VALTIOVARAINMINISTERIÖ

Älypuhelimien tietoturvallisuus – hyvät käytännöt

2007

2/2007 VAHTI

VALTIOVARAINMINISTERIÖ

Älypuhelimien tietoturvallisuus – hyvät käytännöt

2/2007 VAHTI

Taitto: Taina Ståhl
Kannen kuva: www.nokia.com, Press kuva-arkisto

ISBN 978-951-804-761-5 (nid.)
ISBN 978-951-804-762-2 (pdf)
ISSN 1455-2566
Painopaikka Edita Prima Oy
Helsinki 2007

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 39/01/2007

OHJE
15.11.2007

Ministeriöille, virastoille ja laitoksille

ÄLYPUHELIMIEN TIETOTURVALLISUUS - HYVÄT KÄYTÄNNÖT

Valtiovarainministeriön ohessa antaman tietoturvaohjeen (jäljempänä ohje) tavoitteena on edistää ja tukea älypuhelimien tietoturvallista käyttöä. Ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjauksessa ja alaisuudessa. Ohje täydentää laajaa VAHTI-ohjeistoa.

Ohje on tarkoitettu organisaatioiden johdolle ja kaikille niille henkilöille, jotka vastaavat organisaation älypuhelimiin liittyvistä toiminnoista.

Älypuhelimien hallinnointi edellyttää selkeää elinkaarenhallintaa ja vastaavanlaisia prosesseja kuin työasemien hallinnointi. Elinkaarenhallinta kattaa elinkaaren kaikki vaiheet käyttötarvesuunnitelmasta kierrätykseen ja tietoturvalliseen hävittämiseen.

Tietoturvallisuuden varmistamiseksi ja kustannusten hallitsemiseksi älypuhelimien käytön tulee perustua huolelliseen etukäteissuunnitteluun sekä tietoturvallisuuden jatkuvaan kehittämiseen ja tietoturvatietoisuuden lisäämiseen.

Ohjeessa kuvataan suositeltavia hyviä käytäntöjä, joilla ehkäistään tietoturvaongelmia ja pienennetään tietoturvariskejä. Ohjeeseen sisältyy mm. älypuhelinlaitteen suojaamisen hyviä käytäntöjä laitteen fyysisen turvallisuuden, haittaohjelmatorjunnan, tietoliikenneyhteyksien ja etähallinnan osalta.

Ohje ja sen liitteet tulevat VAHTIn Internet-sivuille (www.vm.fi/vahti). Ohjetta kehitetään tarvittaessa muun muassa saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää ja tietoturvapäällikkö Kari Keskitalo (sähköpostit: etunimi.sukunimi@vm.fi)

Hallinto- ja kuntaministeri — Mari Kiviniemi

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: Älypuhelimien tietoturvallisuus – hyvät käytännöt (VAHTI 2/2007)

Esipuhe

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTIn käsittelyn kohteina ovat kaikki tietoturvallisuuden osa-alueet.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (http://www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on valmistellut, ohjannut ja toteuttanut valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta.

VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on saanut kolmena perättäisenä vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

Tämän ohjeen on laatinut VAHTIn alainen älypuhelimien tietoturvallisuus – työryhmä. Ohje on viimeistelty laajan lausuntokierroksen palautteen pohjalta ja hyväksytty julkaistavaksi VAHTIn kokouksessa lokakuussa 2007.

Johdon yhteenveto

Älypuhelimet ovat yleistyneet valtionhallinnossa muutamassa vuodessa siten, että niistä on tullut merkittävä työtapoja muuttava teknologiaratkaisu. Älypuhelimet mahdollistavat ajasta ja paikasta riippumattoman käytön tyypillisesti organisaation sähköpostiin, kalenteriin, yhteystietoihin sekä joissain tapauksissa myös esimerkiksi intranet- tai muihin www-palveluihin. Tulevaisuudessa älypuhelimiin asennettavat client-ohjelmat mahdollistavat entistä kriittisempien organisaation substanssiin liittyvien tietojärjestelmien hyödyntämisen.

Älypuhelimien käyttöönotto on levinnyt organisaatioissa usein ilman ennalta suunniteltua käyttöönottostrategiaa. Nykyaikainen älypuhelin on kuin työasema, niin hyvässä kuin pahassa. Älypuhelinten hallinnointi edellyttää vastaavanlaisia prosesseja ja samanlaista selkeää elinkaarenhallintaa kuin työasemien hallinnointi. Ilman huolellista etukäteissuunnittelua, käyttöönotettava ratkaisu saattaa muodostua niin käyttöönotto- kuin käyttökustannuksiltaan ennakoitua kalliimmaksi sekä vaarantaa organisaation tietoturvallisuuden.

Tietoturvallisuuden osalta älypuhelimiin liittyy samankaltaisia uhkakuvia kuin henkilökohtaisiin tietokoneisiin. Uudet puhelimet ja palvelut aiheuttavat myös uudenlaisia ongelmia. Tämä ohje koskee älypuhelinten tietoturvallisuuteen liittyviä valtionhallinnossa noudatettavaksi suositeltavia hyviä käytäntöjä, joilla ehkäistään tietoturvaongelmia ja pienennetään tietoturvariskejä. Samalla tässä yhteydessä pyritään nostamaan esille niitä seikkoja, joilla käyttöönotettavasta ratkaisusta saadaan mahdollisimman kustannustehokas.

Ohje on tarkoitettu kaikille niille henkilöille, jotka vastaavat organisaation älypuhelimiin liittyvistä toiminnoista.

Ohje sisältää tämän tekniselle henkilöstölle suunnatun ohjeen liitteineen sekä loppukäyttäjille tarkoitetun ”Älypuhelinten turvallinen käyttö”-ohjeen, jonka jokaisen organisaation tulee mukauttaa tukemaan omaa tietoturvapolitiikkaa, infrastruktuuria ja toimintakulttuuria mahdollisimman hyvin. Liitteet on ladattavissa sähköisessä muodossa VAHTI-sivustolta osoitteessa http://www.vm.fi/VAHTI.

Lukijalle

Ohjeistuksen lukemisen helpottamiseksi ohessa on muutama yleisohje dokumentin sanastosta ja rakenteesta. Asiakirjaa tehtäessä osa termistöstä oli vakiintumatonta ja samoilla termeillä tarkoitettiin välillä hieman eri asioita. Olemme liittäneet asiakirjaan sanaston, jossa selvennetään joitakin termejä sekä valaistaan mitä näillä termeillä tarkoitetaan tässä asiakirjassa.

Kokonaisuus on jaettu kolmeen erilliseen tekstiosaan sekä näitä täydentävään Excel-taulukkoon.

1. Hyvät käytännöt -ohje

Tähän asiakirjaan on kerätty hyviä käytäntöjä liittyen älypuhelin-infrastruktuurin elinkaarenhallintaan ja toteuttamiseen. Asiakirjan sisältö on tuotettu pohjautuen työryhmän omaan osaamiseen sekä tapaamisiin, joita työryhmällä on ollut älypuhelinten, älypuhelinratkaisujen ja -palveluiden toimittajien kanssa.

2. Älypuhelimen turvallinen käyttö

VAHTI-sivustolla sijaitseva asiakirja on tarkoitettu malliksi, kun organisaatiossa tehdään käyttäjille älypuhelimen käyttöohjetta. Tähän asiakirjaan on koottu sellaisia asioita, joita on hyvä huomioida ohjeen suunnittelussa. Lisää, poista, muokkaa tai käytä tukilistana tehdessäsi organisaatiosi järjestelmiin ja tietoturvapolitiikkaan sopivaa ohjetta.

3. Tekninen liite

VAHTI-sivustolla sijaitsevassa teknisessä liitteessä käsitellään älypuhelinten historiaa sekä ominaisuuksia tekniikasta kiinnostuneille. Liitteen nykytekniikkaa koskevat tiedot vanhenevat uusien puhelinmallien ja ratkaisujen kehittyessä hyvinkin nopeasti, joten tarkista tietojen ajankohtaisuus ratkaisujen toimittajilta.

Vaatimuskriteeristö-taulukko

Ohjeessa mainittu Excel-taulukko on saatavilla ohjeen VAHTI-sivustosta. Tähän taulukkoon on koottu erilaisia Pushmail- ja etähallintaratkaisujen ominaisuuksia. Taulukon tehtävänä on hahmottaa, minkälaisia ominaisuuksia on dokumentin tekohetkellä ollut saatavilla. Uskomme taulukosta olevan hyötyä, kun organisaatio suunnittelee tuotteiden kilpailutukseen liittyvän kriteeristön tuottamista.

Lisätietoja mobiililaitteiden tietoturvallisuudesta löydät lukuisista aihetta käsittelevistä www-sivustoista. Työryhmä suosittelee tutustumaan esim. Viestintäviraston mobiiliturvasivustoon osoitteessa http://www.ficora.fi/mobiiliturva.

Johdanto

Vaikka valtionhallinnossakin yleistyneitä älypuhelimia koskevat periaatteessa samat lainalaisuudet kuin tietokonelaitteistoa, on niiden vakioinnissa, käytössä ja ylläpidossa (=elinkaarenhallinnassa) otettava huomioon monia erityispiirteitä.

Älypuhelimia ja niiden hallintaa varten ei ole ollut olemassa valtionhallintoa koskevaa ohjeistusta. Organisaatioissa on toistaiseksi laadittu omia erillisiä ohjeita. Jotta laitteiden käyttöönotto ja hallinta saadaan valtion organisaatioissa vakioitua, tarvitaan yleiset ohjeet ja suositukset käytettävistä tekniikoista sekä loppukäyttäjille ajanmukainen turvaohjeistus.

Tässä IT-ylläpitohenkilöstölle suunnatussa hyvät käytännöt -ohjeessa on pyritty nostamaan esille se tietous ja ne parhaat käytännöt, joita viimeisten parin vuoden aikana on kertynyt älypuhelinteknologiaa käyttäviin valtionhallinnon organisaatioihin.

Haluamme erityisesti painottaa tässä ohjeessa sitä, että tietoturvallisuuden merkitys älypuhelimissa on asia, jonka tärkeys tulee nousemaan vuosi vuodelta. Kaikki tietoturvallisuuden eteen, vakiointiin ja etähallintamenetelmiin käytetty työ niin tietokoneissa kuin älypuhelimissa helpottaa suojautumista paitsi nykyisiä myös tulevaisuuden tietoturvauhkia vastaan.

VAHTI-johtoryhmä on ohjannut työryhmän toimintaa siten, että hanketta on käsitelty kokouksissa 11/2006 ja 4/2007 sekä tuotettu materiaali on hyväksytty 10/2007 pidetyssä VAHTI-johtoryhmän kokouksessa.

Tuotettu materiaali toimitettiin lausunnoille heinäkuun alussa, jonka jälkeen organisaatioilla oli lausumisaikaa elokuun loppuun saakka. Työryhmä kokoontui 5.9.2007 workshop-tilaisuuteen, jossa se käsitteli ehdotetut muutokset, jonka pohjalta asiakirjoja täydennettiin annettujen lausuntojen pohjalta.

Työryhmän työskentelyyn ovat osallistuneet seuraavat henkilöt:

Keskitalo Kari	valtiovarainministeriö
Kommonen Mats	Turun yliopisto
Koskinen Mika	Länsi-Suomen ympäristökeskus
Leskinen Juha-Pekka	Eduskunta
Lähteenmäki Janne	Tekes
Puhto Maarit	Stakes
Mäkinen Kimmo	työministeriö
Vähämäki Pekka	Maanmittauslaitos
Rousku Kimmo	Stakes, työryhmän puheenjohtaja
Kuparinen Teemu	Stakes, työryhmän sihteeri

Helsingissä, 29.10.2007.

Kimmo Rousku
Työryhmän puheenjohtaja

Sisällysluettelo

1. Johdanto älypuhelinratkaisuihin

Älypuhelimet ovat kehittyneet ominaisuuksiltaan ja tietoliikenneyhteyksiltään soveltuviksi erilaisten palveluiden päätelaitteiksi. Puhelimella voidaan korvata nykyisin kannettavan työaseman käyttäminen yksittäisessä ratkaisussa, kuten sähköpostien lukemisessa lähiverkon ulkopuolelta. Puhelimen mukana kulkemisen helppous tekee näistä ratkaisuista erittäin houkuttelevia. Puhelin onkin muuttumassa yhä enemmän pelkästä puhelimestä päätelaitteeksi, jolla on mahdollista käyttää erilaisia palveluja ja tietojärjestelmiä organisaation ulkopuolelta.

Älypuhelimet ja yleensä kännykät ovat toisaalta korvanneet usein jo kokonaan perinteiset lankapuhelimet. Älypuhelimeen voidaan integroida tavoitettavuus, etäkäyttö- ja sähköpostiratkaisut. Tällöin puhelinta ei ole järkevää nähdä pelkkänä puhelimena, vaan se on miellettävä osaksi tavoitettavuuden ja kommunikaation kokonaisratkaisua. Puhelimen käyttötarkoituksen laajennettua on tullut ajankohtaiseksi rakentaa puhelimen käyttöä tukevia palveluja ottaen huomioon myös tietoturvallisuus.

