

# Informasjonssikkerhet ved bruk av lommedatamaskiner

Trusselvurderinger, sikkerhetsvurderinger og anbefalinger

Versjon 1.0  
24. juni 2002

KITH Rapport 11/02  
ISBN 82-7846-136-8

# KITH-rapport

Tittel

## Informasjonssikkerhet ved bruk av lommedatamaskiner

### Trusselvurderinger, sikkerhetsvurderinger og anbefalinger

Forfatter(e)

Magnus Alsaker, Bjarte Aksnes

Oppdragsgiver(e)

Sosial- og Helsedirektoratet

# KITH

Kompetansesenter for IT i helsevesenet AS

Postadresse

**Sukkerhuset  
7489 Trondheim**

Besøksadresse

**Sverresgt 15, inng G**

Telefon

**73 59 86 00**

Telefaks

**73 59 86 11**

e-post

[firmapost@kith.no](mailto:firmapost@kith.no)

Foretaksnummer

**959 925 496**

Rapportnummer	URL	Prosjektkode		
R 11/02	<a href="http://www.kith.no/rapportarkiv/lommedata.pdf">http://www.kith.no/rapportarkiv/lommedata.pdf</a>	S-IS02-HUS		
ISBN	Dato	Antall sider	Kvalitetssikret av	Gradering
82-7846-136-8	24. juni 2002	50	Arnstein Vestad	Ingen

Godkjent av

Jacob Hygen  
Adm. direktør

Sammendrag

Bruken av mobile lommedatamaskiner i helsevesenet vil trolig øke i omfang de neste årene. I denne sammenhengen er det viktig å se på hvordan informasjonssikkerheten ivaretas ved innføring av lommedatamaskiner. Det er viktig at slike mobile enheter ikke fører til svekket informasjonssikkerhet i helsevesenet.

Denne rapporten tar for seg ulike trusler mot informasjonssikkerheten ved bruk av lommedatamaskiner, og ulike tiltak som kan iverksettes for å dekke de ulike truslene. Det er i tillegg gitt en omtale av de mest vanlige plattformene (operativsystemene) for lommedatamaskiner med en kort vurdering av de sikkerhetsmekanismer de tilbyr.

Rapporten gir en anbefaling over punkter som er viktige å tenke på ved innføring av lommedatamaskiner i en helsevirksomhet. Det blir også gitt eksempler på ulike bruksområder og hvordan informasjonssikkerheten kan bli ivaretatt på de ulike bruksområdene.

# Innhold

<b>BAKGRUNN</b> .....	<b>1</b>
<b>INFORMASJONSSIKKERHET</b> .....	<b>2</b>
<b>HÅNDHOLDTE ENHETER</b> .....	<b>3</b>
Lommedatamaskiner.....	4
<b>BRUKSOMRÅDER FOR LOMMEDATAMASKINER</b> .....	<b>4</b>
Oppkobling av lommedatamaskiner.....	6
<b>TRUSSELVURDERINGER</b> .....	<b>8</b>
<b>KONFIDENSIALITET</b> .....	<b>8</b>
Lett å stjele eller miste.....	8
Sviktende tilgangskontroll.....	9
Utsiktet utlevering av informasjon.....	9
Personlig bruk.....	9
Manglende autentiseringsfunksjoner.....	10
Overføring av informasjon.....	10
Tapping av informasjon.....	11
Uautorisert tilkobling.....	11
<b>INTEGRITET</b> .....	<b>12</b>
Virus og/eller trojanske hester.....	12
Feil ved synkronisering (overskriving).....	12
Brukerfeil eller feil ved konfigurasjonen (dårlig brukergrensesnitt).....	12
Problemer med batterier.....	13
Tap av registrert informasjon.....	13
Manglende muligheter for sikkerhetskopi.....	13
Egeninstallerte applikasjoner.....	14
<b>TILGJENGELIGHET</b> .....	<b>14</b>
Lite ressurser (CPU, minne).....	14
Lite strøm.....	15
Trådløse nettverk.....	15
Mister eller glemmer lommedatamaskin.....	15
Glemmer passord (kryptering).....	16
Manglende tilgang til mobilnettet.....	16
<b>SIKERHETSVURDERING</b> .....	<b>17</b>
<b>OPERATIVSYSTEMER (OS)</b> .....	<b>17</b>
Windows CE.....	17
Palm OS.....	19
Symbian OS.....	20
Embedded Linux OS.....	22
Vurdering av de ulike OS.....	22
Synkronisering.....	23
Conduits.....	24
<b>SIKERHETSPROGRAMVARE</b> .....	<b>25</b>
Synkronisering og sikkerhetskopi.....	25
Anti-virus.....	26
Ekstern tilgang.....	26
Administrasjon.....	26
Kryptering.....	26
Sikre data på flerbruker lommedatamaskiner.....	26
Adgangskontroll.....	27

Trådløs overføring .....	27
Integritetssikring .....	27
<b>TILLEGGSUTSTYR .....</b>	<b>27</b>
Tap og tyveri .....	27
Smartkort .....	28
<b>ANBEFALINGER .....</b>	<b>29</b>
<b>KONTAKT MED DATATILSYNET .....</b>	<b>30</b>
<b>BESTEM BRUKSOMRÅDE .....</b>	<b>31</b>
<b>UTFØR RISIKOVURDERING .....</b>	<b>31</b>
<b>VURDER UTSTYR/OPPLÆRING .....</b>	<b>32</b>
<b>LAG POLICY OG REGLER .....</b>	<b>32</b>
<b>VURDER APPLIKASJONER .....</b>	<b>33</b>
<b>IMPLEMENTER SIKKERHETSMEKANISMER .....</b>	<b>34</b>
<b>RUTINER VED SIKKERHETSBRUDD .....</b>	<b>34</b>
<b>OPPLÆRING (SIKKERHET) .....</b>	<b>35</b>
<b>UTRULLING .....</b>	<b>35</b>
<b>KONTROLLER (REVISJON) .....</b>	<b>35</b>
<b>LITTERATUR .....</b>	<b>37</b>
<b>VEDLEGG A: OPERATIVSYSTEM .....</b>	<b>38</b>
<b>WINDOWS CE .....</b>	<b>38</b>
<b>PALM OS .....</b>	<b>39</b>
<b>SYMBIAN OS .....</b>	<b>40</b>
<b>VEDLEGG B: FORSLAG TIL SIKKERHETSLØSNINGER .....</b>	<b>42</b>
<b>EKSEMPEL 1: PERSONLIG BRUK .....</b>	<b>42</b>
<b>EKSEMPEL 2: MEDISINSKE APPLIKASJONER .....</b>	<b>43</b>
<b>EKSEMPEL 3: SENSITIVE OPPLYSNINGER .....</b>	<b>43</b>
<b>VEDLEGG C: CASE STUDIE .....</b>	<b>45</b>
<b>INFORMASJONSSIKKERHET .....</b>	<b>45</b>
<b>SIKKERHETSLØSNING .....</b>	<b>45</b>

## Bakgrunn

**Bruk av lommedatamaskiner i helsevesenet vil trolig bli mer vanlig i årene fremover. I denne sammenhengen er det viktig å se på hvordan informasjonssikkerheten ivaretas ved å innføre lommedatamaskiner. I dette kapitlet blir det beskrevet hva som menes med informasjonssikkerhet, hva lommedatamaskiner er og ulike bruksområder de kan tenkes brukt til innen helsevesenet.**

Lommedatamaskiner vil kunne få en viktig rolle i et framtidig helsevesen ved å tilby større mobilitet, bedre tilgjengelighet til viktig informasjon og mer effektiv datafangst ved at helsepersonell kan registrere opplysninger løpende. Ulike aktører i helsevesenet vil kunne dra nytte av denne typen verktøy, og slikt utstyr vil trolig tas i bruk av helsepersonell som leger og pleiepersonell, pasienter og administrativt personale. Slike løsninger vil ha et stort potensial både innenfor sykehusene, primærhelsetjenesten og i kommunehelsetjenesten, for eksempel innenfor hjemmebasert omsorg.

Helsepersonell har behov for mange typer informasjon i arbeidet sitt, og store deler av dette kan tilbys på lommedatamaskiner. I forbindelse med elektroniske journaler vil utstyret kunne benyttes til både framvisning og registrering av pasientdata uavhengig av hvor helsepersonellet befinner seg, for eksempel ved hjemmebesøk eller ved pasientvisitter. Lommedatamaskiner kan også kombineres med ulike former for medisinsk meldingsutveksling, for eksempel ved at lommedatamaskinen benyttes som en reseptblokk for å generere elektroniske resepter, eller for å framvise elektroniske laboratoriesvar.

Helsepersonell genererer og samler også inn informasjon i en rekke sammenhenger og mobilt utstyr som lommedatamaskiner kan gjøre denne innsamlingen mer effektiv. Et eksempel på dette kan være kroppstemperaturmålinger som skal foretas løpende av en pasient.

Pasienter vil kunne ha nytte av lommedatamaskiner under og etter sin kontakt med helsevesenet. Særlig vil lommedatamaskiner kunne være viktige støttespillere i egenbehandling i samarbeid med en ansvarlig lege, for eksempel etter en operasjon eller for diabetikere og for pasienter som er avhengig av jevnlig medisinerings. Lommedatamaskinene kan benyttes til innsamling av data fra pasienter, for eksempel ved ulike former for dagbokføring over kaloriinntak, væskeinntak, søvnperioder osv. Det kan også være aktuelt å sende korte meldinger til/fra ansvarlig lege.

I administrative sammenhenger kan lommedatamaskiner spille en viktig rolle. Kalenderfunksjoner kan kombineres med andre ressursstyringsverktøy for å bidra til at oppdatert informasjon om tilgjengelig personale, tilgjengelige operasjonssaler osv.. I tillegg kan denne typen utstyr fungere som adressebok, telefonkatalog og meldingsformidler (e-post) for ansatte i helsevesenet.

### **Gevinster**

Mange gevinster kan oppnås ved innføring av lommedatamaskiner i helsevesenet. Dette avhegner av bruksområder, men her er noen viktige gevinster:

- En effektivisering av de daglige rutiner - riktig prioritering av arbeidsoppgavene
- Mindre reising/får med det utstyret/de medisiner man har behov for
- Mindre tid til innsamling og registrering av pasientinformasjon
- Oppnår bedre kontroll - fjerner dobbeltregistrering/reducerer feilregistrering
- Dataene er tilgjengelig der man befinner seg
- Bedre arbeidsdag/mindre stress for helsepersonellet
- Mer tid til hver pasient (ansikt til ansikt)
- En økning i produktiviteten
- Oppnå bedre pasientbehandling og et bedre servicetilbud overfor pasientene

### **Informasjonssikkerhet**

Datatilsynet [13] sier at informasjonssikkerhet omfatter:

- Sikring av konfidensialitet, det vil si beskyttelse mot at uvedkommende får innsyn i opplysningene.
- Sikring av integritet, det vil si beskyttelse mot utilsiktet endring av opplysningene.
- Sikring av tilgjengelighet, det vil si sørge for at tilstrekkelige og relevante opplysninger er tilstede.

Datatilsynet sier videre at:

*”Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av ”planlagte og systematiske tiltak”. Begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet skal legges til grunn ved sikkerhetsarbeidet. De tiltak som etableres, skal være både organisatoriske og tekniske. Sikkerhetstiltakene og selve informasjonssystemet skal dokumenteres. Dokumentasjonen skal omfatte beskrivelse av organisering, rutiner for bruk samt registrering av hendelser”.*

Dette vil si at informasjonssikkerhet ikke bare omhandler tekniske spørsmål som brannmurer og adgangskontroll, men omfatter også for eksempel det at brukere følger regler/policyer og opptrer fornuftig ved bruk av datamaskiner.

Ved innføring av lommedatamaskiner i en helsevirksomhet er det viktig at informasjonssikkerheten blir ivaretatt med hensyn på den overnevnte personopplysningsloven fra Datatilsynet. I denne sammenhengen gjelder det da spesielt å ivareta de tre punktene angående konfidensialitet, integritet og tilgjengelighet.

## Håndholdte enheter

Det finnes en rekke ulike typer håndholdte enheter. Her er det listet opp ulike kategorier innenfor håndholdte enheter, og til slutt blir det beskrevet hvilke som omhandlet av denne rapporten:

- *Lomme PC*. Er relativt små enheter, ofte med en 320x240 (1/2 VGA) skjerm. De kommer med integrerte applikasjoner, og kan kommunisere trådløst eller via kabel med andre enheter.
- *Håndholdt PC*. Er litt større enheter, ofte med en 640x840 eller 800x600 (VGA) skjerm. De kan ha en trykksensitiv skjerm eller være tastaturbasert, de kommer med integrerte applikasjoner, og kan kommunisere trådløst eller via kabel.
- *Pocket PC*. Er et uttrykk for de enheter som bruker Microsoft Windows CE operativsystem. Dette kan gjelde både for lomme PCer og håndholdte PCer, men mest vanlig er nok utbredelsen på lomme PCer.
- *PDA (Personlig Digital Assistent)*. Er en samlebetegnelse for ulike typer håndholdte datamaskiner (er ikke det samme som håndholdt PC), og som har en trykksensitiv skjerm og/eller tastatur. PDA brukes for enheter hvor en kan få tilgang til, lagre og organisere diverse informasjon. De mest vanlige funksjonene er kalender, adressebok, e-post, oppgaveliste og notatliste. Noen modeller har også mulighet for enkel tekstbehandling og regneark.
- *PDAfon*. Dette er enheter som er inneholder funksjonalitet typisk for både PDAer og mobiltelefoner. Enten kan det være en mobiltelefon som har fått tillagt PDA egenskaper eller omvendt, men det finnes også produkter hvor de to typene er smeltet sammen fra begynnelsen av.
- *Spesialenheter*. Dette er enheter tiltenkt spesielt for en oppgave, som for eksempel GPS-mottakere.

De ulike betegnelse brukes ofte om hverandre, og spesielt PDA, lomme PC, håndholdt PC, og også lommedatamaskin er uttrykk som gjerne

blir brukt om de samme enhetene. En kan nok også finne at andre definisjoner enn de som er presentert ovenfor. Palm OS er per i dag markedsleder for PDAer, så ofte er PDA forbundet med modeller som benytter Palm OS.

