tekstiviesti matkapuhelinverkossa**
  Kaikkien GSM-verkkojen ominaisuus. Viestien välitys ei aina toimi kaikissa maissa. Käyttökelpoisuutta rajoittaa erittäin pieni siirtokapasiteetti, rajoittuminen tekstimuotoiseen tietoon sekä puutteet palvelun laadussa ja tietoturvassa. Rajoituksista huolimatta mahdollistaa alkeellisen, mutta joissain tilanteissa tarkoituksenmukaisen etäkäytön perusmatkapuhelimilla. Käytöstä veloitetaan per viesti.

Langalliset ja langattomat lähiverkkoyhteydet

Virastoilla ja muilla organisaatioilla on oma lähiverkkonsa, johon organisaation työntekijöiden työasemat ja palvelujärjestelmät on kytketty. Yhä lisääntyvässä määrin lähiverkkoja on syntynyt myös koteihin sekä julkisiin tiloihin kuten hotelleihin, konferenssikeskuksiin tai lentoasemille. Viimemainitut on tarkoitettu vieraiden ja asiakkaiden käyttöön. Kaapelointiin perustuvien ”lankalähiverkkojen” rinnalla ovat hyvää vauhtia yleistymässä langattomat lähiverkot, WLANit, sekä langattomat Bluetooth-yhteydet.

WLAN-verkkojen siirtokapasiteetti on toistaiseksi huonompi kuin lankalähiverkkojen. Ne ovat turvattomampia kuin edellä kuvatut tekniikat. Käyttömukavuudeltaan WLAN-yhteys on hyvä, koska langattomana tekniikkana se ei sido käyttäjää kiinteään käyttöpisteeseen. Yleisten WLAN-palvelujen tuleva laajuus, käyttötavat ja –kustannukset ovat toistaiseksi vielä epäselviä.

Internet-yhteydet

Etäkäyttöyhteydet on usein tarkoituksenmukaista reitittää Internetin avulla. Internetyhteydellä tarkoitetaan tässä Internet-verkon kautta kulkevaa verkkoyhteyden osuutta. Etäkäyttäjä liittyy Internetiin jotain yllä kuvattua tekniikkaa käyttäen. Internet-runkoverkko ei periaatteessa rajoita siirtokapasiteettia, mutta käytännössä verkon ruuhkaisuus voi alentaa nopeutta hitaammaksi kuin mitä etäkäyttäjän ja etäkäyttöpalvelun liittymät sallisivat. Internet-käytön kustannukset ovat yleensä Internet-liittymän kapasiteetista riippuva kiinteä summa per kuukausi. Valtion tietohallinnon internet-tietoturvallisuusohjeessa (Vahti 1/2003) on laajemmin käsitelty internetin tietoturvaan liittyviä kysymyksiä.

ETÄKÄYTTÄJÄN VERKKOYHTEYDEN TOTEUTTAMINEN

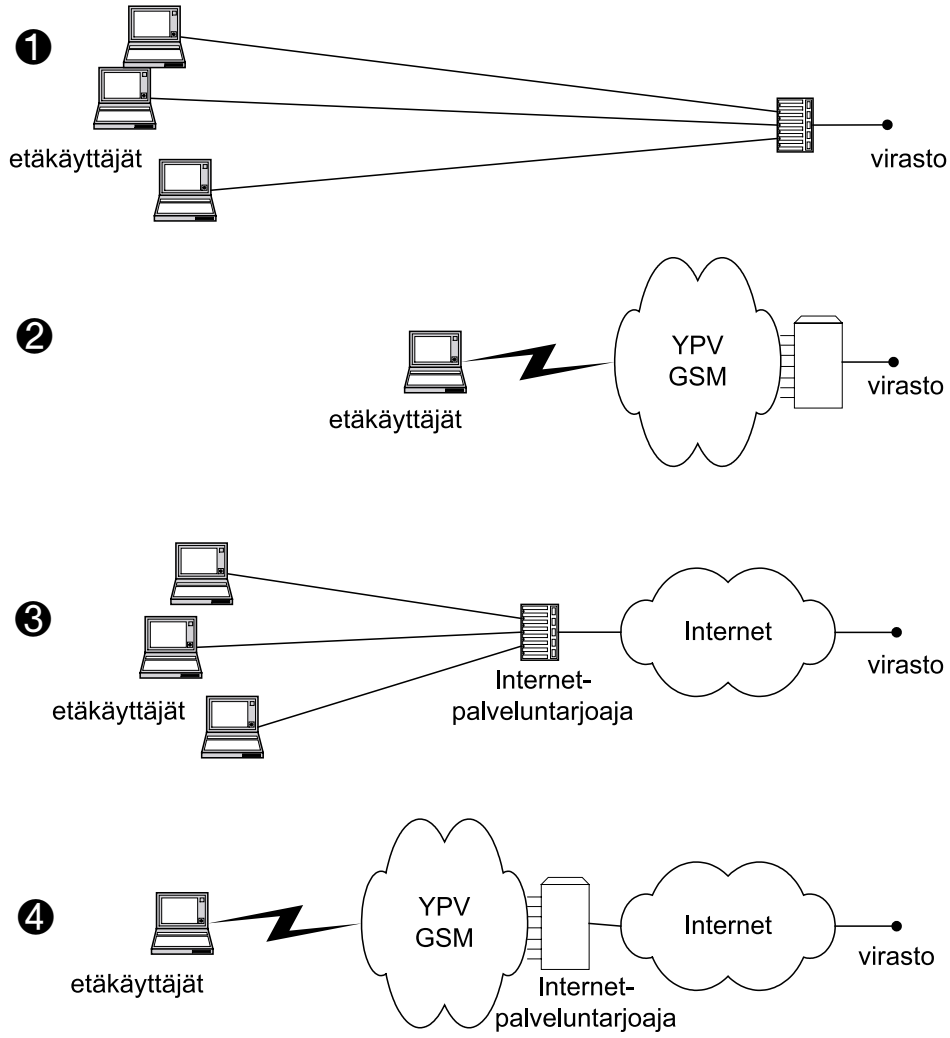
Etäkäyttäjän verkkoyhteys viraston palvelun verkkoliitäntään voidaan toteuttaa jollain *kuvan 5* osoittamista tavoista.

Tapa 1 esittää tilannetta, jossa etäkäyttäjä on kytketty virastoon **kiinteällä yhteydel-**

lä, joka voi olla tarkoitukseen varattu fyysinen yhteys tai virtuaaliyhteys. Yhteys voidaan toteuttaa usein vaihtoehtoisin tekniikoin. Yhteyden siirtokapasiteetti voi olla mitä tahansa käytetyn tekniikan puitteissa.

Tapa 2 esittää tilannetta, jossa virastolla on palvelujärjestelmiensä yhteydessä **oma soittosarja**, johon etäkäyttäjät voivat kytkeytyä yleisen puhelinverkon tai matkapuhelinverkon välityksellä. Etäkäyttäjän verkkotekniikkana voi olla modeemi- tai ISDN-yhteys puhelinverkossa tai matkapuhelinverkon datayhteys.

Kuva 5 Erilaiset tavat toteuttaa etäkäyttäjän verkkoyhteys



Tavat 3 ja 4 esittävät tilannetta, jossa etäkäyttäjien pääsy viraston järjestelmiin on toteutettu **Internetin kautta**. Virastolla on Internetiin riittävän suurikapasiteettinen yhteys, jonka kautta etäkäyttöliikenne ja myös viraston muu Internet-liikenne hoidetaan. Etäkäyttäjät ovat yhteydessä Internetiin kukin omalla tilaajayhteydellään. Tapauksessa 3 etäkäyttäjällä on Internetiin **kiinteä yhteys**. Tapaus 4 ja 2 ovat toisiaan vastaavia. Tapauksessa 4 yhteydenotto tapahtuu viraston oman soittosarjan sijasta **Internet-palveluntarjoajan soittosarjaan**, josta yhteys reititetään edelleen viraston Internet-liittymään.

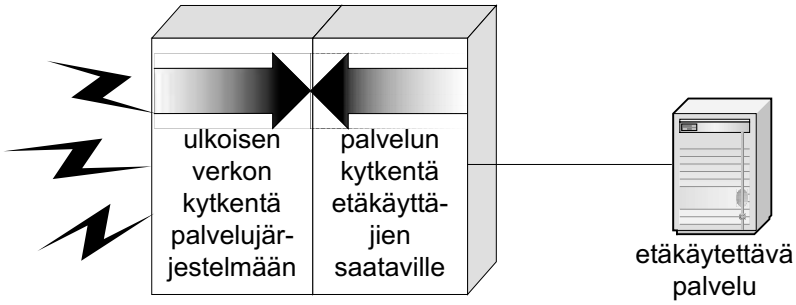
Suuntauksena etäkäyttöyhteyksien toteuttamisessa on nojautua Internet-ratkaisuihin (tavat 3 ja 4). Tähän houkuttavat sekä kustannussyyt että yhteyksien hallinnoinnin ulkoistaminen Internet-palveluntarjoajalle. Uusimmat toteutustekniikat kuten MPLS mahdollistavat myös entistä edullisemmat kiinteät yhteydet. Kääntöpuolena ovat huomattavasti suuremmat tietoturvauhkat.

PALVELUN VERKKOLIITÄNTÄ

Palvelun verkkoliitännällä tarkoitetaan teknisiä ja hallinnollisia järjestelyjä, jotka määrittelevät ja toteuttavat miten sovelluspalvelu on etäkäyttäjien saatavilla ja käytettävissä. Palvelu voi olla nimenomaan etäkäyttöön suunniteltu tai myös paikallisesti käytettävä. Verkkoliitäntä voi rajoittaa etäkäytön vain sovelluksen joihinkin toimintoihin tai tietylle käyttäjäryhmälle. Käyttöön voi liittyä muitakin rajoituksia.

Palvelun verkkoliitäntää voidaan tarkastella kahdesta suunnasta: ratkaisuna, jolla ulkoiset verkkoyhteydet kytketään viraston palvelujärjestelmään sekä ratkaisuna, jolla viraston etäkäyttöiset palvelut kytketään etäkäyttäjien saataville eli ulkoisesta verkosta tavoitettaviksi (*kuva 6*).

Kuva 6 Palvelun verkkoliitännän perustoiminnot



Kuten *kuvassa 5* esitettiin, etäkäyttäjien liittäminen viraston palvelujärjestelmään voidaan toteuttaa:

1. Yksinomaan viraston käytössä olevilla kiinteillä yhteyksillä tai valintayhteyksillä viraston omaan soittosarjaan.
2. Internetin kautta, josta on yhteys viraston palvelujärjestelmiin.

Kuvan 6 osion **ulkoisen verkon kytkentä palvelujärjestelmään** toteutus riippuu siitä kumpaa liitäntätapaa käytetään. On myös mahdollista käyttää molempia. Internet-pohjaisen liitännän toteutus vaatii vankemman varustautumisen verkkouhkien torjuntaan. Ulkoisen verkon kytkennässä käytettäviä tekniikoita ovat mm.

- reitittimet, verkkokeskittimet ja -kytkimet
- soittosarjat
- erilaiset tietoliikenneprosessorit, esim. yhteyden salauksen hoitamiseen
- palomuurit
- erilaiset suojausohjelmistot verkkoliitännässä.

Edellä kuvattu toiminnallisuus mahdollistaa etäkäyttäjien pääsyn viraston palvelujärjestelmien eteiseen. **Palvelun kytkentä etäkäyttäjien saataville** -toiminnallisuuden tehtävä on pitää huolta siitä, että vain asianmukaisilla oikeuksilla etäkäyttäjät pääsevät käsiksi viraston palveluihin. Tämä tarkoittaa ennen kaikkea käyttäjien tunnistamista ja todentamista sekä sovelluksiin pääsyn valvontaa. Lisäksi erilaisia tekniikoita soveltaen pyritään sisäverkossa olevat palvelut eristämään mahdollisimman hyvin ulkomaailmasta. Palvelun kytkennässä käytettäviä tekniikoita ovat esimerkiksi:

- liikenteen suodattimet, esim. palomuurit
- erilliset verkkosegmentit
- välitys- ja edustapalvelimet, jotka hoitavat palvelun käyttöliittymän ja välittävät palvelupyynnöt ja niiden vastaukset etäkäyttäjän ja varsinaisen järjestelmän välillä
- turvapalvelimet, jotka huolehtivat käyttäjien todentamisesta, pääsynvalvonnasta ja käyttötietojen lokikirjanpidosta.

3 ETÄKÄYTTÖTARPEET

3.1 Yleistä

Etäkäytön tarpeet ovat moninaiset ja vaihtelevat. Asia selvisi tämän työn tueksi tehdyssä pienessä selvityksessä. Tarpeellisimmiksi etäkäyttösovelluksiksi ovat osoittautuneet **sähköposti ja kalenteri**, joihin halutaan päästä käsiksi tilanteessa kuin tilanteessa. Intranet-sovelluksiin pääsyä ei nähdä aivan yhtä tarpeelliseksi ehkä osittain siksi, että intranet-palvelujen sisältö ja laajuus vaihtelee. Muiden sovellusten käyttötarpeet rajautuvat jo selvästi pienempään joukkoon.

Etäkäytössä tärkeimpänä **päätelaitteena** näyttäisiin pidettävän **(kannettavaa) tietokonetta**, vaikka sellaista ei työn puolesta kaikissa virastoissa ole kovin yleisesti tarjota työtekijöiden käyttöön. Kommunikaattorien ja PDA-laitteiden sekä matkapuhelimien pääasiallisena käyttökohteena nähdään yhteys sähköpostiin ja jonkin verran vähemmässä määrin kalenteriin. Matkapuhelimien käyttökelpoisuuteen etäkäytössä ei uskota yhtä paljon kuin paremman käyttöliittymän tarjoaviin kommunikaattoreihin/ PDA-laitteisiin.

Kotikäyttö ja matkakäyttö nähdään satunnaiskäytössä tarpeiltaan yhteneväisinä. Toisaalta henkilöillä, jotka säännöllisesti tekevät etätyötä, on laajemmat tarpeet kuin satunnaiskäyttäjillä. Tarvetta etäkäyttöön toisen organisaation verkosta on jonkin verran.

Kotikäyttäjien etäkäyttöyhteyksissä näkyy selvästi yleinen suuntaus siirtyä valintayhteyksistä **kiinteisiin laajakaistayhteyksiin**, erityisesti DSL-tekniikkaan. ISDN-liittymien arvioidaan käytännöllisesti katsoen katoavan käytöstä vuoteen 2005 mennessä. Valintayhteyksien rooli säilyy vahvana matkakäytössä, suuntauksena on kuitenkin siirtyä yleisestä puhelinverkosta **matkapuhelinverkon yhteyksiin**, joiden siirtokapasiteetti nykyään riittää tyydyttävästi sähköpostikäyttöön.

WLAN-käytön virastojen toimitiloissa nähtiin olevan vahvasti kasvussa. Valmiudet toistaiseksi ovat vielä melko vähäiset. Langaton lähiverkko mahdollistaa käyttäjän vapaan liikkuvuuden rajoitetulla alueella esimerikiksi virastokiinteistössä tai kampusalueella. Tätä ei voi pitää varsinaisena etäkäyttönä, mutta siihen liittyy samoja uhkia kuin ”oikeaan” etäkäyttöön.

Olemassa olevien ja potentiaalisten tarpeiden perusteella on hahmoteltu **perusetäkäyttötilanteet**, jotka eri etäkäyttöympäristöihin sovellettuna kattavat etäkäyttötarpeet.

3.2 Käyttötilanteet

Etäkäyttötilanteet on luokiteltu seuraavasti:

- käytön säännöllisyys/satunnaisuus
- etäkäyttöpaikka (tietty kiinteä tai vaihteleva piste)
- käytetyn päätelaitteen hallinta (viraston laite tai ei)
- etäkäyttäjä (viraston oma tai kumppaniorganisaation työntekijä).

Nämä luokitteluperusteet on valittu siksi, että ne yhtäältä vaikuttavat siihen millaiset etäkäyttöratkaisut ovat mahdollisia kussakin tilanteessa, ja toisaalta millaisia uhkia ja riskejä niihin liittyy. Tarkastelemalla kaikkia periaatteessa mahdollisia vaihtoehtoja (ks. *taulukko 1*) päädytään seuraaviin neljään käytännössä esiintyvään peruskäyttötilanteisiin:

Etäkäyttäjänä viraston oma työntekijä

1. Säännöllinen käyttö viraston päätelaitteella kiinteästä pisteestä
2. Tilapäiskäyttö viraston päätelaitteella vaihtelevista pisteistä
3. Käyttö muulla kuin viraston päätelaitteella

Etäkäyttäjänä kumppaniorganisaation työntekijä

4. Kumppanikäyttö

Taulukko 1 Etäkäyttötilanteet

	säännöllinen käyttö (kotoa, komennuspaikalta,....)			tilapäiskäyttö (mistä hyvänsä)	
	kiinteällä yhteydellä	valinta-yhteydellä	kumpp.org. verkosta	kumpp.org. verkosta	valintayhteydellä verkosta X
viraston työntekijä viraston päätelaitteella	**OK**	**OK**	**OK**	**OK**	**OK**
viraston työntekijä omalla päätelaitteella	**rajoitetusti**	**rajoitetusti**			**rajoitetusti**
viraston työntekijä kumpp.org. päätelaitteella					**rajoitetusti**
viraston työntekijä kumpp.org. päätelaitteella			**rajoitetusti**	**rajoitetusti**	
kumppaniorganisaation työntekijä kumpp.org. päätelaitteella			**kumppanikäyttö**		

Viimeisenä mainittu käyttötilanne eli kumppanikäyttö on rajatapaus, sillä usein kumppaniorganisaatioille tarjottavat palvelut ovat erityisiä ekstranet-sovelluksia, jotka ovat rinnastettavissa pikemmin asiakaspalvelusovelluksiin kuin sisäisiin palveluihin. Kuitenkin on myös tapauksia, joissa kumppanien työntekijöille halutaan antaa pääsy joihinkin samoihin resursseihin kuin viraston omille työntekijöille, ja sitä edustaa tässä kumppanikäyttö. Näissä keskeistä on huolehtia hallinnollisista järjestelyistä ja sopimuksista.

Seuraavassa kuvataan peruskäyttötilanteet lähtien tyypillisimmistä tarpeista ja ratkaisuista. Kuvaukset eivät pyri kertomaan miten asiat kaikenkattavasti ovat, tai suositella miten käyttötilanteiden etäkäyttö tulisi ratkaista, vaan niiden tarkoitus on konkretisoida peruskäyttötilanteita.

3.2.1 Säännöllinen käyttö viraston päätelaitteella kiinteästä pisteestä (etätyö)

Käyttötilanteen kuvaus

Käyttö on luonteeltaan etätyötä, jota työntekijä tekee jatkuvasti tai lähes päivittäin kotonaan tai tilapäisessä viraston ulkopuolisessa työpisteessä. Tähän voidaan lukea myös käyttö, jota sovellusten tai järjestelmien ylläpitäjät tekevät päivystysluonteisesti tarvittaessa.