1.1 Älypuhelimen käyttötavat

Älypuhelimen hyödyntäminen päätelaitteena voidaan jakaa kolmeen eritasoiseen osa-alueeseen:

1. Älypuhelimella ei kytkeydytä organisaation tietojärjestelmiin vaan se toimii itsenäisenä päätelaitteena.
2. Älypuhelimella käytetään hyvin rajoitetusti organisaation tietojärjestelmiä (esimerkiksi sähköposti).
3. Älypuhelimella käytetään organisaation tietojärjestelmiä laajasti (esimerkiksi sähköposti, intranet ja etätyöpöytäratkaisut).

Yllämainituista kohdista ensimmäinen kuvaa enimmäkseen mennyttä tilannetta, jossa puhelin on hankittu ominaisuuksiltaan soveltuvana käyttäjälle. Puhelin ei ole muodostanut tietoturvauhkaa organisaation muille järjestelmille, vaan uhat ovat rajoittuneen yhden laitteen ongelmiin.

Toinen kohta on arkipäivää jo useassa organisaatiossa. Rajallinenkin pääsy organisaation tietojärjestelmiin vaatii tietoturvallisuuden miettimistä ja suunnittelemista.

Kolmanteen kohtaan ovat jo siirtymässä ensimmäiset organisaatiot. Tällöin tietoturvapolitiikan tulee olla tarkoin harkittu sekä älypuhelimien elinkaarenhallinnan ohjeistettu ja käyttöönotettu.

Yllä mainitut eri luokitukset voivat tietysti olla käytössä rinnakkain organisaatiossa. Tällöin älypuhelimien käyttäjille on annettu tarpeen mukaan erilaisia käyttömahdollisuuksia organisaation tietojärjestelmiin.

1.2 Älypuhelinratkaisun keskeiset ongelmat

Älypuhelinratkaisuissa tulee huomioida uudet haasteet palveluiden ja älypuhelinten tietoturvallisuudelle. Tietoturvan uhat voidaan jakaa seuraaviin osa-alueisiin:

1. Puhelimeen kohdistuvat uhat, kuten katoaminen, varastaminen tai mobiilihaittaohjelmat. Uhkakuvat ovat varsin samankaltaisia kuin kannettavilla työasemilla.
2. Siirtotiehen ja tiedonsiirtoon kohdistuvat uhat. Siirtotiet ovat lähes poikkeuksetta jonkun muun tahon hallitsemia ja valvomia, jolloin niihin ei voida luottaa tai ne eivät ole aina käytettävissä. Tämä ei estä niiden käyttämistä, kunhan asia tiedostetaan ja huomioidaan ratkaisuissa. Tiedonsiirrolle on määriteltävä tarvittava suojaustaso (tunnistaminen, tietoliikenteen salaus ja eheyden varmistaminen) ja valittava ratkaisu tämä huomioiden.
3. Tarvittaviin palveluihin ja tietojärjestelmiin kohdistuvat uhat. Tietojärjestelmien etäkäytön toteuttaminen siten, että huolehditaan ratkaisujen valinnoissa riittävästi tietoturvallisuuden vaatimukset.
4. Hallinnan haasteet. Tekninen hallinta, ylläpito, käyttäjätuki, koulutus ja ohjeistus.

	Kannettava tietokone	Älypuhelin
Mahdollistaa sähköpostiyhteydet	●	●
Mahdollistaa www-selauksen	●	●
Tukee wlan-tietoliikenneyhteyksiä	●	●
Tukee Bluetooth-tiedonsiirtoa	●	●
Edellyttää aktiivista tietoturvapäivitysten hallintaa	●	❍
Vaatii haittaohjelmien torjuntaohjelman	●	●
Tietojen salaus tehdään salausohjelmilla	●	●
Palomuuriohjelmisto on suositeltava	●	●
Laite voidaan varustaa salasanasuojatulla näytönsäästäjällä	●	❍
Laitteen fyysinen suojaaminen on erityisen tärkeätä	●	●

● kyllä ❍ rajoitetusti tai ei kaikissa malleissa

Esimerkkejä kannettavan tietokoneen ja älypuhelimen yhteisistä tietoturvallisuutta sivuavista ominaisuuksista

2. Älypuhelinympäristön elinkaarenhallinta

2.1 Yleistä elinkaarenhallinnasta

Elinkaarenhallinnalla tarkoitetaan tässä yhteydessä vakiomuotoisen muistilistan käyttämistä hankkeen elinkaaren kaikissa vaiheissa sen varmistamiseksi, että keskeiset asiat tulevat käsitellyiksi johdonmukaisella ja kattavalla tavalla hankkeen koko elinkaaren ajan.

Älypuhelinympäristön elinkaarenhallinnassa voidaan noudattaa vastaavanlaisia periaatteita. Keskeisin asia on, että ei keskitytä yksittäisiin ratkaisuihin (palvelut, esimerkiksi pelkkä sähköposti tai tekniikka, itse puhelinlaitteet) vaan nähdään tämä organisaation koko tietohallintoa, IT-palvelutoimintaa ja tietoturvallisuutta käsittävänä uutena resursointia edellyttävänä itsenäisenä kokonaisuutena. Elinkaarenhallinta voidaan toteuttaa kokonaan omana sisäisenä palveluna, osittain ulkoistettuna tai toiminta voidaan ulkoistaa kokonaisuudessaan palveluntarjoajalle. Vaikka elinkaarenhallinta ulkoistettaisiin, edellyttää se aina osaamista myös ulkoistavassa organisaatiossa.

Älypuhelinpalvelun elinkaarenhallinta jaetaan tässä ohjeessa seuraaviin osa-alueisiin:

a) Käyttötarvesuunnitelma ja/tai esikartoitus tarpeista

- mitä ratkaisulla haetaan?
- mitkä ovat ratkaisun edut ja haitat?
- kenelle hankittava järjestelmä on tarkoitus hankkia?
- käyttäjien profilointi
- kustannuslaskelmat
- prosessien suunnittelu

b) Hankinta

- voimassa olevat organisaation sopimukset
- vaikuttavat Hansel-kilpailutukset
- yhteistyö hallinnon sisällä

c) Tietoturvallisuus

- taustajärjestelmät (palvelin, tietojärjestelmät)
- päätelaite
- tietoliikenneinfrastruktuuri
- käyttäjä
- tietoaineistot
- toimittajat

d) Käytettävät ohjelmistot

- älypuhelimen omat ohjelmistot
  - firmwaren merkitys
- toimisto-ohjelmat ja liitännäiset (pdf-tiedostot)
- tarvittavat lisäohjelmat
  - Pushmail-client
  - VoIP-client
  - haittaohjelmientorjuntaohjelmistot
  - tietojen salaus
  - päätekäyttö (ssh, RDP, ICA-client)
  - muut
    - sanakirja
    - karttasovellus

e) Vakiointi ja esiasennus

- vakioinnin liittäminen puhelimen hankintaan
- organisaation oma ratkaisu
- ulkoistettu ratkaisu
- miten ja mitä vakioidaan?
- vakioinnin ylläpito ja kehittäminen

f) Pushmail-ratkaisu sisältäen sähköpostin, kalenterin, yhteystiedot

- oma infrastruktuuri
- ulkoistettu palvelu
- markkinoilla olevat keskeiset toimijat
- kustannustenhallinta
- tarvittavat liitynnät omiin taustajärjestelmiin

g) Keskitetty hallinta – laiteinventoinnit & raportointi

- mitä kaikkea voidaan hallinnoida?
- oma infrastruktuuri-ratkaisu
- ulkoistettu palvelu
- yleisimpiä ongelmia

h) Koulutus

- tekninen ylläpitohenkilöstö
- loppukäyttäjät
- käyttäjäohjeistus
- tietoturvaohjeistus

i) Helpdesk-tuki

- oma helpdesk
- ulkoistettu palvelu
- tarvittavat SLA-tasot
- mitkä ovat yleisimmät ongelmat?

j) Varalaite-palvelut

- millainen käytettävyys ratkaisulle tarvitaan?
- mitä hyötyä vakioinnista on tässä yhteydessä?

k) Kierrätys

- mitä vanhoille laitteille tehdään?
- mitä tehdään muistikorteille ja muille lisätarvikkeille?
- tietoturvallinen hävittäminen

Elinkaarenhallinnan osa-alueet.

2.2 Käyttötarvesuunnitelma

Käyttötarvesuunnitelman tarkoituksena on varmistua siitä, että organisaatio tietää tarkalleen, mitä kaikkea hankittava järjestelmä tuo mukanaan. Eräs keino miettiä saavutettavia etuja ja vastaavasti painottaa haittapuolia on nelikenttäanalyysi, esimerkiksi SWOT-tyyppisesti:

Vahvuudet	Heikkoudet	Mahdollisuudet	Uhat
• mahdollistaa uudenlaiset käyttötavat ja toiminta-kulttuurin • useimmiten ajasta ja paikasta riippumaton ratkaisu	• ratkaisulla voi olla ”orjuuttava” vaikutus • ei ole käytettävissä aivan kaikkialla • korkeat käyttö-kustannukset	• saattaa vähentää kannettavien tietokoneiden hankintatarvetta • etenkin kalenteri mahdollistaa tehokkaamman ajankäytön • tulevaisuudessa saataville tulee enemmän asiakasohjelmia • puheliikenteen integroituminen tieto-liikenteeseen / yksi päätelaite / yksi käyttäjä	• käyttö ulkomailta voi tulla kalliiksi • kokonaiskustannukset eli TCO-laskelmat tulee suorittaa etukäteen • korkean käytettävyyden takaaminen hyvin hankalaa

Esimerkki SWOT-analyysistä älypuhelinten Pushmail -ratkaisun osalta.

Tässä ohjeessa Pushmail-ratkaisu kattaa sähköposti/kalenteri/yhteystieto -ohjelmistot. Pushmail-ratkaisu poikkeaa sähköpostin synkronointiratkaisusta siinä, että järjestelmän toiminta ei edellytä käyttäjän toimintaa eli sähköposti/kalenteri/yhteystiedot päivittyvät älypuhelimeen automaattisesti ja vastaavasti älypuhelimessa tehdyt muutokset päivittyvät organisaation taustajärjestelmiin automaattisesti.

Tässä kohtaa kannattaa ehdottomasti selvittää ja kysyä kokemuksia muilta oman hallinnonalan tai muilta tutuilta organisaatioilta. Olemme pyrkineet kirjaamaan tähän asiakirjaan kaikki olennaisimmat asiat älypuhelinten elinkaaren eri vaiheiden osalta, mutta on selvää, että keskustelemalla ja tutustumalla

markkinoilla oleviin ratkaisuihin ja alan keskeisiin toimittajiin saadaan aina tuoreempaa ja kenties toimittajakohtaisempaa palautetta.

Ratkaisua mietittäessä tulee myös selvittää tarkkaan henkilöstö, kenelle ratkaisua ollaan tarjoamassa. On selvää, että useimmissa tapauksissa Push-mail-ratkaisu saa todella positiivista palautetta ja tällöin kysyntä saattaa olla ennakoitua kovempaa. Mikäli käyttöönotto ”karkaa tällöin käsistä”, on vaarana sekä kustannusten että työmäärän ennakoimaton karkaaminen. Useimmissa tapauksissa hankittavat järjestelmät pystyvät kasvamaan todella merkittäviin käyttäjämääriin, etenkin jos palvelu ostetaan ulkoistettuna.

Eräs hyväksi havaittu käytäntö on profiloida käyttäjät eri käyttötarpeiden mukaan, jolloin elinkaarenhallinnassa voidaan luoda näitä vastaavat prosessit.

Hankittava järjestelmä on syytä käsitellä organisaation riskianalyysimenetelmällä, koska älypuhelimilla on yhteys organisaation sisäverkkoon.

Syntyvät asiakirjat:
- käyttötarvesuunnitelma
- riskianalyysi

Tarvittavat päätökset
- mahdollinen päätös varsinaisen hankkeen käynnistämiseksi sekä järjestelmän toteuttamiseksi
- päätöksessä ja hankkeen suunnittelussa tulee huomioida sen laajuus, jottei kokeilu kasva käytännöksi

2.3 Hankinta

Järjestelmän hankinta riippuu useasta eri seikasta. Hankintaan vaikuttavia ja samalla erilaisia kustannuksia aiheuttavia seikkoja ovat:
- vakioitavat älypuhelinlaitteet
  - tässä yhteydessä tulee muistaa erilaiset oheislaitteet kuten kotelot, lisäakut, lisälaturit, bluetooth-oheislaitteet jne.
- hankittavat älypuhelimille tarjottavat palvelut
  - keskeisimpänä Pushmail- ja etähallintaratkaisut
- hankittavat sovellukset
  - tärkeimpänä tietoturvatuotteet
  - mahdolliset yrityksen käyttämät client-ohjelmistot
- vakiointi ja käyttöönotto
  - kuka vakioi ja miten?
- koulutus ja ohjeistus
  - kuka kouluttaa ja millä tavalla?
  - muista myös muu mahdollinen materiaali kuin puhelimen mukana tulevat käsikirjat

- helpdesk
  - kuka toteuttaa käyttäjien tukipalvelut?
  - tukipalvelun kulurakenne
  - millainen käytettävyys tukipalvelulla tulee olla?
    - virka-aika, laajennettu virka-aika, 24/7 ?
- varalaite- ja hävittämispalvelut
  - pitääkö käyttäjillä olla varalaitteet saatavissa nopeasti?
  - miten ja kuka hävittää käytöstä poistettavat laitteet?