### *Lommedatamaskiner*

De enhetene som er beskrevet i denne rapporten kan kalles lommedatamaskiner. Lomme sier noe om størrelsen på enhetene, og det er ”typisk” lomme-PC størrelse (for eksempel Compaq, Palm eller Handspring). Datamaskin sier noe om funksjonaliteten til enheten. Med dette menes det at enheten benytter et operativsystem (kan være for eksempel være Palm OS, Windows CE eller Symbian OS) og at det finnes applikasjoner som kan kjøres på dette operativsystemet.

I praksis vil begrepet lommedatamaskiner omfatte alle PDA modeller (både lomme PC og håndholdt PC), og PDAfon modeller (som for eksempel Nokia 9210, Siemens SX45 eller Sony Ericsson P800).

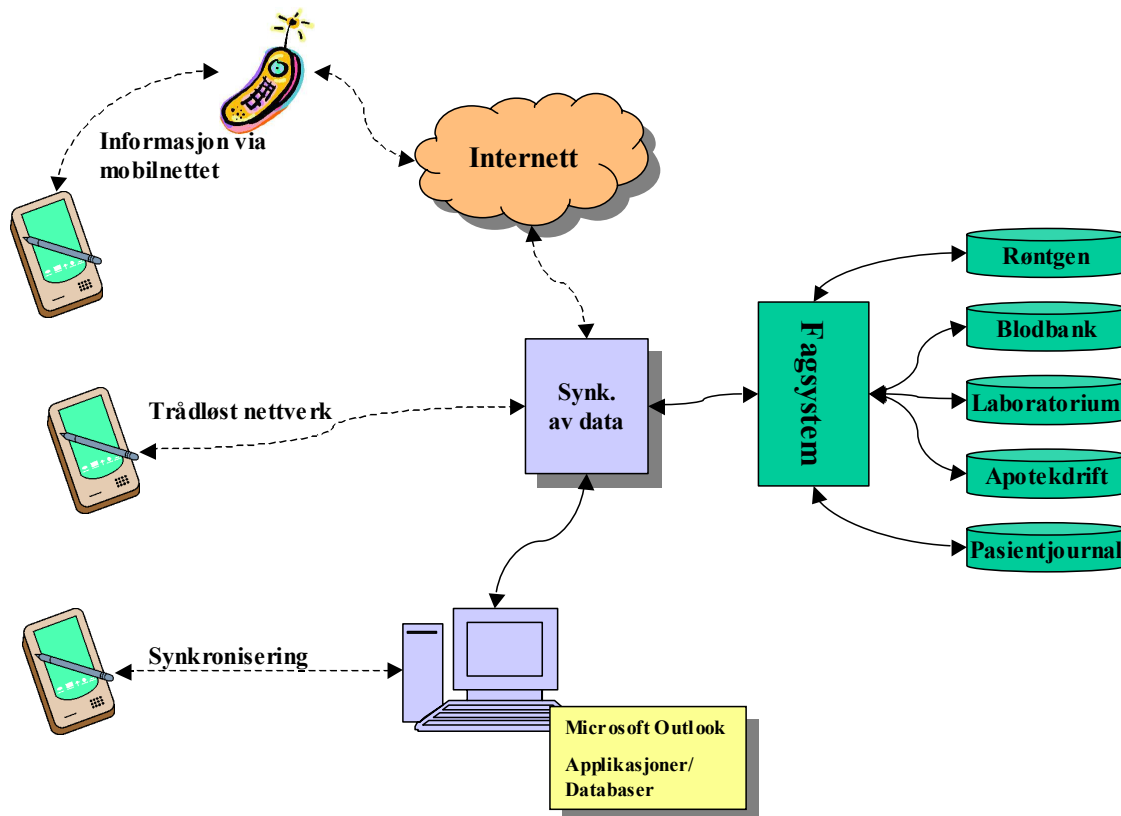
### **Bruksområder for lommedatamaskiner**

En lommedatamaskin kan ha mange ulike bruksområder. Vi vil dele opp bruksområdene i tre ulike hovedkategorier:

1. *Personlig bruk.* Dette vil si at enheten brukes kun til lagring av brukerens personlige data, som for eksempel adresse-, kalender- og avtalebok. Ingen helseopplysninger blir lagret eller går via den håndholdte enheten. Dette er også bruk som gjør at enheten ikke trenger å være knyttet opp mot nettverk og/eller vanlige PCer.
2. *Medisinske applikasjoner.* Dette er bruk som er knyttet opp mot ulike medisinske applikasjoner, men som ikke medfører at sensitive data er lagret på enheten. Dette kan for eksempel være opplysninger om medisiner eller kodeverk.
3. *Sensitiv informasjon.* Dette er bruk der enheten på en eller annen måte er knyttet opp mot for eksempel ulike fagsystem. Enhetene vil derfor inneholde strukturerte sensitive opplysninger. Dette kan eksempelvis være pasientopplysninger knyttet til pasientjournalen. I slike sammenhenger kan det tenkes at lommedatamaskinen kan brukes til registrering og/eller uthentning av informasjon for en gitt pasient. Det kan også tenkes at sensitive opplysninger er lagret i ustrukturerte form. Dette kan for eksempel være notater om en sykdom for en pasient.

Hvordan lommedatamaskiner brukes, vil påvirke hvordan informasjonssikkerheten bør behandles. Se Vedlegg B for eksempler på mer konkrete

bruksområder og hvordan informasjonssikkerheten kan ivaretas med ulike bruksområder innen helsevesenet.



Figur 1: Ulik bruk av lommedatamaskiner

Figuren over viser ulike bruksområder for lommedatamaskiner. Den enkleste formen for bruk er å benytte lommedatamaskinene til personlig bruk, enten med eller uten synkronisering av data mot en PC. Bruk av lommedatamaskiner til behandling av sensitiv helseinformasjon (jf. 3) vil som regel innebære at en må synkronisere informasjon opp mot fagsystem i helsevesenet. Dette kan for eksempel være å motta informasjon om ulike typer medisiner eller å oppdatere en pasientjournal med informasjon om en pasient.

Oppkobling mot ulike fagsystem kan, som figuren over viser, tenkes gjort på flere ulike måter:

1. Ved å synkronisere lommedatamaskinen mot en PC som igjen kommuniserer med fagsystemene.
2. Ved å overføre informasjon via et trådløst nettverk slik at en kommuniserer mer direkte med fagsystemene.
3. Ved at en gjennom bruk av mobiltelefon og Internett kan kommunisere med fagsystemene.

Dette er eksempler på bruk av lommedatamaskiner, og det kan godt tenkes at de blir brukt på andre måter. For eksempel kan Bluetooth benyttes til å overføre data mellom enheter som er innenfor et begrenset område (ca 10-15 meter).

### *Oppkobling av lommedatamaskiner*

I forbindelse med oppkobling av lommedatamaskiner ved overføring eller synkronisering av informasjon vil det være ulike sikkerhetskrav i forhold til ulike bruksområder.

For en virksomhet som har et elektronisk informasjonsnettverk er det vanlig å dele nettverket opp i ulike soner. Nettverksstrukturen kan variere, men en lignende oppdeling av nettverket bør en finne hos de fleste virksomheter:

1. **Eksterne nettverk** er nettverk som virksomheten er tilknyttet, men som den ikke har kontroll over (for eksempel Internett).
2. **Demilitarisert sone (DMZ)** er nettverk som virksomheten har kontroll over, men som er åpne for besøkende, og som gir fri tilgang til bruk av spesielle tjenester (som for eksempel WWW eller FTP).
3. **Interne nettverk** er nettverk som er regnet som private, hvor de ansatte lagrer og jobber med data tilhørende virksomheten. Det interne nettverket er ofte oppdelt i flere sensitive og interne soner. Slike nettverk har som regel ingen eller sterkt begrenset adgang utenfra og inn, og også begrenset adgang innenfra og ut.

Dette vil si at sensitive opplysninger bare bør behandles på det interne sensitive nettverket. Vi gir følgende forslag til oppkobling av lommedatamaskiner med bakgrunn i de tre bruksområdene som ble definert ovenfor:

- **Personlig bruk** kan i utgangspunktet skje i alle tre nettverksområder. Dersom sensitive personopplysninger tilhørende brukeren ligger på lommedatamaskinen, bør oppkobling skje i demilitarisert sone (eller i det interne nettverket).
- **Medisinsk bruk** ble definert til ikke å være av sensitive art, så oppkobling kan i utgangspunktet skje på alle tre nettverksområdene.
- **Sensitiv informasjon** bør bare bli brukt i forbindelse med oppkobling i det interne sensitive nettverket. Denne bruken bør ikke sammenblandes med personlig bruk.

Dette er bare et generelt forslag og oppkobling av lommedatamaskinene mot de ulike nettverkssonene må vurderes i ulike tilfeller hos hver enkelt

## BAKGRUNN

helsevirksomhet.

# Trusselvurderinger

**Dette kapitlet tar for seg noen av truslene mot informasjonssikkerheten ved bruk av lommedatamaskiner. Det er ikke utført noen form for risikoanalyse, men vi vil peke på noen områder som vi mener kan være trusler mot informasjonssikkerheten.**

Hendelser som for eksempel strømbrudd, overoppheting av tjenere eller diskkrasj blir ikke behandlet i denne rapporten, da dette er hendelser som ikke går direkte på bruken av håndholdte enheter. Dette er problemområder som likevel bør gås gjennom ved innføring av nye datasystem. Ved vurdering av de ulike aktuelle truslene har vi tatt utgangspunkt i trusler mot henholdsvis konfidensialitet, integritet og tilgjengelighet (jf. Datatilsynet).

Som sagt er det ikke gjennomført noen risikovurdering, men denne rapporten kan fungere som grunnlag for eventuelle risikovurderinger som senere blir utført.

## Konfidensialitet

Konfidensialitet vil si at informasjon gjøres utilgjengelig for uautoriserte. Her er det beskrevet noen områder hvor bruk av lommedatamaskiner kan tenkes å true konfidensialiteten:

### *Lett å stjele eller miste*

En lommedatamaskin er relativt liten og lett, og er derfor lett å glemme igjen eller miste. Dette har også sammenheng med at den tas med rundt omkring og brukes på ulike steder. Den er også lettere å stjele enn en stasjonær PC som er mye større og tyngre, og en lommedatamaskin er som regel ikke fysisk tilkoblet noe nettverk eller lignende. En lommedatamaskin er i tillegg trolig relativt lett å omsette.

Dersom lommedatamaskiner blir stjålet eller mistet mens den er koblet opp mot for eksempel en server, kan uvedkommende i verste fall få full adgang til virksomhetens nettverk som lommedatamaskinen er koblet opp mot.

### Mulige tiltak

Ved bruk kan lommedatamaskinen fysisk festet fast til brukeren eller den PCen den synkroniseres opp mot. Når enhetene ikke blir brukt kan de

låses inne i skap/rom, eller oppbevares i områder med adgangskontroll. Andre tiltak kan for eksempel være automatisk frakobling mot server når det har gått en tid uten aktivitet.

### *Sviktende tilgangskontroll.*

Mange lommedatamaskiner har i utgangspunktet ingen krav om passord. Derfor kan det være enkelt å få tilgang til informasjon lagret på en lommedatamaskin. Skulle lommedatamaskinen ha god tilgangskontroll kan det bli ”irriterende” for brukeren for eksempel å måtte logge seg inn gjentatte ganger i løpet av en arbeidsdag. Dette har sammenheng med at den håndholdte enheten trolig blir brukt mange ganger i løpet av arbeidsdag, og da i relativt korte tidsrom av gangen.

Selv om en lommedatamaskin skulle være låst kan en få tilgang til informasjonen som er lagret på lommedatamaskinen. Dette kan for eksempel gjelde dersom det blir stjålet og den blir koblet opp mot en vanlig PC og en får tilgang til informasjon ved å laste informasjonen fra lommedatamaskinen til PC. Det kan også tenkes at personer greier å omgå adgangskontrollen som er på lommedatamaskinen. Dette gjelder spesielt dersom en bruker de tilgangskontrollene som følger med lommedatamaskinene.

### **Mulige tiltak**

Ta i bruk passordfunksjonene på lommedatamaskinene og kreve at brukerne bruker passord som ikke er intuitive. En sikkerhetspolicy for passord vil for eksempel kunne sette krav om både tall og bokstaver, og ingen repeterende (hhh) eller følger av tegn (abc, 123). En kan også installere ekstra programvare som tar hånd om adgangskontroll. Dersom streng adgangskontroll er nødvendig, kan bruk av smartkort være aktuelt.

### *Utsiktet utlevering av informasjon*

Stort sett all utlevering av elektronisk informasjon medfører en fare for at en utsiktet utleverer informasjon. Det er også fare for utsiktet overføring ved bruk av lommedatamaskiner, noe som kan skyldes alt fra dårlige brukergrensesnitt til brukerfeil. Utsiktet utlevering kan skje for eksempel ved bruk av e-post, ved synkronisering eller ved trådløs overføring (IR, bluetooth).

### **Mulige tiltak**

Opplæring i bruk av lommedatamaskiner og programvare, og konfigurering slik at dette unngås.

### *Personlig bruk*

Personlig bruk (for eksempel bruk av e-post, kalender eller notatbok) av lommedatamaskinen kan medføre at en får tilgang til sensitiv jobbinformasjon. Dette kan være en trussel dersom andre (ektefelle, barn, venner

eller lignende) bruker lommedatamaskinen og gjennom slik personlig bruk får tilgang til sensitiv informasjon.

Et annen trussel er at den personlige bruken kan endre på lagret jobbinformasjon uten at en er klar over det, dette kan være at informasjon blir slettet, endret eller lagt til. Dette kan skje utilsiktet, men kan også skje ved at uvedkommende får tilgang til lommedatamaskinen og endrer eller tar med seg informasjon ved en bevisst handling.

### **Mulige tiltak**

Installere programvare som gjør at en kan opprette flere brukerprofiler på lommedatamaskinen. Da kan en brukerprofil være tiltenkt jobbruk og en brukerprofil være tiltenkt personlig bruk. Disse sikres så med passordbeskyttelse.

### *Manglende autentiseringsfunksjoner*

Autentiseringsprosedyrer må være uavhengige om en bruker en lommedatamaskin eller en vanlig PC. Bruk av lommedatamaskiner må ikke føre til at en benytter prosedyrer for autentisering som gir mindre sikkerhet enn dersom en for eksempel hadde benyttet en vanlig PC.