Tähän käyttötilanteeseen liittyvät laajimmat etäkäyttötarpeet. Palvelut, joita etätyöntekijä käyttää, ovat ääritapauksessa samat kuin viraston paikalliskäyttäjilläkin, mutta peruspalveluiksi voidaan katsoa:

- sähköposti ja kalenteri, myös liitetiedostojen vastaanotto ja lähetys
- toimistosovellukset eli mahdollisuus käsitellä tekstinkäsittely-, taulukkolaskenta- jne. ohjelmilla samoja dokumenttitiedostoja kuin paikalliskäytössäkin
- intranet-palveluista (virastokohtaisia) ainakin infoluonteiset palvelut kuten puhelinluettelot ja viraston sisäiset uutispalvelut
- pääsy Internetiin viraston politiikan mukaisessa laajuudessa.

Luonteenomaista tälle käyttötilanteelle on hyvät mahdollisuudet toteuttaa se kaikilta osin kontrolloidusti ja minimoiden riskit lähes samalle tasolle kuin paikalliskäyttäjillä.

Etätyöntekijän etäkäyttöratkaisut

Päätelaitteena käytetään pöytäkonetta tai kannettavaa tietokonetta. Verkkoyhteys on yleensä viraston työntekijälle järjestämä ja on useimmiten kiinteä liittymä Internetin kautta.

Toimistosovellusten ja intranet-palvelujen käyttö saattaa edellyttää käytännössä kirjautumista viraston paikalliseen verkkoalueeseen käyttäjän normaaleilla paikallisilla verkkotunnuksilla. Mahdollista on kuitenkin myös, että käyttöä kontrolloidaan hienojakoisemmin edellyttämällä kuhunkin sovellukseen kirjautumista erikseen, tai tarjoamalla palveluja esimerkiksi Windows-päätepalvelinratkaisulla tai erityisen viraston etäkäyttöportaalin kautta.

3.2.2 Tilapäiskäyttö viraston päätelaitteella vaihtelevista pisteistä

Käyttötilanteen kuvaus

Käyttäjät ovat viraston työntekijöitä, joilla on satunnaisesti, esimerkiksi matkoilla, koulutuksessa, konferensseissa tai muuten työpaikan ulkopuolella ollessaan tarve käyttää viraston järjestelmiä. Käyttöympäristönä voi olla lähes mitä tahansa hyvän yksityisyyden tarjoavista tiloista julkisiin paikkoihin.

Päätelaitteena on tässä tapauksessa jokin mukana kuljetettava laite: kannettava tietokone, PDA-laite, kommunikaattori, älypuhelin tai tavallinen matkapuhelin. Verk-

koyhteytenä on joko valintayhteys (matka)puhelinverkossa tai Internet-yhteys jonkin julkisen tai kaupallisen palveluntarjoajan kautta. Satunnaiskäyttäjän käyttötarpeet ovat rajatummat kuin etätyöntekijällä. Usein pääsy sähköpostiin ja kalenteriin riittää.

Tämän käyttötilanteen kontrollointimahdollisuudet ovat melko huonot. Kontrolloida voidaan kohtalaisen hyvin etäkäytön teknistä toteutusta ja palveluvalikoimaa. Vaihteleviin etäkäyttöympäristöihin ja päätelaitteeseen liittyvien riskien hallinta jää hyvin pitkälti käyttäjän vastuulle. Esimerkkejä riskeistä ovat laitteen joutuminen vääriin käsiin tai tuhoutuminen sekä päätteen käyttö tilanteissa, joissa luottamuksellista tietoa voi paljastua sivullisille.

Viraston päätelaitteella tapahtuvan tilapäiskäytön etäkäyttöratkaisut

Tilapäiskäyttäjänkin päätelaitteen suositellaan olevan viraston omistama ja kontrolloima. Verkkoyhteys muodostetaan tarpeen mukaan. Verkkoyhteys voi olla modeemin avulla muodostettava valintayhteys puhelinverkossa tai CSD/GPRS-modeemin avulla muodostettava yhteys matkapuhelinverkossa. Matkapuhelinverkon yhteys voidaan muodostaa myös käyttäen matkapuhelinta, johon päätelaite kytketään kaapelilla, infrapunalinkillä tai yhä useammin Bluetooth-yhteydellä. Joissain tapauksissa päätelaite voidaan kytkeä paikalliseen fyysiseen tai langattomaan lähiverkkoon, jonka kautta on pääsy Internetiin ja sieltä viraston palveluihin.

Viraston päätelaitetta käyttäville tilapäiskäyttäjille tarjotaan minimissään pääsy viraston sähköposti- ja kalenterisovelluksiin. Tarjota voidaan myös jotkut tai kaikki edellisessä tapauksessa luetelluista peruspalveluista. Riittävän turvallista etäkäyttöratkaisua käytettäessä etäkäyttäjän voidaan sallia viraston päätelaitteella kirjautua viraston paikalliseen verkkoon.

3.2.3 Tilapäiskäyttö muulla kuin viraston päätelaitteella

Käyttötilanteen kuvaus

Työntekijöillä on tarve käyttää viraston järjestelmiä, mutta heillä ei ole käytettävissään viraston päätelaitetta. Tähän ryhmään voi käytännössä kuulua sekä sellaisia joilla on säännölliset ja laajahkot etäkäyttötarpeet että satunnaiskäyttäjiä. Edellisten käyttöympäristönä on useimmiten koti tai kumppaniorganisaatio. Jälkimmäisillä se voi olla esimerkiksi Internet-kioski.

Säännöllisten käyttäjien päätelaitteena on tyypillisesti käyttäjän kotitietokone tai oma kannettava tietokone. Moni näistä käyttää verkkoyhteytenä myös itse hankkimaansa laajakaistaliittymää Internetiin.

Oman päätelaitteen sijasta tai ohella voidaan käyttää myös yleisiä päätelaitteita esim. Internet-kioskeja. Tällöin päätelaitteena on tyypillisesti pöytäkone tai erityinen kioskipääte, joka on kytketty Internetiin.

Etäkäytön salliminen muulla kuin viraston hallinnoimalla päätelaitteella kasvattaa etäkäytön tietoturvariskejä kertaluokalla. Tavoitetilassa säännöllistä käyttöä omalla koneella ja yhteydellä ei pitäisi lainkaan sallia, mutta nykyisin se on todellisuutta esimerkiksi yliopistoissa, joissa monet työntekijät tekevät säännöllistä etätyötä. Heille ei kuitenkaan voida kustantaa viraston päätelaitetta eikä verkkoyhteyttä. Parhaiten kontrolloitavissa käyttötapauksista on luotetun kumppaniorganisaation sisäverkon päätelaitteelta tapahtuva käyttö.

Muulla kuin viraston päätelaitteella tapahtuvan tilapäiskäytön ratkaisut

Tilapäisluonteisen etäkäytön ratkaisut ovat teknisesti periaatteessa samantyyppisiä riippumatta siitä, kenen hallinnoimalla päätelaitteella etäkäyttöä harrastetaan. Ratkaisussa ei voida nojata laitteen erityisominaisuuksiin. Verkkoyhteys muodostetaan yleensä tarpeen mukaan ja voi olla mikä tahansa tarjolla olevista ratkaisuista.

Tilapäiskäyttäjille tarjotaan minimissään pääsy viraston sähköpostiin ja kalenteriin. Tarjota voidaan myös jotkut tai kaikki muut edellä luetelluista peruspalveluista. Mitä vähemmän virastolla on kontrollia käytettyyn päätelaitteeseen ja käyttöympäristöön, sitä pidättyväisempi on syytä olla palvelujen tarjonnassa. Jos viraston etäkäyttöratkaisulle määrittelemät perusedellytykset eivät täyty, käyttöä ei sallita.

3.2.4 Kumppanikäyttö

Käyttötilanteen kuvaus

Joitakin viraston palveluja tai resursseja saatetaan tarjota etäkäyttönä myös toisten organisaatioiden työntekijöille. Kumppanikäyttö tapahtuu tavallisesti pöytäkoneella käyttäjän omasta työpisteestä, jolloin yhteys viraston verkkoon on käytännössä yhtä kuin kumppaniorganisaation ja viraston paikallisten verkkojen osittainen yhdistäminen. Lähiverkot on kytketty joko yksityisellä yhteydellä tai Internetin kautta.

Kumppanikäyttö voidaan luotetun kumppaniorganisaation, johon on olemassa turvatut yhteysjärjestelyt, tapauksessa rinnastaa hyvin kontrolloituun säännölliseen käyttöön viraston päätelaitteella, mutta joskus taas se voi rinnastua lähes kontrolloimattomissa olevaan käyttöön muulla kuin viraston päätelaitteella.

Kumppanikäytön ratkaisut

Käyttäjän päätelaitteena on pöytä- tai kannettava tietokone, joka on kiinteästi kytketty lähiverkkoon. Viraston palveluihin etäkäyttäjä pääsee joko kumppaniorganisaation ja viraston välistä yleisistä verkoista eristettyä yhteyttä käyttäen tai Internetin kautta.

Kumppanikäyttäjän palvelut riippuvat tapauksesta ja voivat olla esimerkiksi pääsy tiettyihin rajattuihin viraston resursseihin, ei välttämättä muissa tapauksissa kysymykseen tuleviin peruspalveluihin. Palvelun tarjoajan ja käyttäjän on erikseen sovittava käytöstä.

4 ETÄKÄYTÖN UHKAT JA NIILTÄ SUOJAUTUMINEN

4.1 Johdanto

Tässä luvussa kuvataan etäkäytön toiminnallisen ympäristön eri osiin kohdistuvia uhkia ja niiden torjuntaa erilaisten tarjolla olevien suojausratkaisujen avulla. Turvallisen etäkäytön arkkitehtuurin toteuttamista kuvattuja suojausratkaisuja soveltaen tarkastellaan seuraavassa luvussa (*luku 5*), jossa esitetään arkkitehtuurin toteutukseen ja käyttöön liittyvät suositukset.

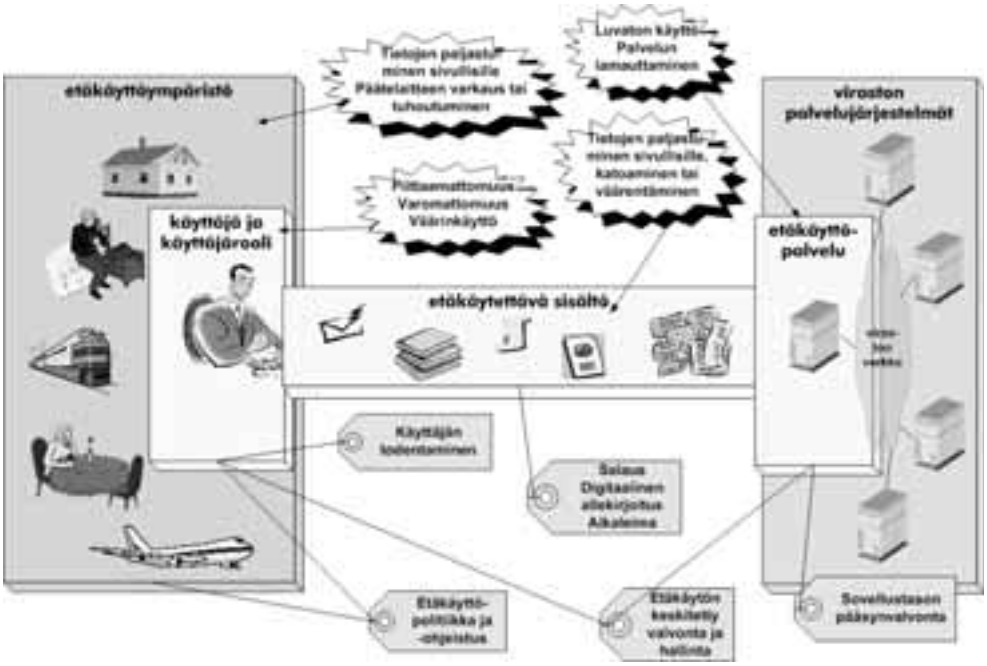
4.2 Etäkäyttöratkaisusta riipumattomat uhkat ja niiltä suojautuminen

Kuvan 7 pohjana on edellä esitetty etäkäytön ympäristökuva. Siihen on merkitty kokonaisuuteen kohdistuvat etäkäyttöratkaisusta riippumattomat uhkat (sahalaitaiset ”tarrat”) sekä uhkilta suojautumiskeinot (”nimilaput” kuvan alaosassa). Kuva ei ole uhkien ja suojautumiskeinojen kattava luettelo, vaan pyrkii tuomaan esiin yleistettynä niistä keskeisimmät. Etäkäytön uhkia ja niiltä suojautumiskeinoja on kuvattu VAHTI:n *Valtion etätyön tietoturvallisuusohjeen (3/2002) liitteessä 1* (uhkat) ja *liitteen 2 luvussa 3* (suojautumiskeinot). Kuvassa näkyvät uhkat ja keinot ovat pääosin ohjeessa esitetyn mukaisia.

4.2.1 Etäkäyttöympäristön uhkilta suojautuminen

Etäkäyttöympäristöön liittyviä pääuhkia ovat etäkäytettävien tietojen paljastuminen sivullisille sekä päätelaitteen joutuminen ulkopuolisten käsiin tai tuhoutuminen joko

Kuva 7 Etäkäyttöratkaisusta riippumattomat uhkat ja niiltä suojautuminen



vahingossa tai tahallisesti. Uhkat ovat suurimmillaan matkoilla ja julkisilla paikoilla, ja pienimmillään, kun etäkäyttöä varten on olemassa siihen erityisesti tarkoitettu kontrolloitavissa oleva työtila.

Käyttöympäristön uhkilta suojautuminen on suuressa määrin **toimintapolitiikkaa**. Varsinkin luottamuksellisia tietoja sisältävien tai muuten kriittisten sovellusten etäkäyttö tulisi rajata vain tilanteisiin ja aikoihin, joissa etäkäyttöön on välttämätön tarve. Käyttäjille tulee olla selkeät **ohjeet** toiminnasta erilaisissa etäkäyttöympäristöissä ja –tilanteissa sekä päätelaitteiden käsittelystä ja turvaamisesta.

4.2.2 Käyttäjään liittyviltä uhkilta suojautuminen

Käyttäjä on etäkäyttöratkaisusta ja käytetyistä teknisistä suojauskeinoista huolimatta aina viime kädessä vastuussa etäkäytön turvallisuudesta. Käyttäjä voi tahattomasti, huolimattomalla toiminnallaan, tai tahallaan, vahingonteon tai hyödyn tavoittelemisen tarkoituksessa, toimia annettujen ohjeiden vastaisesti ja aiheuttaa luottamuksellisten tietojen joutumisen vääriin käsiin. Hän voi myös altistaa etäkäyttöjärjestelmän hyökkäyksille tai haittaohjelmille. Näitä uhkia on teknisillä ratkaisuilla mahdoton eliminoida, mutta siihen voidaan vaikuttaa etäkäyttöoikeuksia myönnettäessä, ohjeis-

tamalla ja valvomalla etäkäyttäjien toimintaa sekä tarkastamalla säännöllisesti, että etäkäyttöpäätteet ja -ratkaisut ovat asianmukaisessa kunnossa.

Viraston palveluja käytettäessä on olennaista, että etäkäyttäjä **tunnistetaan ja todennetaan luotettavasti**. Tunnistaminen perustuu käyttäjäidentiteettiin, jonka käyttäjä itse ilmoittaa esimerkiksi **käyttäjätunnuksen** muodossa. Käyttäjän tunnistaminen ja todentaminen tapahtuu varsinaisesti viraston palvelujärjestelmässä. Käyttäjälle näkyvä ja hänen toimintaansa välittömästi vaikuttava osa tunnistamisesta ja todentamisesta on **todentamismenetelmä**, joka tarkoittaa menettelyä ja siihen mahdollisesti liittyviä välineitä. Todentamismenetelmiä on monenlaisia perustuen jaettuun salaisuuteen, ulkoiseen todentajaan tai käyttäjän biologisiin ominaisuuksiin.

Oheisessa *taulukossa 2* tarkastellaan käytännössä kysymykseen tulevia todennusmenetelmiä sen suhteen millaista **välineistöä** tai millaisia (ulkoisia) **todentajia** ne edellyttävät.

Taulukko 2 Todennusmenetelmät ja niiden vaatima infrastruktuuri

Todennusmenetelmä	**Todennusväline**	**Todentaja**
Salasana – kiinteä – vaihtuva – kertakäyttöinen	 – salasanalista –	 – – –
Haaste-vaste -menetelmä (esim. *SecurID*)	haastelukulaskin (esim. *SecurID*:n) tms.	–
Matkapuhelinliittymä – puhelinsoitto[1] – kertakäyttö-salasanan välitys SMS-viestillä	 matkapuhelin matkapuhelin	 televerkko televerkko
PKI-varmenne – toimikortilla – matkapuhelimen (S)WIM-kortilla – softavarmentee-na päätelaitteen muistissa	 toimikortti ja sen lukija päätelaitteessa GSM-puhelin + (S)WIM-kortti päätelaite joka mahdollistaa varmenteen turvallisen säilytyksen	 varmentaja X (voi olla virasto itse) varmentaja X (voi olla virasto itse) varmentaja X (voi olla virasto itse)
Biometrinen todentaminen (esim. sormenjälkitunnistus) Luotetun kolmannen osapuolen varmennus	biometrinen tunnistin päätelaitteessa riippuu toteutustavasta	– todentaja Y

[1] Käyttäjä soittaa puhelimellaan turvapalvelimeen, jolle televerkko kertoo soittavan liittymän numeron, tai turvapalvelin soittaa käyttäjän rekisteröityyn matkapuhelinliittymään (takaisinsoitto). Ks. myös *kuva 8*, jossa tätä todennustapaa on havainnollistettu.

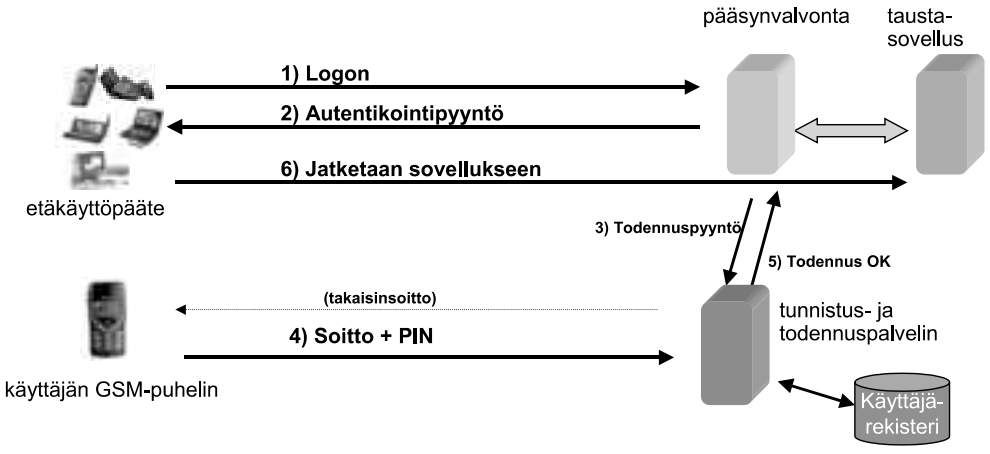
Jotkut todennusmenetelmistä kuten toimikorttipohjaisen PKI-varmenteen tai biometrisen tunnistuksen käyttö edellyttävät etäkäyttäjän päätelaitteelta erityisvalmiuksia. Toisaalta todennusväline voi olla laadultaan sellainen, että käytännöllisesti katsoen kaikilla käyttäjillä sellaisen voidaan olettaa olevan esimerkiksi matkapuhelin.