Kaikki edellä olevat osa-alueet voidaan toteuttaa joko organisaation omana eli sisäisenä palveluna tai tämä voidaan joko kokonaan ulkoistaa tai vain haluttuja osa-alueita siitä voidaan ulkoistaa. Ulkoistamista on käsitelty erikseen kohdassa 2.13 Ulkoistaminen.

On hyvin todennäköistä, että organisaatiossa ei ole voimassa olevia hankintasopimuksia kaikkien yllä mainittujen osa-alueiden osalta. Tällöin kannattaa tarkistaa Hanselin www-sivuilta http://www.hansel.fi voimassa oleviin näihin ratkaisuihin liittyvät puitesopimukset tai suunnitteilla olevat kilpailutukset.

Mikäli joudut toteuttamaan kilpailutuksen esimerkiksi sen takia, että kaikkia tarvitsemiasi osa-alueen palveluita tai tuotteita ei ole saatavilla valmiiksi kilpailutettuna, kannattaa samaan kilpailutukseen yrittää saada mukaan myös muita osallistujia, koska tällöin tehdystä työstä saadaan saman tien hyötyä useammalle organisaatiolle.

Hankinnan yhteydessä kannattaa suorittaa laskelmat käyttöönotettavan toteutuksen käyttökustannuksista esimerkiksi ainakin yhden, kahden ja neljän vuoden osalta. Esimerkiksi alempana laskelma 50 älypuhelinta varten, johon otetaan mukaan kaikki keskeiset palvelut.

Älypuhelimien mallien valinnassa ja vakioinnissa suosittelemme malleja, joiden ominaisuudet riittävät tietoturvaohjelmistojen ja asetusten keskitettyyn hallintaan. Listahinnaltaan kalleimmat puhelimet voivat kokonaiskuluissa tulla halvemmaksi, kun edullisimpien puhelimien hajautettu asentaminen ja häiriöiden selvittäminen. Laskettaessa älypuhelinratkaisun kokonaiskustannuksia, ohessa laskentaesimerkkiä niistä asioista, joita tulisi laskennassa ottaa huomioon. Esimerkiksi on valittu 50 käyttäjän älypuhelinympäristö. Korvaa x-kohdat saamasi tarjouksen mukaisilla hinnoilla.

1. 50 kpl älypuhelimia, keskihintainen malli
   50 * x €

2. Vakiointi ja esiasennus
   50 * x €

3. Pushmail
   50 *x €/ kk - ulkoistettu palvelu
   50 *x € / kk - itse ylläpidetty palvelu

4. Laitehallinta
   50 *x € / kk - ulkoistettu palvelu
   50 *x € / kertamaksu - itse ylläpidetty palvelu

5. Haittaohjelmientorjunta
   50 *x € / kk - ulkoistettu palvelu
   50 *x € / kertamaksu - itse hankittu lisenssi

6. Salaustuotteet
   50 *x € / kk - ulkoistettu palvelu
   50 *x € / kertamaksu - itse hankittu lisenssi

7. Koulutus
   50 *x € / käyttäjä / koulutus

8. Helpdesk-tukipalvelu
   50 *x € / kk tai - ulkoistettu palvelu
   x € / helpdesk-tapahtuma

9. Varalaitepalvelut
   50 *x € / kk - ulkoistettu palvelu

10. Hävittäminen
   50 *x € / kk - ulkoistettu palvelu

11. Puhe- ja dataliittymä
   50 *x € / kk - ulkoistettu palvelu

Tällöin esimerkiksi täysin ulkoistettuna kokonaishankintahinta olisi x € / vuosi eli x € / kk tai kolmessa vuodessa x €. Mikäli valtaosa palveluista toteutettaisiin itse, vuosikustannus olisi x € ja vastaavasti kolmen vuoden kokonaiskustannukset olisivat x €.

On huomattava, että vakiointi / ulkoistaminen ei poista oman asiantuntemuksen sekä oman hankintaosaamisen tarvetta!

Työryhmä suosittelee tarkoituksenmukaista älypuhelinten elinkaarenhallinnan eri osa-alueiden ulkoistamista. Huomaa, että kaikissa tilanteissa ulkoistaminen ei ole tarkoituksenmukaisin vaihtoehto, vaan siihen vaikuttavat esimerkiksi seuraavat seikat:

- olemassa oleva henkilöstö ja osaaminen
- käyttöönotettava Pushmail / etähallintaratkaisu
  - etenkin, jos älypuhelimilla otetaan yhteys suoraan puhelimesta sähköpostijärjestelmään ilman välityspalvelimia, Pushmail-ratkaisun ulkoistamisella ei välttämättä saavuteta etua
- tarvittava palvelutaso
  - etenkin oman 24/7 tai muuten virka-ajan ylittävän palvelun toteuttaminen saattaa olla käytännössä mahdotonta toteuttaa omin voimin

Syntyvät asiakirjat:

- hankinta-asiakirjat
- sopimukset toimittajien kanssa
- palvelusopimukset

Tarvittavat päätökset:

- hankintapäätökset

2.4 Tietoturvallisuus

Elinkaarenhallinnan osalta tarkasteltuna tietoturvallisuus muodostaa kokonaisuuden, joka edellyttää jatkuvaa ylläpitoa, valvontaa ja kehittämistä. Toistaiseksi useat älypuhelimiin liittyvät uhkatekijät ovat lähinnä median tai alalla toimivien tietoturvayritysten esille nostamia uhkia, jotka eivät ole konkretisoituneet tai aiheuttaneet niin merkittäviä ongelmia kuin etukäteen on spekuloitu.

Voidaan siten todeta, että käyttöönotettavilla tietoturvaratkaisuilla etenkin virusten- ja haittaohjelmien suhteen älypuhelimissa suojaudutaan tulevia uhkia vastaan.

Tietoturvallisuuden osalta elinkaarenhallinnassa voidaan ottaa esille esimerkiksi seuraavat vaiheet:

- laitteiston vakiointi ja ”lukitseminen”
  - käytettävien firmware- ja muiden ohjelmaversioiden päättäminen
  - hävinneiden tai varastettujen laitteiden lukitsemis- tai tyhjentämisprosessin suunnittelu
  - ohjelmistojen asentamisen estäminen
  - asetusten muutosten estäminen
  - vakioiduista sovelluksista päättäminen

- tietoliikenneasetusten vakioiminen
- SIM- ja muiden puhelinasetusten, esimerkiksi PIN- ja suojakoodi kyselyt, vakiointi ja lukitseminen

- käyttöönotettavien tietoturvatuotteiden valitseminen, testaaminen ja konfiguroiminen
  - haittaohjelmientorjunta
  - palomuuri
  - etähallinta
  - tietojen salakirjoittaminen

- tietoturvatuotteiden ja älypuhelinympäristön tietoturvallisuuden valvominen
  - lokit ja erilaiset hälytykset

- älypuhelimella käytettävien tietoliikenneyhteyksien tietoturvallisuudesta huolehtiminen
  - GPRS/EDGE/UMTS/HSDPA/HSUPA-yhteydet
  - WLAN-yhteydet
  - bluetooth-yhteydet
  - infrapuna-yhteydet

- Puhelimen sijoittaminen infrastruktuuriin
  - työasemaan liitetty puhelin voi avata yhteyden lähiverkkoon organisaation palomuurien ohi

- älypuhelimella käsiteltävien tietoaineistojen tietoturvallisuudesta huolehtiminen
  - tietoturva- ja tietosuojaohjeet
  - tietojen salakirjoittaminen
  - tietojen varmistaminen

Kuten kaikessa muussa tietoturvallisuudessa, täydellistä, ilman mitään tietoturvariskiä olevaa älypuhelinympäristöä on mahdotonta toteuttaa. Tämän asiakirjan tarkoituksena on osaltaan toimia ohjeena ja muistilistana, jonka avulla pyritään huolehtimaan siitä, että mitään keskeisiä tietoturvallisuuteen liittyviä asioita ei jätetä huomioimatta.

Päätelaitteen ominaisuuksien ja niiden rajallisuuden ei tule antaa heikentää tiedon turvallisuutta missään käsittelyn vaiheessa. Jos älypuhelimen ominaisuudet tai niiden rajallisuus estävät tarvittavien tietoturvatuotteiden käyttämisen (esim. salaus tai pääsynvalvonta), niin sen käyttäminen tietoon pääsemiseen tai sen tallentamiseen tulee estää. Tietoturvallisuutta on käsitelty erikseen luvussa 4. Älypuhelimien tietoturvallisuus.

2.5 Käytettävät ohjelmistot

Myöhemmin kuvatun vakioinnin ja esiasennuksen oleellinen merkitys on varmistaa käytettävien sovellusten ja älypuhelinjärjestelmän keskinäinen yhteensopivuus.

Toistaiseksi älypuhelimien merkittävin sovellus on erilaiset Pushmail-ratkaisut, mutta markkinoille on tulossa uudenlaisia tunnettujen yritysohjelmistojen älypuhelinlaitteisiin sovitettuja client-ohjelmistoja, jolloin älypuhelimien käyttömahdollisuuksia voidaan entisestään laajentaa.

Kaupallisten tuotteiden rinnalla on saatavilla sekä toimittajakohtaisia ilmaisohjelmistoja että netistä ladattavia ilmais- ja shareware-ohjelmistoja. Etenkin jälkimmäisten suhteen pitää olla selkeä hyväksyttämisprosessi, jossa tietohallinto / tietoturvaorganisaatio testaa ja hyväksyy vakioituun ympäristöön tuotavat uudet ohjelmistot.

Edellä kuvattujen ohjelmistojen ohella kysyntää on jatkossa esimerkiksi seuraavanlaisille sovelluksille:

- karttasovellukset
  - saatavilla ilmaiseksi esimerkiksi Nokian Smart to Go
    http://www.smart2go.com/en/
  - sekä Googlen:
    http://www.google.com/gmm
- sanakirjat
  - esimerkiksi Kielikoneen tuotteet

- päätepalvelintuotteet
  - Citrix-client
  - VNC-client

- pikaviestintä
  - IM-client-ohjelmat
  - videoneuvottelu- ja läsnäolotietous -tuotteet

- olemassa olevien varusohjelmien korvaavat tuotteet
  - Opera-www-selain
    http://mini.opera.com
  - FExplorer-tiedostojenhallinta
    http://www.gosymbian.com

Markkinoilla on saatavilla tuhansia erilaisia lisäohjelmistoja niin Symbian kuin Windows Mobile-alustalle. Oleellista on kuitenkin se, että käyttäjiltä on estetty sovellusten asentaminen laitteiden käytettävyys- sekä tietoturva- että ohjelmistolisenssiteknisistä syistä. Tällöin organisaation tietohallinto tai muu älypuhelimien hallinnasta vastaava on ainoa taho, joka voi huolellisen testauksen jälkeen tarvittaessa muuttaa vakiointia ohjelmistojen ja asetusten osalta.

2.6 Esiasennus ja vakiointi

Esiasennuksen ja vakioinnin tärkeys riippuu paljon siitä, millaisista älypuhelimien käyttöönottomääristä on kyse. Jos puhutaan pienestä organisaatiosta ja muutamasta puhelimesta vuositasolla, hyvin dokumentoidulla itse tehdyllä asennuksella saatetaan saavuttaa kustannustehokkain ratkaisu.

Kun hankintamäärät kasvavat vuositasolla kymmeniin, nousee esiasennuksen ja vakioinnin merkitys. Tällöin mallilaitteiden vakiointiin ja esiasennuksen suunnitteluun kuluva ”ylimääräinen” aika saadaan takaisin moninkertaisesti sen jälkeen kun vakiointiprosessi on saatu käyttöön uusien laitteiden osalta.

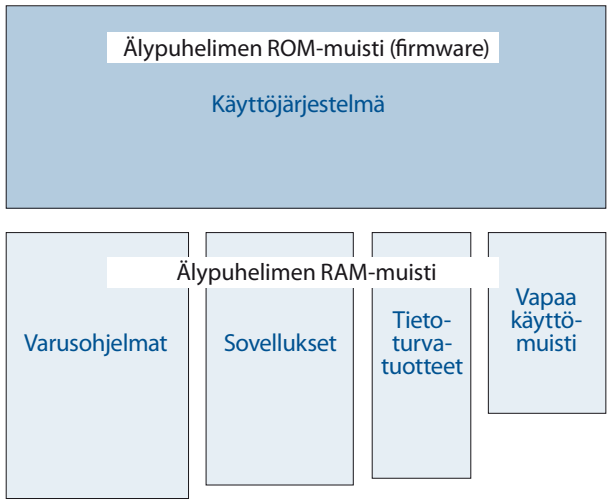
Vakiointiin ja esiasennukseen liittyviä tietoturva-asioita on käsitelty edeltävissä kappaleissa. Esiasennus voidaan toteuttaa useimmilla kehittyneillä etähallintaohjelmilla, jolloin se voidaan toteuttaa joko organisaation omin voimin tai ulkoistettuna palveluna.

Esiasennus kannattaa ottaa huomioon myös siinä mielessä, että sille saattaa löytyä tarvetta laitteissa varsinaisen käyttöönoton jälkeen, jos

a) älypuhelin hajoaa/häviää/varastetaan tai
b) älypuhelin sekoaa / siinä tulee ohjelmistoyhteensopivuusongelmia, jolloin joudutaan palaamaan takaisin lähtötilanteeseen.