Lommedatamaskiner kan også ha manglende støtte for sterk autentisering (dette vil si at en har to-faktor autentisering - betyr at autentiseringen består av noe fysisk (for eksempel smartkort) og noe en vet (for eksempel et passord)) til enheten. Dette kan for eksempel gjelde muligheter for å benytte smartkort, passordkalkulatorer, fingeravtrykk el. Dette kan føre til at personer som ikke skulle hatt tilgang til informasjon, likevel greier å opptre som en autentisert bruker ved for eksempel å få tilgang til brukernavn og passord.

### **Mulige tiltak**

Installere nødvendig programvare og eventuell maskinvare/tilleggsutstyr som gjør at en kan nytte seg av de nødvendige autentiseringsfunksjoner og/eller autentiseringsutstyr (for eksempel smartkort).

### *Overføring av informasjon*

Ved bruk av lommedatamaskiner vil en ofte overføre informasjonen til en lagringsplass utenfor enheten. Dette kan gjelde ved synkronisering mot PC gjennom kabel, bruk av IR eller Bluetooth, eller bruk av trådløst nettverk. Ved slike handlinger kan det tenkes at informasjon overføres feil eller kan gå tapt. Det er også mulighet for at uvedkommende kan få tilgang til informasjon for eksempel ved overføring ved hjelp av trådløst nettverk eller Bluetooth.

### **Mulige tiltak**

Opplæring i bruken av slike funksjoner, og innfør policyer for slik bruk. Konfigurer enheter som kommuniserer med hverandre slik at det minimaliserer risikoen for at noe går feil. Et annet tiltak er å kryptere infor-

masjon slik at uvedkommende ikke har nytte av den uten en gyldig krypteringsnøkkel.

### *Tapping av informasjon*

Tapping av informasjon kan være et problemområde ved bruk av håndholdte enheter i trådløse nettverk. Ved fysiske nettverk må en fysisk være tilkoblet nettverket, mens ved bruk av trådløse nettverk er det nok å være innenfor det området som det trådløse nettverket dekker. Dette vil si at en for eksempel kan sitte på utsiden av en bygning og likevel ha kontakt med det trådløse nettverket. Dette kan utnyttes for eksempel ved at noen avlytter informasjonen på nettverket.

Tapping av informasjon kan også skje ved bruk IR(Infrarød). For eksempel kan en enhet med IR port (bærbar PC eller lommedatamaskin) koble seg opp mot en lommedatamaskin og for eksempel starte en automatisk synkronisering.

### **Mulige tiltak**

Send informasjon kryptert slik at bare de med gyldige nøkler kan gjøre seg nytte av den. Lås alltid PCer og lommedatamaskiner når de ikke er i bruk, og krev passord når informasjon for eksempel skal synkroniseres mellom en PC og en lommedatamaskin.

### *Uautorisert tilkobling*

Et annet problemområde kan være at det er lett for uautoriserte å koble seg opp mot PC/lommedatamaskin slik at de kan hente data fra PC til lommedatamaskinen eller omvendt. For eksempel dersom en PC står ulåst og er utstyrt med kabel og programvare for synkronisering mot lommedatamaskiner, kan en utenforstående person med sin egen lommedatamaskin laste ned informasjon fra PC og til lommedatamaskinen. Det samme kan tenkes utført dersom noen ”finner” en ulåst lommedatamaskin og har tilgang til en maskin (eller en har med egen bærbar PC eller lommedatamaskin) som kan motta data fra lommedatamaskinen. Slik uautorisert oppkobling kan også tenkes skje gjennom bruk av trådløs kommunikasjon.

Andre konsekvenser av at uautoriserte kobler seg opp er ikke bare at de kan hente informasjon ut av nettverket, men også legge inn informasjon som skader en virksomhet eller installere virus eller annen ondartet programvare.

### **Mulige tiltak**

Kreve passord når en skal synkronisere data mellom PC og lommedatamaskin eller trådløst gjennom et nettverk. Sperr PCer og lommedatamaskiner for uautoriserte når de ikke er i bruk.

## **Integritet**

Integritet vil si at informasjonen ikke er endret, lagt til, slettet eller på annen måte forandret av noen andre enn de som har hatt gyldig tilgang til informasjonen.

Her er noen områder hvor bruk av håndholdte enheter kan tenkes å true integriteten til informasjonen:

### *Virus og/eller trojanske hester*

På samme måten som vanlige PCer er også lommedatamaskiner utsatt for virus og trojanske hester. Dette kan være aktuelt i forbindelse med at lommedatamaskinen er tilknyttet et nettverk, at den blir koblet opp mot Internett eller at personlig bruk introduserer virus eller trojanske hester. Ikke bare kan selve lommedatamaskinen få virus, det kan også tenkes at virus/trojanske hester kan overføres til en PC og resten av nettverket når en synkronisering blir gjort.

### **Mulige tiltak**

Installere virusprogrammer på lommedatamaskiner og PCer for å hindre ondsinnet programvare. Unngå bruk av Internett på maskiner som inneholder sensitiv informasjon. En kan også sperre PC og lommedatamaskiner når de ikke er i bruk slik at maskinene ikke står åpne for ”planting” av ondsinnet programvare.

Et annet enkelt tiltak er unngå enheter, programvare og operativsystemer som en vet er utsatt for ondsinnet programvare på grunn av sin oppbygning og arkitektur.

### *Feil ved synkronisering (overskriving)*

Dersom den håndholdte enheten blir synkronisert mot en vanlig PC kan det tenkes at det skjer feil i denne prosessen. Dette kan være at data blir overskrevet, eller at konfigurasjonen er satt opp feil slik at synkroniseringen går feil vei og data kan gå tapt. Rene tekniske ting i forbindelse med en synkronisering blir stort sett håndtert av programvaren, men et viktig punkt er at det bør være muligheter for å kunne reversere (gjøre en roll back) en synkronisering.

### **Mulige tiltak**

Konfigurer enheter som synkroniserer med hverandre slik at risikoen for feil minimaliseres. Gi opplæring i synkronisering slik at brukerfeil unngås. Et annet tiltak er å innføre automatisk sikkerhetskopiering før en foretar en synkronisering.

### *Brukerfeil eller feil ved konfigurasjonen (dårlig brukergrensesnitt)*

Å bruke en lommedatamaskin er ikke det samme som å bruke en vanlig PC. En liten skjerm som er trykksensitiv og kanskje mangel på et vanlig

tastatur gjør at det kan føles mer tungvint å bruke en lommedatamaskin enn en vanlig PC. For eksempel kan utilsiktet berøring på den trykksensitive skjermen føre til at data blir slettet, eller at informasjon blir sendt til en som ikke skulle hatt det. Det kan også skje feilregistreringer av data som følge av at brukeren skriver inn feil verdier eller tegn.

Et annet problemområde kan være feil i oppsettet av konfigurasjonen på lommedatamaskinen. Dette kan for eksempel gjelde sikkerhetsinnstillinger, synkronisering eller nettverk.

### **Mulige tiltak**

Gi opplæring i bruk av lommedatamaskiner, og ta i bruk programvare som gjør at for eksempel en felles IT-ressurs kan konfigurere alle lommedatamaskiner. Et naturlig tiltak vil være å velge de lommedatamaskinene som er mest brukervennlige og som har det beste brukergrensesnittet for bruksområdet til lommedatamaskinene.

### *Problemer med batterier*

Til bruk ute i ”felten” baserer lommedatamaskiner seg på strøm fra batteri. Trusler her kan være at batteriet går tomt eller at det skjer en feil slik at batteriet slutter å fungere. Følgene av dette er for det første at enheten ikke er funksjonell, men det kan også tenkes at informasjon går tapt.

### **Mulige tiltak**

Installere programvare som tar hånd om sikkerhetskopiering av informasjon som ligger lokalt på lommedatamaskinen. Innfør rutiner som gjør at tomme batterier unngås midt i en arbeidsdag.

### *Tap av registrert informasjon*

Dersom informasjon blir lagret lokalt på den lommedatamaskinen, enten for kortere eller lengre tid, er det en fare for at informasjonen kan mistes. Dette kan skyldes flere forhold, for eksempel brukerfeil, strømtap eller at lommedatamaskinen blir mistet, glemt eller stjålet.

Et annet problem kan være at lommedatamaskinen ”henger” seg, noe mange IT-brukere opplever fra tid til annen. Dette kan føre til at informasjon som ikke er lagret (eller synkronisert) går tapt.

### **Mulige tiltak**

Installere programvare som tar hånd om sikkerhetskopiering av informasjon som ligger lokalt på lommedatamaskinen. Innfør rutiner som for eksempel kan inkludere synkronisering eller overføring av data via trådløst nettverk som gjør at risikoen for å miste data blir minimalisert.

### *Manglende muligheter for sikkerhetskopi*

Sikkerhetskopiering av informasjon er aktuelt når informasjon blir lagret lokalt på lommedatamaskinen. Dette kan være et problem fordi lommedatamaskiner nødvendigvis ikke har funksjoner for sikkerhetskopiering.

Dette kan igjen føre til at informasjon oftere må synkroniseres mot PC eller overføres via det trådløse nettverket. Dette igjen medfører risikofaktorer som allerede er omtalt. Dette fører også til at mer tid går med til å sikre at ikke informasjon går tapt.

#### **Mulige tiltak**

Installere programvare som tar hånd om sikkerhetskopiering av data som ligger lokalt på lommedatamaskinen, og innfør rutiner om synkronisering av data fra lommedatamaskin til PC.

#### *Egeninstallerte applikasjoner*

Dersom lommedatamaskinen også blir brukt til personlig bruk, kan det tenkes at brukeren installerer applikasjoner selv på lommedatamaskinen. Uten å være klar over det kan disse applikasjonene påvirke ”jobb-bruken” eller den kan slette informasjon som ligger på lommedatamaskinen. Å installere egne applikasjoner medfører også en risiko for at disse kan inneholde virus eller andre elementer som kan på virke oppførselen til lommedatamaskinen.

#### **Mulige tiltak**

Innfør rutiner/regler som tar hånd om installering av egne (personlige) applikasjoner. Installer programvare som hindrer andre enn for eksempel en administrator i å installere applikasjoner på lommedatamaskinen.

### **Tilgjengelighet**

Tilgjengelighet vil si at informasjonen er tilgjengelig for autoriserte når og der det er behov for det.

Her er noen områder hvor bruk av håndholdte enheter kan tenkes å true tilgjengeligheten til informasjon:

#### *Lite ressurser (CPU, minne)*

Håndholdte enheter har på grunn av sin størrelse og vekt lite ressurser i forhold til en stasjonær eller bærbar PC. Dette gjelder først og fremst prosessorkraft (CPU) og minne. Ved mye bruk av lommedatamaskinen kan det derfor oppstå situasjoner der minnet er fullt slik at informasjon ikke kan lagres, eller at enheten er utilgjengelig fordi all prosessorkraft går med til for eksempel å overføre data til nettverket.

Ved bruk av tunge applikasjoner kan det også tenkes at lommedatamaskinen fungerer tregt, og det tar lang tid for eksempel å registrere informasjon.

#### **Mulige tiltak**

Innfør rutiner om synkronisering/overføring av informasjon slik at en unngår at lommedatamaskinen får minnet oppfylt. Hindre at applikasjoner som ikke er nødvendige blir installert på lommedatamaskinen.

***Lite strøm***

På grunn av størrelse og vekt har håndholdte enheter begrenset brukstid før de må lades opp eller tilkobles strøm. Dersom lommedatamaskinene brukes så mye på en dag at det fører til lite strøm, vil dette kunne føre til at den ikke kan brukes. Utladingen kan skje hurtigere dersom lommedatamaskinene også blir brukt personlig, slik at dette tapper enheten for strøm.

**Mulige tiltak**

Innfør rutiner som gjør at en unngår at lommedatamaskinen går tom for strøm midt i en arbeidsdag. Redusere/unngå bruk av lommedatamaskinen til personlig (og annen "unødig") bruk.

***Trådløse nettverk***

Trådløse nettverk er delte medium, som betyr at kapasiteten deles mellom de som bruker det samme trådløse nettverket. Mange brukere på et trådløst nettverk vil altså kunne føre til at det blir mindre kapasitet på hver bruker. Dette kan føre til at overføring går tregt, og også bli brutt, som følge av stor belastning på det trådløse nettverket.

Et annet problemområde kan være dersom noen utenfra kommer seg inn på nettverket og "okkuperer" store deler av nettverket slik at andre overføringer blir brutt eller forsinket. Det samme gjelder også for DOS-angrep (tjenestenektingsangrep) slik at ikke ansatte i virksomheten ikke får nytte av nettverket.

**Mulige tiltak**

Innfør rutiner/regler som gjør at unødvendig ressursbruk av det trådløse nettverket minimaliseres, og at unødvendig tilgang til nettet reduseres. Innfør rutiner/regler for overføring av informasjon slik nettverkets kapasitet blir utnyttet best mulig.

***Mister eller glemmer lommedatamaskin***

På grunn av størrelsen er en lommedatamaskin både lettere å miste og glemme igjen enn for eksempel en bærbar PC. Har man ikke lommedatamaskinen har man heller ikke tilgang til data som er lagret på enheten. I beste fall fører dette til en periode hvor man ikke har tilgang til en bestemt lommedatamaskin. I verste fall fører dette til at man kan ha mistet (sensitive) opplysninger for godt, og at disse blir funnet av noen som ikke skulle hatt tilgang til dem.

**Mulige tiltak**

Innfør regler/rutiner som for eksempel gjør at lommedatamaskinene ikke forlater bruksområdet, eller at all oppbevaring skjer på et sentralt sted.

***Glemmer passord (kryptering)***

Ved bruk av håndholdte enheter er det en mulighet for at en glemmer passord for å komme seg inn på enheten eller for kryptering. Glemte passord for kryptering kan føre til at en ikke får tilgang til data som er lagret kryptert på enheten, eller at en må sende sensitiv informasjon ukryptert. Glemte passord kan også føre til at en må "bryte" seg inn på lommedatamaskinen slik at informasjon eventuelt kan gå tapt.

**Mulige tiltak**

Passord blir lagret i kryptert form på et sted hvor brukerne har tilgang. Dette vil i praksis si at passord blir kryptert med en nøkkel som brukeren så oppbevarer på et tilgjengelig sted.