Menetelmiä voidaan yhdistellä, jolloin todentamisen varmuus paranee. Esimerkiksi PKI-varmennetta käyttäessään käyttäjä joutuu osoittamaan varmenteeseen liittyvän salaisen avaimen omistajuutensa henkilökohtaisella tunnusluvullaan (PIN). Vastaavasti puhelinsoittoon perustuvassa todentamisessa normaalisti käytetään myös kiinteätä tai kertakäyttösalasanaa tai vaikkapa biometriikkaa (käyttäjän äänen tunnistus). Todentamisen varmuutta voidaan parantaa myös **käyttämällä todentamiseen eri tiedonsiirtokanavaa** kuin sovellus (*kuva 8*).

Yhtä ainoaa turvatasoltaan vaativimpiinkin tarpeisiin soveltuvaa ja samanaikaisesti eri tyyppisiin käyttötilanteisiin sopivaa todentamismenetelmää ei ole olemassa. Siksi vähänkin monipuolisempia palveluja tarjoavassa ympäristössä on lähdettävä siitä, että käytössä on useita eri todentamismenetelmiä, joilla on osittain päällekkäin menevät käyttöalueensa.

Edellä luetelluista todentamismenetelmistä turvatasoltaan hyvä, logistiikaltaan ja käytöltään helppo ja silti kustannuksiltaan edullinen on **matkapuhelimen käyttö todennusvälineenä (puhelinsoitto sekä kiinteä tai kertakäyttöinen tunnusluku)**. Se sopii myös lähes kaikissa käyttötilanteissa käytettäväksi.

Kuva 8 Esimerkki käyttäjän todentamisesta käyttäen siihen eri kanavaa (matkapuhelisoitto) kuin sovelluskommunikointiin



Kumppanikäytössä kysymykseen voi tulla myös **luotetun kumppaniosapuolen suorittama todennus**. Tällöin kumppanin omassa verkossaan luotettavasti todentama käyttäjä voidaan olettaa todennetuksi myös viraston palveluun pyrkiessään. Tällainen ns. **federoitu todennus- ja auktorisointimalli** on pohjana mm. *Liberty Alliance*n valmisteilla olevissa suosituksissa.

Vahvaa tunnistamista vaativissa sovelluksissa on syytä käyttää **PKI-varmenteisiin** tai jotain **biometriseen tunnistamiseen** perustuvaa todentamismenetelmää.

4.2.3 Etäkäytettävän sisällön suojaus

Etäkäyttöyhteydellä siirrettävien tietojen ja aineistojen sisältöön kohdistuu monenlaisia uhkia, jotka riippuvat käytettävästä etäkäyttöratkaisusta. Etäkäytettävän aineiston suojaus samastuu pitkälti verkkoyhteyden ja päätelaitteen suojaukseen.

Sisällön suojaamiseen liittyviä toimintoja ovat sanomien ja aineistojen yksilöinti, todentaminen ja suojaaminen sekä tapahtumien kiistämättömyyden takaaminen. Sanomien yksilöintiin ja todentamiseen käytettäviä tekniikoita ovat erilaiset tunnisteet, tarkistussummat ja sähköinen allekirjoitus. Sanomien ja koko verkkoyhteyden suojaamiseen käytetään salakirjoitusta. Kiistämättömyyden takaamiseen liittyviä tekniikoita ovat sähköinen allekirjoitus ja varmennetut aikaleimat. Sanomaliikenteen eheyden takaamiseen ja viestien perillemenon varmuuteen vaikuttaa myös käytetty yhteyskäytäntö.

Luottamuksellisia tai viraston toiminnan kannalta muuten kriittisiä tietoja ei turhaan saa säilyttää etäkäyttäjän päätelaitteella. Luottamuksellisia sisältöjä voidaan kuitenkin joutua säilyttämään päätelaitteella. Päätelaitteen suojauksin voidaan vaikeuttaa asiattomiin tietoihin käsiksi pääsemistä. Paras suoja edellyttää luottamuksellisten tietojen tai mieluiten koko päätelaitteen pysyväismuistin, esimerkiksi tietokoneen kovalevyn **tietojen salaamista**. Päätelaitteella säilytettävien tietojen tuhoutumisuhkaa vastaan voidaan suojautua huolehtimalla säännöllisesti **tietojen varmuuskopioinnista** mieluiten verkon kautta viraston palvelimelle.

4.2.4 Etäkäyttöpalvelun suojaaminen

Etäkäyttöpalvelun suojaaminen tarkoittaa käytännössä kahta asiaa: 1) **pääsynvalvontaa** eli palvelun, sen kautta saatavilla olevien tietojen sekä palvelun käyttöön liittyvien tietojen suojaamista asiattomalta käytöltä, sekä 2) **palvelujärjestelmän toimintakyvyn turvaamista**.

Käytännössä viimemainittu suojaus sekä suuri osa pääsynvalvonnasta toteutetaan normaalisti **palvelun verkkoliitännässä.** Tämä toimii suojamuurina palvelun ja sen

käyttäjien välillä. Verkkoliitännän avulla palvelu pyritään eristämään mahdollisimman hyvin turvattomasta ulkoisesta verkkoympäristöstä sekä suojaamaan sitä myös viraston käyttäjien tai sisäverkon aiheuttamilta uhkilta. Sovellusten sisäinen, toiminto- tai tietokohtainen pääsynvalvonta on toteutettava palvelun osana, jos näin hienojakoista kontrollia tarvitaan.

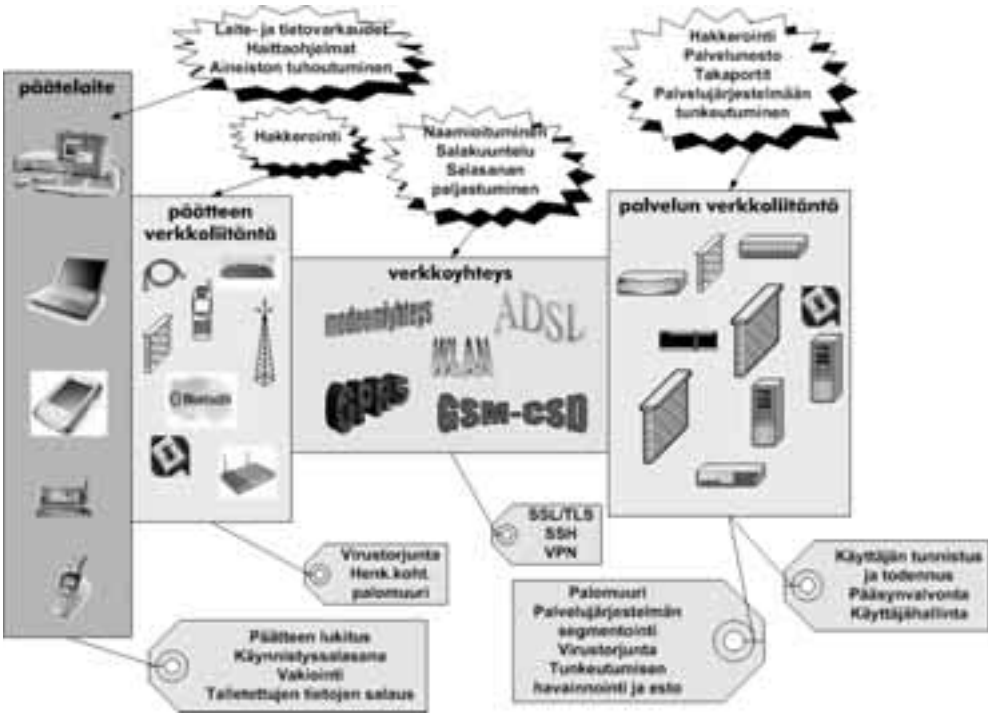
4.3 Etäkäyttöratkaisuun liittyviltä uhkilta suojautuminen

Kuva 9 esittää eri komponentteja sekä niihin liittyviä uhkia ja niiden torjuntakeinoja.

4.3.1 Päätelaitteen suojaus

Päätelaitteen suojauksilla estetään laitteella olevien tietojen ja yhteyden asiaton käyttö sen joutuessa vääriin käsiin. Päätelaite on suojattava mahdollisilta haittaohjelmilta.

Kuva 9 Etäkäyttöratkaisuun liittyvät uhkat ja niiltä suojautuminen



Suojausten määrä ja taso vaihtelee laitetyypeittäin. Monipuolisimmat suojaukset on kannettavissa tietokoneissa. Siirryttäessä PDA-laitteista älypuhelinten kautta matkapuhelimiin suojausmahdollisuudet vähenevät lähes olemattomiin. Koska pienemmillä päätelaitteilla on myös suurempi riski hävitä, niiden käyttö tulisi rajata vähiten kriittisiin sovelluksiin.

Keinoja asiattoman tietoihin käsiksi pääsemisen estämiseksi ovat käynnistyssalasana sekä säilytettävien tietojen, mahdollisesti koko pysyväismuistin salaus. Päätteen, esim. kannettavan tietokoneen, varastamista voi vaikeuttaa fyysisellä lukolla sekä turvallisella säilyttämisellä kuljetusten aikana. Tietojen tuhoutumisen haittoja ehkäistään säännöllisillä varmuuskopioinneilla sekä välttämällä tietojen tarpeetonta säilyttämistä etäkäyttöpäätelaitteella.

PDA-laitteiden, älypuhelinten ja matkapuhelinten keskitetyt hallinnointimahdollisuudet eivätkä muutkaan käyttöominaisuudet ole samalla tasolla kuin PC-päätelaitteilla. Laitteiden asetuksia ei voi vakioida eikä ohjelmien latausta laitteille estää. Laitteille ei myöskään välttämättä ole saatavilla tietojen ja yhteyksien suojaamisohjelmistoja kuten salaus-, virustorjunta- tai VPN-ohjelmistoja. Toisaalta niihin kohdistuvien hyökkäysten ja haittaohjelmistojen uhka ei ainakaan vielä ole kovin merkittävä, mutta tilanne voi jatkossa muuttua. Rajoitteet suojausmahdollisuuksissa kaventavat kevyimpien päätelaitteiden käyttöaluetta etäkäytössä.

Päätteiden käytössä peruslähtökohtana tulisi pitää, että käytetään **vain viraston hallinnoimia laitteita**. Hallinnoinnilla tarkoitetaan tässä yksinomaista päätäntävaltaa laitteen tyypistä, perusohjelmistosta, käytettävistä sovelluksista, ohjelmistojen asetuksista, päätteiden ohjelmistopäivityksistä, valvonnasta sekä käytöstä. Mitä vähemmän organisaatio tietää jonkun päätelaitteen ominaisuuksista ja käytöstä ja pystyy vaikuttamaan niihin, sitä suurempi uhka tuo päätelaite on etäkäytössä organisaation tietoturvallisuudelle.

Joissain virastoissa kaikille etäkäyttöä tarvitseville ei voida järjestää viraston päätelaitetta. Tällöin etäkäyttöoikeuksia myönnettäessä niihin liittyvä ylimääräinen riski on tiedostettava ja käyttäjien etäkäyttömahdollisuudet on rajattava välttämättömimpään.

4.3.2 Päätelaitteen verkkoliitännän suojaaminen

Myös etäkäyttäjän päätelaite voi altistua ulkoisille hyökkäyksille. Varsinkin silloin kun verkkoyhteys on Internetin kautta. Päätelaitteella olevien tietojen paljastumisen tai tuhoutumisen lisäksi hyökkääjä voi käyttää etäkäyttäjän päätelaitetta palvelunestohyökkäyksen välikappaleena tai virusten, matojen yms. levittäjänä. Tunkeutumalla päätelaitteelle hyökkääjä voi myös päästä suojatun verkkoyhteyden kautta palvelujärjestelmään verkkoliitännän suojauksien ohi. Päätelaitteen verkkoliitännän suojauksen tarkoituksena on suojella päätelaitteen tietoja ja ohjelmistoja näiltä uhilta.

Riskit ovat suurimmat, jos etäkäyttäjän päätelaite on kytketty Internetiin kiinteällä yhteydellä (esimerkiksi ADSL) ja pienin, jos etäkäyttäjä on liitetty kiinteällä tai valintayhteydellä suoraan viraston järjestelmäympäristöön. Jos päätelaitetta käytetään muissa verkoissa ja muuhun kommunikointiin kuin viraston etäkäyttöön, päätelaitteen saastumisriski kasvaa. Päätelaitteelle ei koskaan tulisi sallia kahta tai useampaa samanaikaisesti aktiivista verkkoliitäntää. Haittaohjelma voi joutua etäkäyttäjän päätelaitteelle myös esimerkiksi sähköpostin liitteenä tai muutoin siirretyn tiedoston yhteydessä.

Verkkoliitännän suojauksen perusvälineet ovat **ajan tasalla ja aktiivisessa käytössä oleva virustentorjuntaohjelmisto** sekä **henkilökohtainen palomuuri**. Ensin mainittu antaa suojan myös tietovälineiden kautta leviäviä haittaohjelmistoja vastaan. Viimeksi mainittu torjuu sekä verkosta tulevat päätelaitteelle tunkeutumisyritykset että päätelaitteelle tavalla tai toisella päässeiden haittaohjelmien yritykset liikennöidä ulospäin. Palomuurin tulisi olla keskitetysti hallinnoitavissa. Henkilökohtaisen palomuurin vaihtoehtona voidaan joskus käyttää erillistä palomuurilaitetta.

Markkinoilla verkkoliitännän suojaukseen on valmiita paketteja, joihin sisältyy palomuuri, siihen liittyvä lokikirjanpito, virustentorjunta sekä joskus myös VPN-*client*. Etäkäyttäjien palomuurivalintoja tehtäessä kannattaa varmistaa yhteensopivuus palvelujärjestelmän suojausratkaisujen kanssa, sillä eri valmistajien tuotteet ovat usein yhteensopimattomia. Yhteensopivuusongelmia on usein mobiililaitteissa.

Verkkoliitännän toteuttamisessa yleistyvät **langattomat liitäntätavat** (WLAN, Bluetooth) parantavat käyttömukavuutta, mutta kasvattavat tietoturvariskejä, koska langattoman verkon kuuluvuusaluetta ei voi helposti rajoittaa esim. tietyn kiinteistön sisälle. Langatonta liitäntää käytettäessä tarvitaan ylimääräisiä varotoimia. **Langattoman yhteyden tietoliikenne on salattava.** Paras ratkaisu tässä on käyttää VPN-tekniikkaa.

Nykyisin yleisimmässä käytössä olevien **IEEE802.11b**-suosituksen mukaisten WLAN-verkkojen salausmenetelmä on *Wireless Equivalent Privacy (WEP)*, joka on eri yhteyksissä osoitettu helposti haavoittuvaksi. Tekeillä on uusi **802.11i**-suositus, jossa salaukseen liittyvät puutteet on tarkoitus korjata. Lisäksi käyttöön on tarkoitus tuoda muita tärkeitä turvallisuusominaisuuksia. Yhtenä niistä käyttäjien todentaminen. Suositus ei kuitenkaan ole vielä valmis.

Tilapäisapuna WLANien turvaongelmiin **Wi-Fi Allianssi** on määritellyt spesifikaation nimeltä **Wi-Fi Protected Access (WPA)**, johon on otettu piirteitä kehitteillä olevasta 802.11i-suosituksesta. Sitä markkinoidaan nyt Wi-Fi Allianssiin kuuluvien toimittajien laitteiden välillä yhteensopivana, riittävän turvatason tarjoavana ja tulevan 802.11i-suosituksen kanssa yhteensopivana turvaratkaisuna. Vaihtoehtona sille ovat toimittajakohtaiset WEP-menetelmän täydennykset.

4.3.3 Verkkoyhteyden suojaus

Turvallisin tapa toteuttaa etäkäyttöä olisi kiinteä tai piirikytkentäinen valintayhteys suoraan viraston järjestelmäympäristöön, mutta sekään ei ole riskitön ja voi muodostua kustannuksiltaan ja hallinnoinniltaan raskaaksi. Siksi on tarkoituksenmukaista toteuttaa yhä suurempi osa etäkäytöstä Internetiä hyödyntävillä verkkoyhteyksillä.

Yleisten tietoliikenneverkkojen, erityisesti ”villin” Internetin kautta kulkevat verkkoyhteydet ovat alttiita erilaisille tietoturvahyökkäyksille. Hyökkääjät voivat salakuuntelemalla saada yhteydeltä haltuunsa luottamuksellisia tietoja, väärentää yhteydellä liikkuvia tietoja tai lähettää vääriä tietoja yhteyden osapuoleksi tekeytyen. Tietoja voi teknisistäkin syistä hävitä tai ne voivat muuttua.

Verkkoyhteyden suojaus pyrkii siihen, että yhteydellä siirrettävien tietojen eheys ja luottamuksellisuus säilyvät, ja että osapuolet voivat olla varmoja siitä, kenen kanssa kommunikoivat. Ratkaisuna tietojen eheyteen ja luottamuksellisuuteen on joko **siirrettävien tietojen salaaminen** tai ulkopuolisilta **suojattu verkkoyhteys** *virtual private network* (VPN). Edellinen tarkoittaa käytännössä **TLS-** tai **WTLS**-yhteyskäytäntöä, jonka yleisin sovellus on selainpohjainen S-HTTP-käyttö. Jälkimmäinen on yleensä joko **IPSec**-pohjainen VPN-toteutus tai **SSH**-yhteys. VPN-verkkoyhteys mahdollistaa periaatteessa minkä tahansa tiedonsiirtokäytännön ”tunneloimisen”. TLS-tuki liittyy tiettyyn sovellusprotokollaan (esim. HTTP + TLS = S-HTTP).

Verkkoyhteyden suojaus merkitsee lisäkuormaa kommunikoiville järjestelmille. Haittaa voidaan kuitenkin vähentää käyttämällä laitteistopohjaisia toteutuksia (TLS-kiihdyttimet, laitteisto-VPN:t), jos se on mahdollista.