Valitettavasti matkapuhelimista puuttuu ”järjestelmän palautuspiste” –tyyppinen toiminto, jolla voitaisiin palauttaa älypuhelin takaisin jotain toimenpidettä edeltäneeseen tilaan.

Vakioinnissa paljon työtä aiheuttava asia on erilaisten sovellusten keskinäisen toiminnan tarkastaminen etenkin tietoturvatuotteiden osalta. Markkinoilla olevien laitteiden suorituskyky ja käytettävissä oleva RAM-muisti asettavat rajoituksia siten, että lataamalla riittävä määrä tietoturvatuotteita käyttöön saadaan aikaan merkittävä käytettävyyden lasku, kun valtaosa älypuhelimen suorituskyvystä ja RAM-muistista kuluu tietoturvatuotteiden pyörittämiseen.



Älypuhelimien keskeinen ongelma on se, että sovelluksille käytettävissä oleva vapaa muistialue jää valitettavan pieneksi sen jälkeen, kun laitteeseen on vakioitu pakolliset tietoturvaohjelmistot.

Valittaessa tietoturvatuotteita, varmista etukäteen toimittajilta ohjelmien yhteensopivuus tarkkaan, ei pelkästään yleisesti sovellusohjelma-tasolla, vaan tarkkaan ohjelmaversioittain. Useissa yhteyksissä on törmätty tilanteeseen, jossa tietyt ohjelmat edellyttävät jopa tarkalleen tietyn älypuhelimen firmware-version ja tietyn version ohjelmasta toimiakseen sulassa sovussa keskenään. Varmistaminen tulee toteuttaa myös käytännön testein.

Osaltaan tämän takia on hyvin oleellista, että älypuhelinten vakiointiin ja luotettavuuden ja käytettävyyden testaamiseen käytetään aikaa. Vastaavasti uusien älypuhelimen firmware- tai ohjelmapäivitykset edellyttävät huolellista testausta ennen vakioinnin muuttamista.

Tässä yhteydessä ei voi olla korostamatta huolellisen ja ajan tasalla säilytettävän dokumentaation ja versiohistorian merkitystä. Jos jotain ongelmia tapahtuu, tehtyjen dokumenttien avulla pitäisi pystyä selvittämään, mikä ongelman on aiheuttanut.

Palveluntarjoajalta tulee edellyttää samanlaista dokumentaatiota, mitä itse vastaavanlaista palvelua ylläpidettäessä tuottaisi.

Merkittäviä ongelmia on ollut esimerkiksi seuraavassa kombinaatiossa, jolloin on yritetty saada toimimaan kaikki neljä seuraavanlaista tietoturvatuotetta samassa älypuhelimessa:

- haittaohjelmientorjunta-ohjelmisto
- palomuuriohjelmisto
- salakirjoitusohjelmisto
- etähallintaohjelmisto

2.7 Pushmail-ratkaisu sisältäen sähköpostin, kalenterin ja yhteystiedot

Pushmail-ratkaisun valintaan vaikuttaa käytössä oleva oma sähköpostijärjestelmä. Kaikista laajin tuki on saatavilla Microsoft Exchange-sähköpostipalvelimen varaan, mutta tuotteita löytyy monille tunnetuille tuotteille kuten Lotus Notes, Novell GroupWise ja Teamware Office. Pushmail-ratkaisua käsitellään laajemmin seuraavassa luvussa 3. Pushmail-ratkaisut.

Elinkaarenhallinnan kannalta Pushmail-ratkaisu on kenties kaikista keskeisin älypuhelimiin liittyvä ratkaisu, jonka takia olisi toivottavaa, että valintaprosessi kohdistuisi heti ensimmäisellä kerralla organisaation tarpeet täyttävään ratkaisuun. Tämä sen johdosta, että Pushmail-ratkaisun vaihtaminen toimittajasta toiseen hiemankaan laajemman käyttöönoton jälkeen on työläs tehtävä.

Pushmail-ratkaisun keskeinen kysymys liittyy siihen, kuinka ulkoistetusti palvelu on tarkoitus toteuttaa? Organisaatioissa tulee ottaa huomioon sähköpostissa kulkevien tietoaineistojen luottamuksellisuus. Vaikka tietoliikenne salataan aina sähköpostijärjestelmästä Pushmail-client laitteelle, järjestelmän ylläpidosta vastaava taho pääsee useissa tapauksissa kiinni järjestelmän tuottamiin teletietoja vastaaviin sähköpostin tunnistetietoihin.

2.8 Keskitetty hallinta – laiteinventoinnit ja raportointi

Keskitetyllä hallinnalla eli etä- tai laitehallinnalla, jota nimitystä tästä kohdasta usein myös käytetään, organisaation tietohallinto tai muu älypuhelimien hallinnoinnista vastaava taho saa tarvitsemansa tiedot (inventointi) laitteista ja sovelluksista, pystyy muuttamaan älypuhelimien asetuksia sekä jakelemaan sovelluksia. Laitehallintaan on käsitelty tarkemmin luvussa 5. Etähallinta.

Elinkaarenhallinnan osalta keskitetty hallinta/laitehallinta-ratkaisu on keskeinen tekijä. Käytössä olevien laitteiden määrä tulee jatkamaan kasvuaan ja käytettävien laitteiden käytettävyysvaatimukset asettavat entistä suurempia haasteita. Laite-/etähallintatuotteiden käyttöönotto on tulossa pakolliseksi työvälineeksi.

Samalla tavalla kuin Pushmail-ratkaisussa, markkinoilla olevien tuotteiden toiminnallisuus vaihtelee merkittävästi. Tämän takia työryhmän vahva suositus on tutustua markkinoilla oleviin ratkaisuihin erittäin huolellisesti ennen lopullista päätöstä.

Laitehallinta voidaan toteuttaa useimmissa älypuhelimissa olevan laitteen ROM-muistissa sijaitsevan client-ohjelman avulla tai se voi rakentua toimittajan tekemän laitehallinta-client-ohjelman varaan. Tietoturvallisuuden kannalta keskeiset ominaisuudet liittyvät käytettävissä olevien sovellusten käytön rajoit-

tamiseen, bluetooth- ja muiden tietoliikennelaitteiden asetusten vakioimiseen / laitteiden poistamiseen sekä ohjelmistojen jakeluun ja päivittämiseen.

Hallintaohjelmiston raportointiominaisuuksien avulla voit raportoida käytössä olevista laitteista hyvin monipuolisesti. Voit tuottaa erilaisia hälytyksiä ja tilastotietoja laitteiden tilasta, esimerkkinä muistienkulutus ja täyttöaste sekä älypuhelimessa käynnissä olevista prosesseista.

2.9 Koulutus

Koulutuksen merkitystä onnistuneessa älypuhelinpalvelun käyttöönotossa on syytä korostaa. Kokemukset ovat osoittaneet, että älypuhelinympäristön tehokas hyödyntäminen edellyttää vähintään parin tunnin mittaista käyttökoulutusta.

Koulutukseen oleellisesti liittyvässä kirjallisessa käyttöohjeessa tulee olla tarkasti ohjeistettuna elinkaarenhallinnan kannalta sellaiset osa-alueet, joita ilman loppukäyttäjä ei tule toimeen. Mitä paremmin koulutus-osio toteutetaan, sitä vähemmän organisaation käyttämä helpdesk-ratkaisu työllistyy.

2.10 Helpdesk-tuki

Helpdeskin merkitys korostuu palvelun piirissä olevien käyttäjämäärien kasvaessa. Helpdesk-palvelun käyttömäärään vaikuttaa oleellisesti, kuinka edellä kuvattu koulutus, ohjeistus ja älypuhelimien vakiointi on onnistuttu toteuttamaan ja ohjeistamaan.

Haasteeksi voi muodostua ulkomailla olevien ja helpdeskin välinen aikaero. Halutessaan palvella käyttäjiään tehokkaasti on 24/7 tuki ainoa, joskin kallis vaihtoehto.

Tuetut päätelaitemallit kieliversioineen on sovittava helpdeskin kanssa. Tämä on myös kerrottava käyttäjille koulutuksessa ja käyttöohjeissa.

2.11 Varalaite-palvelut

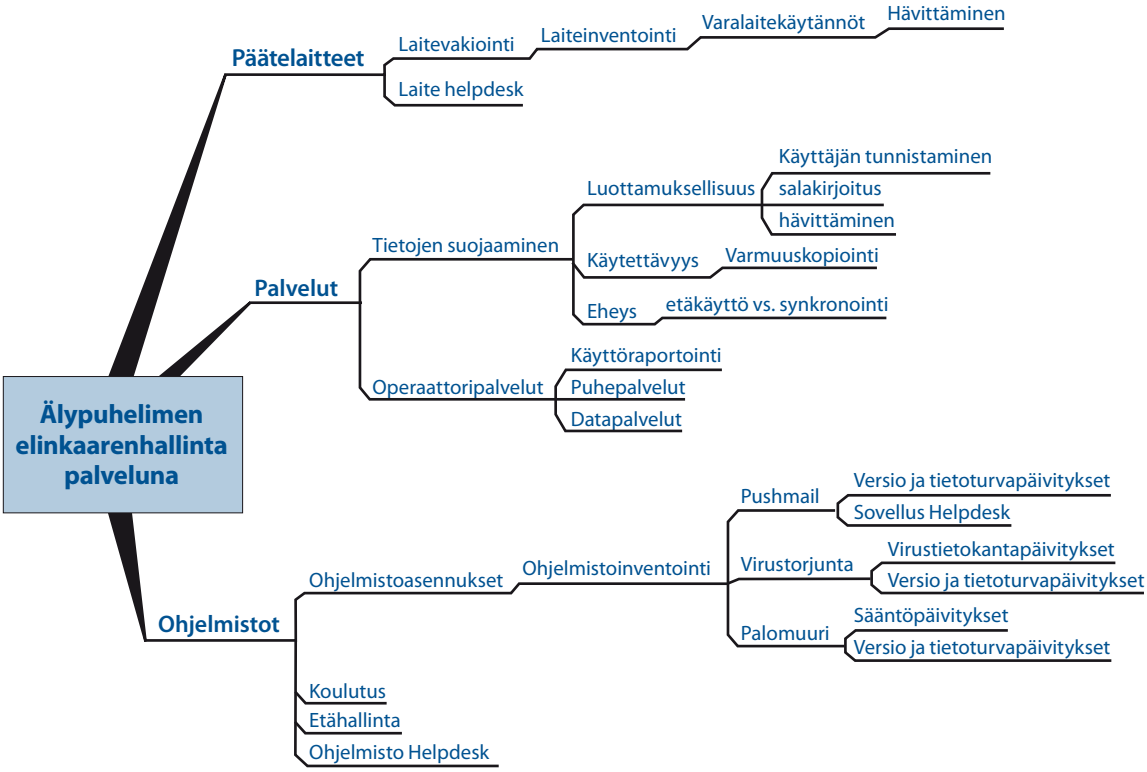
Varalaitteiden merkitys korostuu vasta laitemäärän ja käytettävyystarpeiden kasvaessa. Parhaimmillaan varalaitepalvelu toimii siten, että organisaatiossa on varastoituna valmiiksi asennettuina keskeisiä malleja. Nämä otetaan käyttöön välittömästi, kun käyttäjän puhelimella tuntuu olevan ongelmia, joiden korjaaminen esimerkiksi etähallinnan avulla ei onnistu. Kun käytössä on vakiointiympäristö, käyttäjän tietojen palauttaminen onnistuu vaivattomasti ja kokema käyttökatkos on lyhyt.

2.12 Kierrätys

Elinkaarenhallinta päättyy yleensä laitteen tai tuotteen jonkinlaiseen hävittämisprosessiin. Älypuhelin ei juuri poikkea työaseman elinkaarenhallinnan tästä osa-alueesta. Älypuhelimien oikeaoppinen hävittämien edellyttää selkeätä, yksityiskohtaisesti dokumentoitua hävittämisprosessia, jossa huolella varmistutaan laitteissa olevan ns. jäämätiedon tietoturvallisesta hävittämisestä.

2.13 Ulkoistaminen

Elinkaarenhallinnan kaikki osa-alueet tai valikoiden yksittäisiä osa-alueita on mahdollista myös ulkoistaa.



Ulkoistamiseen liittyviä elinkaarenhallinnan osa-alueita.

Yllä olevasta kuvasta voidaan havaita, että älypuhelimen elinkaareen mahtuu useita hallittavia asioita. Lisäksi hallittavat kohteet näyttäisivät lisääntyvän kiihtyvällä tahdilla. Laitteiden ja ohjelmistojen keskinäinen riippuvuus toisis-

taan saa aikaan sen, että ns. puhelinvastaavilla ei yleensä ole mahdollisuutta ylläpitää useita kymmeniä älypuhelinympäristön suoja-asetuksia tai sovellusylläpitoa ilman keskitettyä hallintaa.

Keskitetty hallinta vaatii yleensä tarkoitusta varten hankittua yhtä tai useampaa palvelinta, joiden elinkaarenaikainen ylläpito lisää työmäärää. Näin älypuhelinten keskitettyä hallintaa ei käytännössä kannata itse ylläpitää aivan pienelle määrälle puhelimia.