***Manglende tilgang til mobilnettet***

Noen applikasjoner kan tenkes å bruke mobilnettet for å sende data (dette kan for eksempel gjelde en hjemmesykepleier ute på jobb), vha. SMS-meldinger eller WAP (Wireless Application Protocol) applikasjoner. Dersom en ikke har tilgang til mobilnettet (dårlig dekning, basestasjoner ute av drift) får en ikke sendt den informasjonen en har tenkt. Mer kritisk kan det være dersom en skal ha tilgang til informasjon, men at det ikke er mulig av de nevnte grunner over.

Et annet trusselområde kan være at det er ulovlig å bruke mobiltelefon i noen områder. Dette kan for eksempel gjelde på sykehusområder hvor det finnes mye teknisk utstyr som kan påvirkes av mobiltelefonbruk. Dette kan for eksempel føre til at en ikke kan bruke visse typer applikasjoner som er nevnt ovenfor.

**Mulige tiltak**

Vanskelig å gi konkrete tiltak, da tilgang til mobilnettet ikke er noe en selv kan styre. Organisatoriske tiltak som for eksempel å sende/motta data før en drar inn i et område som en vet har dårlig dekning for mobilnettet (eller hvor bruk er ulovlig) kan være en løsning.

Fremtidige tiltak vil kunne være å ha alternative kommunikasjonslinjer dersom primærlinjen er utilgjengelig (eller ulovlig). Den alternative kommunikasjonslinjen vil for eksempel kunne ha redusert ytelse, men vil likevel kunne fungere i et kort tidsrom som en reservelinje.

# Sikkerhetsvurdering

**Dette kapitlet tar for seg hvordan lommedatamaskiner kan håndtere informasjonssikkerhet. Det blir sett på hva som finnes av mekanismer i de mest vanlige operativsystemene brukt på lommedatamaskiner, og litt om hva som finnes av programvare og tilleggsutstyr for å bedre håndteringen av informasjonssikkerheten.**

Vanligvis følger det med ”enkle” mekanismer for å ta vare på informasjonssikkerheten når en kjøper en lommedatamaskin. Dette kan være passordbeskyttelse av enten hele eller deler av lommedatamaskinen. I tillegg er det sjelden noe krav til passordet med tanke på antall tegn, bruk av tall eller at det skiller mellom store og små tegn. Skal en ha mer avanserte mekanismer må en som regel installere programvare og/eller skaffe tilleggsutstyr som gjør at en får det sikkerhetsnivået som er ønskelig.

## Operativsystemer (OS)

Det finnes flere ulike OS for bruk på lommedatamaskiner i dag, blant annet Palm OS, Windows CE, Casio OS, Symbian OS (EPOC) og Linux. Det som har vært mest utbredt frem til nå er Palm OS, men også Symbian og spesielt Windows CE har fått en betydelig utbredelse. Symbian OS er mest aktuelt i forbindelse med såkalte PDAfoner (omtalt i kapittel 2). PDAfoner ble i kapittel 2 omtalt som aktuelle lommedatamaskiner, og en vurdering av Symbian OS er derfor tatt med her.

Vedlegg A gir en mer detaljert beskrivelse av de tekniske løsningene for å håndtere ulike sikkerhetsmekanismer.

### *Windows CE*

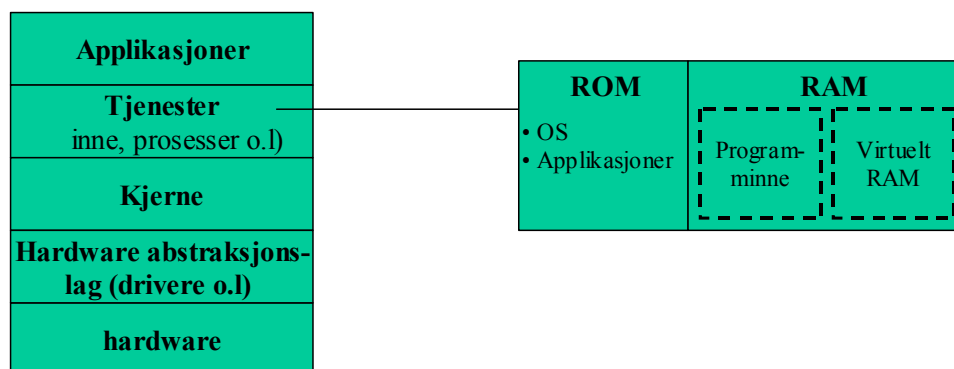
Windows CE er utviklet av Microsoft og brukes blant annet i Compaq, Hewlett Packard og Casio sine lommedatamaskiner. Windows CE ble lansert i 1996, og den grunnleggende arkitekturen er lik den en finner på Windows utgaver for vanlige PCer. Dette betyr at det er bygget på deler av Win32 API som en finner igjen i ”vanlige” Windows versjoner. Windows CE er per i dag et svært avansert operativsystemet for lommedatamaskiner, og har støtte for blant annet lyd-, bilde- og musikkfiler. Enkle versjoner av Microsoft Word og Excel er tilgjengelige for Windows CE. Minnebruket i Windows CE og applikasjonene er stort, men lommedatamaskiner som kjører Windows CE er også relativt kraftige, prosessorer på omkring 200 MHz og minne på 32 MB er å finne på for eksempel

Compaq sine modeller. Windows CE tillater også at en på lik line med et vanlig Windows OS kan kjøre flere prosesser (flere ulike applikasjoner) samtidig. Dette vil for eksempel si at mens en skriver et notat i Pocket Word, kan nettleseren motta data via det trådløse nettverket eller en applikasjon kan laste opp data fra en database.

Lommedatamaskiner med Windows CE er utviklet slik at de skal fungere som miniutgaver av vanlige PCer. Dette kan en se på det grensesnittet som brukeren møter og de muligheter som Windows CE gir.

### OS arkitektur

I et Windows CE basert system inneholder ROM (Read Only Memory) hele operativsystemet, sammen med applikasjonene som kommer med OSet. Dersom en programmodul ikke er komprimert blir den kjørt i ROM. Dersom den er komprimert, blir programmodulen dekomprimert og lastet over til RAM (Random Access memory) før den blir kjørt. Alle lese-/skrivedata blir lastet inn i RAM.



Figur 2. Windows CE arkitektur

RAM er delt inn i to områder, en del for programminne og en virtuell RAM disk. Den virtuelle RAM disken inneholder data som blir tatt vare på dersom systemet er suspendert, og mange lommedatamaskiner har en egen sikkerhetskopi av innholdet i RAM dersom det for eksempel skulle skje noe med strømmen. Resten av RAM er forbeholdt programminne, og det fungerer som på en vanlig PC. Det tar vare på informasjon om applikasjoner som er kjørende.

Windows CE bruker virtuelt minne og MMU (Memory Management Unit), noe som fører til at ingen applikasjoner har adgang til hverandres minneområder fordi de kjøres i beskyttede minneområder.

### Informasjonssikkerhet

Windows CE har støtte for flere ulike sikkerhetsmekanismer. OSet støtter bruk av SSL (Secure Socket Layer) 2.0 og 3.0 for sikre nettverksforbindelser, kryptering ved hjelp av Microsoft Cryptographic

delser, kryptering ved hjelp av Microsoft Chryptographic API (CAPI), digitale sertifikat og bruk av smartkort. Dette gjør at Windows CE kan bygges ut slik at det bidrar til både konfidensialitet og autentisering. Når det gjelder autorisering må det installeres ekstra programvare dersom en ønsker flere muligheter enn den passordbeskyttelsen som allerede finnes på lommedatamaskinen.

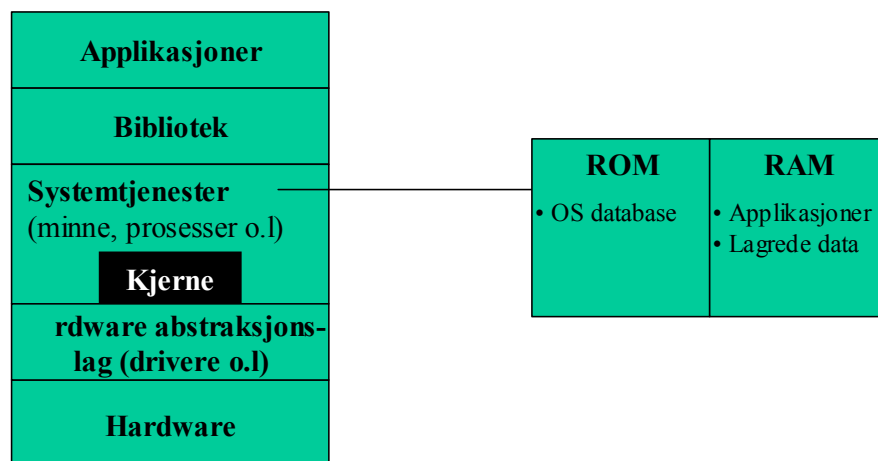
### *Palm OS*

Palm OS blir brukt av lommedatamaskinprodusenter som Palm Pilot, Sony og Handspring. Palm OS har vært det den mest brukte plattformen på lommedatamaskiner, og hadde i 1999 oppunder 80% av markedet. Denne andelen har gått nedover de siste årene, men Palm er fortsatt det mest brukte. Palm OS bruker ikke et tradisjonelt filsystem, men er utviklet med tanke på at det skal være optimalisert med tanke på synkronisering med en primærenhet (en PC), og at det skal bruke så lite ressurser som mulig. Små og enkle programmer fungerer derfor raskt og bra på et Palm OS.

Til forskjell fra Windows CE er ikke Palm OS sin arkitektur bygget opp på samme måten som et OS for en vanlig PC. Palm OS er mer rendyrket for å fungere på en lommedatamaskin, og har derfor sine begrensinger med tanke på muligheter og funksjonalitet i forhold til Windows CE. Lommedatamaskiner med Palm OS er ofte mindre kraftige enn de som kjører Windows CE. Prosessor på 20 MHz og 8 MB minne er ikke uvanlig for en lommedatamaskin med Palm OS. Derfor har også lommedatamaskiner med Palm OS ofte vært billigere enn de med Windows CE. Palm OS kan, til forskjell fra Windows CE, bare kjøre en type applikasjoner om gangen. Palm OS er også hendelsesstyrt, dette vil forenklet si at OSet går fra en tilstand til enn annen basert på hvilke hendelser som skjer. Brukeren kan ikke avslutte eller gå ut av en applikasjon, han kan bare velge å kjøre en annen applikasjon. For eksempel kan en slå av lommedatamaskinen mens en legger inn en ny avtale i kalenderen, og når en slår på lommedatamaskinen er OSet i samme modus (en kommer dit en var når en slo av lommedatamaskinen).

### **OS arkitektur**

I Palm OS inneholder RAM informasjon om den kjørende applikasjonen, og det fungerer som permanent lagringssted for data og applikasjoner. Ved oppstart av en applikasjon blir den kjørt fra der den ligger i RAM, det er ikke bruk av noe virtuelt minneområde. Alle applikasjoner bruker samme område, så ulike applikasjoner har tilgang til hverandre sitt minne. Alt i et Palm OS er lagret i samme området, utenom databaser for selve operativsystemet. De blir lagret i ROM eller på flashkort, men andre applikasjoner kan også få tilgang til disse områdene.



Figur 3. Palm OS arkitektur

### Informasjonssikkerhet

Palm OS støtter i likhet med Windows CE flere ulike sikkerhetsmekanismer. Gjennom Cryptographic Provider Manager (CPM) gis det støtte for flere ulike krypteringsteknikker. Palm OS 5.0 har også innebygd 128-bit kryptering. OSet støtter også SSL 3.0 (Secure Socket Layer) og TLS 1.0 (Transport Layer Security) for sikker kommunikasjon, i tillegg finnes det både en Autorisering og Autentisering Manager. Autoriserings Manageren tillater at applikasjoner kan spesifisere et sett av regler som må oppfylles før en får adgang til data på enheten. Palm OS støtter også bruk av smartkort og digitale signaturer.

Palm OS bidrar til både konfidensialitet og autentisering. Når det gjelder autorisering finnes det ikke i utgangspunktet muligheter for å opprette flere brukerprofiler, men en kan sette restriksjoner på tilgang til ulike applikasjoner og data.

### Symbian OS

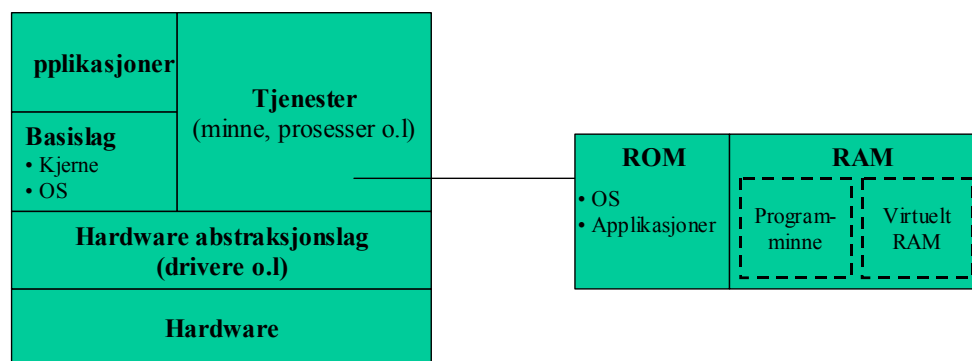
Symbian OS er utviklet kanskje mest med tanke på bruk på fremtidige PDAfoner, og flere store mobilaktører (blant andre Nokia, Ericsson og Motorola) står bak selskapet som utvikler dette operativsystemet. Symbian startet som Psion i 1981, men gikk i 1998 over til å hete Symbian. De har utviklet operativsystemt EPOC OS, som senere har blitt kjent som Symbian OS. Dette operativsystemet kjører på 32-bit CPU.

Symbian ligger mellom Windows CE og Palm OS når det gjelder hvilke muligheter det gir. Det tillater at flere applikasjoner kan kjøre samtidig og har enkle programmer for tekstbehandling og regneark, men har for eksempel ikke samme støtte for multimedia (lyd, film og bilde) som Windows CE. På den annen side krever det ikke like store ressurser som Windows CE.