Molempiin yhteyden suojaamistapoihin liittyy salaustoimintojen lisäksi mekanismit, joilla kommunikoivat osapuolet voivat **tunnistaa ja todentaa toisensa**. VPN-tuotteiden tapauksessa yleensä käytetään **RADIUS**-suosituksen mukaista tunnistus- ja todentamispalvelua. Se tarjoaa käyttäjätunnukseen ja salasanaan pohjautuvan tunnistamisen ja todentamisen lisäksi myös muita menetelmiä. TLS-tukee sekä *asiakkaan* että *palvelimen* todentamista, mutta Internet-käytössä *asiakkaan* todentaminen on vielä erittäin harvinaista. Etäkäytössä tätä mahdollisuutta tulee hyödyntää.

Tekniikka, jolla kaikki mainitut suojauskeinot voidaan toteuttaa, on **PKI-varmenteiden** käyttö. Tämä on hyvin luontevaakin silloin, kun myös käyttäjän todentamisessa käytetään PKI-varmenteita. Kommunikoivat osapuolet voivat varmenteiden avulla generoida ja liittää välitettäviin viesteihin sähköisen allekirjoituksensa, jolla toinen osapuoli voi tunnistaa viestin alkuperän ja vakuuttua viestin aitoudesta. Sähköisen allekirjoituksen ja mahdollisesti myös varmennettujen aikaleimojen avulla voidaan osoittaa palvelutapahtuman kiistämättömyys.

PKI-tekniikkaa käyttäen voidaan viestejä tai niiden osia tarvittaessa myös salakirjoittaa. Viestintä voidaan salata kätevimmin käyttämällä standardoitua TLS- tai VPN-

yhteyksiä, mutta viestin tai sen osan salaaminen tämän lisäksi on mielekästä esimerkiksi, jos tieto halutaan säilyttää tai välittää edelleen salattuna.

Sähköpostin liitteiden tai muiden siirrettävien tiedostojen salaamiseen liittyy kuitenkin myös oma vaaransa. Sähköpostipalvelimen virustorjunta ei pysty havaitsemaan salatun tiedoston virusta, matoa tai muuta haittaohjelmaa ennen kuin suojaus on purettu. Tämä vaara korostaa tarvetta pitää päätelaitteen turvaohjelmistot mahdollisimman hyvässä kunnossa.

VPN- tai SSH-yhteys suojaa erinomaisesti verkkoyhteyden, mutta on avoin molemmista päistään. Jos hyökkääjä onnistuu pääsemään jommastakummasta päästä sisälle verkkoyhteyteen, koko yhteys vaarantuu salakavalasti. Siksi on erityisesti palvelujärjestelmässä harkittava tarkoin mihin VPN-yhteys viedään, jotta sitä ei voida käyttää porsaanreikänä, josta hyökkääjä pääsee viraston sisäverkkoon.

4.3.4 Palvelun verkkoliitännän suojaus

Palvelun verkkoliitäntä on eristävä rajapinta tai suojamuuri varsinaisen palvelujärjestelmän ja palvelun etäkäyttäjien välille. Palvelun verkkoliitäntä saa päästää läpi vain auktorisoitujen käyttäjien yhteys- ja palvelupyynnöt. Sen tulee myös turvata palvelujärjestelmän toiminta eliminoida järjestelmää vastaan tehdyt hyökkäysyrityksiä. Tapauksissa, joissa verkkoliityntä havaitsee epänormaalia toimintaa, se voi hälyttää ylläpitäjät.

KÄYTTÄJIEN TUNNISTAMINEN, TODENTAMINEN JA PÄÄSYNVALVONTA

Pääsynvalvonnalla tarkoitetaan kaikkia niitä menettelyjä, joilla etäkäyttäjä tunnistetaan ja todennetaan, ja lisäksi valvotaan, että tämä pääsee käyttämään vain niitä palveluja, joihin hänellä on käyttöoikeus.

Tunnistus ja todennus –toiminto suorittaa käyttäjän tunnistamisen ja todentamisen pääsynvalvonnan pyynnöstä. Tarvittaessa se huolehtii myös palvelun todentamisesta käyttäjälle. Pääsynvalvonnasta vastaava komponentti kommunikoi tunnistus- ja todennuskomponentin kanssa käyttäen jotain todennuskäytäntöä. Yleisimmät standardoidut todennuskäytännöt ovat **RADIUS** ja **TACACS+** sekä **LDAP**. RADIUS ja TACACS+ ovat toiminnallisesti jokseenkin samanlaiset. RADIUS on laajimmin tuettu – sitä tukevat myös monet pääsynvalvonnassa käytetyt laitteet.

Pääsynvalvonnan tukena tarvitaan **käyttäjärekisteri**, joka sisältää tiedot palvelujen käyttöön oikeuksista. Käyttäjärekisterinä voidaan käyttää olemassa olevaa käyttäjätietokantaa, jos se tietosisältönsä ja käyttöominaisuuksiensa puolesta soveltuu tarkoitukseen. Jos käyttäjätietoja on useissa hakemistoissa ja tietokannoissa, kannattaa perustaa uusi käyttäjärekisteri joko metahakemistotekniikkaa käyttäen tai luomalla uusi rekisteri etäkäyttöön.

Mahdollisimman laajan yhteensopivuuden takaamiseksi rekisterin olisi hyvä tarjota **LDAP-rajapinta**. Kaikissa tapauksissa LDAP-rajapintaa ei kuitenkaan voida suoraan käyttää. Tällöin vaihtoehtoina voi olla esim. RADIUS tai ODBC-/JDBC-tietokantaliittymä.

Käyttäjärekisteri sisältää palvelujen käytössä ja käyttäjän tunnistamisessa ja todentamisessa tarvittavien käyttäjän perustietojen lisäksi tiedot, joiden perusteella voidaan käyttäjäkohtaisesti hallita palvelujen käyttöä. Normaali menettely pääsynvalvontaan on määritellä käyttäjille **käyttöoikeudet**, jotka määrittelevät käyttäjän valtuudet joko luokittelutietojen (käyttäjäryhmät, käyttäjän roolit) kautta tai luettelemalla suoraan käyttäjälle sallitut palvelut. Pääsynvalvonta ja tunnistus ja todennus –toimintojen lisäksi käyttäjärekisteriä tarvitsevat myös varsinaiset palvelusovellukset silloin kun palvelujen käyttöä halutaan kontrolloida yksittäisten tietojen ja toimintojen tasolle asti.

Käyttäjän tunnistamiseen, vahvaan todentamiseen ja käyttöoikeuksien tarkistamiseen perustuva pääsynvalvonta on turvallisin ja käyttöominaisuuksiltaan joustavin pääsynvalvontaratkaisu. Muita lähinnä täydentävänä hyödyllisiä pääsynvalvontatekniikoita ovat **tikettipohjainen valvonta** (*Kerberos*-suositus), **pääsynvalvontalistat**, **IP-osoitteiden suodatus**, **kuitit** tai ***reverse proxyt***. Palvelun käytön aikainen valvonta perustuu tavallisesti onnistuneen sisäänkirjautumisen yhteydessä luotavan istunnon (*session*) voimassaolon valvontaan.

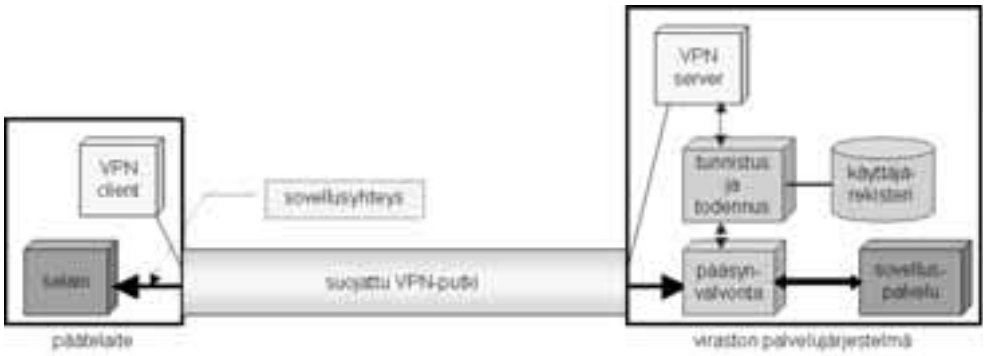
Toisen organisaation henkilön todentaminen ja käyttöoikeuksien määrittäminen on mutkikkaampaa kuin oman henkilökunnan, koska yksilön tunnistamisen sijasta tai lisäksi on tunnistettava ja todennettava henkilön organisaatio sekä rooli organisaatiossa.

Joillain sovelluspalveluilla voi olla lisäksi omat turvajärjestelmänsä omine käyttäjätunnuksineen ja salasanoineen tms. Tällöin joskus pyritään toteuttamaan pääsynvalvonta siten, että käyttäjä voi kertakirjautumisella palvelujärjestelmään päästä käyttämään kaikkia hänelle oikeutettuja palveluja. Tällainen ns. ***single sign-on* –pääsynvalvonta** (SSO) edellyttää käyttäjärekisteriä, joka kattaa sovellusten käyttäjätiedot sekä myös tiedot menettelyistä, joita tarvitaan sovelluksiin kirjautumiseksi. Laajamittaiset SSO-toteutukset ovat hallinnaltaan monimutkaisia ja myös riskialttiimpia kuin monitasoinen (”*defence in depth*”) periaatteen mukaisesti toteutettu suojaus.

Erityisesti tulisi pyrkiä pitämään erossa toisistaan luonteeltaan **tekninen, infrastruktuuritason pääsynvalvonta** kuten VPN- tai TLS-yhteyksien hallinnointi, ja **sovellustason pääsynvalvonta**. Toisin sanoen VPN- tai TLS-yhteyden onnistuneesti palvelujärjestelmään muodostanut käyttäjä tulisi erikseen todentaa ja auktorisoida pyytämiensä sovelluspalvelujen käyttäjäksi. Tätä havainnollistetaan *kuvassa 10*. Siinä esitetään tilanne, jossa etäkäyttäjä haluaa päästä käyttämään viraston selainpohjaista sovelluspalvelua päätelaitteeltaan. Palvelun käytön edellytyksenä on VPN-yhteys.

VPN-yhteyden muodostaminen edellyttää käyttäjän todentamista, minkä palvelujärjestelmässä oleva VPN-palvelin suorittaa käyttäjän etäkäyttötunnuksen perusteella viraston tunnistus- ja todennuspalveluun nojautuen ja sovittua todennusmenetelmää käyttäen. Kun VPN-yhteys on muodostettu, käyttäjä yhdistetään sovellustason pääsynvalvontaan, jossa hänen käyttöoikeutensa tarkistetaan suorittaen mahdollisesti vaadittava sovellustason todennus, ja vasta tämän jälkeen hänet päästetään sovelluspalveluun. Näin teknisen tason ja sovellustason pääsynvalvonta ovat erillisiä toimintoja, vaikka nojautuvatkin samaan taustalla olevaan tunnistus- ja todentamispalveluun ja käyttäjärekisteriin.

Kuva 10 Esimerkki teknisen tason ja sovellustason pääsynvalvonnasta



PALVELUJEN SUOJAUS VERKKOLIITÄNNÄSSÄ

Viraston sovelluspalvelujen etäkäyttö edellyttää, että palvelujärjestelmiin avataan pääsy ulkoisesta verkosta. Jos ulkoinen verkko koostuu viraston yksinomaisessa käytössä olevista yhteyksistä ja tietoliikennelaitteista, virasto voi olettaa palvelujärjestelmiensä olevan kohtuullisen hyvässä turvassa. Käytännössä nykyään kuitenkin etäkäyttöyhteydet toteutetaan suurimmalta osin yleisten verkkojen ja erityisesti Internetin kautta, jolloin ulkoiset yhteydet ovat portteja vihamieliseen ulkomaailmaan. Uhkien torjunta vaatii suojamuureja ja portinvartijoita, jotka mahdollisimman tehokkaasti eristävät viraston palvelujärjestelmät ulkomaailmasta ja sallivat vain luvallisen liikenteen.

Keskeiset menetelmät palvelun verkkoliitännän suojaamisessa ovat **palvelujen ryhmittely ja ryhmien eristäminen toisistaan**, **liikenteen suodattaminen** sekä **puskurivyöhykkeiden** luonti, jotta palvelun toteuttavat varsinaiset järjestelmät eivät ole tarpeettomasti näkyvissä. Tämän lisäksi voidaan käyttää **tunkeutumisen havainnointijärjestelmiä** (*Intrusion Detection Systems, IDS*) hyökkäysten havainnointiin ja rekisteröintiin. Olennaista on myös kaikkien rajapinnassa havaittujen järjestelmään

kirjautumisyritysten – sekä onnistuneiden että epäonnistuneiden – kirjaaminen **pääsynvalvontalokiin**. Loki on syytä tallettaa palvelimella, joka on erityisen hyvin suojattu tunkeutumisyrityksiä vastaan. Se ei saa näkyä ulos sisäverkosta.

Palvelujen ryhmittely

Palvelujen ryhmittelyllä ja eristämisellä toisistaan tarkoitetaan **sisäverkon lohkomista toisistaan eristettyihin osaverkkoihin**, segmentteihin, joiden välinen kommunikointi on mahdollista vain viraston palomuurin tai muun liikennettä suodattavan laitteen sekä käyttäjän tunnistamisen ja todentamisen kautta. Segmentointia voi tehdä fyysisesti tai loogisesti (VLAN).

Jos sisäverkon kaikki palvelut sijoitetaan yhteen ja samaan verkkosegmenttiin, on olemassa vaara, että verkkoon kaikista varotoimista huolimatta päässyt tunkeilija voi lamauttaa koko verkon toiminnan tai aiheuttaa muuta laajaa vahinkoa. Kun verkko on lohkottu pienempiin osaverkkoihin, mahdolliset vahingot voidaan rajoittaa pienemmälle alueelle. Toisaalta segmentointi mahdollistaa samaan etäkäyttöluokkaan kuuluvien palvelujen sijoittamisen samaan verkkosegmenttiin, mikä yksinkertaistaa palomuurien ohjelmointia.

Liikenteen suodattaminen

Liikenteen suodattaminen tarkoittaa tulevien datapakettien tutkimista joko pelkästään osoitetietojen osalta tai myös pakettien sisällön osalta. Kaikki sellaiset paketit, joiden lähettäjä, vastaanottaja, tyyppi tai muu ominaisuus tai edellisten yhdistelmä ei löydy sallitun liikenteen listoilta (suodatussäännöt), pysäytetään ja tuhotaan. Vain määritellyt ehdot täyttävä liikenne päästetään läpi. Liikenteen suodattamisesta huolehtivat useimmiten **palomuurit**. Rajoittuneempia suodatusominaisuuksia on eräissä muissakin laitteissa kuten reitittimissä.

Puskurivyöhykkeen luonti

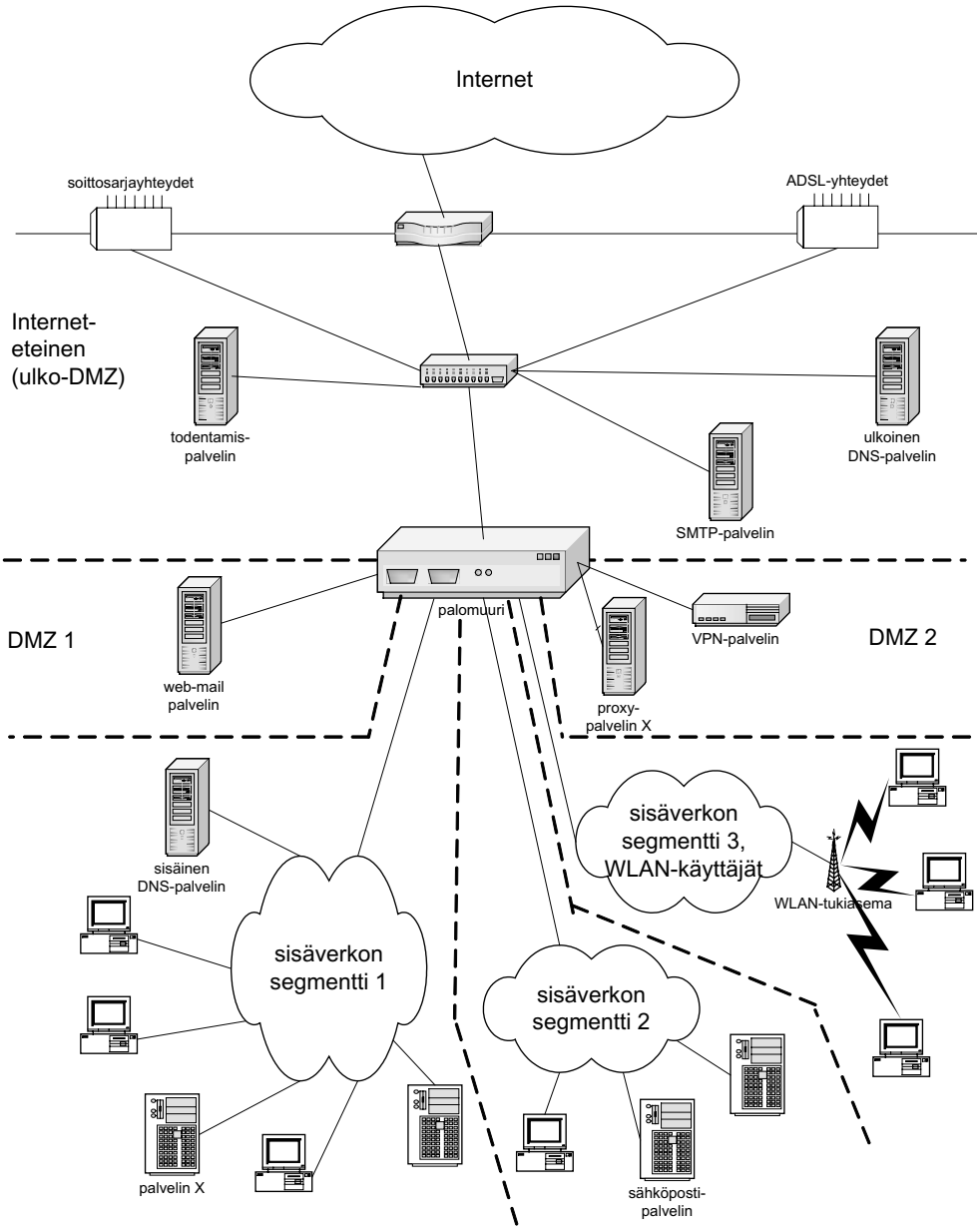
Puskurivyöhykkeellä tarkoitetaan ulkoisen verkon ja varsinaisten palvelujärjestelmien välille luotavaa **eteistä, DMZ**. Eteinen rajataan palomuureilla, ja sille sijoitetaan toimintoja, jotka näkyvät ulkoverkkoon. Sisä- ja ulkoverkko on näin erotettu toisistaan. DMZ:lla olevat palvelimet toimivat ulkoisen liikenteen välittäjinä. Sille sijoitettavia palveluja ovat muun muassa tunnistus-, todennus- ja pääsynvalvontapalvelut, viraston ulkoiset nimipalvelut sekä erilaiset sovelluspalvelujen välityspalvelimet kuten esim. web-postipalvelin, päätepalvelin, FTP-palvelin ja ehkä ulkoinen SMTP-palvelin. Myös eteispalvelut kannattaa tarvittaessa sijoittaa eri verkkosegmentteihin.