Jos hallittavia puhelimia on useita satoja tai tuhansia, niiden keskitetty ylläpito saattaa olla järkevämpää hoitaa itse. Kannattavuus riippuu palveluntarjoajan hinnoittelumallista sekä tarjotun palvelun räätälöitävyydestä, eli mahdollisuudesta jakaa käyttäjiä erilaisiin ryhmiin ja palvelutasoihin.

Kasvava trendi näyttäisi olevan, että pöytäpuhelimet ovat jäämässä kokonaan pois käytöstä ja henkilöt tavoitetaan yhdestä numerosta, yhdestä älypuhelimesta. Samaan aikaan laitevakiointi saa aikaan sen, että yhdestä laitemallista löydetty haavoittuvuus altistaa kaikki organisaation puhelimet uhalle.

Näin organisaation toiminta saattaa lamaantua oleellisesti yhdestä haittaohjelman aiheuttamasta epidemiasta tai yhdestä virheellisestä ohjelmistoviasta.

Monet palveluntarjoajat ja operaattorit ovat tunnistaneet tämän ongelmallisuuden ja tarjoavat jo keskitettyjä kokonaisratkaisuja esimerkiksi kiinteää kuukausimaksua vastaan.

Edellä olevaa kaaviota mukailevaa aputaulukkoa voidaan käyttää sopivaa kumppania kartoitettaessa ja käyttötarvesuunnitteluun palvelukuvausta valmisteltaessa. Houkuttelevinta olisi löytää yksi palveluntarjoaja, jolta palvelut saisi mahdollisimman kattavasti koko älypuhelimen elinkaaren ajan.

3. Pushmail-ratkaisut

3.1 Mitä Pushmail-ratkaisu pitää sisällään?

Älypuhelimissa mobiili-sähköpostiratkaisu (usein käytetty termi Pushmail) pitää tyypillisesti sisällään sähköpostin, kalenterin ja osoitetietojen hallintamahdollisuudet. Joissakin ratkaisuissa kokonaisuutta on laajennettu myös tiedostojen synkronointimahdollisuudella.

IMAP, POP, SMTP ja SyncML ovat laite- ja ohjelmistotoimittajista riippumattomia protokollia, joita yleisesti käytetään keskusteluyhteyden luomisessa sähköpostipalvelimen ja älypuhelimen välille. Lisäksi käytössä on valmistajakohtaisia http-protokollan päällä kuljetettavia xml-pohjaisiin viesteihin perustuvia ratkaisuja. Edellä luetellut protokollat edellyttävät älypuhelimesta löytyvän jo valmiiksi asennettuna (tai jälkikäteen asennettavaksi) sovelluksia esimerkiksi sähköpostisovelluksen. Sovellusten lisäksi on mahdollista, että Pushmail-ratkaisu tai käytössä oleva sähköpostijärjestelmä tarjoaa wap- ja web-käyttöliittymät sähköpostiin. Näin esimerkiksi älypuhelimen web-selaimella on mahdollista käyttää sähköpostijärjestelmää. Huomioitavaa kuitenkin on, että Web-sähköpostin vapaan käytön salliminen on riippuvainen organisaation tietoturvapolitiikasta.

Älypuhelimen ja organisaation sähköpostipalvelimen välisen keskusteluyhteyden (=Pushmail) rakentamiseen on käytössä useita erilaisia ratkaisumalleja:

- Pushmail-ratkaisu erikseen palveluna ostettuna esimerkiksi operaattorin kautta
- Pushmail-ratkaisu hankittuna organisaation omaan palvelinympäristöön
- Pushmail-tuki integroituna suoraan sähköpostipalvelimeen

Jos organisaatio hankkii Pushmail-ratkaisun palveluna, on seuraavat asiat syytä ottaa huomioon:

- talletetaanko yksittäisten käyttäjien sähköpostisalasanoja palveluntarjoajan Pushmail-palvelimeen
- millaiset oikeudet, mahdollisuudet ja menettelytavat palveluntarjoajan ylläpitohenkilökunnalla on käsitellä organisaation käyttäjätietoja, lokitietoja ja erityisesti yksittäisiä sähköposteja

- miten vian raportointi ja selvitys on organisoitu
- kuinka moni henkilö palvelun tarjoajalla osallistuu ylläpitotehtäviin
- edellyttääkö Pushmail-ratkaisun käyttöönotto kolmannen osapuolen ohjelmiston asentamista organisaation sähköpostipalvelimen yhteyteen

Lisäksi on syytä selvittää:

- miten hyvin Pushmail-ratkaisu integroituu osaksi organisaation käytössä olevaa sähköpostijärjestelmää
- miten hyvin Pushmail-tuote tukee salasanan vanhenemista sähköpostijärjestelmän päässä
- mitä käytännön rajoituksia Pushmail-ratkaisu asettaa esimerkiksi liitetiedostojen hakemiseen ja kalenterivarausten tekemiseen
- mitä päätelaitteita Pushmail-ratkaisu tukee
- tukeeko Pushmail-ratkaisu tietojen ajastettua hakemista, esimerkiksi sähköpostien päivittäminen, vain arkipäivinä ja virka-aikaan
- miten ja millaisessa aikajaksoissa uusia päätelaitteita tuodaan Pushmail-tuotteen tukemiksi
- onko organisaatiolla syytä rajoittaa Pushmail-ratkaisun käyttöä esimerkiksi kustannus- tai tietoturvasyistä
- miten Pushmailin käytön kouluttaminen / ohjeistaminen on organisoitu

3.2 Pushmail-ratkaisun tietoturvasta

Organisaation on syytä varmistaa, että kaikki tietoliikenne älypuhelimen ja Pushmail-ratkaisun välillä on salattu. Jos käytössä on tcp/ip-pohjainen yhteyskäytäntö niin salaukseen suositellaan käytettäväksi TLS-protokollaa (tai SSL 3.0 protokollaa). Pelkän ilmarajapinnan (GPRS, WLAN yms.) salaus ei ole riittävä.

TLS/SSL-salausta käyttöönotettaessa tulee tarkistaa, että hankittavat älypuhelimet tukevat salauksen käyttöönottoa kaikissa yhteystavoissa (sähköpostin lähettäminen, sähköpostin vastaanottaminen ja SyncML). Päätelaitteessa tulee olla joko valmiina tai konfiguroitavissa palvelimen varmenteen myöntäneen tahon CA-varmenne. Ns. client-varmenteita ei ole toistaiseksi käytetty pushmail-ratkaisuissa.

Yleisesti käytössä olevia tietoliikenneportteja, joita käytetään Pushmail rajapinnan kanssa keskustellessa:

- tcp-portti 993 salattu imap (sähköpostin noutaminen)
- tcp-portti 465 salattu smtp (sähköpostin lähettämiseen)
- tcp-portti 443 salattu http (kalenteritietojen synkronointi, mutta osa ratkaisuista käyttää myös sähköpostin käsittelyssä)

Pushmail-ratkaisun käyttöönotto voi edellyttää kolmannen osapuolen liitäntäohjelmiston asentamista. Liitäntäohjelmisto sijaitsee sähköpostipalvelimen ja älypuhelimen välissä. Liitäntäohjelmiston asennuksessa tulee tarkkaan harkita, mikä on ohjelmiston oikea sijoituspaikka tietoturva-, tietoliikenne- ja käytettävyysnäkökulmat huomioiden.

Esimerkiksi ohjelmiston asennus samaan fyysiseen laitteeseen, missä sähköpostipalvelin sijaitsee, tulee harkita tarkkaan. Liitäntäohjelmisto voi edellyttää kommunikointiparametreissaan admin-tason tunnusta sähköpostipalvelimeen, jolloin tunnuksen käytön dokumentointi on ensiarvoisen tärkeää.

Lisäksi on syytä tarkkaan selvittää ja dokumentoida, mitkä ovat liitäntäohjelmiston käyttämät tietoliikenneyhteydet, mihin suuntaan ja kenen toimesta yhteyksiä avataan. Liitäntäohjelmiston palvelin on suositeltavaa sijoittaa ns. DMZ-verkkoon ja suojata palvelin palomuurin taakse. Liitäntä palvelimella tallentuvien Pushmail-käyttäjätunnus ja salasanaparien tietoturvallisuus tulee huomioida tarkasti.

Sähköpostin liitetiedostojen lataamisessa älypuhelimeen on syytä noudattaa varovaisuutta. Kaikki liitetiedostot eivät aukea älypuhelimessa ja suuren liitetiedoston lataus voi kestää pitkään riippuen käytettävästä tietoliikenneyhteydestä. Lähtökohtaisesti liitetiedostot tulisi tallentaa salakirjoitetulle muistialueelle. Liitetiedostojen tallettaminen muistikortille ilman salausta ei ole suositeltavaa.

Älypuhelimessa on suositeltavaa käyttää haittaohjelmientorjuntaohjelmistoa. Haittaohjelmientorjuntaohjelmistosta huolimatta on syytä ohjeistaa käyttäjiä varovaisuuteen ja olemaan avaamatta epämääräisiä viestejä.

Puhelin kannattaa suojata suojakoodilla, jonka tulee lukittua automaattisesti, jos näppäimistöön ei ole koskettu tietyn ajan kuluessa. Näin voidaan estää tai ainakin vaikeuttaa pääsyä sähköpostissa oleviin tietoihin, jos puhelin katoaa tai varastetaan.

Mahdollisen varkaustapauksen tai puhelimen häviämisen yhteydessä tulee aina huolehtia, että älypuhelin voidaan tyhjentää etäältä. Tyhjennyksen tulee koskea vähintään sähköpostin, kalenterin ja osoitekirjan tietoja.

3.3 Tunnistaminen

Älypuhelinkäyttäjä tunnistetaan Pushmail-ratkaisuissa yleensä käyttäjätunnuksen ja salasanan perusteella. Lisäksi on olemassa ratkaisuja, joissa käyttäjätunnuksen ja salasanan lisäksi tai vaihtoehdoksi tunnistetaan älypuhelinkäyttäjän puhelinnumero (ns. A-tilaajanumero).

Käytettäessä GPRS-verkkoa on mahdollista sopia mobiili-operaattorin kanssa organisaatiolle dedikoidusta GPRS-APN:stä (Access Point Name). Oman APN:n avulla voidaan rajoittaa tietoliikennettä niin, että vain organisaation omat mobiili-liittymät pääsevät mobiiliverkosta organisaation Pushmail-palveluun.

SIM-kortille talletettua mobiili-varmennetta (PKI-arkkitehtuuriin nojaava malli), jota käytettäisiin hyväksi tunnistaumisessa mobiili-sähköpostipalveluun, ei ainakaan toistaiseksi ole käytetty.

3.4 Kalenteri- ja osoitetietojen synkronointi

Kalenteri- ja osoitetietojen synkronoinnissa on yleisesti käytössä kaksi eri teknologiaa. Open Mobile Alliance, OMA on laite- ja ohjelmistotoimittajien yhteenliittymä, jossa on määritelty Device Syncronization (ent. nimeltään SyncML) niminen määritys. Toinen yleinen synkronointiteknologia nojaa Microsoftin määrittelemään ActiveSync-tekniikkaan. ActiveSync on käytössä Windows Mobile-käyttöjärjestelmällä varustetuissa älypuhelimissa. SyncML on yleisesti käytössä Symbian-pohjaisissa älypuhelimissa.

Älypuhelimiin on yleensä valmiiksi asennettu tai asennetaan jälkikäteen ohjelmistotoimittajan toimesta synkronointi-client esim. natiivi-Symbian-sovellus, Windows Mobile tai Java J2ME-sovellus.

Ensimmäisessä synkronoinnissa (ns. slow sync) laite alustetaan tuomalla älypuhelimeen synkronointialueen sisällä oleva tieto. Tämä vaihe voi kestää ajallisesti pitkäänkin riippuen käytettävän tietoliikenneyhteyden nopeudesta ja synkronoitavan tiedon määrästä. Synkronointialue voi pitää sisällään esim. kaikki kalenteritapahtumat kuudeksi kuukaudeksi eteenpäin ja kaikki osoitetiedot. Eri ohjelmistoissa on usein rajoituksia, kuinka pitkälle ajassa eteenpäin kalenteritietoja voidaan synkronoida älypuhelimeen.

Normaalisti päivittäisessä käytössä kalenteritietojen synkronointi älypuhelimen ja sähköpostipalvelimen välillä suoritetaan vain niiltä osin, mitkä käyttäjän kalenteritiedot ovat muuttuneet älypuhelimessa ja sähköpostipalvelimella. Tämä synkronointitapa on yleensä ajallisesti nopea.

Käyttäjän kannattaa pyrkiä käyttämään pääsääntöisesti yhtä synkronointikanavaa. Jos mahdollista, kannattaa välttää yhdistelmää, jossa älypuhelimella käytetään yhtä aikaa paikalliseen työasemaan asennettua synkronointisovellusta ja palvelimella olevaa synkronointiohjelmistoa. Tiedossa on tapauksia, joissa useamman synkronointikanavan yhtäaikainen käyttö on luonut sekä yhteystietoihin, että kalenterimerkintöihin kaksoismerkintöjä eli duplikaatteja.