## OS arkitektur

Symbian OS gjør også bruk av virtuelle minneområder slik som Windows CE, slik at ulike applikasjoner ikke har tilgang til hverandre sine minneområder. OS kjernen kjører i privilegert modus og allokerer minne til de applikasjoner som kjører i brukermodus (uprivilegert modus). Disse applikasjonene kan bare aksessere områder som er blitt tildelt av OS kjernen. Symbian OS har strenge regler når det gjelder minneallokering, og dette skal føre til at programmer ikke skal feile selv om de kjører på lite minne. Dette gjelder også alle tredjepartsprogrammer.

Minnehåndteringen på Symbian OS er styrt av MMU (Memory Management Unit). ROM inneholder OS og alle applikasjoner som kommer med OSet. Disse applikasjonene blir ikke lastet til RAM, men kjøres fra der de ligger i ROM. RAM benyttes til de applikasjoner som er kjørende og av en del av systemkjernen (likt det en finner på Windows CE).



Figur 4. Symbian OS arkitektur

## Informasjonssikkerhet

Gjennom en kryptografimodul med støtte for både symmetriske og asymmetriske algoritmer tar Symbian OS hånd om sikker kommunikasjon. I tillegg finnes det en egen modul for autentisering som håndterer ulike typer sertifikater. Det finnes også en egen modul som håndterer installasjon av applikasjoner, og som blant annet kan bruke digitale signaturer for å autentisere at software kommer fra godkjente leverandører.

Ved bruk av kommunikasjonsprotokoller som TLS/SSL, WTLS & IPSec, støtter Symbian OS både konfidensialitet og integritet. I tillegg støtter Symbian OS bruk av digitale signaturer og smartkort.

Når det gjelder autorisering er det i utgangspunktet bare passord for å komme inn på enheten. Skal en for eksempel hindre adgang til visse applikasjoner eller visse data, så må ekstra programvare installeres.

### *Embedded Linux OS*

Linux OS ble startet utviklet i 1991 og er et "open source" OS. Dette vil i praksis si at utviklere over hele verden har vært med å bidratt til utviklingen av OSet, det er i utgangspunktet gratis, og en kan bruke kildekode slik en selv vil. På grunn av dette finnes Linux OS i mange ulike varianter, tilpasset ulike bruksområder. Linux er i utgangspunktet gratis, men det finnes mange "ferdigpakker" bestående av ulike varianter av OSet med tilhørende programvare. Linux OS er på mange måter utfordren til Windows OS, og det finnes mye gratis programvare som kan kjøres på Linux. Linux vil derfor kunne være et billigere alternativ enn Windows OS.

Embedded Linux for lomme-datamaskiner finnes også i mange ulike versjoner, men de grunnleggende trekkene er likevel felles for de ulike versjonene.

### **OS arkitektur**

Linux er et moderne OS hvor kjernen blant annet støtter minnehåndtering, prosess- og trådhåndtering, TCP/IP nettverk og RAM filsystem. Det har et UNIX lignende hierarkisk filsystem og det har både ROM og RAM.

Embedded Linux har virtuell minnehåndtering, noe som vil si at ulike applikasjoner kjører i beskyttede minneområder. De aller fleste versjoner av Embedded Linux har også MMU (Memory Management Unit). Det er også mulig å kjøre flere ulike applikasjoner på en gang, i likhet med Windows CE og Symbian OS. Som på de andre OSene finnes både ROM og RAM, og i senere utgaver tillates det å kjøre applikasjoner fra der de ligger i ROM.

### *Vurdering av de ulike OS*

Her blir det foretatt en kort sammenligning av Windows CE, Symbian OS og Palm OS [2].

Det blir ikke vurdert her om noen av de omtalte OSene er bedre enn andre, men en kan konstatere at alle omtalte OS ovenfor har støtte for de mest aktuelle sikkerhetsmekanismene. Dette vil blant annet si passord, kryptering, digital signatur, digitale sertifikater og bruk av smartkort. Alt dette er med å kunne gi støtte for autorisering, autentisering og integritet. Det som i midlertidig er viktig å huske på, er at en må se de ulike OS opp mot den aktuelle bruken de skal benyttes til. Et OS med for eksempel gode sikkerhetsmekanismer er ikke nødvendigvis det som er best egnet til det aktuelle bruksområdet.

Et annet spørsmål er hvor lett det å ta i bruk de ulike sikkerhetsmekanismene og hvor gode de ulike løsningene er? Hvilket OS som er det beste kan også avhenge litt av hvilke sikkerhetsmekanismer det er behov for.

### **Adgangskontroll**

Alle de tre operativsystemene kan bli beskyttet mot uønsket bruk ved å kreve passord for å komme inn på lommedatamaskinen. Ingen av OSene tillater mer enn en brukerprofil, slik at det er ikke mulig å ”stenge” av deler av systemet.

### **Filsystem**

Palm OS er forskjellig fra de andre ved at det ikke har et hierarkisk filsystem, alle data og applikasjoner er lagret i Palm OS sin database. Symbian OS og Windows CE har organisert filsystemet på en hierarkisk måte. Siden ingen av de tre OS-ene tilbyr mer enn en brukerprofil, kan de heller ikke i utgangspunktet tilby adgangsrettigheter basert på brukere.

### **Kryptering**

Palm OS (versjon 4.0 og nyere) støtter kryptering og dekryptering av Palm OS databasen. Verken Symbian OS eller Windows CE støtter kryptografi direkte, men har støtte for at tredjepartsprogramvare kan implementere dette. Palm OS har også støtte for slik tredjepartsprogramvare.

### **Minnehåndtering**

Sikkerhetsmessig er Palm OS svakest fordi det ikke kjører applikasjoner i et beskyttet minneområde. Dette betyr at ulike applikasjoner har tilgang til andre applikasjoners minne, som igjen kan åpne for at ondsinnet programvare kan utnytte dette. Både Symbian OS og Windows CE kjører sine applikasjoner i beskyttede minneområder. Dette betyr at ulike applikasjoner ikke direkte har tilgang til hverandres minneområder.

### **Adgangskontroll basert på programmoduler**

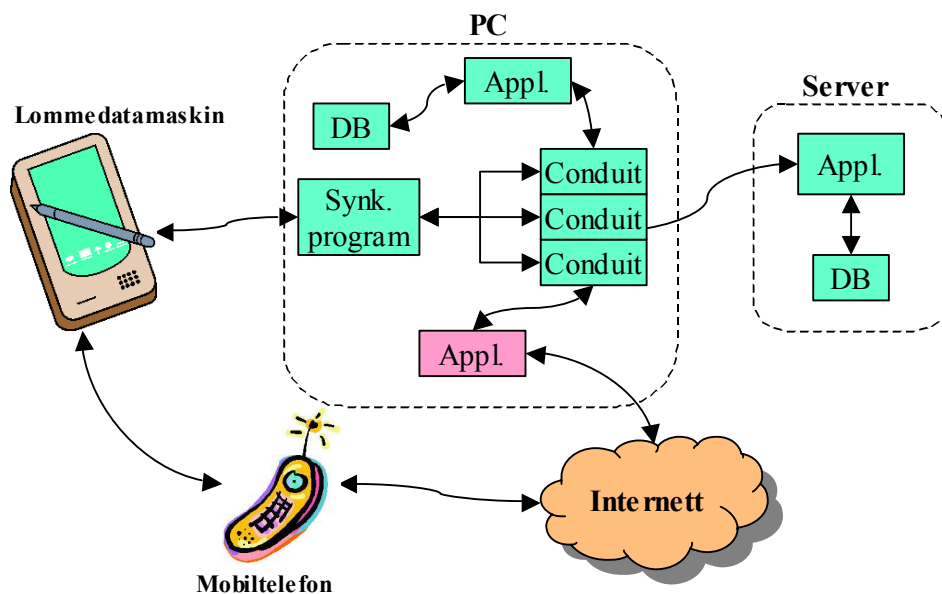
Windows CE er det eneste OS som tilbyr at adgangsrettigheter kan bli satt til hver programvaremodul individuelt. Verken Palm eller Symbian sine OS har noe støtte for å sette slike adgangsrettigheter.

### **Synkronisering**

Synkronisering av data har vært, og er en av de viktigste funksjonene med lommedatamaskiner. Dette gjør at data kan overføres fra PC til lommedatamaskin eller omvendt, eller en kan ha applikasjoner begge steder som synkroniserer hverandres informasjon. Felles for lommedatamaskinene er at de kommer med programvare som tar hånd om synkroniseringen av data (denne programvaren finnes både på lommedatamaskinen og på PCen den synkroniseres opp mot). De tekniske løsningene

og/eller funksjonalitet kan variere, men i utgangspunktet gjør de stort sett det samme. Slik programvare kan som regel også konfigureres. Eksempelvis kan det velges hvilke data som skal overføres og om informasjonen skal synkroniseres begge veier eller bare en vei.

Programmene synkroniserer i utgangspunktet stort sett informasjon i forbindelse med e-post, kalender, adressebok, oppgaveliste og lignende, men kan synkronisere flere ting. For eksempel kan programmer som jobber mot databaser eller Internett, også settes opp slik at de synkroniserer informasjon når en lommedatamaskin og en PC blir synkronisert mot hverandre. Dette viser figuren under en oversikt over.



Figur 5: Oversikt over synkroniseringen av data

### Conduits

I tillegg finnes det applikasjoner på den vanlige PCen som tar hånd om de dataene som skal synkroniseres. Denne programvaren fungerer som en bro, og bestemmer hva som skjer med dataene som sendes fra PC til lommedatamaskin eller omvendt. Dette gjør at dataene sendt for eksempel fra lommedatamaskinen blir forståelige for en vanlig PC. Slike applikasjoner kalles ofte for Conduit (se figur over), og tar hånd om en spesiell del (for eksempel kalenderdata) data som sendes når en synkronisering blir gjort. Slike omtalte Conduits opererer uten at brukeren trenger å aktivere dem, så ved synkronisering av data legger ikke brukeren merke til dem.

Nedenfor er det kort tatt for seg den synkroniseringsprogramvaren som kommer med de ulike operativsystemene.

**Windows CE: ActiveSync**

Windows CE bruker ActiveSync for å synkronisere informasjon mellom vanlige PCer og OSet. ActiveSync støtter ikke synkronisering mellom Windows CE enheter, eller mellom en Windows CE enhet og servere. Viktige funksjoner er sikkerhetskopiering og gjenoppretting av data på Windows CE enheten, og installering og fjerning av program. Den støtter interaksjonsmåter som datasynkronisering, filkonvertering og import/eksport av databasefiler.

**Palm OS: HotSync**

Palm OS bruker HotSync for å synkronisere informasjon mellom vanlige PC er og OSet. HotSync støtter synkronisering av data mellom lommedatamaskiner og PCer, sikkerhetskopiering og gjenoppretting av data på lommedatamaskinen og installasjon av databaser som har vært lagret på PCen.

**Symbian OS: SyncML**

SyncML er en åpen industristandard for datasynkronisering som i utgangspunktet kan overføre hvilke som helst data, til hvilken som helst enhet, og over ethvert nettverk. SyncML kan overføre alle typer data, men er særlig egnet for å overføre personlig informasjon som kalender, adressebok og oppgavelister.

**Sikkerhetsprogramvare**

Det finnes mye programvare som er utviklet for å forbedre sikkerheten på lommedatamaskiner. Det meste av den aktuelle programvaren må en betale for, men det finnes også noe programvare som er gratis (freeware). Dette gjelder stort sett programvare som støtter passordbeskyttelse og kryptering.

Nedenfor er det et utvalg av ulike kategorier programvare, og kort hvilken funksjonalitet de ulike kategoriene typisk har. Det er verdt å merke seg at mye av den programvaren som finnes på markedet i dag dekker mer enn bare ett sikkerhetsbehov. Et program kan for eksempel gi støtte for både kryptering av informasjon og adgangskontroll til lommedatamaskinen.

***Synkronisering og sikkerhetskopi***

Dette er programvare som tar hånd om synkronisering av data mellom lommedatamaskin og Pc, og som kan ta sikkerhetskopi av innholdet på lommedatamaskinen. Dette er ofte standard programvare som kommer med OSet når en kjøper en lommedatamaskin (omtalt ovenfor), men det finnes også tilleggsprogramvare som kan tilby flere funksjoner når det gjelder synkronisering og sikkerhetskopiering.

### *Anti-virus*

Lommedatamaskiner har til nå ikke vært like utsatt for virus o.l som vanlige PCer, men det første viruset ble registrert i 2000. En tror problemet med virus vil øke i takt med det økende antallet lommedatamaskiner. Det at flere lommedatamaskiner blir tilkoblet nettverk, flere laster ned programvare for lommedatamaskiner og flere får e-post på lommedatamaskinen vil trolig også føre til at det er større risiko for å få virus.

Programvare av denne typen kan kontrollere data som ligger lokalt på lommedatamaskinen, og den kan foreta virussjekk for eksempel når en gjør en synkronisering mot PC eller når en slår på lommedatamaskinen.

### *Ekstern tilgang*

Dette er programvare som for eksempel tar hånd om trådløs oppkobling av lommedatamaskiner mot et nettverk gjennom bruk av VPN (Virtuelle Private Nettverk). Dette gjør at det for eksempel blir etablert en sikker tunnel for å kryptere trafikk mellom en lommedatamaskin og en VPN gateway på intranettet.

### *Administrasjon*

Dette er programvare som gjøre det mulig å håndtere behandling av lommedatamaskiner fra en sentral lokasjon. Dette kan være å installere og/eller vedlikeholde applikasjoner, distribusjon av informasjon eller å forandre software eller hardware konfigurasjon. Noen programmer gjør det også mulig å ta sikkerhetskopi av det som befinner seg på lommedatamaskinene.

### *Kryptering*

Dette er programvare som ivaretar det å gjøre informasjon ugjenkjenne-  
lig. Dette kan for eksempel være at en krypterer alle notater på lommedatamaskinen, at visse applikasjoner blir kryptert, eller at en krypterer hele innholdet på lommedatamaskinen (Palm OS 4.0 og nyere har mulighet for dette). Et annet aktuelt område er å kryptere passord, slik at blir for eksempel lommedatamaskinen stjålet er det vanskelig å få tak i gyldig passord.

### *Sikre data på flerbruker lommedatamaskiner*

Dette er programvare som gjør at en lommedatamaskin kan settes opp med flere brukerprofiler (gjøres av en administrator). De ulike brukerprofilene kan så settes opp slik at det kreves passord for å få adgang til ulike applikasjoner, eller at en bruker bare har tilgang til visse applikasjoner. En bruker kan også hindres i å gjøre visse handlinger, for eksempel installere applikasjoner. Slik programvare har også mulighet for å låse lommedatamaskinen hver gang den blir slått av, slik at det kreves passord hver gang en slår på lommedatamaskinen.