Tunkeutumisen havainnointijärjestelmät

Tunkeutumisen havainnointijärjestelmät tutkivat tulevaa liikennettä ja pyrkivät löytä-

mään siitä merkkejä tunnetuista hyökkäysyrityksistä. Ne pitävät kirjaa havainnoistaan ja hälyttävät käyttöhenkilöstön hyökkäysyritykseksi tulkitsemansa tilanteen huomatessaan. Jotkut ohjelmistot osaavat toimia yhdessä palomuurin kanssa siten, että ne komentavat palomuurin sulkemaan tietyn portin tai sulkemaan liikenteen tietystä.

Kuva 11 Esimerkki palveluliitännän suojauksen toteuttamisesta



Mitä lähempänä palveluliitännän ulkoreunaa IDS-järjestelmä on, sitä suuremman liikennemäärän se joutuu analysoimaan. Myös vääriä hälytyksiä ja analysoitavia lokitietoja syntyy enemmän. Realistinen ratkaisu on sijoittaa IDS varsinaisten palvelujen tai niiden DMZ:lla sijaitsevien välityspalvelimien yhteyteen. Tällöin edessä olevat suojakerrokset ovat karsineet mahdollisen tunkeilijaliikenteen. IDS-järjestelmien parhaista käyttötavoista ja niillä saavutettavista todellisista hyödyistä ei ole vielä riittävästi tietoa. Sellaisen käyttöönotto vaatii huolellista suunnittelua ja kokeiluja.

Kuvassa 11 on palveluliitännän suojausratkaisu, jolla pyritään havainnollistamaan edellä kuvattuja periaatteita.

Kuvan yläosassa näkyvät palvelujärjestelmän **ulkoiset verkkoyhteydet**, joita on kolmenlaisia: Internet-liitäntä sisääntulevaa ja ulosmenevää liikennettä varten, soittosarja ja laajakaistaisia ADSL-yhteyksiä. Internet-liittymässä on reititin, jossa määritellyt suodatussäännöt suorittavat tulevan liikenteen esikarsintaa estäen esim. sisäverkosta tulevaksi väärennetyn liikenteen (ns. *spoofing*-hyökkäys) sekä mahdollisesti myös tietyistä vaarallisiksi tiedetyistä osoitteista tulevan liikenteen.

Ulkoiset yhteydet päättyvät **Internet-eteiseen**, joka on viraston uloin DMZ. Sen ulkorajalla oleva reititin suorittaa liikenteen suodatusta. Internet-eteisessä **sijaitsevat tunnistus- ja todennuspalvelin**, viraston **ulkoinen DNS-palvelin** ja **ulkoinen sähköpostin välityspalvelin**. Kaikki liikenne sisäverkon, sisempien DMZ-segmenttien ja Internet-eteisen välillä kulkee viraston **palomuurin** kautta.

Esimerkkikuvan seuraava taso kohti sisäverkon palveluita kuljettaessa on **sisä-DMZ:at**, joita tässä tapauksessa on kaksi kappaletta. Segmentointiperiaatetta voidaan soveltaa myös tällä tasolla. DMZ 1:lle on sijoitettu **web-postipalvelin**. Käyttäjät kommunikoivat web-postipalvelimen kanssa suojattua S-HTTP-yhteyskäytäntöä käyttäen ulkoverkosta. Palomuurisäännöt sallivat web-postipalvelimen kommunikoivan ainoastaan sisäverkon segmentissä 2 sijaitsevan sähköpostipalvelimen kanssa. DMZ 2:lle, on sijoitettu **VPN-palvelin**, johon kaikki VPN-yhteydet päättyvät. Lisäksi siellä on sisäverkon segmentissä 1 sijaitsevan palvelin X:n (esim. jokin http-palvelin) **proxy-palvelin**, joka toimii liikenteen välittäjänä etäkäyttäjien ja varsinaisen palvelimen välillä.

Sisäverkon segmenttien välinen liikenne kulkee palomuurin kautta. Sisäverkkoon on muodostettu oma **segmentti WLAN-käyttäjistä**, koska näitä tulee kohdella kuten ulkoverkon käyttäjiä. WLAN-käyttäjien on ensin muodostettava VPN-yhteys DMZ 2:lle sijaitsevaan VPN-palvelimeen; sieltä he pääsevät eteenpäin sisäverkon palveluihin vasta tultuaan asianmukaisesti todennetuksi ja käyttöoikeudet auktorisoiduksi.

Kuvassa 11 ei ole erikseen esitetty IDS-toiminnallisuuden sijoittelua, mutta sopivia paikkoja sille on DMZ 1:llä ja 2:lla sijaitsevien sovelluspalvelinten yhteydessä.

5 TURVALLISEN ETÄKÄYTÖN ARKKITEHTUURIN TOTEUTTAMINEN

5.1 Johdanto

Turvallisen etäkäytön arkkitehtuurin lähtökohtana on, että kaikki käytettävät järjestelmäkomponentit on asianmukaisesti **suojattu**, käyttäjillä on riittävät **ohjeet** ja tarvittaessa **tukea** saatavilla ja että etäkäyttötoiminnalla on **sovitut pelisäännöt**, joiden toteutumista ja käyttöä myös **valvotaan**.

Tässä luvussa kuvataan askeleet ja niihin liittyvät yksityiskohtaiset suositukset, joiden mukaisesti edellä esiteltyjä suojausperiaatteita ja –ratkaisuja käyttäen toteutetaan virastokohtainen turvallisen etäkäytön arkkitehtuuri.

5.2 Askel 1: määritellään viraston etäkäyttöpolitiikka

Tässä keskitytään tekniikkaan, mutta sitä ei voi tarkastella ilman periaatteita, jotka määrittelevät puitteet viraston etäkäytölle, viraston etäkäyttöpolitiikkaa. Teknisiä ratkaisuja sovelletaan sen osana. Tätä aihetta on käsitelty varsin kattavasti *Valtionhallinnon etätyön tietoturvallisuusohjeessa*, VAHTI 3/2002.

Etäkäyttöpolitiikka on asiakirja, jossa määritellään toimintapoliittiset linjaukset viraston tietojärjestelmäpalvelujen etäkäytölle. Eräs keskeinen etäkäyttöpolitiikassa määriteltävä asia on sovelluspalvelujen etäkäyttöluokittelu, jossa sovellukset ryhmitellään sen mukaan miten vahvasti suojattu etäkäyttöratkaisu sen käyttäjiltä edellytetään. Etäkäyttöpolitiikassa tulee lisäksi määritellä etäkäytön laitteisto- ja yhteyspolitiikka, käyttöajat, koulutus-, ohjeistus- ja tukipalvelut sekä etäkäytön hallinnointiperiaatteet ja organisointi. Seuraavassa esitetyt toimenpidesuositukset ovat nimenomaan turvallisen etäkäytön arkkitehtuuria tukevia toimintaohjeita.

Suositukset

Organisaation sisäverkkoon saa liittää vain organisaation hallitsemia laitteita.

Etäkäyttäjille pitää antaa tarvittavat päätelaitteet, verkkoyhteydet, käyttötuki ja ohjeistus, myös miten toimitaan kolmansien osapuolten, esim. Internet-palveluntarjoajien, kanssa.

Etäkäyttäjiltä pyydetään sitoumus noudattaa annettuja turvaohjeita.

Etäkäyttäjän päätelaitteen käyttöä tulee koskea samat säännöt kuin toimistopäätelaitteita. Esimerkiksi päätelaitetta saa käyttää vain työasioihin.

Jos päätelaite on kiinni aktiivisella yhteydellä viraston verkkoon, sitä ei saa jättää ilman valvontaa.

Tarvittaessa tulee järjestää työntekijälle myös fyysisen turvallisuuden vaatimukset täyttävät työtilat kotiin.

Tietojen varmistus on tehtävä säännöllisesti ja varmuuskopioidut tiedot säilytettävä turvallisesti. Paras ratkaisu on varmuuskopioitujen tietojen säilyttäminen viraston palvelimilla. Verkon yli kopiointi on tehtävä turvallisesti.

Jos etäpäätelaitteen tietojen etävarmistus ei ole mahdollista, virasto hankkii varmuuskopiointiin tarvittavan varustuksen etätyöntekijälle.

Luottamuksellisten tietojen säilytystä päätelaitteella tulee välttää.

Jos luottamuksellisia tietoja kuitenkin säilytetään päätelaitteella, ne tulee salata. Turvallisinta on koko pysyväismuistin salaus, koska se kattaa myös tilapäis- ja sivutustiedostot. Ongelmia tietojen elvyttämisessä voi syntyä muistirikon tapauksessa.

Jos käyttäjä tallettaa luottamuksellisia tietoja liikuteltavalle medialle ja jos tietoja ei ole salattu, tietovälinettä tulee säilyttää lukitussa säilytyspaikassa.

Luottamuksellisia tietoja ei ilman lupaa saa viedä organisaation toimitilojen ulkopuolelle.

Ulkomaille matkustettaessa luottamukselliset tiedot tulee pitää salattuina ja niiden tulee olla koko ajan käyttäjän hallussa.

Matkalla mukana olevia luottamuksellisia tietovälineitä (ml. papereita) tulee kuljettaa lukitussa salkussa tms., eikä niitä saa jättää autoon, hotellihuoneeseen, toimistoon tai muuhun julkiseen paikkaan vartioimatta.

Luottamuksellisia tietoja ei saa asettaa paljastumiselle alttiiksi julkisilla paikoilla esimerkiksi lukemalla niitä päätelaitteella.

5.3 Askel 2: luokitellaan viraston etäkäytettävät sovellukset

Tärkeä elementti turvallisen etäkäytön arkkitehtuurin rakentamisessa on viraston sovelluspalvelujen etäkäyttöluokittelu. Etäkäyttöluokittelulla tarkoitetaan jaottelua, jossa otetaan huomioon

- sovellusta etäkäytössä tarvitsevien henkilöiden lukumäärä ja roolit
- sovelluksessa käsiteltävien tietosisältöjen luottamuksellisuus[2]
- päätelaitteet ja yhteystyypit, joilla suoritettavaa etäkäyttöä on tarkoitus tukea.

Nämä tekijät ovat sidoksissa toisiinsa. Mitä laajemmalle käyttäjäkunnalle ja päätelaitespektrille etäkäyttöpalvelua halutaan tarjota, sitä suuremmat riskit ovat luottamuksellisen tiedon vuotamiseen. Kääntäen, mitä luottamuksellisempaa tai muuten kriittistä tietoa sovelluksessa käsitellään, sitä valikoidummalle etäkäyttäjäkunnalle sitä tarjotaan. Luottamuksellisimpien sovellusten etäkäyttöä ei tule lainkaan sallia.

Kunkin viraston tulee itse tehdä oma etäkäyttöluokittelunsa, koska mahdolliset etäkäyttöpalvelut ja jossain määrin myös toimintaperiaatteet ovat virastokohtaisia.

[2] VAHTI-ohjeen *Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje*, VM 19.1.2000 sekä Valtion tietoaineistojen käsittelyn tietoturvaohjeen (2/2000) mukaisesti.

Suositukset

Viraston etäkäyttöiset sovelluspalvelut tulee ryhmitellä etäkäyttöratkaisulta edellytetyn suojaustason mukaisiin luokkiin.

Lähtökohtana voidaan pitää palvelussa käsiteltävien tietoaineistojen turvaluokittelua sekä etäkäyttösovellusten käyttäjärooleja ja niihin liittyviä käyttöoikeuksia.

Myös paikalliskäyttöiset sovelluspalvelut kannattaa luokitella vastaavasti.

5.4 Askel 3: määritellään kunkin etäkäyttöluokan hyväksyttävät etäkäyttöratkaisut ja niiden minimisuojaustaso

Tämän askeleen tehtävänä on määritellä kullekin edellisessä vaiheessa määritellylle etäkäyttösovellusten luokalle niiden käytössä hyväksyttävät etäkäyttöratkaisut sekä näiltä vaadittava minimisuojausvarustus, joka tarkoittaa

a. päätelaitteita ja niiden suojaamista
b. päätelaitteiden verkkoliitäntöjä ja niiden suojaamista
c. verkkoyhteyksiä ja niiden suojaamista
d. käyttäjien tunnistamista, todentamista ja pääsynvalvontaa
e. palvelujen verkkoliitäntää ja sen suojaamista.

Minimisuojauksella tarkoitetaan suojauksia, joiden olemassaolo antaa oikeuden käyttää kyseisen luokan ja sitä alhaisemman suojaustason luokkien sovelluspalveluja.

5.4.1 Päätelaitteiden suojaamiseen liittyvät suositukset

Etäkäytössä käytettävien päätelaitteiden ja niiden ohjelmistojen tulee olla viraston hallinnoimia ellei muuta sovita.

Etäkäyttäjän päätelaitteen ohjelmistoasennusten tulee olla viraston etäkäyttöpolitiikan mukaisia ja rajoitettuja vain työkäyttöön. Ohjelmisto-

päivitykset on hoidettava säännöllisesti.

Käyttäjältä tulee kieltää tai estää viraston päätelaitteiden laitteisto- ja ohjelmistoasennusten omatoiminen muuttaminen.

Päätelaitetta ei saa luovuttaa perheenjäsenten tai muiden sivullisten käyttöön.

Päätelaitteiden fyysistä suojausta (lukitukset, turvallinen säilytys) on käytettävä. Matkan aikana päätelaitetta ei saa kuljetuttaa matkatavarana.

Päätelaitteen käynnistys- ja BIOS-salasanoja on käytettävä. Ne estävät koneen käynnistyksen ja manipuloinnin asiattomilta. BIOS-salasana voidaan murtaa, jos koneeseen pääsee käsiksi.

Käyttöjärjestelmän tiedostosuojauksia kannattaa käyttää.

PC-konfiguraatioissa huomionarvoisia asioita ovat:
– vahvat salasanat
– tiedosto- ja kirjoitinjaot
– käyttöjärjestelmäpäivitykset ajan tasalla (turva-aukkojen tukkiminen)
– virustorjunta
– sähköpostin vaaralliset liitteet
– vakoiluohjelmat (*spyware*).

Myös selainten turvalliseen käyttöön pitää kiinnittää huomiota:
– viraston tulee määritellä selainsovellustensa toiminnalliset vaatimukset (ml. turvallisuus) ja valita tämän perusteella käyttämänsä selain
– tarpeettomien ja turvattomien plug-inien ja aktiivikomponenttien käyttöä tulee välttää; jos käytetään määritellään viraston varmennepolitiikassa tahot, joiden allekirjoittamat komponentit ainoastaan hyväksytään
– aktiivikomponenttien ja plug-inien lataaminen sallitaan vain nimetyistä paikoista
– evästeiden käyttöön tulee ottaa kantaa selainten konfiguroinnissa.

5.4.2 Päätelaitteen verkkoliitännän suojaamiseen liittyvät suositukset

Etäkäyttäjän päätelaitteella tulee olla toimiva virustentorjuntaohjelmisto, jos sellainen on laitteelle saatavissa.

Virustentorjuntaohjelmisto on tehokas suoja haittaohjelmistoja vastaan vain jos sitä pidetään jatkuvasti automaattisesti ajan tasalla.

Etäkäyttäjän päätelaitteella tulee käyttää henkilökohtaista palomuuria, jos sellainen on laitteelle saatavilla.

Henkilökohtaisen palomuurin tulisi olla keskitetysti hallittava antaakseen parhaan suojan. Jos käyttäjä voi muuttaa palomuurin asetuksia, sen antama suoja on kyseenalainen.

Henkilökohtaisen palomuurin konfigurointiohjeita:
– estetään ulkoa tulevat yhteydet
– estetään koneen turha näkyvyys verkkoon
– suljetaan kaikki turhat portit
– käytetään palomuurin lokia (IP-osoite ja ajankohta)
– sallitaan pakettien lähetys vain sallittuihin palveluihin
– toimitaan *stealth*-moodissa, eli palomuuri ei vastaa mitään hylättyihin paketteihin
– yhteys suljetaan kun sitä ei käytetä
– ilmoitukset yhteydenottoyrityksistä käyttäjälle / keskitettyyn hallintaan
– hallinnointisalasanat muutetaan oletusarvoista
– rajataan hallintayhteydet ja -mekanismit ja määritellään niihin liittyvät osoitteet
– huolehditaan säännöllisesti laitteisto- ja *firmware*-päivityksistä.

Todennettua, aktiivista valintayhteyttä viraston palvelujärjestelmiin ei missään oloissa saa ohjata edelleen toiselle yhteydelle.

Valintayhteyden käytön päättyessä käyttäjän tulee suorittaa asianmukainen uloskirjautuminen, eikä vain katkaista yhteyttä.

Etäkäyttäjän päätelaitteen verkkoliitäntä ei saa hyväksyä tulevia kutsuja, ellei sitä ole erikseen hyväksytty.

Päätelaitteelta uloslähtevät Internetin kautta kulkevat yhteydet ovat sallittuja vain jos ne on turvattu viraston määrittelemällä suojaustavalla.

Käyttäjä saa käyttää vain viraston hyväksymiä valinta- tai Internet-yhteyksiä. Kaiken etäkäyttäjän Internet liikenteen pitää kulkea viraston hyväksymän palomuurin kautta.

Kaikkia WLAN-verkossa olevia päätelaitteita tulee kohdella kuin ne olisivat Internetissä.

Pelkkä WEP-salaus ei riitä.

Kun IEEE802.11i-suositus valmistuu ja laitteet sitä tukevat, sen ominaisuuksia tulee hyödyntää soveltuvin osin.

WLAN-yhteyksillä on käytettävä salaavia yhteysmuotoja, esimerkiksi SSH:ta tai IPSEC-suositusten mukaista VPN-ratkaisua.S.

Vaikka WLAN-yhteydellä käytettäisiin salaavia yhteysmuotoja, verkon omia salaustoimintoja kannattaa myös käyttää.

WLAN- konfigurointi- ja käyttöohjeita:
– vaihdetaan hallinnointisalasanat
– nimetään verkko (SSID) tavalla, joka ei ole heti arvattavissa
– estetään pääsy WLANista muuhun verkkoon ilman käyttäjän todentamista
– käytetään verkossa MAC-tunnistusta
– estetään SSID broadcasting
– estetään SNMP-käyttö langattomasti
– rajataan hallintayhteydet ja määritellään hallintamekanismit ja osoitteet
– pidetään lokia verkon käytöstä.

Bluetoothin turvakäytännöt ovat vakiintumattomia ja riskit eivät vielä kaikin puolin ymmärrettyjä. Bluetooth-käyttöön tulee suhtautua varovaisesti.

5.4.3 Verkkoyhteyksien suojaamiseen liittyvät suositukset

Verkkoyhteyden suojaus on välttämätöntä paitsi käytettäessä kiinteää fyysistä yhteyttä tai valintayhteyksiä viraston omaan soittosarjaan. Näissäkin tapauksessa suojauksen käyttöä suositellaan.