Osoitetietojen synkronoinnissa sähköpostipalvelimen kanssa kannattaa huomioida, että osoitetietojen noutaminen voi tuoda älypuhelimen osoitekirjaan puhelinnumerot ja sähköpostiosoitteet. Lisäksi osa Pushmail-tuotteista kykenee joko hakemaan tai muuten hyödyntämään organisaation käyttämän yhteisen hakemiston osoitetietoja. Osoitetietojen synkronoinnista on hyötyä, jos puhelin esim. hajoaa tai varastetaan. Uuden älypuhelimen käyttöönotto on helppoa, koska kaikki osoitetiedot saadaan synkronoitua sähköpostipalvelimelta.

SyncML-protokolla tukee suoraan useamman eri päätelaitteen yhtäaikaista käyttöä kalenteri- ja osoitetietojen synkronoinnissa. Yksittäiset laitteet, tässä tapauksessa älypuhelimet, voidaan tunnistaa laitteen IMEI-koodin perusteella. Jos käyttäjällä on käytössään useita älypuhelimia, Pushmail-palvelin kykenee pitämään kirjaa kunkin laitteen tilasta ja synkronoimaan älypuhelimessa tapahtuneet paikalliset muutokset sähköpostipalvelimelle. Ominaisuudesta on hyötyä varsinkin jos ns. multi-SIM puhelinliittymät yleistyvät. Multi-SIM mahdollistaa saman puhelinnumeron kahdelle tai useammalle SIM-kortille.

Kalenteri- ja osoitetietojen lisäksi osa Pushmail-tuotteista tarjoaa mahdollisuuden synkronoida myös tehtäväluettelon. Tehtäväluettelon synkronointi ei kuitenkaan ole vielä tässä vaiheessa yhtä laajasti tuettuna eri päätelaitteissa ja Pushmail-tuotteissa kuin mitä kalenteri- ja osoitetietojen synkronointi on.

3.5 Sähköposti

Mobiilisähköpostissa voidaan erottaa kaksi pääasiallista toimintamallia. Ensimmäinen malli perustuu ns. ”pull”-tekniikkaan ja toinen malli perustuu ns. ”push”-malliin. ”Pull”-malli on perinteinen ratkaisu, jossa käyttäjä tai sähköpostisovellus tarkistaa aika ajoin, onko sähköpostipalvelimelle saapunut uusia viestejä. ”Pull”-toimintamallia täydentämään on älypuhelinmaailmassa yleistynyt ”Push”-toimintamalli, joka perustuu sähköpostin noutamiseen taustalla käyttäjän huomaamatta. ”Push” -toimintamallia käytetään yleisesti myös kalenteri- ja yhteystietojen synkronoinnissa. ”Push”-mallissa älypuhelinlaite vastaanottaa yhteydenoton Pushmail-palvelimelta esim. binääri-tekstiviestin muodossa. Yhteydenotto aktivoi älypuhelimeen hakemaan uudet sähköpostit / kalenterimerkinnät sähköpostipalvelimelta. Näin mahdollistetaan se, että älypuhelimessa oleva tieto on aina ajan tasalla.

Vaikka S/MIME-salauksen tuki löytyy useista älypuhelimista, niin varmenteiden käyttäminen esim. SIM-kortille talletettujen varmenteiden muodossa ei ole yleistynyt. Tätä tekstiä kirjoitettaessa Suomessa laatuvarmenteita myöntävän organisaation varmenteen, esimerkiksi virkavarmenteen, sijoittaminen SIM-kortille ja käyttäminen sähköpostin salaamiseen Pushmail-palvelussa ei ole vielä kaupallisissa tuotteissa toteutettu.

Sähköpostin käytössä älypuhelimissa on usein eroavaisuuksia verrattuna normaaliin työasemassa tapahtuvaan sähköpostin käsittelyyn. Esimerkiksi liitetiedostojen noutaminen ja käsittely voi olla hyvin rajallista. Toinen yleinen rajoite liittyy sähköpostipalvelimella käytössä olevien kansioiden hakemiseen älypuhelimeen. Osa Pushmail-tuotteista ja älypuhelimen sähköpostiohjelmista kykenee hakemaan kansioiden sisällön, osa tuotteista vain esimerkiksi yhden eli Saapuneet -kansion sisällön.

3.6 Hyviä käytäntöjä ja muistettavia asioita – Pushmail-ratkaisu

- huomioi ja laske Pushmail-kokonaisuuden TCO-laskelmat 1-2-4 vuoden osalta, jotta käyttökulut eivät tule aikanaan yllättämään (Total Cost of Ownership eli kokonaiskustannuslaskelmat)
- varaudu hankkimaan uusi puhelin viimeistään 3 vuoden kuluttua
- muista auditoida käyttämäsi ratkaisu käyttöönoton yhteydessä ja myös jatkossa säännöllisesti
- älypuhelinjärjestelmän toiminta on kiinni kokonaisuudesta, jonka muodostavat puhelimen firmware-versio, käytettävä sovellus sekä vapaana oleva muistin ja prosessoritehon määrä
- Pushmail- ja muissa ratkaisuissa on hyvä pitää mielessä esimerkiksi Nokian ilmaisen PC-suite-ohjelmiston mahdollisuudet sekä muut datakaapeliyhteyden kautta toimivat sovellukset.
- eräs erityisesti ulkomailla yllättäviä kustannuksia aiheuttava seikka on yhteyden aloitusmaksu (riippuu operaattorista). Tämä tarkoittaa sitä, että vaikka hinta per megatavu olisi kohtuullinen, jokainen datayhteyden avaus aiheuttaa tietyn lisämaksun. Tällainen avausmaksu on vaarallinen etenkin sellaisissa kohteissa, joissa tukiasemaverkko ei ole kovinkaan kattava ja yhteydet pätkivät esimerkiksi liikuttaessa kiinteistöjen sisäpuolella tai autolla. Organisaation kannattaa ohjeistaa käyttäjiä, jotta nämä ymmärtävät tarkistaa kohteen roaming-hinnoittelusta Mt-tiedonsiirtohinnan osalta myös ko. avausmaksun.

4. Älypuhelimien tietoturvallisuus

Tässä hyvät käytännöt -asiakirjassa on pyritty nostamaan esille elinkaarenhallinnan osa-alueiden yhteydessä erilaisia kyseiseen alakohtaan liittyviä mahdollisia tietoturvaan liittyviä niin muistettavia seikkoja kuin mahdollisia ongelmia. Tässä kappaleessa keskitytään erityisesti tietoturvatuotteiden hyödyntämiseen liittyviin asioihin älypuhelimien yhteydessä.

4.1 Nykytila – uhkakuvat

- tietoliikenneyhteyksien kautta tapahtuvat mahdolliset hyökkäykset
- virukset ja haittaohjelmat – bluetooth-, mms-yhteyksien kautta
- muistikortit – sekä tietoaineistojen kautta että haittaohjelmien tartuttamisvälineenä
- tietoaineistojen käsittely – sähköposti, kalenteri-tiedot, älypuhelimeen tallennetut asiakirjat
- istutetut vakoiluohjelmat – ammattimainen vakoilu
- tietoliikenneyhteydet eivät ole käytettävissä
- älypuhelimen katoaminen tai varastaminen
- koulutuksen ja ohjeistuksen puute

4.2 Tulevaisuuden uhat

- kun taloudellinen hyöty keksitään, älypuhelimia vastaan kehitetään uudenlaisia hyökkäyskeinoja (vrt. roskapostitus ja phishing)
- mahdollisen zero day -turva-aukon löytyminen Symbian- / Windows Mobile- käyttöjärjestelmäalustasta
- kasvava roskaposti / sms-mainonta / puhemainonta
- jatkossa WLAN-yhteyksien kautta kohdistuvat ongelmat
- VoIP-teknologian tuomat vaarat puheviestinnässä
- gps-paikannusteknologian tuomat mahdollisuudet paikkatietoisuuden lisääntyessä

4.3 Yleistä älypuhelimien tietoturvallisuudesta

Tällä hetkellä älypuhelimiin kohdistuvia uhkia voidaan pitää merkittävästi pienempinä kuin esimerkiksi työasemiin kohdistuvia uhkia. Merkittävimmät uhat liittyvät älypuhelimen fyysiseen tietoturvallisuuteen eli siihen, että laite häviää tai se varastetaan, jolloin merkittävässä asemassa ovat seuraavat asiat:

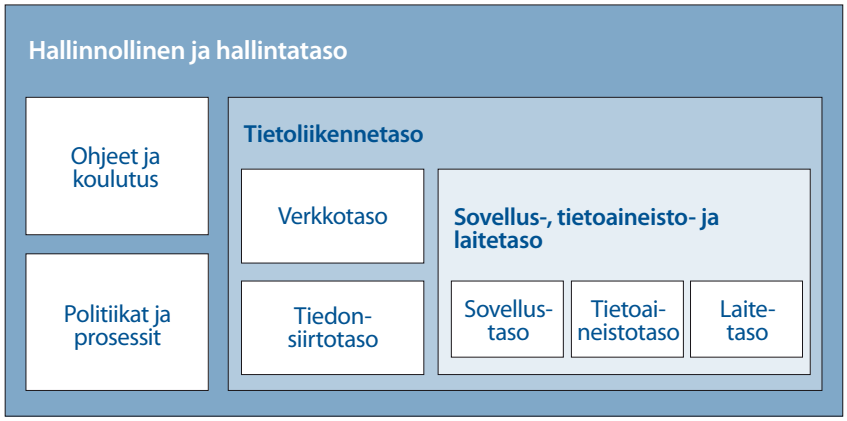
- millaista tietoaineistoa älypuhelimelle on tallennettu?
- millaisia suojauksia puhelimella käytetään, esimerkiksi automaattilukituksen aikaviive, mahdollinen älypuhelimen tiedostojen salakirjoitus, sim-kortin suojaus?
- onko käytettävissä etähallintaohjelmistoa, jolla älypuhelin voidaan tyhjentää ja lukitsemalla estää sen hyödyntäminen?
- onko käyttäjät ohjeistettu tällaisten tilanteiden varalta?
- onko organisaation puhelinvastaava(t) ja muu IT-henkilöstö koulutettu näitä tilanteita varten?
- organisaation tietojärjestelmien käyttäminen on sallittua vain organisaation omistamilla tai hallinnoimilla työvälineillä.

Toinen keskeinen uhkatekijä ovat erilaiset haittaohjelmat. Toistaiseksi haittaohjelmat ovat olleet yksittäisiä tapauksia ja työasemien kaltaista epidemiaa ei ole koettu. Teoriassa sellaisen aukon löytyminen puhelimissa olevista käyttöjärjestelmistä, joka mahdollistaisi tietokonemadon kaltaisen nopean leviämisen, on mahdollista, mutta ei kovinkaan todennäköistä. Mikäli tällainen mato saataisiin luotua, operaattoreiden olisi todennäköisesti mahdollista estää tällaisen leviäminen omilla tietoturvatuotteilla.

Älypuhelimissa olevilla haittaohjelmien torjuntaohjelmistoilla suojaudutaan tällä hetkellä ennen kaikkea tulevaisuuden uhkakuvilta.

Työryhmä suosittelee haittaohjelmien torjuntaohjelman käyttöönottoa älypuhelimissa.

Mikäli jokin merkittävä tietoturvauhka konkretisoituu, siinä vaiheessa tällaisten tietoturvatuotteiden hankkiminen, testaaminen ja jakeleminen kiireellisellä aikataululla ei ole käytännössä mahdollista ja suojaavat toimenpiteet onnistuvat vain keskitetyn hallinnan kautta.



Älypuhelimien tietoturvallisuus voidaan jakaa kolmeen eri tasoon alkaen hallinnollisesta tasosta päätyen tietoliikennetason kautta sovellus- tietoaineisto- ja laitetasoon.

Hallinnollinen ja hallintataso
Tällä tasolla tulee huolehtia tietohallintoon ja tietoturvallisuuteen liittyvistä asioista yleisellä tasolla, elinkaaren kokonaishallinta, käyttäjähallinta, tarvittava hallinnollinen dokumentaatio ja hyväksyttäminen.

Tietoliikennetaso
Tämä taso jakaantuu verkkotasoon ja tiedonsiirtotasoon. Verkkotasolla on otettava huomioon että älypuhelinliikenteessä käytetty verkko on ulkopuolisen tahon (esimerkiksi operaattorin) omistama ja hallinnoima verkko ja sen takia organisaation tietoturvan kannalta tätä täytyy pitää ns. ”epäluotettavana” verkkona. Sama koskee jatkossa wlan-tekniikkaa. Tämä ei estä verkon käyttöä, mutta asia on tiedostettava tietoturvaratkaisujen suunnittelussa ja valinnassa. Tiedonsiirtotasossa on määriteltävä, millaista suojaa tietoliikenne tarvitsee erilaisissa käyttötapauksissa. Tietoliikenteen suojaamiseen kuuluu esimerkiksi todentaminen, tietoliikenteen salaaminen ja tietoliikenteen eheyden varmistaminen.

Sovellus- ja laitetaso
Laitetaso koostuu sovellustasosta, tietoaineistotasosta sekä laitetasosta. Sovellustasolla tulee huolehtia käytettävien sovellusten tietoturvallisuudesta. Tietoaineistotasossa on huolehdittava tiedon elinkaaren vaiheista alkaen tiedon luomisesta tai vastaanottamisesta, tiedon käsittelystä, tiedon tallentamisesta ja tiedon hävittämisestä tai arkistoimisesta. Laitetasolla on huolehdittava laitteen ja sen ohjelmistojen suojaamisesta haittaohjelmia ja palvelunestohyökkäyksiä vastaan.