### *Adgangskontroll*

Dette er programvare som beskytter tilgang til en lommedatamaskin ved å kreve at brukeren oppgir passord. Slik programvare gjør for eksempel at hver gang en enhet slås på, må et gyldig passord oppgis for å få tilgang til enheten. En bakdel med slik programvare kan være at det blir ”irriterende” for brukeren å måtte taste inn et passord bare en skal gjøre et lite notat. Et alternativ er da å bruke programvare som gjør at bare visse applikasjoner er adgangskontrollert, slik at det er fri tilgang til for eksempel kalender og notatblokk.

Det finnes også program som gjør at en kan bruke en signatur i stedet for et tradisjonelt passord for å komme seg inn på lommedatamaskinen.

### *Trådløs overføring*

De senere årene har Bluetooth blitt en vanlig standard for trådløs overføring mellom enheter innenfor korte avstander (innenfor 10-15 meter). Programvare av denne typen vil kunne konfigureres hvordan lommedatamaskinen kommuniserer med andre enheter via Bluetooth. Dette kan for eksempel være om lommedatamaskinen skal kunne kommunisere med en eller flere enheter samtidig.

### *Integritetssikring*

Dette er programvare som skal sikre integriteten til en gitt datamengde. Dette kan for eksempel være en oversikt over hvem og når noen har sett på et dokument eller om det er uforandret siden et gitt tidspunkt.

### **Tilleggsutstyr**

Dette er ikke programvare, men ekstra utstyr som en kan koble til eller nytte seg av i forbindelse med bruk av lommedatamaskiner.

### *Tap og tyveri*

Dette er utstyr som for eksempel gjør at en fysisk kan feste lommedatamaskinen fast til noe, for å unngå at den blir mistet eller stjålet. Dette er ikke så aktuelt når den blir tatt med rundt om kring, men kan være aktuelt dersom det blir gjort synkronisering mot PC slik at lommedatamaskinen over et tidsrom befinner seg på samme fysiske sted.

Det finnes også utstyr som gjør at en lommedatamaskin fysisk kan bli ”lenket” fast til brukeren. Dette kan være aktuelt når brukeren bringer med seg lommedatamaskinen rundt omkring. En ulempe med slike løsninger kan være at det går ut over bevegelsesfriheten til brukeren.



**Figur 6: PDA Saver fra Kensington**



**Figur 7: PDA lenke fra Force Technology**

### *Smartkort*

Alle de omtalte operativsystemer i denne rapporten har støtte for bruk av smartkort. Smartkort er enkelt forklart et lite plastkort som inneholder en liten datamaskin (også kalt chip) med filsystem og som kan programmeres. Et smartkort kan ha mange bruksområder, men et av de viktigste er at de er en relativ trygg lagringsplass for elektroniske nøkler. Disse nøklene kan for eksempel benyttes for å lage digitale signaturer som gjør at brukeren av smartkortet kan bruke det for autentisering eller signering av data.

For å kunne nytte seg av smartkort, må en også ha en smartkort leser, som enkel forklart er en liten ”automat” hvor en bruker smartkortet (se figur under), koblet opp mot lommedatamaskinen. Bruk av slike smartkortlesere kan gå utover mobiliteten til lommedatamaskinene dersom brukeren også må ha med seg smartkortleseren der hvor lommedatamaskinene blir brukt.



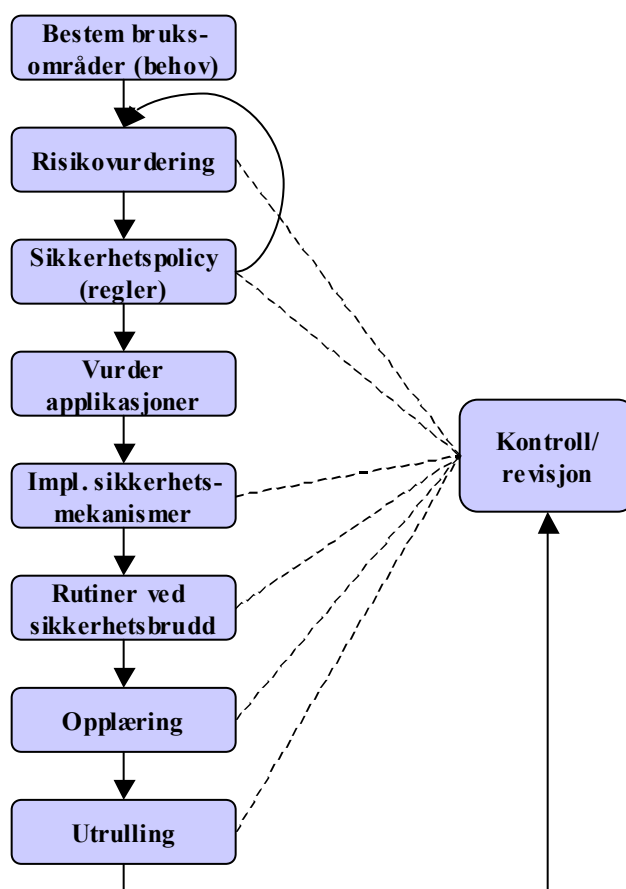
**Figur 8: PalmSmart smartkortløsning for Palm lommedatamaskin**

KITH vet per i dag ikke om konkrete prosjekter hvor bruk av smartkort i forbindelse med lommedatamaskiner har vært benyttet.

## Anbefalinger

I dette kapitlet vil vi komme med anbefalinger angående det å ta i bruk lommedatamaskiner. Dette er en plan som ikke må følges slavisk dersom en skal ta i bruk lommedatamaskiner, men er heller en generell overordnet ramme over hva vi synes er viktige punkter som bør tenkes gjennom.

Nedenfor kommer en beskrivelse av de punktene som vi mener bør gåes igjennom i forbindelse med innføring av lommedatamaskiner. En slik plan må sees i sammenheng med hva lommedatamaskinene skal brukes til. Lommedatamaskiner som kun benyttes til personlig bruk behøver kanskje ikke en overordnet plan i det hele tatt, mens bruk i forbindelse med sensitive pasientopplysninger setter høyere krav til sikkerhetsbevisstheten og bør kanskje ha en relativt detaljert overordnet plan.



Figur 9: Modell av innføring av et informasjonssystem

Figur 9 viser oversikt over fasene som kan være nyttig å gjennomføre i forbindelse med innføring av lommedatamaskiner i en helsevirksomhet. Igjen presiserer vi at dette primært er en generell oversikt og at det kan finnes flere eller andre punkter som en helsevirksomhet bør vurdere ved innføring av lommedatamaskiner. En viktig del av innføringsprosessen er å gjennomføre kontroll/revisjon av hvordan bruken av lommedatamaskinene ivaretar informasjonssikkerheten i helsevirksomheten. Figuren over antyder at denne kontrollen/revisjonen bør gjelde flere av fasene i innføringsprosessen.

## Kontakt med Datatilsynet

Dersom bruken av lommedatamaskinene innebærer lagring, behandling, videresending eller annen bruk av pasientopplysninger, kan kontakt med Datatilsynet for å få informasjon/veiledning om slik bruk være en god fremgangsmåte. Ofte vil dette være en dialog hvor helsevirksomheten melder fra om sin (planlagte) bruk av pasientopplysninger og Datatilsynet kommer med råd/anbefalinger om hvordan helsevirksomheten bør behandle pasientopplysningene.

Ved behandling av sensitive pasientopplysninger må det søkes om konsesjon fra Datatilsynet dersom behandlingen ikke er hjemlet i egen lov, mens for ikke-sensitive pasientopplysninger er hovedregelen at det er meldeplikt til Datatilsynet om slik bruk. Datatilsynet er uansett en god kilde for å få informasjon, råd eller veiledning når det gjelder å behandle pasientopplysninger.

Aktuelle lover og forskrifter kan variere med hensyn på bruksområdene til helsevirksomheten, men her er det mest aktuelle:

- **Helsepersonelloven** omhandler helsepersonells plikter og ansvar i forbindelse med utøvelse av yrket.
- **Helseregisterloven** gir retningslinjer for behandling, registrering og lagring av helseopplysninger.
- **Journalforskriften** tar for seg journalføringsplikten, journalinnhold, journalsystemer, oppretting og organisering av journaler, journalansvarlig, epikrise, personvern, innsyn i journaler, krav til oppbevaring, retting, sletting og overføring av journaler.
- **Pasientrettighetsloven** har til hensikt å sikre befolkningen lik tilgang på helsehjelp av god kvalitet ved å gi pasientene rettigheter overfor helsevesenet.
- **Personopplysningsloven** har som hovedformål å møte de utfordringene som informasjonssamfunnet skaper i forhold til personvernet.

## Bestem bruksområde

Det første en helsevirksomhet (kan være et foretak/sykehus, en avdeling eller lignende) bør finne ut, er hvilke bruksområder lommedatamaskinene skal dekke. Utgangspunktet for dette kan være de tre kategoriene (personlig bruk, medisinske applikasjoner og sensitiv informasjon) som ble omtalt i kapittel 1. Brukskategorien gir føringer i forhold til resten av arbeidet med å ta i bruk lommedatamaskiner. Bruksområdene må kanskje senere i prosessen vurderes på nytt, dersom en for eksempel finner ut at ønsket bruksområde krever for mye i forhold til krav om informasjonssikkerheten. En risikoanalyse kan for eksempel avdekke at risikoen er for stor i forhold til den gevinsten en kan oppnå.

Å bestemme bruksområde inkluderer også å se på hvilke kommunikasjonsløsninger en skal bruke. Dette kan for eksempel være om lommedatamaskinene skal overføre data via synkronisering mot PC eller via det trådløse nettverket. De valgene organisasjonen gjør her vil kunne få betydning for senere valg av applikasjoner og sikkerhetsløsninger.

## Utfør risikovurdering

En risikovurdering vil peke på hvilken risiko man løper dersom nødvendige sikringstiltak ikke gjennomføres, og den kan gi forslag til hvilke tiltak som bør prioriteres. I forbindelse med en risikovurdering bør man sette opp akseptkriterium, noe som vil si at man aksepterer risikoen knyttet til hendelse dersom:

- Sannsynligheten for at hendelsen inntreffer er tilstrekkelig lav og/eller
- Konsekvensene av hendelsene er tilstrekkelige ufarlige (eventuelt kan kontrolleres)

Dersom man ikke oppfyller de gitte akseptkriterium, må man gå gjennom aktuelle tiltak, og prøve å redusere risikoen slik at man oppfyller akseptkriteriene.

Risikovurderingen bør gjennomføres av noen som kjenner til informasjonssystemet og virksomheten som det er en del av, samt noen med kunnskap om gjennomføring av risiko- og sårbarhetsanalyser. Dette kan være eksterne personer, men på sikt bør en organisasjon bygge egen kompetanse med tanke på å kunne gjennomføre slik analyser selv.

Det er viktig at en slik risikovurdering ikke blir for omfattende, men at den står i stil med omfanget og kritikaliteten av informasjonssystemet. KISS (Keep It Simple Stupid) kan være et godt begrep å huske på i en slik sammenheng. Det er trolig bedre å gjøre ting på en enkel måte, istedenfor å prøve å gjøre en for omfattende vurdering.

Kapittel 2 kan være et godt utgangspunkt for å gjennomføre en risikovurdering knyttet til lommedatamaskiner, og i tillegg gir KITH sin veiledning "Risikoanalyse – metodegrunnlag og bakgrunnsinformasjon", en mer grundig gjennomgang av hvordan en kan gjøre risikovurderinger.

## Vurder utstyr/opplæring

Etter at organisasjonen har bestemt bruksområdet og gjort en risikovurdering, må den se på hvilket utstyr som det er behov for. Det er ikke sikkert organisasjonen har behov for samme utstyr dersom lommedatamaskinene skal brukes til personlig bruk, som hvis de skal brukes til sensitive opplysninger. En må også være klar over at lommedatamaskiner med mange sikkerhetsfunksjoner som egner seg til bruk av sensitive opplysninger, ikke nødvendigvis er det beste utstyret dersom lommedatamaskinen bare skal brukes personlig med stort sett bruk av kalender, adressebok og oppgaveliste.

Organisasjonen må også se på hvilke andre funksjoner lommedatamaskinene kan tilby i tillegg til sikkerhetsfunksjonene. Dette kan for eksempel være om utstyret støtter det å vise bilder og/eller film. I denne sammenhengen er det også aktuelt å se på brukervennligheten til utstyr som er aktuelt. Gode brukergrensesnitt kan bidra til å øke sikkerheten ved at det for eksempel forhindrer feilsending av sensitiv informasjon.

Organisasjonen må også vurdere i hvor stor grad opplæring må gis ved innføring av lommedatamaskinene. Dette kan være opplæring knyttet til selve bruken av lommedatamaskiner generelt, men kan også gjelde de ulike spesifikke applikasjonene og eventuelle sikkerhetsmekanismer som blir innført.

En viktig egenskap som bør vurderes er hvor lett det er å skrive/registrere informasjon på lommedatamaskinene, dersom det er aktuelt å bruke lommedatamaskinene til dette. I forbindelse med dette bør en vurdere om det er behov for litt større lommedatamaskiner med integrert tastatur, istedenfor mindre lommedatamaskiner med kun en trykksensitiv skjerm.

## Lag policy og regler

Etter at en har sett på bruksområde og aktuelt utstyr, er neste fase å tenke på hvordan innføringen av det nye utstyret skal skje. Dette er kanskje den mest omfattende og krevende delen med å innføre et nytt datasystem. En sikkerhetspolicy er et dokument som beskriver målsetninger, regler og retningslinjer for hvordan informasjonssikkerhet skal etableres og vedlikeholdes i en virksomhet. Målsetningen for en slik sikkerhetspolicy er blant annet å bidra til å sikre personvernet og pasientsikkerheten i helsevesenet, på en måte som understøtter og bedrer kvalitet, service, produktivitet og effektivitet i helsetjenestene.