Yleispätevä ratkaisu verkkoyhteyden suojaamiseen on VPN. Sen rinnalla voidaan käyttää selainkäytössä TLS:ää ja WTLS:ää, sekä erityiskäytössä SSH:ta.

VPN-yhteyttä ei tule pitää päällä muuten kuin yhteyttä aktiivisesti käytettäessä.

VPN-ratkaisun tulee olla IPSec-suosituksen mukainen.

SSL:stä tulee käyttää vain versiota 3.

Vanhaa SSH1:tä ei tule käyttää eikä tarjota.

SSH:ta käytettäessä on julkisten avainten välittäminen osapuolille hoidettava turvallisesti jotain muuta tiedonsiirtokanavaa käyttäen.

Viestien tai niiden osien erillistä salausta, digitaalisia allekirjoituksia tai aikaleimoja tulee tarvittaessa käyttää siirrettävien tietoaineistojen suojaamiseen, todentamiseen ja kiistämättömyyden aikaansaamiseen.

Suositeltava salausstandardi on AES. Myös 3DES tai Blowfish tulevat kysymykseen, DES-salausta ei tule käyttää.

Kaikkien verkkoyhteyden suojaustapojen yhteydessä tulee yhteys todentaa käyttäen jotain viraston etäkäyttöpolitiikan mukaista todentamistapaa.

Todentamispalvelimen tulee tukea viraston etäkäyttöpolitiikassaan määrittelemiä todentamistapoja.

VPN turvaa liikenteen, mutta riskinä on hyökkääjän pääsy jommastakummasta päästä sisään yhteyteen. Siksi on olennaista suojata myös kommunikoivat järjestelmät ja niiden verkkoliitännät.

5.4.4 Käyttäjien tunnistamiseen, todentamiseen ja pääsynvalvontaan liittyvät suositukset

Kaikki organisaatioon tulevat yhteydet tulee ohjata pääsynvalvontajärjestelmän kautta.

Kaikki etäkäytön pääsynvalvonta perustuu käyttäjien todentamiseen viraston etäkäyttöpolitiikassa määriteltyjä todentamismenetelmiä käyttäen.

Etäkäytön tunnistamis- ja todentamistarpeista huolehtii vaadittuja todentamismenetelmiä tukeva turvapalvelin.

Kaikki onnistuneet ja epäonnistuneet yhteydenottoyritykset tulee kirjata hyvin suojatun palvelimen lokiin.

Tunnistus- ja todentamispalvelimen ja pääsynvalvonnan taustalla on viraston yhtenäinen käyttäjä- ja käyttöoikeusrekisteri.

Käyttäjä- ja käyttöoikeusrekisterin suositeltu palvelurajapinta on LDAP. Muita kyseeseen tulevia rajapintoja ovat RADIUS ja ODBC/JDBC.

Teknisen tason (VPN-, TLS- tai SSH-yhteydet) todentaminen ja pääsynvalvonta sekä sovellustason pääsynvalvonta tulee pitää erillisinä toimintoina.

Kullekin etäkäyttöluokalle määritellään yksi tai useampia mahdollisia todentamistapoja.

Jos etäkäyttöluokka on tarkoitettu myös matkakäyttäjille, todentamistavoista ainakin yhden on oltava sellainen että se ei edellytä etäkäyttäjän päätelaitteelta mitään erityisvalmiuksia.

Käyttäjätunnus ja kiinteä salasana todentamismenetelmänä kelpaa vain julkisia aineistoja käsittelevien sovellusten käyttöön.

Suositeltuja todentamistapoja ovat matkapuhelimen käyttö (puhelinsoitto sekä kiinteä tai kertakäyttöinen tunnusluku) sekä PKI-varmenteet joko toimikortilla tai matkapuhelimessa vahvinta suojaa vaativia sovelluksia käytettäessä.

PKI-pohjaisessa todentamisessa tulee ottaa huomioon valtionhallinnon ohjeet ja säädökset virkamieskortista ja sähköisten varmenteiden käytöstä.[3]

5.4.5 Palvelujen verkkoliitännän suojaamiseen liittyvät suositukset

Etäkäytettävät palvelut tulee luokitella. Eri luokkiin kuuluvat palvelut eristetään segmentoimalla verkkoa ja suojaamalla segmenttejä palomuureilla.

Kaikki viraston ja sen etäkäyttäjien liikenne tulee ohjata viraston hyväksymän palomuurin kautta.

Palomuurin loki tulee kirjoittaa hyvin suojatulle palvelimelle.

Käyttäjien todennus ja viraston sovelluksiin pääsyn valvonta tapahtuu palvelujärjestelmien eteisessä, DMZ:lla.

VPN-yhteydet päätetään palomuuriin tai eteisverkossa olevaan VPN-palveluun, josta pääsee sovelluspalveluun vain tunnistautumalla ja palomuurin kautta.

VPN-yhteyttä tai muuta salattua yhteyttä ulkoverkosta palomuurin läpi suojaamattomaan sisäiseen palvelujärjestelmään ei pidä sallia, koska sitä voidaan käyttää porsaanreikänä sisäverkkoon.

Palvelinten sijoitteluperiaatteita:
– ulkoisia palveluja tarjoavat palvelimet sijoitetaan omalle suojatulle alueelleen (ulko-DMZ)
– sisäiset palvelimet sijoitetaan sisemmälle DMZ:lle
– palvelimet eristetään toisistaan palvelunestohyökkäysten varalta segmentoimalla verkkoa.

3 SM:n ohje Virkamiesten sähköisestä asiointikortista ja varmenteista (3.10.2000); Eduskunnan hallintovaliokunnan mietinnössä 25/2002 esitetty lausumaehdotus (11.2.2003); Laki henkilökorttilain muuttamisesta (11.4.2003)

Tunkeutumisen havainnointijärjestelmän (IDS) käyttöä palvelujärjestelmissä kannattaa harkita.

Reitittimien ja muiden tietoliikennelaitteiden ja ohjelmistojen sekä palomuurien konfiguroinnit pitää standardoida pyrkien mahdollisimman suureen yksinkertaisuuteen ja helppoon ylläpidettävyyteen.

Palvelun verkkoliitännän toteuttamisessa olennaisinta on järjestelmäkokonaisuuden huolellinen ja oikea suunnittelu. Se käsittää sallitun tietoliikenteen ja palvelujen käytön kuvaamisen ja rajaamisen, palvelinten tietoturvallisen pystyttämisen sekä palvelujärjestelmäympäristön tarkoituksenmukaisen fyysisen ja loogisen segmentoinnin.

5.5 Askel 4: Määritellään ja suunnitellaan etäkäytön keskitetty valvonta ja hallinta

Etäkäyttöön liittyvät riskit ovat sitä paremmin hallittavissa mitä paremmin on organisoitu etäkäytön keskitetty valvonta ja hallinta. Mitä heterogeenisempia etäkäyttäjien päätelaitekanta ja yhteysratkaisut ovat ja mitä enemmän suositelluista turvatoimista jää pelkästään käyttäjien omalle vastuulle, sitä heikommalla pohjalla riskien hallinta on.

Suuri osa etäkäytön keskitettyyn valvontaan ja hallintaan liittyvistä periaatteista on tullut esiin jo muiden turvallisen etäkäytön arkkitehtuurin komponenttien kohdalla esitetyissä suosituksissa. Näitä ovat päätelaitteiden etäkäyttökonfiguraatioiden määrittely ja hallinta, perus- ja suojausohjelmistojen säännöllisistä päivityksistä huolehtiminen, tietoliikenne- ja turvakomponenttien kuten henkilökohtaisten palomuurien valvonta ja päivitykset, etäkäyttäjien varmuuskopiointijärjestelyt, hyökkäysyritysten valvonta ja toiminta uhkien toteutuessa, etäkäyttäjätietojen ylläpito, todennusvälineiden (esim. toimikortit) hallinnointi ja logistiikan hoito, viraston palomuurien ja muiden suojausten ylläpito.

Virasto määrittelee itse tietoturvan tason tietoturvapolitiikassaan, mutta sen toteuttamiseen kannattaa käyttää apuvoimia, jos viraston oma osaaminen tietoturva-asioissa ei ole riittävää. Myös etäkäytön keskitetyn valvonnan ja hallinnan voi ulkoistaa Turvalliseen etäkäyttöön liittyy paljon erikoisasiantuntemusta, jolloin myös usealle virastolle yhteinen valvonta- ja hallintaorganisaatio voisi olla järkevä ratkaisu.

Suositukset

Toteutetaan etäkäyttäjien etäkäyttöratkaisujen keskitetty konfigurointi, asennus, valvonta ja hallinta koskien
– päätelaitteita ja niiden perusohjelmistoja
– päätelaitteilla käytettäviä suojausohjelmistoja
– varmuuskopiointijärjestelyjä
– tietoliikenneyhteyksiä.

Organisoidaan viraston etäkäyttöjärjestelmien valvonta ja ylläpito.

Organisoidaan etäkäyttäjien rekisteröinti, ohjeistus, käytön tuki ja valvonta.

Organisoidaan hyökkäysyritysten seuranta ja suunnitellaan toiminta viraston järjestelmiin murtautumisen tai muun hyökkäysuhkan toteutuessa.

Sovitaan etäkäyttöympäristön toteutukseen ja ylläpitoon osallistuvien ulkopuolisten organisaatioiden kanssa toimintaperiaatteista ja vastuunjaosta, ja valvotaan näiden toimintaa.

5.6 Muista myös nämä

Kuvattujen turvallisen etäkäytön periaatteiden toteuttaminen viimeistä piirtoa myöten ei tarkoita, että sen jälkeen etäkäytön turvallisuusriskit voidaan unohtaa. Mitkään käytännössä mahdolliset torjuntamenetelmät eivät anna sataprosenttista suojaa, vaan aina on olemassa **äärellinen jäännösriski**, jonka todennäköisyys pyritään minimoimaan suositelluilla torjuntakeinoilla.

Muista jäännösriski – älä tuudittaudu väärään turvallisuudentunteeseen.

Turvariskien minimoinnissa yleispätevä, hyvä periaate on **suojausten moninkertaisuus ja monitasoisuus**, ”*defence in depth*”. Missä on mahdollista käyttää samanaikaisesti useita suojausmekanismeja, niitä kannattaa myös käyttää.

Älä luota yhteen suojausmenetelmään, suojaa monitasoisesti.

Tietoturvallisuudesta vastaavan on tiedettävä mitä suojaukset kattavat ja mitä ne eivät kata, tuntematon on sama kuin suojaamaton.

Mitä et itse tiedä, sitä et tiedä.

Käytä tarvittaessa apunasi asiantuntijoita, jotka tietävät.

Mitä monimutkaisempi suojausratkaisu, sitä suurempi todennäköisyys sille, että se ei pysy hallinnassa, vaan pettää silloin, kun sitä tarvittaisiin.

Pyri mahdollisimman yksinkertaisiin, hallittavissa oleviin ratkaisuihin.

5.7 Yhteenveto turvallisen etäkäytön arkkitehtuurin toteuttamisesta

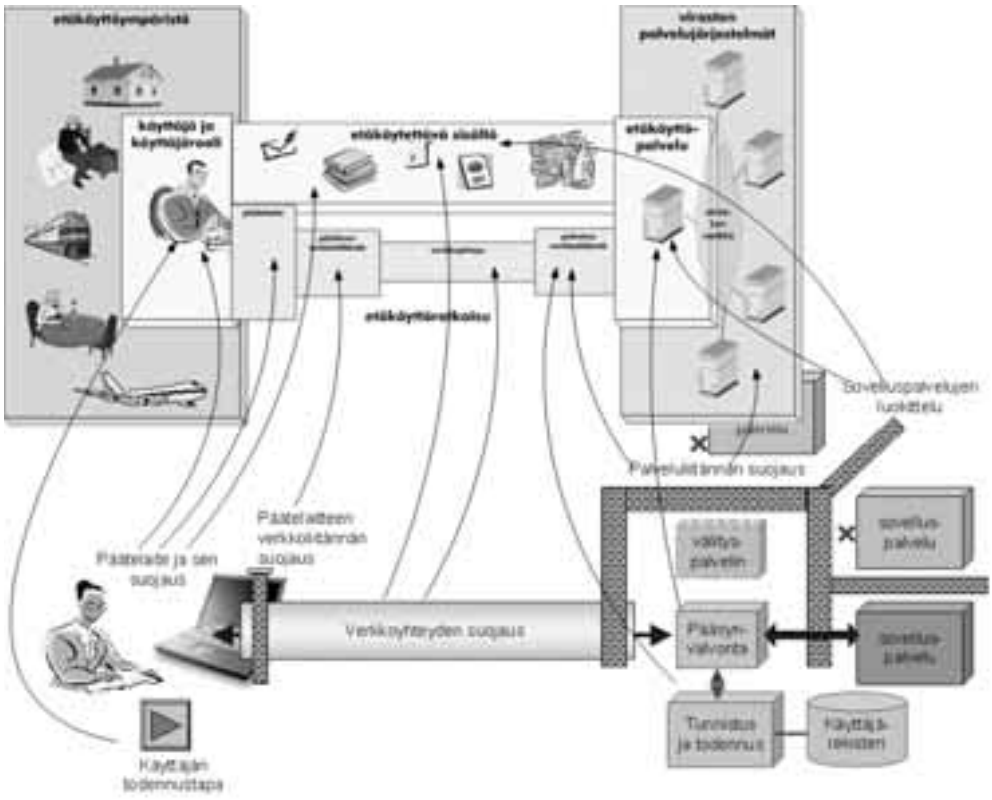
Kokonaispuitteet turvallisen etäkäytön arkkitehtuurille asettaa viraston **etäkäyttöpolitiikka**. Siinä määritellään viraston etäkäyttöä ohjaavat periaatteet ja käytännöt, jotka koskevat kaikkia etäkäytön toiminnallisen ympäristön osapuolia ja komponentteja. Tärkeä etäkäyttöpolitiikkaan liittyvä linjaus on viraston **sovelluspalvelujen luokittelu**, joka kertoo mitkä viraston sovelluksista ovat etäkäytön piirissä ja määrää edellytykset, joilla kuhunkin sovellukseen voidaan olla ulkoverkosta yhteydessä.

Etäkäyttöpolitiikan ohella toinen koko etäkäytön toiminnallista ympäristöä koskettava turvallisen etäkäytön arkkitehtuurin peruskivi on **etäkäytön keskitetty valvonta ja hallinta**. Se on väline, jonka avulla etäkäyttöpolitiikan noudattamista tuetaan ja valvotaan osittain teknisin, automatisoiduin välinein, osittain tukiorganisaation avulla.

Oheinen *kuva 12* pyrkii havainnollistamaan miten edellä esitetyin periaattein määritelty turvallisen etäkäytön arkkitehtuuri turvaa etäkäyttöympäristön. Kuvassa näkyvät nuolet osoittavat, mihin ympäristön komponentteihin liittyviin uhkiin turvallisen etäkäyttöarkkitehtuurin eri elementit tarjoavat suojaa.

Käyttäjälle välittömästi näkyviä ja hänen toimintaansa vaikuttavia turvallisen etäkäytön arkkitehtuurin elementtejä ovat **päätelaite ja sen suojaus**, **päätelaitteen verkkoliitännän suojaus**, **verkkoyhteyden suojaus** sekä **käyttäjän todentamistapa**. Viraston palvelujärjestelmissä toteutettavia turvallisen etäkäytön arkkitehtuurin elementtejä ovat **tunnistus- ja todentamispalvelu, pääsynvalvonta** sekä **palveluliitännän suojaus**.

Kuva 12 Turvallisen etäkäytön arkkitehtuurin elementit



5.8 Turvallisen etäkäytön arkkitehtuuri tietoturvallisuuden toteuttajana

Valtionhallinnon tietoturvallisuuskäsitteistössä (VAHTI 1/2000) on esitetty yleisesti käytetty tietoturvallisuuden kahdeksan toiminta-aluetta, jotka ovat **hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus**. *Taulukossa 3* esitetään, mihin tietoturvan toiminta-alueisiin elementit vaikuttavat (X = vaikuttaa, - = ei vaikuta).

Taulukko 3 Turvallisen etäkäytön arkkitehtuuri tietoturvallisuuden toteuttajana

	Hallinnollinen turvallisuus	Henkilöstö-turvallisuus	Fyysinen turvallisuus	Tietoliikenne-turvallisuus	Laitteisto-turvallisuus	Ohjelmisto-turvallisuus	Tietoaineisto-turvallisuus	Käyttö-turvallisuus
Päätelaite ja sen suojaus	–	–	X	X	X	X	X	X
Päätelaitteen verkkoliitännän suojaus	–	–	–	X	–	X	–	X
Verkkoyhteyden suojaus	–	–	–	X	–	–	X	X
Todennustapa	–	X	–	X	–	–	–	X
Tunnistus, todennus ja pääsynvalvonta	–	X	–	X	–	–	–	X
Palveluliitännän suojaus	–	–	–	X	–	X	–	X
Sovelluspalvelujen luokittelu	X	X	–	–	–	–	X	X
Etäkäyttöpolitiikka	X	X	X	X	X	X	X	X
Etäkäytön valvonta ja hallinta	X	X	–	X	–	X	–	X

6 ESIMERKKI SUOSITUSTEN TOTEUTTAMISESTA

Tässä luvussa kuvataan pelkistettynä esimerkkinä suositusten mukaisen etäkäyttöarkkitehtuurin toteuttamista.

6.1 Askel 1: etäkäyttöpolitiikan määrittely

Kaikki seuraavissa askeleissa tehtävät turvallisen etäkäytön arkkitehtuurin määrittelyyn liittyvät linjaukset ovat osa etäkäyttöpolitiikan toteutusta. Kokonaisuuden kannalta keskeisiä linjauksia ovat etäkäyttöpalvelujen luokittelu (askel 2) sekä päätökset siitä, mikä käyttö sallitaan muilta kuin viraston päätelaitteilta ja mitkä ovat viraston hyväksymät todentamistavat eri etäkäyttöluokissa (askel 3).

6.2 Askel 2: etäkäyttöpalvelujen luokittelu

Käytetään seuraavaa yksinkertaista hypoteettista etäkäyttösovellusten luokittelua. Tässä esitettyä luokittelua ei pidä ymmärtää suositeltavana malliluokitteluna. Se on keksitty vain havainnollistamaan esimerkkiä. Esimerkiksi sähköposti on hankala luokitella. Ohjeiden mukaan sähköpostilla ei salaamatta pidä lähettää luottamuksellista aineistoa, mutta vastaanottajan on mahdotonta kontrolloida tätä ja samoin hän voi saada kirjesalaisuuden piiriin kuuluvia yksityisviestejä. Kummankin lukeminen yleisellä paikalla voi johtaa tietojen joutumiseen vääriin käsiin.