4.4 Hyviä käytäntöjä tietoturvallisuuden toteuttamiseksi

4.4.1 Älypuhelinlaitteen suojaaminen

Suosittelemme seuraavia asioita mietittäväksi älypuhelinten fyysisessä turvallisuudessa:

a) SIM-kortti ja liittymä

- pin-suojauksen käyttöönotto
  - jos sim-kortti sijoitetaan toiseen puhelinlaitteeseen, pitää pin-koodi aina kysyä, jotta liittymän väärinkäyttö ja toisen henkilön nimissä esiintyminen ei olisi mahdollista
  - oletus-pin-koodit ja muut oletustunnukset pitää aina vaihtaa

- puhelimen automaattilukitus 5 – 10 minuutin aikaviiveellä
  - tällä estetään se, että puhelimen hävitessä satunnainen löytäjä pääsisi käyttämään laitetta ilman suojausten murtamista

- liittymään ei kannata aktivoida sellaisia palveluita, joita sillä ei ole tarkoitus käyttää (esimerkiksi MMS-palvelu, multimediaviestien käyttöön ei ole välttämättä kaikilla käyttäjillä tarvetta)
  - MMS on eräs haittaohjelmien leviämiskeino, joka voi lisäksi aiheuttaa korkeita käyttökustannuksia väärinkäytettynä

- data-yhteyksien osalta kannattaa pyrkiä yksittäisten data-pakettien sijaan hankkimaan isompi datapooli, joka mahdollistaa vapaammin data-yhteyksien hyödyntämisen. Mikäli älypuhelinta käytetään joko www-selaamiseen tai kannettavan tietokoneen modeemina, on suositeltavaa hankkia kiinteällä kuukausimaksulla ja rajoittamattomalla datamäärällä toimiva liittymä.

b) Haittaohjelmien torjunta

- automaattisesti itsensä päivittävä haittaohjelmien torjuntaohjelma, jossa on lisäksi mahdollisuus palomuuritoimintoihin
  - haittaohjelmientorjunta
    - varmistu siitä, että käyttöön otettavaksi tarkoitettu tuote sisältää sovelluksen ja tietokantakuvausten automaattisen päivitystoiminnon
  - palomuuriohjelmisto
    - mahdolliset muut client-sovellukset saattavat hankaloittaa palomuurin käyttöönottoa

- älypuhelimen salakirjoitusohjelmiston käyttö on suositeltavaa
  - tässä keskeinen ongelma on siinä, että jos käytössä on useita tietoturvatuotteita, älypuhelimen muisti ja prosessorin suorituskyky eivät riitä kaikkien tuotteiden riittävän tehokkaaseen ajamiseen ja puhelimen käyttö hidastuu merkittävästi
  - osassa Pushmail-ohjelmistoja on sisäänrakennettu ominaisuus, joka salakirjoittaa esimerkiksi posti-kalenteri-yhteystiedot automaattisesti, jolloin lähinnä vain käyttäjän itsensä tekemät tiedostot ovat oletuksena salakirjoittamattomia

c) Tietoliikenneyhteydet

Älypuhelimen bluetooth-yhteydet pitää poistaa käytöstä, jos käyttäjä ei käytä bluetooth-laitteita. Jos yhteydelle on tarvetta, pitää asetukset saattaa siihen tilaan, että bluetooth-yhteydet eivät mainosta laitetta muille bluetooth-laitteille eli tila on piilotettu.

- Bluetooth on toistaiseksi yleisin haittaohjelmien leviämiskanava, tämän takia käyttäjille pitäisi erityisesti ohjeistaa, että älypuhelimen näyttöön tuleviin erilaisiin asennus- tai muihin vastaaviin kyselyihin vastataan tarkoituksenmukaisesti, yleensä Ei (No)
- mikäli Bluetooth-yhteyksiä tarvitaan, laite tulee nimetä siten, että laitetta ei voida suoraan nimestä tunnistaa
- huomaa, tehokkailla suunta-antenneilla Bluetooth-yhteyksiä on voitu kaapata jopa yli kilometrin etäisyydeltä
- teoriassa langattoman handsfree-laitteen kautta tapahtuva keskustelu hf-laitteen ja älypuhelimen välillä voidaan kaapata ja salakuunnella
- älypuhelimen wlan-yhteydet tulee ottaa pois käytöstä, mikäli organisaation tietoturvaohjeissa wlanin käyttö ei ole sallittu. Joillakin etähallintasovelluksilla voidaan wlan verkot jakaa sallittuihin ja kiellettyihin. Tällöin voidaan sallia esimerkiksi organisaation oman tietoturvallisen wlan-infran käyttö
- wlan-yhteydet muodostavat älypuhelimissa samanlaisen vaaran, mitä kannettavissa tietokoneissakin. Teoriassa ottamalla yhteys vääränlaisen wlan-tukiaseman kautta käyttämällä suojaamattomia yhteyksiä, väärinkäyttäjä saattaa saada selville luottamuksellista tietoa
- mikäli organisaation tietoturvaohjeissa avoimien wlan-yhteyksien käyttö on sallittu, pitää käyttäjien osata varmistua siitä, että käytettävät access point-tukiasema on tarkoitettu yleiseen käyttöön eikä ole esimerkiksi jonkin organisaation suojaamaton tukiasema tai mahdollisen tietomurtautujan ns. honey pot-tukiasema
- puhelin voidaan liittää organisaation lähiverkossa olevaan työasemaan. Tällöin mahdollisesti avataan tietoliikenneyhteys, jota ei ole suojattu lähiverkon tietoturvaratkaisuilla.

d) Etähallinta

- etähallinta on keskeinen ohjelma tietoturvallisuuden toteuttamisessa älypuhelinympäristössä, koska sillä voidaan rajoittaa useimpia älypuhelimen käyttöön liittyviä toimintoja sekä vastata älypuhelimen vakiointiin ja varmistamiseen liittyvistä toiminnoista.
- käyttäjiä tulee tiedottaa puhelinten etähallintamahdollisuudesta
- käyttäjää tulee tarpeen mukaan tiedottaa etähallinnalla tehtävistä toimenpiteistä etukäteen

5. Etähallinta

Etähallinnan roolia on korostettu tämän asiakirjan useammassa aikaisemmassa luvussa. Kuten useissa muissakin teknologioissa, etähallinta ei ole välttämättä aivan pienempiin ympäristöihin sopiva ratkaisu, paitsi kenties ulkoistettuna ratkaisuna.

5.1 Mitä etähallinta mahdollistaa?

Etähallinta mahdollistaa tyypillisesti seuraavia asioita:

- **laitteen teknisten tietojen kerääminen**
  - luettelee käynnissä olevat sovellukset, muistin kulutuksen, tietoliikennemäärät ja mahdollisesti näihin liitettävät hälytykset, laitteen ja ohjelmistojen versiotiedot
  - mikäli etähallintaohjelma osaa kertoa esimerkiksi cell id tai muita laitteen paikkatietoja, tällaisten paikkatietojen käsittelemisessä tulisi noudattaa voimassa olevaa lainsäädäntöä (SVT 516/2004, 16§) sekä organisaation tietoturvapolitiikkaa

- **asetusten vakioiminen**
  - joissain etähallintaohjelmistoissa voit vaikuttaa myös laitteen SIM-kortin asetuksiin / liittymäasetuksiin
  - asetusten katsominen, muuttaminen ja lukitseminen
  - erityisesti tiettyjen tietoturvaohjelmien asetusten vakioimisen ja muuttamisen suhteen etähallintasovelluksissa on eroa. Kannattaa varmistaa, että käyttöön hankittavalla etähallintasovelluksella pääset muuttamaan käyttöön hankittavien tietoturvatuotteiden asetuksia tai käytettävissäsi on jokin muu keino esimerkiksi haittaohjelmien torjuntaohjelmien aktivoimiseen ja asetusten muuttamiseen

- **asetusten rajoittaminen**
  - esimerkiksi sovellusten asentamisen estäminen tai yksittäisten sovellusten suorituksen esto

- tällä tavalla voidaan estää esimerkiksi sovellusten asentaminen, kun estetään Symbianin käyttämän installer-sovelluksen käyttö. Vastaavalla tavalla voidaan estää esimerkiksi kamera-sovelluksen tai muiden sovellusten käyttäminen

- **tiedostojen kopioiminen ja varmistaminen**
  - esimerkiksi käyttäjien datatiedostojen varmistaminen tai haitta-ohjelmien tietokantojen automaattinen päivittäminen voidaan toteuttaa myös etähallinnan omilla toiminnoilla

- **komentojen suorittaminen**
  - sovelluksella voidaan ajastaa tai pakottaa ajettavaksi komentoja toimintoja haluttuna ajankohtana

- **viestit ja hälytykset**
  - ylläpitohenkilökunta voi tiedottaa omilla viesteillään käyttäjälle / kaikille käyttäjille mahdollisista ylläpitotoiminnoista / lähettää muita hälytyksiä
  - tätä voidaan käyttää myös muuhun kuin akuuttien = ajankohtaisten asioiden viestittämiseen

- **laitteiden lukitseminen ja/tai etätyhjentäminen**
  - kadonnut laite voidaan joko tyhjentää suoraan tai vaarattomimmissa tilanteissa lukita se
  - osa hallintaohjelmia hallitsee myös esimerkiksi muistikorteilla olevien tietojen hävittämisen
  - hallintaohjelmilla voidaan laite myös palauttaa tehdasasetuksiin

- **yhteyksien hallinta**
  - laitteen tietoliikenneyhteyksien vakioiminen (esim.wlan access pointit salliminen/kieltäminen)

- **visuaalinen etähallinta(vrt. etätyöpöytä)**
  - osassa sovelluksia on mahdollista kaapata älypuhelin samanlaiseen etähallintaan, kuin työasema eli siten, että avustaja näkee etänä avustettavan puhelimen näyttökuvan ja näppäimistön sekä voi sitä kautta tehdä etähallintaa. Tällaisen etäkaappauksen käyttö on useissa tapauksissa käytettävissä olevien tietoliikenneyhteyksien takia hidasta ja edellyttää aina käyttäjän hyväksyntää.

5.2 Mitä etähallinnalla ei voi tehdä?

Markkinoilla on kohtalainen määrä erilaisia älypuhelinten hallintaan tarkoitettuja sovelluksia. Osa on tarkoitettu lähinnä operaattorikohtaisiksi työvälineiksi pääpainon ollessa liittymänhallintaan ja laitteen käyttöönottoon liittyvissä asioissa. Toisen joukon muodostaa organisaatioiden IT-tuelle suunnatut hallintavälineet, joista osassa käytettävissä olevien client-ohjelmistojen määrä sisältää älypuhelimien ohella laajan joukon PDA-laitteita ja mahdollistaa myös Windows-työasemien etähallinnan.

Eräs keskeinen ominaisuus, jota useimpiin älypuhelimiin ei voi vielä etähallintatuotteiden avulla tehdä, on puhelimen firmware-ohjelmiston päivittäminen. Osa markkinoilla olevista matkapuhelimista tukee ns. OTA (Over the Air) -päivityksiä, mutta teknologia ei ole vielä kovinkaan yleinen.

5.3 Hyviä käytäntöjä ja muistettavia asioita – etähallinta

- työryhmä on tehnyt erillisen Excel-taulukon, johon on koottu keskeisiä hankinnassa selvitettäviä kriteereitä sekä Pushmail-sovellusten että etähallintasovellusten osalta. Taulukkoa löytyy VAHTI-ohjesivustosta.
- etähallinta ei auta siinä vaiheessa, jos puhelin hajoaa tai sen tietoliikenneyhteydet eivät ole toiminnassa
- etähallinnan osalta kannattaa muistaa se, että niillä alueilla, joilla tietoliikenneyhteydet eivät ole toiminnassa, etähallinnalla ei päästä laitteeseen käsiksi
- selvitä myös käyttöönotettavan etähallintatuotteen aiheuttama tietoliikennekuorma ja pyri optimoimaan se mahdollisimman kustannustehokkaaksi ja tarkoituksenmukaiseksi
- kiinnitä erityistä huomiota etähallinta- ja Pushmail-palvelinympäristöjen suojaamiseen, koska mahdollinen väärinkäyttäjä tai tietomurtautuja yrittää hyökätä sellaisia vastaan niitä löytäessään
- kuten Pushmail-ratkaisussa, etähallintaratkaisu tulee säännöllisesti auditoida sekä käydä läpi säännöllisesti riskianalyysi sen toimintaan liittyen

6. Älypuhelimien käyttö tulevaisuudessa

Miten älypuhelimien rooli tulee muuttumaan tulevaisuudessa? Pushmail-ratkaisut yleistyvät ja niiden sovellukset vastaavat ominaisuuksiltaan työasemien sähköpostiratkaisuja.

Koska uusien IT-järjestelmien suunnittelussa ja toteutuksessa otetaan huomioon erilaiset päätelaitteet, yrityssovellusten ulottaminen älypuhelimilla käytettäväksi helpottuu.

Parantunut näyttöteknologia ja nopeammat tietoliikenneyhteydet mahdollistavat pääte- ja etäkäytön organisaation lähiverkkoon.