Sikkerhetspolicyen bør utarbeides sammen med de aktuelle brukerne av informasjonssystemet. Dette for å få en felles forståelse for hvorfor sikkerheten er viktig i et informasjonssystem, og for at brukerne ikke skal få følelsen av maktesløshet når det gjelder å ta i bruk et nytt informasjonssystem. Det er også viktig at alle parter blir enige om felles mål og metoder. Det er liten vits i å lage gode regler dersom ingen brukere har interesse av å følge dem opp.

Det er også viktig at alle involverte parter i organisasjonen er motiverte

for innføringen av et nytt informasjonssystem. Dette gjør at innføringen vil kunne gå lettere, samtidig med at noen få umotiverte medarbeidere i organisasjonen er nok til at effekten av en slik innføring reduseres.

Her er et forslag til hva en policy for lommedatamaskiner kan omhandle:

- hvem autoriserer anskaffelse og tildeling av lommedatamaskiner
- hvem kontrollerer og forvalter utstyret
- hvilke administrative retningslinjer skal gjelde
- hvilke sikkerhetsmessige retningslinjer skal gjelde

Administrative retningslinjer i forbindelse med lommedatamaskiner kan omfatte:

- regler for anskaffelse og merking av utstyret
- regler for påbudte sikkerhetsmekanismer med tilhørende drift
- autentisering
- autorisasjon, tilgangskontroll
- passordpolicy
- krav til kryptering og andre sikkerhetsmekanismer
- krav til synkronisering
- forbud mot å låne bort utstyr
- forbud mot bruk av privateid utstyr
- forbud mot uautorisert fjerning av sikkerhetsverktøy
- krav til viruskontroll
- forbud mot installasjon av nye applikasjoner

## Vurder applikasjoner

Neste fase bør være å se på funksjonaliteten til applikasjonene som skal brukes på lommedatamaskinene (i denne sammenhengen tenkes det primært på funksjonalitet med tanke på informasjonssikkerheten). Dette har sammenheng med hvilket bruksområde de skal brukes til, men her går en mer i detalj og ser på hva som kreves av informasjonssikkerhet. Dette kan for eksempel være at det kreves at informasjon blir sendt kryptert, eller at brukerne må logge seg på med passord.

En må i denne sammenhengen vurdere om noen applikasjoner medfører bedre sikkerhet enn andre. Dette kan for eksempel være at en applikasjon har et bedre grensesnitt slik at det reduserer risikoen for utilsiktet utlevering av informasjon. OS arkitekturen og den generelle oppbygningen av en applikasjon vil også kunne påvirke hvor robust en applikasjon er mot ondsinnet programvare.

## Implementer sikkerhetsmekanismer

Neste fase vil være å implementere aktuelle sikkerhetsmekanismer for å oppnå den ønskede sikkerhetsnivået. Dette vil i en oppstartsfasen for eksempel kunne testes ut i et avgrenset omfang for å finne ut om de valgte sikkerhetsmekanismer gir den ønskede sikkerheten. Valget av sikkerhetsmekanismer vil avhenge av risikovurderingen og hvilke krav en setter til funksjonalitet for de ulike applikasjonene. Dersom en finner ut at ønsket sikkerhet ikke oppnås, må en gå en ny runde med vurdering av informasjonssikkerheten og risikovurdering. Dette vil for eksempel kunne være å se på andre typer lommedatamaskiner, vurdere funksjonalitet til de ulike aktuelle applikasjonene, eller innføre strengere sikkerhetsmekanismer.

Aktuelle sikkerhetsmekanismer er omtalt i kapittel 3, og dette kan for eksempel gjelde programvare som sikrer at ulike brukere må logge seg på med hver sine passord, eller at en gjør lommedatamaskinene klare for bruk med smartkort.

Et viktig moment når det gjelder sikkerhetsmekanismer er at en må vurdere sikkerheten mekanismene gir, mot hvor enkelt det er å bruke mekanismene. Dersom det blir for mange mekanismer som er tungvinte å bruke, vil en til slutt trolig oppleve at brukerne ikke orker å gjøre seg nytte av de ulike sikkerhetsmekanismene.

## Rutiner ved sikkerhetsbrudd

Ved brudd på informasjonssikkerheten bør en ha rutiner/regler for hva som skal skje. Først og fremst er det viktig at brudd på informasjonssikkerheten blir meldt fra til de ansvarlige slik at de kan gjøre de nødvendige tiltak. En melding om et brudd kan for eksempel inneholde følgende:

- hvor bruddet oppsto
- hva som skjedde (hvordan ble det oppdaget)
- grunnen til at bruddet oppsto (dersom en kan si noe om det)
- konsekvenser (dersom en kan si noe om det)

Dersom en slik melding blir for omfattende må de ansvarlige få beskjed om at et brudd er skjedd og hvor det ble oppdaget.

### Tiltaksplan

En tiltaksplan beskriver prosedyrer som bør iverksettes når det skjer et brudd på informasjonssikkerheten. Dette kan være alt fra tekniske tiltak for å gjenopprette tapte data eller forhindre bruk av tapt informasjon, til meldingsrutiner og tiltak/kontroller som bør iverksettes for å minimalisere konsekvensene ved et brudd på informasjonssikkerheten. I en slik tiltaksplan bør det også sies noe om hvem som ansvar for å gjøre noe etter at et brudd er oppdaget, og hvilke tiltak vedkommende har mandat til å gjøre. Dette er viktig å avklare på forhånd, slik at folk som oppdager et

brudd vet hvem de skal rapportere til, og at vedkommende det blir rapportert til vet hva som skal (og kan) gjøres.

### **Kontroll**

Etter at tiltak/prosedyrer er iverksatt etter et brudd, er det viktig at det blir gjort en kontroll/sikkerhetsrevisjon som viser om informasjonssikkerheten er blitt god nok til å hindre fremtidige brudd. Dersom kontrollen viser at sikkerhetsnivået fortsatt ikke er godt nok, bør en på nytt vurdere sikkerhetspolicyer, applikasjoner, sikkerhetsmekanismer eller andre forhold som virker inn på informasjonssikkerheten i virksomheten.

### **Opplæring (sikkerhet)**

Etter at en har funnet utstyr/programvare som gir den ønskede informasjonssikkerheten, kan en innføre det nye datasystemet. Dette innebærer at informasjonssystemet blir tatt i bruk i fall skala, og ofte vil dette kreve at brukerne får opplæring i informasjonssikkerheten. Dette vil ha betydning for hvordan det nye informasjonssystemet vil fungere i praksis, og ikke minst hvordan informasjonssikkerheten blir ivaretatt.

### **Utrulling**

Etter opplæring er neste fase å innføre det nye informasjonssystemet i praksis, dette vil si at brukerne tar i bruk informasjonssystemet i full skala. I denne fasen skal all planlegging settes ut i live, og brukerne skal gjøre seg nytte av det nye informasjonssystemet og opplæring de har hatt rundt det.

I forbindelse med utrulling kan det være lurt å etablere et apparat for brukerstøtte. Ved innføring av nye informasjonssystemer er det ”normalt” at brukere opplever problemer, og en slik tjeneste kan gjøre innføringen lettere. Enn annen grunn for å ha et slikt apparat for brukerstøtte, er at en da finner ut hvilke problemer det er som brukerne opplever. Dette kan være nyttig for senere revisjoner/gjennomganger av informasjonssystemet med tanke på å finne ut hva som har vært bra/ikke bra med det nye informasjonssystemet.

### **Kontroller (revisjon)**

Et av de viktigste punktene i forbindelse med å innføre et nytt informasjonssystem (se figur 9), er å kontrollere hvordan det fungerer i bruk. Dette kan for eksempel gjøres en tid (4-5 måneder) etter at informasjonssystemet er tatt i bruk, og så etter det med faste mellomrom (for eksempel en gang i året). Dette er viktig for finne ut om informasjonssystemet virkelig gjør det som det var tiltenkt, og om det er andre hendelser som kommer frem etter bruk som gjør at noe må forandres.

I en revisjon bør blant annet følgende områder vurderes:

- Risikovurderingen.

## ANBEFALINGER

- Om sikkerhetspolicyen følges?
- Om sikkerhetsmekanismene fungerer tilstrekkelig?
- Om tiltaksplanen fungerer godt nok?
- Om oppfølgingen er god nok?

Det er viktig at en slik revisjon blir gjort, det er slik en virksomhet finner ut hvordan det som ble planlagt og gjennomført for å ivareta informasjonssikkerheten fungerer.

En revisjon har to hovedformål; det ene er å se om en virksomhet følger regler, prosedyrer, policyer og lignende (samsvarsrevisjon), mens det andre er å se hvordan en virksomhet kan nå sine mål (operasjonell revisjon). KITH sin rapport *"IT-revisjon – Med fokus på IT-sikkerhetsrevisjon"* være en god bakgrunnskilde for hvordan en gjennomfører slike revisjoner.

# Litteratur

## Kilder som har vært brukt i denne rapporten.

- [1] KITH: *"Håndbok for informasjonssikkerhet i informasjonsnett"*. 1998, ISBN 82-7846-048-5
- [2] Jukka Ahonen: *"PDA OS Security: Application Execution"*. 2001, Helsinki University of Technology
- [3] Ganesh Sivaraman: *"Report on EPOC – An overview of Symbian OS"*. 1999
- [4] Gregory Haerr: *"Overview of Linux for the Embedded Application Developer"*. Century Software INC
- [5] Threats to PDAs: <http://www.symantec.com>
- [6] Information Security Reading Room: <http://rr.sans.org/PDAs/>
- [7] Microsoft om Windows CE: <http://msdn.microsoft.com/library/>
- [8] Microsoft om mobile enheter: <http://www.microsoft.com/mobile/handheldpc/default.asp>
- [9] Palm OS: <http://www.palmos.com>
- [10] Symbian OS: <http://www.symbian.com>
- [11] KITH: *"Risikoanalyse – Metodegrunnlag og bakgrunnsinformasjon"*. 2000, ISBN 82-7846-091-4
- [12] KITH: *"IT-revisjon – Med fokus på IT-sikkerhetsrevisjon"*. 2002, ikke utgitt
- [13] Datatilsynet: *"Sikkerhetsbestemmelsene i personopplysningsforeskriften med kommentarer"*



# Operativsystem

**Dette vedlegget gir en oversikt over hvordan de tre mest utbredte operativsystemene på lomme-datamaskiner, Windows CE, Palm OS og Symbian OS, støtter ulike sikkerhetsmekanismer. Arkitekturen til operativsystemene ble omtalt i kapittel 3, og er derfor ikke behandlet noe mer i dette vedlegget.**

## Windows CE

Windows CE støtter blant annet følgende sikkerhetsmekanismer:

### **Security Support Provider Interface (SSPI):**

SSPI tilbyr et felles grensesnitt mellom transportlagapplikasjoner og sikkerhetstilbydere. Sikkerhetstilbydere som er inkludert i Windows CE er Windows NT® LAN Manager (NTLM), Secure Sockets Layer (SSL) versjon 2.0 og 3.0 (kanskje best kjent fra bruk av nettbanker), og Private Communication Technology (PCT) versjon 1.0.

SSPI gjør at autentisering (det å kunne verifisere en påstått identitet) og kryptering (det å gjøre informasjon ugjenkjennelig) kan bli ivarettatt. SSPI er utviklet for at ulike applikasjoner som har behov som for eksempel autentisering eller kryptering, kan aksessere DLL (Dynamic Link Libraries) som inneholder felles skjemaer for autentisering og kryptografi. Disse aktuelle DLLene kalles for Security Support Providers (SSP), og gjør ulike sikkerhetsløsninger (kalt sikkerhetspakker) tilgjengelige for ulike applikasjoner. En sikkerhetspakke mapper SSPI funksjoner til sikkerhetsprotokollen som er spesifisert i sikkerhetspakken. En applikasjon som implementerer SSPI kan bruke hvilken som helst sikkerhetspakke som er tilgjengelig i systemet uten å vite detaljer om sikkerhetsprotokollen som sikkerhetspakken implementerer.

### **Kryptografi:**

Windows CE støtter Microsoft Cryptographic API (CAPI) som gjør at Windows CE skal kunne ha sikker kommunikasjon. Microsoft kryptografi systemet består av flere ulike deler, og de tre kjørbare delene er applikasjonen, operativsystemet og Cryptographic Service Provider (CSP). Applikasjoner kommuniserer med operativsystemet gjennom CAPI, og operativsystemet kommuniserer med CSP gjennom Cryptographic Service Provider Interface (SCPI). Alle kryptografioperasjoner blir så gjennomført av uavhengige moduler som er kjent som CSPs. CSP skal blant

annet lage og ødelegge nøkler, og bruker dem på ulike måter for å gjennomføre ulike kryptografioperasjoner.

#### **Digitalt sertifikat:**

Windows CE støtter bruk av digitale sertifikater som gjør at sterk autentisering kan benyttes. X.509 digitalt sertifikat er den standarden som CAPI (Cryptographic API) i Windows CE støtter. X.509 inneholder foruten brukerens navn og offentlige nøkkel, også annen informasjon om brukeren som for eksempel e-post adresse eller autorisering til ulike tjenester. X.509 og andre sertifikater har tidsbegrensning, slik at de etter en tid kan bli ugyldige.

#### **Smartkort:**

Windows CE støtter bruk av smartkortlesere. Dette gjør at for eksempel nøkler til dekryptering kan legges på slike smartkort.

Windows CE smartkort subsystem består av følgende:

- Smart Card Service Provider (SSP) er Base Service Providers (DLLs) som tillater aksess til spesifikke tjenester.
- Resource Manager bruker Win32 API for å håndtere tilgang til flere lesere og smartkort.
- Spesifikke smartkortleser-drivere mapper konseptuelle drivertjenester til spesifikke hardware lesertjenester.
- Smartkortleser bibliotekhjelp for support og hjelp.

Smart Card Resource Manager er det som styrer tilgang til lesere og smartkort. Det er mulig å benytte Resource Manageren som tar seg av de sikkerhetsfunksjoner som finnes i det underliggende operativsystemet.

## **Palm OS**

Palm OS støtter blant annet følgende sikkerhetsmekanismer:

#### **Kryptografi:**

Palm OS sin Cryptographic Provider Manager (CPM) gir støtte for kryptering av informasjon. Som en del av CPM pakken er også streng 128-bit kryptering. I samarbeid med RSA Security støtter også Palm OS RC4, SHA-1 og signatur verifikasjon.

CPM tillater også at andre krypteringsalgoritmer som for eksempel Advanced Encryption Standard (AES).