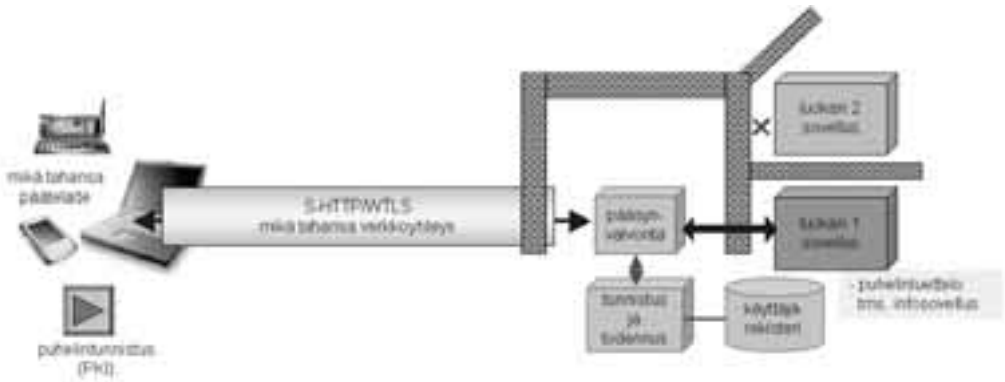
- Luokka 1: **Viestintäpalvelut**
  Tähän luetaan esimerkissämme sähköposti ja kalenteri, puhelinluettelo ja yleiset infosovellukset
- Luokka 2: **Luottamukselliset sovelluspalvelut**
  Tähän luetaan esimerkissämme viraston toimistosovelluspalvelut, kirjau-

tuminen sisäverkkoon, päätepalvelinkäyttö sekä muut luottamukselliset sovellukset

6.3 Askel 3: määritellään etäkäyttöluokkien hyväksyttävät etäkäyttöratkaisut

6.3.1 Luokan 1 etäkäyttöratkaisun minimivaatimukset

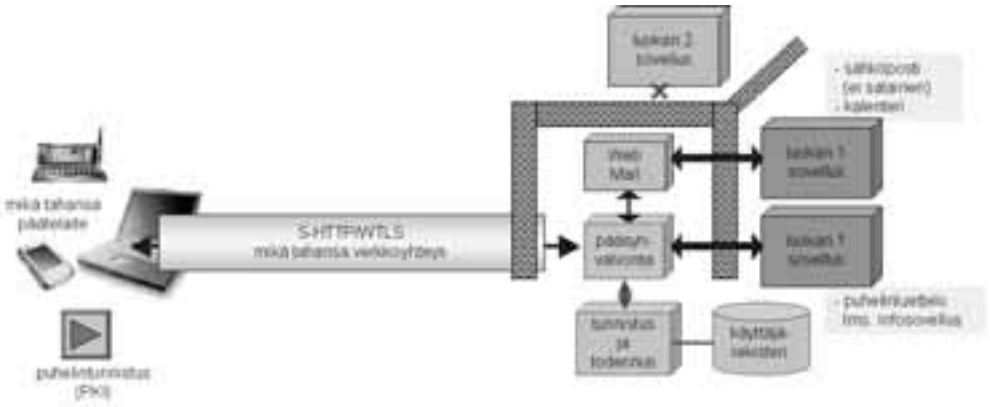
Kuva 13 Luokan 1 palvelujen vaatima etäkäyttöratkaisu



Kuva 13 esittää luokan 1 sovelluspalvelujen käytössä edellytettävää minimivaatimukset täyttävää etäkäyttöratkaisua.

Luokan 1 palveluja voidaan käyttää millä tahansa päätelaitteella oli se sitten viraston tai käyttäjän oma laite tai jokin julkinen pääte vaikkapa Internet-kahvilassa. Verkkoyhteys virastoon voi olla myös mitä tahansa, eli se voi kulkea Internetin kautta ja siihen voi sisältyä WLAN- tai Bluetooth-etappeja. Verkkoyhteydellä edellytetään kuitenkin käytettävän yhteyden salaavaa S-HTTP- tai WTLS-yhteyskäytäntöä, joka mahdollistaa viraston selainpohjaisten luokan 1 sovelluspalvelujen käytön. Käyttäjän todentamisessa perusvaatimus on puhelintunnistus käyttäjän matkapuhelimella. Vaihtoehtoisesti voidaan käyttää myös PKI-pohjaista todentamista käyttäjän virkamiesvarmenteella, jos käyttäjällä ja hänen käyttämällään päätelaitteella on siihen valmiudet. Viraston palvelujärjestelmät on suojattu palomuurilla ja palveluverkon segmentoinnilla.

Kuva 14 Luokan 1 palvelujen etäkäyttöratkaisu johon sisältyy posti- ja kalenterijärjestelmään pääsy web-posti -edustajärjestelmän kautta



Kuvan 13 mukainen ratkaisu ei sellaisenaan salli viraston sähköpostin ja kalenterin etäkäyttöä. Tämä voidaan mahdollistaa *kuvan 14* mukaisella ratkaisulla, jossa viraston eteisverkossa toimii sähköpostijärjestelmän web-posti –edustajärjestelmä, jota käytetään S-HTTP-/WTLS-yhteyskäytännöllä, ja jonka välityksellä käyttäjä kommunikoi viraston sähköpostijärjestelmän kanssa.

Tässä määritellyn luokan 1 etäkäyttöratkaisun minimivarustuksen soveltuvuus *luvussa 3.2* kuvattuihin peruskäyttötilanteisiin:

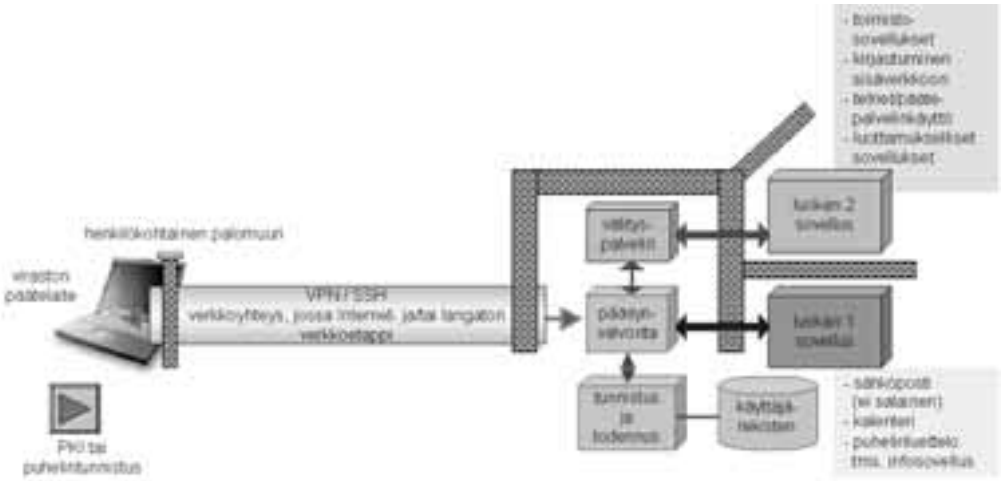
Käyttötilanne	**soveltuvuus**
Säännöllinen käyttö viraston päätelaitteella kiinteästä pisteestä (etätyö)	ei
Tilapäiskäyttö viraston päätelaitteella vaihtelevista pisteistä	OK
Tilapäiskäyttö muulla kuin viraston päätelaitteella	OK
Kumppanikäyttö	OK

6.3.2 Luokan 2 etäkäyttöratkaisun minimivaatimukset

Kuva 15 esittää luokan 2 sovelluspalvelujen käytössä edellytettävää minimiratkaisua siinä tapauksessa, että käytettävä verkkoyhteys kulkee Internetin kautta tai sisältää langattoman WLAN- tai Bluetooth-etapin. Päätelaitteen tulee olla viraston hallitsema ja siinä tulee olla henkilökohtainen palomuuri sekä VPN- tai SSH-valmiudet. Tämä rajaa päätelaitetyypit tätä kirjoitettaessa (kesä 2003) henkilökohtaisiin tietokoneisiin.

Käyttäjän todentaminen tapahtuu PKI-virkamiesvarmenteita tai vaihtoehtoisesti puhelintunnistusta käyttäen. Viraston palvelujärjestelmät on suojattu palomuurilla ja palveluverkon segmentoinnilla. Käyttäjällä on pääsy mihin tahansa viraston luokan 2 ja luokan 1 sovelluksiin.

Kuva 15 Luokan 2 palvelujen vaatima etäkäyttöratkaisu käytettäessä yleisiä verkkoyhteyksiä

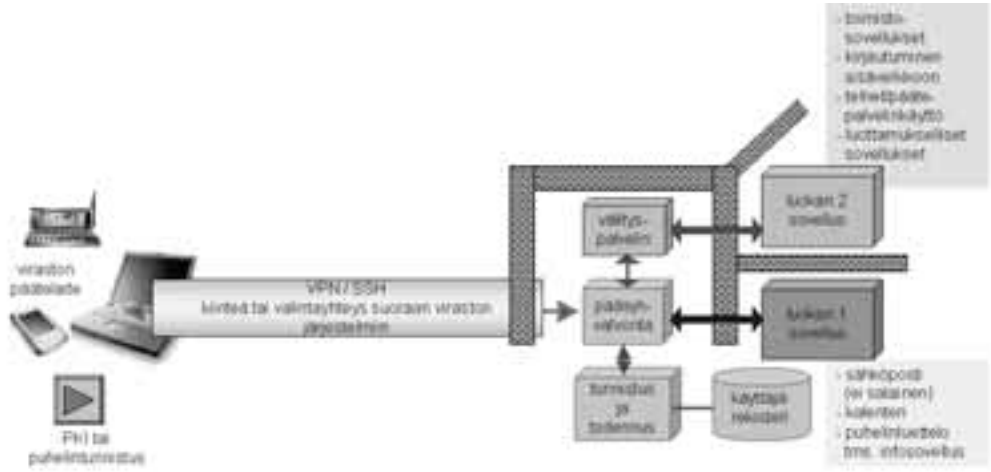


Tämän luokan 2 etäkäyttöratkaisun minimivarustuksen soveltuvuus luvussa 3.2 kuvattuihin peruskäyttötilanteisiin:

Käyttötilanne	**soveltuvuus**
Säännöllinen käyttö viraston päätelaitteella kiinteästä pisteestä (etätyö)	OK
Tilapäiskäyttö viraston päätelaitteella vaihtelevista pisteistä	OK
Tilapäiskäyttö muulla kuin viraston päätelaitteella	ei
Kumppanikäyttö	ei

Kuva 16 esittää luokan 2 käytössä tarvittavaa minimiratkaisua siinä tapauksessa, että käytettävä verkkoyhteys on kiinteä tai valintayhteys suoraan viraston järjestelmiin (so. siinä ei ole langattomia etappeja eikä se kulje Internetin kautta). Tässä tapauksessa vaadittava etäkäyttöratkaisu on muuten sama kuin edellä, paitsi että päätelaitteessa ei nyt tarvita henkilökohtaista palomuuria. Tämä lisää sallittujen päätelaitteiden valikoimaan PDA-laitteet ja älypuhelimet/kommunikaattorit, joille on saatavilla viraston käyttämän VPN-ratkaisun *client*-ohjelma.

Kuva 16 Luokan 2 palvelujen vaatiman etäkäyttöratkaisu käytettäessä viraston omia yhteyksiä



Tämän luokan 2 etäkäyttöratkaisun minimivarustuksen soveltuvuus luvussa 3.2 kuvattuihin peruskäyttötilanteisiin:

Käyttötilanne	**soveltuvuus**
Säännöllinen käyttö viraston päätelaitteella kiinteästä pisteestä (etätyö)	OK
Tilapäiskäyttö viraston päätelaitteella vaihtelevista pisteistä	OK
Tilapäiskäyttö muulla kuin viraston päätelaitteella	ei
Kumppanikäyttö	ei

LYHENTEITÄ JA TEKNISIÄ TERMEJÄ

Oheiseen luetteloon on koottu Turvallinen etäkäyttö -raportissa mainitut lyhenteet ja tekniset termit sekä niiden lyhyet selitykset. Jotkut selityksistä pohjautuvat joko suoraan tai hieman muutettuna *VAHTI-tietoturvasanastoon* (VAHTI 1/2000) tai *Valtionhallinnon etätyön tietoturvallisuusohjeen* (VAHTI 3/2002) liitteen 4 sanastoon. Suurin osa selityksistä on kuitenkin tätä tarkoitusta varten tehtyjä joko siksi, että em. lähteissä ei ko. lyhenteitä/termejä lainkaan esiinny, tai niille siellä annettu määritelmä ei toimi parhaalla mahdollisella tavalla tässä yhteydessä. Annetut selitykset eivät pyri olemaan asioiden tarkkoja määritelmiä, vaan epämuodollisempia luonnehdintoja. Liitteessä selitetyt lyhenteet ja termit on lihavoitu silloin kun niitä on käytetty toisten selityksissä.

2G, 3G	Matkapuhelintekniikoiden sukupolvia. **GSM** luetaan toiseen sukupolveen (2G), **UMTS** kolmanteen (3G).
3DES	**DES**-salakirjoitusmenetelmän kehittyneempi versio, joka käyttää 168 bitin pituista avainta, ja jonka turvallisuudesta ollaan montaa mieltä. Hidas.
ACL	*Access Control List* = pääsynvalvontalista. Tietojoukko, joka määrittelee käyttäjän pääsyoikeudet johonkin järjestelmään tai johonkin objektiin liittyvät käyttöoikeudet.
Active-X	**Aktiivikomponentti**, joka on Windows-käyttöjärjestelmän laajennus, käyttöjärjestelmässä täysillä oikeuksilla suoritettava ohjelma. Active X-komponenttien noutaminen verkosta tuo mukanaan suuria tietoturvallisuusriskejä.
ADSL	*Asymmetric Digital Subscriber Line*. Tällä hetkellä (2003) Suomessa yleisimmin käytetty **DSL**-tekniikka.
AES	*Advanced Encryption Standard*. Belgiassa kehitetty symmetrinen standardoitu lohkosalausmenetelmä, jota USAn hallitus on v. 2000 lähtien suositellut käytettäväksi **DES**-standardin sijasta.
aktiivikomponentti	Ohjelman muodossa tai toisessa sisältävä komponentti, joka sisältyy web-sivulle tai muuhun dokumenttiin. Komponentin sisältävä ohjelma voi olla hyödyllinen dokumentin käsittelyssä, mutta voi olla myös vahinkoa aiheuttava haittaohjelma, mistä syystä verkosta vastaanotettaviin aktiivi-

	komponentteihin tulee suhtautua terveen epäluuloisesti.
ATM	*Asynchronous Transfer Mode*. Digitaalinen verkkoteknologia, jossa tieto siirretään pieninä, kiinteämittaisina paketteina.
biometrinen tunnistus	Ihmisen fyysiseen ominaisuuteen, kuten sormenjälki, käden muoto, verkkokalvo, ääni, perustuva tunnistus.
BIOS	*Basic Input/Output System*. Mm. tietokoneen käynnistyksen mahdollistava käyttöjärjestelmän perusosa, joka useimmiten on sijoitettu aina saatavilla olevaan lukumuistiin (ROM).
Blowfish	Symmetrinen lohkosalausmenetelmä, jota suositellaan käytettäväksi vähintään 256-bitin avainpituudella.
Bluetooth	Lyhyen kantaman langaton tekniikka, joka on tarkoitettu esim. samassa työpisteessä olevien tai käyttäjän mukanaan kuljettamien laitteiden väliseen kommunikointiin.
cookie	= kuitti, eväste. Internet-verkossa palvelimen verkkoaseman web-selaimelle lähettämä merkkijono, jonka avulla palvelin, tai sovelluksesta riippuen jokin toinen palvelin, ylläpitää yhteyttä selaimeen.
CSD	*Circuit-Switched Data*. Piirikytkentäinen tiedonsiirto GSM-verkossa. Nopeus 9.6 kbit/s.
DES	*Data Encryption Standard*. 56-bittiseen avaimeen perustuva symmetrinen standardoitu salausalgoritmi, jonka käyttöä ei enää suositella.
DMZ	*Demilitarized Zone* = eteinen. **Palomuurin** muista verkkolohkoista eristämä verkkolohko, johon voidaan sijoittaa esimerkiksi organisaation ulkoisia palveluja tai liikennettä sisäverkkoon hoitavia **välityspalvelimia**.
DNS	*Domain Name System*. Tietoverkoissa käytetty aluenimijärjestelmä ja -palvelu, joka muuttaa verkkonimet **IP**-osoitteiksi ja päinvastoin.
DSL	*Digital Subscriber Line*. Yleisnimitys siirtotekniikoille, joita käyttäen tavalliselle puhelintilaajajohdolle voidaan toteuttaa laajakaistainen (jopa useita kymmeniä Mbit/s) tiedonsiirtoyhteys. Käytännön toteutustekniikoita ovat mm. **ADSL**, SDSL, VDSL.

eteinen	ks. **DMZ**
eväste	kuitti, ks. **cookie**
federoitu verkko-identiteetti	*Federated Network Identity*. Mm. **Liberty Alliancen** ajama käyttäjien **tunnistamiseen** ja **todentamiseen** liittyvä toimintamalli, jossa eri palveluntarjoajien järjestelmissä olevat **käyttäjän identiteettitiedot** on kytketty käyttäjän valvomalla tavalla yhtenäiseksi, ”federoiduksi” verkko-identiteetiksi.
firewall	ks. **palomuuri**
firmware	Tietoteknisen laitteen lukumuistiin kirjoitettu ohjelma.
flash-muisti	Tietojen uudelleenkirjoittamisen mahdollistava pysyväismuistitekniikka.
frame relay	Pakettivälitteinen laajakaistaisten televerkkoyhteyksien toteutustekniikka
FTP	*File Transfer Protocol*. **TCP/IP**-pohjainen standardoitu tiedostosiirtokäytäntö.
GPRS	*General Packet Radio Service*. **GSM**-verkkojen pakettivälitteinen tiedonsiirtoteknologia, joka mahdollistaa teoriassa jopa 115 kbit/s siirtonopeuden.
GSM	*Global System for Mobile Communications*. Euroopassa ja laajalti muuallakin maailmassa käytössä oleva matkapuhelinverkkostandardi.
HSCD	*High-Speed Circuit-Switched Data*. **GSM**-verkon piirikytkentäisen tiedonsiirtoteknologian laajennus, joka mahdollistaa jopa 43.5 kbit/s siirtonopeuden.
HTML	*Hypertext Mark-up Language.* Internetin selainsovellusten dokumenttien määrittelykieli.
HTTP	*Hypertext Transfer Protocol*. **IETF**:n määrittelemä Internet-selainkäytön yhteyskäytäntö. HTTP:n **TLS**-salaukselle varustettu versio on S-HTTP.
IDS	*Intrusion Detection System* = tunkeutumisen havainnointijärjestelmä. Järjestelmä, joka pyrkii havaitsemaan tunkeutumisyritykset palvelujärjestelmään tarkkailemalla sisääntulevaa liikennettä.