Pikaviestintä yleistyy valtionhallinnossa ensin työasemakäytössä. Ratkaisu mahdollistaa reaaliaikaisen monikanavaviestinnän yhdelle tai useammalle käyttäjälle samanaikaisesti. Useissa pikaviestimissä on tekstipohjaisen viestienvaihdon lisäksi myös muita ominaisuuksia. Videokuvan, äänen, tiedostojen sekä läsnäolotietojen välittäminen on useissa pikaviestimissä mahdollista. Tällaisesta unified communications -ratkaisusta tulee merkittävä osa organisaation tietoliikenne- ja puheinfrastruktuuria.

Uusimmat älypuhelinmallit tukevat pikaviestintäominaisuuksia täydentäen nykyisiä tekstiviesti- ja Pushmail-ratkaisuja.

Älypuhelimien ominaisuuksien kehittyessä niihin kohdistuu samanlaisia tietoturvauhkia kuin työasemiin. Työasemissa käytössä olevat tietoturvaratkaisut tulee sovittaa älypuhelinlaitteisiin.

Liite 1. Sanasto

2G
Termiä käytetään yleensä kuvaamaan toisen sukupolven matkapuhelinteknologiaa, keskeisimpänä GSM- sekä HSCSD-data-yhteydet (High-Speed Circuit-Switched Data).

2.5G
Termillä kuvataan edellisen teknologian kehittyneempää versiota, jossa päästään selvästi korkeampiin tiedonsiirtonopeuksiin esimerkiksi GPRS- tai EDGE-tekniikoilla. Tyypillisiä tiedonsiirtonopeuksia ovat noin 40 kbps (GPRS) ja 236,8 kbps (EDGE). 2.5G-teknologia on huomattavasti edullisempi toteuttaa kuin esimerkiksi 3G-teknologia.

3G
Termi, jota käytetään kuvaamaan kolmannen sukupolven matkapuhelintekniikkaan liittyviä asioita, tiedonsiirrossa käytetään UMTS-tekniikkaa (Universal Mobile Telecommunications System), jossa tyypillinen tiedonsiirtonopeus on 384 kbps.

3.5G
Edellisestä kehitetty teknologia, jossa tiedonsiirtonopeutta on saatu kasvatettua HSDPA-tekniikan (High-Speed Downlink Packet Access) avulla. Tyypillisiä nopeuksia ovat 1,8 ja 3,6 Mbps, tulevaisuudessa 7,2 ja 14,4 Mbps.

3.75G
Tällä hetkellä nopein mobiilidatayhteyksissä käytettävä teknologia, joka pohjautuu HSUPA-tekniikkaan (High-Speed Uplink Packet Access), jonka tiedonsiirtonopeus voi olla 5,76 Mbps. HSUPA-tekniikka nopeuttaa etenkin tiedonsiirtoa päätelaitteesta takaisin verkkoon päin.

Android
Googlen perustama alusta matkapuhelimia varten. Kehitystyöstä vastaa Open Handset Alliancen http://www.openhandsetalliance.com/press_110507.html -nimellä kulkevaa yhteenliittymää, joka kehittää open source-ohjelmiston varassa toimivaa käyttöjärjestelmää puhelimiin.

Bluetooth
Bluetooth on lyhyen kantaman tietoliikenneyhteys, joka on tarkoitettu puhelimissa tietojensiirtoon puhelimien välillä tai puhelimen ja oheislaitteen, kuten langattomien kuulokkeiden tai GPS-vastaanottimien välillä.

EDGE
Enhanced Data Rates for Global Evolution laajentaa ja nopeuttaa GPRS-verkkoa mahdollistaen suuremmat tiedonsiirtonopeudet.

Etähallintasovellus
Älypuhelimien etähallintasovelluksella tarkoitetaan ohjelmistoa, jolla voidaan toteuttaa matkapuhelimien hallintaan liittyvät toimenpiteet ilman fyysistä kontaktia puhelimeen. Etähallintaan kuuluvia keskeisiä asioita ovat esimerkiksi laiteinventoinnit, sovellusten jakelu ja rajoitustoimenpiteet, asetusten muuttaminen ja vakioiminen sekä tiedostojen varmuuskopioiminen.

Firmware
Laitteiston toimintaa ohjaava ohjelmisto. Nimensä mukaisesti ohjelmisto on jossain ohjelman ja laitteiston välimaastossa toimivaa koodia. Symbian puhelimien käyttöjärjestelmä on firmware-pohjainen, joka tekee siitä tiukasti laitteeseen sidotun.

GPRS
General Packet Radio Service mahdollistaa data-yhteydet GSM-verkkoa käyttävissä puhelimissa, sen käyttö ei edellytä 3G-verkkoa.

HSDPA
High-Speed Downlink Packet Access on UMTS-verkon laajennus, jolla verkon nopeutta ja ennen kaikkea verkon latenssia (verkkoviive) on saatu pienennettyä.

Honey pot
Järjestelmä, jonka tarkoituksena on houkutella käyttäjiä ansaan. Esimerkiksi vapaaksi mainostettu WLAN-tukiasema, jonka läpi kulkevaa liikennettä ”salakuunnellaan” ja nauhoitetaan. Voi toimia myös tietoturvallisuutta edistävänä järjestelmänä, jonka avulla kerätään tietoa mahdollisista murtautumiskeinoista.

IMEI
IMEI-koodi (International Mobile Equipment Identity) on matkapuhelimen 15-numeroinen laitetunnus, joka löytyy esimerkiksi puhelimen takapuolelta tai puhelimen akun alta. Useissa matkapuhelimissa IMEI-koodin saa näytölle näppäilemällä koodin: *#06#

HOTJ
Haittaohjelmien torjuntajärjestelmä, HOTO tarkoittaa haittaohjelmien torjuntaohjelmistoa.

MMS
Multimedia Messaging Service mahdollistaa multimediaviestien lähettämisen ja vastaanottamisen matkapuhelimella. Multimediaviestit voivat sisältää esim. kuvia, ääntä, tekstiä ja videota. Tietoturvallisuuden kannalta MMS muodostaa tietoturvariskin.

OTA
Over the air, langaton siirtotie, ilmateitse tapahtuva. OTA-lyhennettä käytetään esimerkiksi puhuttaessa laitteiden firmware-ohjelmistojen päivityksistä, joka toistaiseksi onnistuu OTAn avulla vain harvoilla toimittajilla ja harvoilla malleilla.

OMA
Open Mobile Alliance on vuonna 2000 perustettu, lähes 200 mobiililaitteiden kanssa toimivan yrityksen yhdessä muodostama yhteenliittymä, jonka tehtävänä on kehittää rajapintoja ja palveluliittymiä, joilla mobiililaitteiden käyttöä voidaan jatkossa tehostaa.

OMA DS
Open Mobile Alliance Data Synchronization spesifikaatiot määrittelevät, miten mobiililaite synkronisoi esimerkiksi kalenteritietoja palvelimen kanssa. DS:n edeltäjä on laitevalmistajien yhdessä määrittelemä SyncML niminen protokolla, joka on DS:n perustana.

PIN
Personal Identification Number eli henkilökohtainen 4–8 merkkiä pitkä tunnusluku suojaa matkapuhelimessa olevan SIM-kortilla sijaitsevan liittymän väärinkäytöksiltä, jos joku esimerkiksi varastaa SIM-kortin puhelimesta. Jos syötät PIN-koodin kolme kertaa peräkkäin väärin, puhelimesi lukkiutuu, jolloin sen avaaminen edellyttää 8-numeroisen PUK-koodin.

PIN2
PIN2-koodi on PIN-koodin lisäkoodi, jolla voi suojata tiettyjä puhelimen ominaisuuksia/toimintoja. Se toimii samalla tavalla kuin PIN-koodi, sen toiminnasta on kerrottu tarkemmin päätelaitteen käyttöoppaassa.

PUK
Personal Unblocking Key-koodia tarvitaan, kun puhelimen PIN-koodi on syötetty riittävän monta kertaa väärin ja puhelin halutaan aktivoida jälleen toi-

mintaan. PUK-koodi on 8-merkkinen koodi, jonka voit pyytää puhelinvastaavaltasi, joka hankkii sen operaattorilta tai palveluntarjoajalta. Jos käyttäjä syöttää virheellisen PUK-koodin esimerkiksi kymmenen kertaa peräkkäin, SIM-kortista tulee käyttökelvoton.

PUK2
Mikäli PIN2-koodi syötetään virheellisesti useamman kerran peräjälkeen, puhelimesi saattaa pyytää PUK2-koodia. Jos käyttäjä kirjoittaa virheellisen PUK2-koodin esimerkiksi kymmenen kertaa peräkkäin, PIN2-koodin käyttämistä edellyttävät toiminnot poistuvat käytöstä.

Pushmail-ratkaisu
Tässä ohjeessa Pushmail-ratkaisu kattaa sähköposti/kalenteri/yhteystieto -ohjelmistot. Pushmail poikkeaa sähköpostin synkronointiratkaisusta siinä, että järjestelmän toiminta ei edellytä käyttäjän toimintaa eli sähköposti/kalenteri/yhteystiedot päivittyvät älypuhelimeen automaattisesti sekä älypuhelimessa tapahtuvat muutokset päivittyvät automaattisesti takaisin taustajärjestelmään.

SIM
Subscriber Identity Module on puhelimen sisälle laitettava tunnistekortti, jonka avulla puhelimen käyttäjä tunnistetaan ja käyttäjälle rekisteröidyt palvelut aktivoidaan käyttöön kyseiseen laitteeseen.

SMS
Short Message Service eli lyhytviesti tai yleisemmin tekstiviestipalvelu vastaa lähes kaikissa matkapuhelimissa käytettävissä olevan tekstiviestipalvelun toiminnoista.

Symbian
Symbian on keskeisten matkapuhelinvalmistajien yhdessä perustama yritys, jonka tehtävänä on kehittää Symbian-käyttöjärjestelmää, jota useimmat älypuhelimien valmistajat käyttävät laitteissaan käyttöjärjestelmänä.

Sähköpostin synkronointiratkaisu
Aikaisemmin kuvattua Pushmail-teknologiaa vanhempaa sukupolvea oleva teknologia, joka edellyttää, että käyttäjä joko halutessaan itse aktivoi tai järjestelmä ajastettuna käy tarkistamassa uusien posti/kalenteri/yhteystietojen olemassaolon ja huolehtii tietojen lataamisesta.

UMTS
Universal Mobile Telecommunications System on kolmannen sukupolven laajakaistayhteys, jota on sittemmin nopeutettu HSDPA- ja HSUPA-tekniikalla.

UMTS on nopeudeltaan selvästi GPRS-yhteystapaa nopeampi, mutta sen kattavuus (kuuluvuusalue) on Suomessa toistaiseksi selvästi GPRS-yhteyksiä rajoittuneempi.

WAP
Wireless Application Protocol on OMA:n matkapuhelimiin määrittelemä protokolla, joka mahdollistaa IP-pohjaisten palveluiden tuomisen matkapuhelimeen. WAP-protokolla määrittelee mobiili-ympäristöön optimoituina mm. tiedonsiirtoprotokollia, XML-sanomien sisällön ja selaintoteutuksen. WAP-protokollaa hyödynnetään esimerkiksi MMS-sanomien välittämisessä ja binääri-muotoisissa asetustekstiviesteissä.

Windows Mobile
Windows Mobile on Microsoftin kehittämä, Symbian-käyttöjärjestelmää vastaava älypuhelinkäyttöjärjestelmä.

WLAN
Wireless Local Area Network mahdollistaa uusimmissa älypuhelimissa esimerkiksi internetin käyttämisen langattomien WLAN-verkon tukiasemien (access point) kautta.

Älypuhelin
Tässä asiakirjassa älypuhelimella tarkoitetaan sellaista puhelinlaitetta, joka sisältää oman käyttöjärjestelmän ja joka mahdollistaa kyseiselle käyttöjärjestelmälle tarkoitettujen sovellusten ajamisen.

Zero day-aukko
Paljastunut tietoturva-aukko, johon ei ole vielä saatavilla olevaa korjausta.

Liite 2. Voimassa olevat VAHTI-julkaisut

VAHTI 2/2007 Älypuhelimien tietoturvallisuus – hyvät käytännöt
VAHTI 1/2007 Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006 Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006 Tietoturvakouluttajan opas
VAHTI 10/2006 Henkilöstön tietoturvaohje
VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006 Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006 Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006 Electronic-mail Handling Instruction for State Government
VAHTI 1/2006 VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005 Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005 Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005 Information Security and Management by Results
VAHTI 5/2004 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004 Datasäkerhet och resultatstyrning
VAHTI 3/2004 Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004 Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004 Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006
VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 4/2003 Valtionhallinnon tietoturvakäsitteistö (uudistettavana)
VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003 Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002 Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002 Etätyön tietoturvaohje

VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001	Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001	Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus (uudistettavana)
VAHTI 2/2001	Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001	Valtion viranomaisen tietoturvallisuustyön yleisohje (uudistettavana)
VAHTI 3/2000	Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000	Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta (http://www.vm.fi/VAHTI) ja ohjeita saa myös tilattua painotalo Editasta.

Muistiinpanoja

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

VAHTI
2/2007
marraskuu 2007

ISSN 1455-2566
ISBN 978-951-804-761-5 (nid.)
ISBN 978-951-804-762-2 (pdf)