#### **Sikker kommunikasjon:**

Palm OS har støtte for Secure Socket Layer (SSL), som gir støtte for kryptering for kommunikasjons-, nettverks- og e-commerce applikasjoner. Det er også flere muligheter for en nettverksadministrator å identifisere unike enheter, gjennom Flash ID, Mobile Access Number (MAN) og Elektronisk Serienummer (ESN).

Gjennom SSL og TSL tilbyr Palm OS ende-til-ende forbindelser over Internett ved å bruke streng (128-bit) SSL kryptering. Bruk av algoritmen RC4 gjør at Palm OS støtter en mye brukt protokoll for kryptering brukt ved dataoverføring.

Palm OS støtter Microsoft sin Challenge Handshake Authentication Protocol (CHAP), og flere VPN (Virtuelle Private Nettverk) klienter støtter bruk av Palm OS (blant andre Certicom og SafeNet). CHAP gjør at autentiseringsagenten kan sende klientprogrammet en nøkkel som blir brukt for å kryptere brukernavn og passord. Dette gjør at brukernavn og passord kan sendes kryptert og hindre at noen ”snapper” dem opp.

#### **Autorisering og autentisering:**

Palm OS støtter metoder for både autorisering og autentisering. Autoriserings Manageren gjør at applikasjoner kan kreve at et sett av regler er oppfylt før en kan aksessere data på enheten.

Autentiserings Manageren vil kunne håndtere flere ulike måter å verifisere aksess på. Dette gjelder for eksempel passord, passfraser eller PINs, men også biometrisk (for eksempel stemme eller fingeravtrykk) verifisering og bruk av smartkort. Autentisering Manageren vil også ha støtte for ”signert kode”, slik at kun applikasjoner som har en gyldig digital signatur kan aksessere visse data og ressurser.

#### **Sikkerhetskopi:**

Palm OS gir støtte for sikkerhetskopiering mot blant annet servere, som sentralt kan håndtere og distribuere informasjon.

## **Symbian OS**

Symbian OS støtter blant annet følgende sikkerhetsmekanismer:

#### **Kryptografimodul:**

Krypteringsalgoritmer for kryptering og dekkkryptering som støtter både symmetriske og asymmetriske algoritmer (chiphers). I tillegg er det også støtte for hash-funksjoner og pseudo-random generator for å generer krypteringsnøkler.

#### **Kryptografirammeverk:**

Dette rammeverket gjør det mulig å integrere support for flyttbare hardware enheter, som for eksempel WIM-moduler. Rammeverket består i hovedsak av to deler:

1. et rammeverk som gjør det mulig for applikasjonskode å spørre systemet for tilgjengeligheten av implementasjonen av spesifikke kryptografiske grensesnitt.
2. definisjonen av et sett av kryptografiske grensesnitt.

#### **Sertifikater:**

Sertifikat Manageren er brukt for autentisering av andre entiteter (som tredjeparts entiteter eller webservere) som er i kontakt med lommedata-

maskinen, og for autentisering av brukeren av en lommedatamaskin. Managere støtter WTLS og X.509 sertifikater.

- *Installasjon:*  
Software installasjonssystemet brukes blant annet til autentisering av software komponenter ved hjelp av digitale sertifikater for å verifisere at det en installerer kommer fra ”tillitsfulle” leverandører.

# Forslag til sikkerhetsløsninger

**Her kommer forslag til hvilke sikkerhetsmekanismer en bør implementere for ulike bruksområder. Dette er ikke løsninger som kan overføres direkte til en virksomhet sin bruk, men kan være et utgangspunkt eller eksempler på hvilke sikkerhetsløsninger en selv skal velge.**

I tillegg til det som blir beskrevet under, er det også aktuelt å se på det som ble beskrevet angående oppkobling av lommedatamaskiner i kapittel 1.

## **Eksempel 1: Personlig bruk**

I dette eksempelet tas det utgangspunkt i at lommedatamaskinene blir innført primært for at de ansatte i helsevirksomheten skal bruke de til kalender- avtale- og adressebok. I denne sammenhengen regnes det ikke med at noen sensitive helseopplysninger er lagret på lommedatamaskinene. Det er i midlertidig regnet med at opplysninger av sensitiv karakter relatert til brukeren selv og/eller helsevirksomheten kan befinne seg på lommedatamaskinen.

## **Anbefalte sikkerhetsløsninger**

I denne sammenhengen vil det trolig først og fremst være å ivareta konfidensialiteten til informasjonen som befinner seg på lommedatamaskinen. Dette kan gjøres ved ta i bruk de mekanismene for passordbeskyttelse som finnes på lommedatamaskinene. Dersom det er flere brukere på en lommedatamaskin, er det aktuelt å legge inn programvare som tillater flere brukerprofiler på samme lommedatamaskin. Dersom det er sannsynlig at informasjon av sensitive karakter befinner seg på lommedatamaskinen, kan det være aktuelt å kryptere innholdet på lommedatamaskinen. Dette kan enten gjøres ved bruk av mekanismer i OSet på valgt lommedatamaskin har funksjoner for dette (Palm OS 4.0 og senere), eller ved at en installerer ekstra programvare som gjør dette.

I tillegg bør virusprogramvare installeres på lommedatamaskinene for å hindre at det ved for eksempel synkronisering mot PC eller installasjon av applikasjoner kan komme ondartede programmer på lommedatamaskinen.

## Eksempel 2: Medisinske applikasjoner

I denne eksempelet blir lommedatamaskinene innført primært for medisinsk bruk, men det blir ikke lagret noen sensitiv helseinformasjon. Som i eksempel 1 tas det utgangspunkt i at lommedatamaskinene kan bli brukt til personlig bruk, og således vil de samme problemstillingene og anbefalingene gjelde her som i eksempel 1. De medisinske opplysningene er ikke sensitive, men det kan være viktig at de ikke blir mistet eller endret.

### Anbefalte sikkerhetsløsninger

I denne sammenhengen er ikke konfidensialitet det viktigste (det gjelder fortsatt for personlig bruk), men heller kravet om at integriteten ivaretas. Dette kan for eksempel være at opplysninger om en type medisin er korrekte. Av sikkerhetsmekanismer er det først og fremst passordbeskyttelse av den medisinske informasjonen, men det kan også benyttes krypteringsmekanismer for å ivareta integriteten. Det bør også installeres programvare som gjør at personlig bruk ikke kommer i konflikt med jobbbruk. Dette kan for eksempel være å opprette to brukerprofiler, slik at den personlige brukerprofilen ikke har adgang til de dataene som er lagret under jobb-bruker profilen (og omvendt).

Videre kan det anbefales programvare for å ta sikkerhetskopi av det medisinske innholdet, dette kan gjøres ved å overføre dataene til en vanlig PC. Som i eksempel 1 bør det også her benyttes virusprogramvare.

## Eksempel 3: Sensitive opplysninger

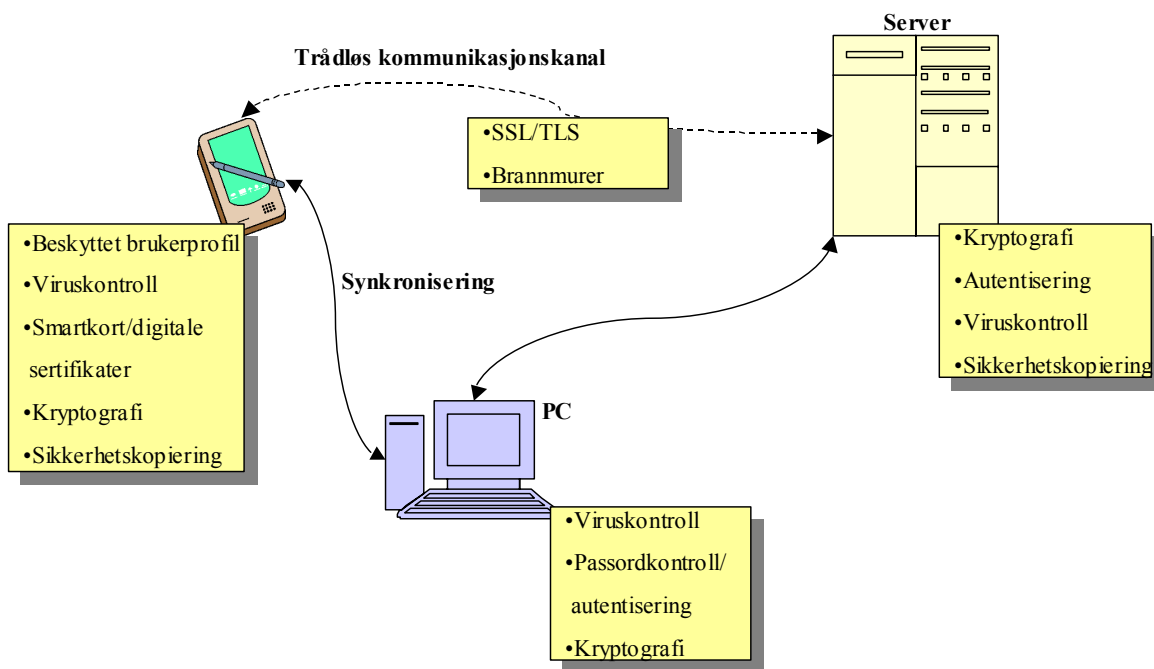
I dette eksempelet tas det utgangspunkt i at sensitiv helseinformasjon er lagret og/eller går via lommedatamaskinen. Vi tenker oss at lommedatamaskinen kommuniserer med ulike fagsystem (for eksempel via faste infrarøde baser), og at den er tilkoblet et trådløst nettverk. Vi legger også til grunn at lommedatamaskinen i utgangspunktet ikke er tilkoblet Internett, men at dette kan skje for eksempel ved sending av e-post. Også i dette eksempelet tenker vi oss at lommedatamaskinene kan bli brukt til personlig bruk som i eksempel 1.

### Anbefalte sikkerhetsløsninger

I denne sammenhengen er behovet for konfidensialitet og integritet størst, men også tilgjengeligheten må ivaretas. Siden den kommuniserer med et trådløst nettverk, bør informasjon til/fra lommedatamaskinen krypteres. Det bør også installeres viruskontroll på lommedatamaskinen for å oppdage ondsinnet programvare. Dette kan være aktuelt ved mottak av informasjon gjennom nettverket, og ved synkronisering mot PC. Som i de to andre eksemplene bør det også her være passordbeskyttelse på selve lommedatamaskinen. Dersom lommedatamaskinen kan bli brukt til personlig bruk, bør det også installeres programvare som gjør at ikke

den personlige bruken kommer i konflikt med jobb bruken (muligheter for flere brukere). I tillegg til dette bør det også installeres administrativ programvare slik at lommedatamaskinene kan konfigureres slik at ikke brukeren selv kan installere applikasjoner lastet ned fra Internett.

For å ivareta sikker autentisering av brukeren og muligheter for digital signering av for eksempel meldinger, benyttes smartkort for å autentisere brukeren.



Figur 10: Forslag til sikkerhetsløsning

Figur 10 viser en skisse over hvordan informasjonssikkerheten kan bli ivarettatt ved bruk som er beskrevet over. De fleste sikkerhetsmekanismene er i forbindelse med lommedatamaskinen, men også PCer, servere og kommunikasjonskanaler som lommedatamaskinen kommuniserer med må sikres. For brukeren er det først og fremst pålogging på lommedatamaskin/PC og bruk av smartkort som den vil merke i sin daglige bruk. Resten av sikkerhetsmekanismene vil i stor grad kunne automatiseres slik at brukeren ikke merker de.

Andre konsekvenser av sikkerhetsmekanismer som brukeren vil kunne oppleve er for eksempel at installasjon av egne applikasjoner på lommedatamaskin ikke er tillatt, eller at det blir foretatt ekstra sjekk ved sending av e-post for å gradere innhold og verifisere mottakere.



## Case studie

### **Her blir det presentert et prosjekt som ble gjennomført i Alta kommune med bruk av mobile enheter i helsevesenet.**

I denne arbeidssituasjonen benyttet hjemmesykepleiere en mobil terminal utstyrt med trådløskort som kommuniserte med et trådløst bredbåndsnett. Kommunikasjon fra den mobile enheten og til trådløsnettet skjedde via en mobil basestasjon som ble festet på bilen til sykepleierne. I forbindelse med dette ble det utviklet en applikasjon (Mobil Profil) hvor sykepleierne kunne hente ut og legge inn informasjon fra en database. Mobil Profil ga sykepleierne bare adgang til informasjon relevant for den brukeren. På den lokale helsesentralen fantes det i tillegg en applikasjon (Profil) hvor en hadde mer tilgang og funksjonalitet enn det som Mobil Profil gav.

### **Informasjonssikkerhet**

Siden informasjon blir sendt over et trådløst nettverk, er konfidensialitet og integritet de viktigste punktene for å ivareta informasjonssikkerheten. Dette ble ivaretatt ved kryptering av den informasjonen som ble sendt over det trådløse nettverket.

Ved å bruke PKI teknologi (bruk av en privat og en offentlig nøkkel) ble krypteringen brukt som autentisering mellom server og klient (den mobile terminalen). På denne måten kunne klienten kryptere med serveren sin offentlige nøkkel, slik at kun serveren kunne dekryptere ved å bruke sin private nøkkel. Det samme gjaldt for å sende data motsatt vei.

Ulempen med denne typen offentlig kryptering var at den krevde mye ressurser, slik at bare en pakke i en melding ble kryptert på denne måten. Resten av meldingen ble kryptert ved hjelp av å bruke delte nøkler, noe som krevde mindre ressurser.

### **Sikkerhetsløsning**

Av sikkerhetsmekanismer er det først og fremst sikker autentisering av brukeren ved pålogging som mangler. Det som ble benyttet var den normale påloggingen til den mobile terminalen. Alternativet hadde vært å benytte seg av smartkort (eller tilsvarende) for å ivareta en sikrere autentisering av brukeren.

I tillegg til sikker autentisering var funksjoner som ikke-benektning og sporbarhet heller ikke direkte tatt hånd om av systemet. Dette kunne vært ivaretatt ved å utnytte det at kryptering ble benyttet som autentisering

## CASE STUDIE

mellom server og klient. I praksis utgjorde denne delen en slags digital signatur som ved å bli ”loggført” kunne ha støttet funksjoner som ikke-benektning og sporbarhet.