IEEE	*Institute for Electrical and Electronics Engineers*. Organisaatio, jonka laatimat standardit ovat levinneet laajaan käyttöön erityisesti lähiverkkojen toteutuksessa (IEEE 802 -standardiperhe).
IETF	*Internet Engineering Task Force.* Internet-suosituksista ja standardeista ensisijaisesti vastaava elin.
IMAP	*Internet Message Access Protocol*. Käyttäjän päätelaitteen ja sähköpostijärjestelmän välinen salaamaton yhteyskäytäntö, jonka nykyisin käytössä oleva versio on 4 (IMAP4).
IP	*Internet Protocol.* Internetin verkkokerroksen standardi yhteyskäytäntö.
IPSec	*Internet Protocol Security*. **IETF**-suositus **IP**-verkon liikenteen suojaamiseksi pakettitasolla käyttämällä salaustekniikkaa.
ISDN	*Integrated Services Digital Network*. Televerkkostandardi, jonka pohjalta nykyinen puhelinverkko on enimmäkseen toteutettu.
IT	*Information Technology* = tietotekniikka
Java Applet	Java-ohjelmointikielellä laadittu **aktiivikomponentti**, joka usein ladataan verkosta päätelaitteella suoritettavaksi.
JavaScript	Makro-/komentokieli, jota käytetään yleisesti **HTML**-sivuilla toteuttamaan **aktiivikomponentteja** esimerkiksi suorittamaan tarkistusrutiineita.
JDBC	*Java Database Connectivity*. **ODBC**:n Java-kieliseen ympäristöön sovitettu tietojen saantikäytäntö.
julkisen avaimen järjestelmä	ks. **PKI**
kertakirjautuminen	ks. **SSO**
kommunikaattori	**Älypuhelin**, erityisesti Nokian 9000-sarjan laitteista käytetty nimitys.
kuitti	eväste, ks. **cookie**
kämmentietokone	ks. **PDA**
LDAP	*Lightweight Directory Access Protocol*. Internet-ympäristöön sovitettu ja yksinkertaistettu versio standardoidusta

	X.500-yhteyskäytännöstä, jota käytetään tietojen hakuun tietohakemistoista.
Liberty Alliance	Sun Microsystemsin aloitteesta syntynyt avoin noin 150 yrityksen yhteisö, joka kehittää ja julkaisee ns. federoituun todentamismalliin perustuvia todentamissuosituksia.
MAC-tunnistus	Lähiverkossa olevan laitteen fyysiseen, yksiselitteiseen verkko-osoitteeseen perustuva päätelaitteen tunnistustapa.
MMS	*Multi-Media Message Service*. **WAP**-yhteyskäytäntöihin nojautuva mobiiliverkkojen palvelu, joka mahdollistaa monimediaviestien välittämisen.
MPLS	*Multi-Protocol Label Switching*. **IETF**:n määrittelemä siirtoyhteys- ja verkkokerroksen käytäntö, joka antaa teleoperaattorille entistä monipuolisemmat mahdollisuudet hallinnoida **IP**-pohjaista liikennettä verkossaan.
ODBC	*Open Database Connectivity*. Tietojen standardoitu, toimittajariippumaton saantimenetelmä.
palomuuri	Järjestelmä, joka on suunniteltu estämään luvaton ja asiaton liikenne verkosta tai verkkosegmentistä toiseen. Usein palomuurin päätehtävä on toteuttaa suojamuuri Internetin tai muun avoimen verkon ja organisaation sisäisen suljetun verkon välille. Palomuuritekniikka perustuu muurin läpi kumpaankin suuntaan kulkevan liikenteen suodattamiseen edeltä määriteltyjen sääntöjen mukaisesti. Vain luvalliset paketit päästetään läpi, muut hylätään.
PDA	*Personal Digital Assistant* = kämmentietokone. Alun perin lähinnä henkilökohtaisen ajankäytön hallintaan ja muistiokäyttöön suunniteltu laitekonsepti, joka on kehittymässä yhtäältä täysiverisen PC-laitteen ja toisaalta viestimen suuntaan.
PIN	*Personal Identification Number*. Henkilön yksilöimiseksi tai tietojärjestelmän käyttöoikeuden varmistamiseksi käytettävä tunnus, koodi tai salasana.
PKI	*Public Key Infrastucture* = julkisen avaimen järjestelmä. Epäsymmetriseen salaukseen perustuva infrastruktuuri, joka mahdollistaa osapuolten luotettavan todentamisen sekä siirrettävän tiedon luottamuksellisuuden, eheyden ja kiistämättömyyden.

plug-in	Laitteistoon tai ohjelmistoon helposti kytkettävissä oleva sen toiminnallisuutta laajentava moduuli.
Pocket PC	Microsoftin Windows-käyttöjärjestelmän kämmentietokoneille tarkoitettua versiota käyttävien **PDA**-laitteiden yleisnimitys.
POP	*Post Office Protocol*. Käyttäjän päätelaitteen ja sähköpostijärjestelmän välinen salaamaton yhteyskäytäntö, jonka nykyisin käytössä oleva versio on 3 (POP3).
proxy	= välipalvelin, välityspalvelin. Tietoverkon ja paikallisen järjestelmän välissä oleva palvelin, joka voi toimia esimerkiksi tietojen hakua nopeuttavana välivarastona tai turvapalvelimena.
pääsynvalvontalista	ks. **ACL**
RADIUS	*Remote Authentication Dial-in User Services*. Tietoverkoissa yleisesti käytetty todennuskäytäntö, joka ei ole varsinainen standardi, mutta kuitenkin **IETF**:n ylläpitämä.
reverse proxy	**Välityspalvelin**, joka piilottaa taustallaan olevien palvelinten verkkoidentiteetin ja näkyvyyden käyttäjille. Nimitystä käytetään erottamaan ko. **proxy** ”*forward proxy*”:sta, joka piilottaa palvelimelta niitä käyttävien käyttäjien verkkonäkyvyyden.
SecurID	RSA-yhtiön tavaramerkki ja yleisesti käytetty haaste-vaste todennusmenetelmään perustuva tuote.
S-HTTP	**HTTP**-yhteyskäytännön **TLS**-turvakäytäännön avulla suojattu versio. S-HTTP-käytäntöä vaativan web-sivun tunnus alkaa “https:”.
SIM	*Subscriber Identity Module*. Pienikokoinen toimikortti, joka sisältää **GSM**-puhelinliittymän tunnistustiedot.
SMS	*Short Message Service*. **GSM**-verkon tarjoama lyhytviestipalvelu.
SMTP	*Simple Mail Transfer Protocol*. Internetin sähköpostipalvelinten välisessä tiedonvälityksessä käytetty standardi yhteyskäytäntö.
SNMP	*Simple Network Management Protocol*. Standardoitu verkonhallintayhteyskäytäntö.

SOAP	*Simple Object Access Protocol*. Kevyt, **XML**-pohjainen yhteyskäytäntö, joka on yksi **Web Services** –standardien peruskivistä.
spoofing	= tekeytyminen. Tietojärjestelmän harhauttaminen pitämään väärää käyttäjää oikeana.
spyware	= vakoiluohjelmisto. Ohjelmisto, joka asentuu päätelaitteelle ja seuraa päätelaitteen käyttäjän verkkokäyttäytymistä käyttäjän tietämättä ja raportoi siitä esim. markkinatietoja keräävälle yritykselle.
SSH	*Secure shell*. Suomessa kehitetty suojattu yhteyskäytäntö, joka perustuu hybridisalaukseen.
SSID	*Service Set Identifier*. 32-merkkinen **WLAN**in tunniste, joka toimii tunnussanana kun **WLAN**-käyttäjä kytkeytyy verkkoon.
SSL	*Secure Sockets Layer*. Netscape-yhtiön kehittämä yhteyskäytäntö, jossa salaista avainta käyttämällä luodaan turvallinen tiedonsiirtoyhteys **TCP/IP**-verkossa. Ks. myös **TLS**.
SSO	*Single Sign-On* = kertakirjautuminen. Menettely, jossa käyttäjä järjestelmään kirjautumalla pääsee käyttöoikeuksiensa puitteissa ilman eri kirjautumista järjestelmän piirissä oleviin muihin sovelluksiin/-resursseihin
stealth-moodi	**Palomuurin** toimintatapa, jossa hylättyihin paketteihin ei reagoida mitenkään, jolloin niiden lähettäjä ei tiedä, onko niiden aiottua kohdetta olemassakaan.
SWIM	**GSM**-puhelimen **SIM**-kortti, jolle on integroitu **WIM**-toiminnallisuus.
Symbian	Matka- ja älypuhelinten standardoitu käyttöjärjestelmä.
TACACS/TACACS+	*Terminal Access Controller Access Control System*. TACACS on Unix-ympäristöissä laajasti käytetty standardoitu todentamiskäytäntö, jonka uudempi TACACS+-versio vastaa toiminnallisesti **RADIUS**-käytäntöä.
TCP	**Transport Control Protocol**. Internetin kuljetuskerroksen standardi yhteyskäytäntö.
tekeytyminen	ks. **spoofing**

telnet	**TCP/IP**-pohjainen **IETF**:n yhteyskäytäntösuositus päätekäyttöön.
TLS	*Transport Layer Security*. **SSL**-yhteyskäytäntöön perustuva, siitä edelleen kehitetty yhteyskäytäntösuositus, jonka versio 1.0 vastaa toiminnallisesti SSL v.3.0:aa.
tunkeutumisen havainnointijärjestelmä	ks. **IDS**
UMTS	*Universal Mobile Telecommunications System*. Mobiiliverkkojen tulevan sukupolven (**3G**) yleisnimi ja teknologia.
vakoiluohjelmisto	ks. **spyware**
VLAN	*Virtual Local Area Network* = virtuaalinen lähiverkko. Yhteen fyysiseen lähiverkkoon muodostettu looginen verkkosegmentti.
VPN	*Virtual Private Network*, suojaverkko. Avoimeen verkkoon tiettyjen käyttäjien välille muodostettu suljettu verkko, jonka sisäisessä liikenteessä käytetään salakirjoitusta ja käyttäjän todennusta, joten se säilyy luottamuksellisena muilta avoimen verkon käyttäjiltä. Tässä raportissa ja yleensä myös jokapäiväisessä puheessa VPN:llä tarkoitetaan **IPSec**-suosituksiin perustuvaa suojaverkkoa.
välityspalvelin, välipalvelin	ks. **proxy**
WAP	*Wireless Application Protocol*. Langattoman kommunikoinnin standardiperhe, jonka lähtökohtana on ollut Internetin **HTML**-selainteknologian sovittaminen matkapuhelinlaitteille.
web-postipalvelin	Palvelin, joka tarjoaa käyttäjille selainpohjaisen liittymän organisaation sähköpostiin.
Web Services	Yleisnimitys standardointihankkeelle, jonka tavoitteena on mahdollistaa Internet-ympäristön sovellusten helppo integrointi. Web Services –perusstandardeja ovat **XML**, **SOAP** ja **WSDL**.
WEP	*Wired Equivalent Privacy*. **IEEE** 802.11b –standardissa määritelty turvaton **WLAN**-verkon suojausmenetelmä.

Wi-Fi Alliance	Yli kahdensadan organisaation muodostama yhteenliittymä, jonka tavoitteena on edistää **IEEE** 802.11 –standardeihin pohjautuvien **WLAN**-verkkojen toimittajariippumatonta käyttöä.
WIM	*Wireless Identity Module*. **WAP**-ympäristössä käytettäväksi tarkoitettu turvamoduuli, joka mahdollistaa **PKI**-pohjaisten turvatoimintojen (todentaminen, sähköinen allekirjoitus) käytön. WIM voi periaatteessa olla integroitu matkapuhelinlaitteistoon, erillinen puhelimeen asetettava toimikortti tai integroitu **GSM**-puhelimen **SIM**-kortille.
Windows-päätepalvelin	Palvelin, jonka välityksellä voidaan käyttää Windows-sovelluksia tarvitsematta asentaa niitä käyttäjän laitteelle.
WLAN	*Wireless Local Area Network* = langaton lähiverkko. Radiotekniikkaan perustuva lähiverkko, jonka toteutus useimmiten perustuu **IEEE** 802.11 –standardiperheeseen.
WTLS	*Wireless transport Layer Security.* **TLS**:ää toiminnallisesti vastaava **WAP**-mobiililaitteiden käyttöön tarkoitettu yhteyskäytäntö.
WPA	*Wi-Fi Protected Access*. **Wi-Fi Allianssin** määrittelemä **IEEE** 802.11 **WLAN**-ympäristön tilapäisluonteinen suojausmääritys, jolla paikataan **WEP**in puutteita monitoimittajaympäristössä yhteensopivalla tavalla.
WSDL	*Web Service Description Language*. **XML**-pohjainen kieli, jolla **Web Services** –ympäristössä määritellään kommunikoivan osapuolen toiminnallisuus.
WTLS	*Wireless Transport Layer Security*. **TLS**-suositusta langattomien mobiililaitteiden kommunikoinnissa vastaava standardi.
YPV	yleinen puhelinverkko
XML	*Extensible Mark-up Language*. Merkkipohjainen kuvauskieli, joka on Internetissä käytettyjen dokumentti- ja tietomääritysten ja yhä laajemmin yleisemminkin erilaisten tietomääritysten standardi.
älypuhelin	Matkapuhelin, jolla on **PDA-**ominaisuudet ja jossa on mahdollisuus asentaa ja ajaa erillisiä sovellusohjelmia.

LÄHTEITÄ

Etäylläpitoyhteydet Teknillisessä korkeakoulussa
HTKK:n Määräys 25.4.03

Laki henkilökorttilain muuttamisesta (11.4.2003)

Fujitsu Invian asiantuntijat (maalis-huhtikuu 2003)

Eduskunnan hallintovaliokunnan mietintö 25/2002 (11.2.2003)

VTT:n tietoliikennestrategia 2003-2007, v.0.89 (3.2.2003)

Valtionhallinnon etätyön tietoturvallisuusohje (VAHTI 3/2002)

Wireless Network Security: 802.11, Bluetooth and Handheld Devices
Recommendations of the National Institute of Standards and Technology (November 2002)

Mobile Security Exposures, Trends and Remedies
Gartner Research, SPA-18-6438 (21.11.2002)

Wireless LANs: An Overview
Gartner Research, DPRO-89978 (17.10.2002)

Kenneth Forward: Appropriate Use of Network Encryption Technologies (20.9.2002)
SANS Institute Reading Room, http://www.sans.org/rr/encryption/appropriate.php

Security for Telecommuting and Broadband Communications *Recommendations of the National Institute of Standards and Technology* (August 2002)

Rik Farrow: VPN Vulnerabilities
Network Magazine 5.6.2002, http://www.networkmagazine.com/article/NMG20020603S0004

Bluetooth Wireless Technology: An Overview
Gartner Research, DPRO-91115 (18.4.2002)

Al Maslowski-Yerges: Securing the Enterprise from the Dangers of Remote Access: Analysis of New Options Available for Personal Firewall Management in Comparison with Other Established and Emerging Remote Access Solutions (27.3.2002)
SANS Institute Reading Room, http://www.sans.org/rr/telecom/dangers.php

Telework Project (ITSPSR-14)
Governement of Canada, Communications Security Establishment CSE (March 2002)
http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/product_reports/TeleworkProject_e.pdf

Guidelines on Firewalls and Firewall Policy
Recommendations of the National Institute of Standards and Technology (January 2002)

Underlying Technical Models for Information Technology Security
Recommendations of the National Institute of Standards and Technology (December 2001)

James Babcock Hughes: Road Warriors: Protecting Them from the Wolves - and the Organization from Them (18.12.2001)
SANS Institute Reading Room, http://www.sans.org/rr/telecom/warriors.php

Christopher Smith: IPsec's Role in Network Security: Past, Present, Future (17.9.2001)
SANS Institute Reading Room, http://www.sans.org/rr/encryption/ipsecs_role.php

Gordon Jenkins: Mitigating Teleworking Risks (28.8.2001)
SANS Institute Reading Room, http://www.sans.org/rr/telecom/telework.php

Deploying Safe Wireless LANs
Gartner Research, DF-13-8250 (5.7.2001)

Chris Mahn: Three Tiered DMZ's (21.5.2001)
SANS Institute Reading Room, http://www.sans.org/rr/firewall/3_tiered.php

Ohje virkamiesten sähköisestä asiointikortista ja varmenteista
SM (3.10.2000)

Sharon Gaudin: VPN Vulnerability
Network World 14.8.2000, http://www.nwfusion.com/research/2000/0814featsidethree.html

Security Risks in Telecommuting
F-Secure Corporation White Paper (April 2000)

Practices for Protecting Information Resources Assets
State of Texas, Department of Information Resources (March 2000)
http://www.dir.state.tx.us/IRAPC/practices/

Recommendations for the Protection against Distributed Denial-of-Service Attacks in the Internet

Bundesamt für Sicherheit in der Informationstechnik (2000)
http://www.bsi.bund.de/taskforce/ddos_en.htm

Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje
VM 19.1.2000

Key Policies and Procedures for Managing Telework: A Summary Based on the Practices of Exemplary Telework Organizations
Telework Consortium, http://www.teleworkconsortium.org/Theory_and_Practice/policy_issues.asp

Security Issues for Telecommuting
http://www.itl.nist.gov/lab/bulletns/archives/telecomm.htm

Lueteltujen lähdedokumenttien lisäksi aiheeseen liittyviä suosituksia ja kirjallisuutta löytyy mm. seuraavista lähteistä:

- **Valtionhallinnon tietoturvallisuusohjeet**
  http://www.vm.fi/vahti
- **NIST (*National Institue of Standards and Technology*) Computer Security Resource Center (CSRC)**
  http://csrc.nist.gov/
- **SANS (*SysAdmin, Audit, Network, Security*) Institute**n web-sivut, erityisesti *Reading Room*, josta löytyy yli 1300 artikkelia tietoturvallisuuden eri osa-alueilta
  http://www.sans.org/rr/

LIITE 3

Valtiovarainministeriön ja VAHTIn tietoturvallisuusohjeistoa

- Suositus turvallisen etäkäytön arkkitehtuurista, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuuusohje, VAHTI 1/2003
- Arkaluonteisten kansainvälisten aineistojen käsittelyohje, VAHTI 4/2002
- Etätyön tietoturvaohje, VAHTI 3/2002
- Tunnistamisperiaatteet valtionhallinnon verkkopalveluissa, VM 27/01/2002
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Tietotekniikan turvallisuus ja toiminnan varmistaminen, VM ja PTS, 2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Tietotekniikkahankintojen tietoturvallisuustarkistuslista, VAHTI 6/2001
- Sähköpostin ja lokitietojen käsittely, VAHTI 5/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmistoilta suojautumisen yleisohje, VAHTI 4/2000
- Tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtion tietoaineistojen käsittelyn tietoturvaohje, VAHTI 2/2000
- Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 1/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 5/01/2000
- Tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 1/01/1999, 31.12.1998
- Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, VAHTI 2/1997

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

2/2003

TURVALLINEN ETÄKÄYTTÖ TURVATTOMISTA VERKOISTA

ISSN 1455-2566
ISBN 951-804-395-7