Mobil Elektronisk Pasientjournal – Studie av anvendbarhet, sikkerhet og muligheter

av

Vegar Kristensen
Bård Eirik Lyche

Hovedoppgave til mastergraden i informasjons- og kommunikasjonsteknologi

Høgskolen i Agder
Grimstad, mai 2003

Sammendrag

Overgangen fra papirbaserte til elektroniske pasientjournaler (EPJ) fører til et behov for datautstyr tilgjengelig der hvor pasientene befinner seg. Sørlandet Sykehus HF Arendal (SSA) ligger helt i front når det gjelder utviklingen mot et mobilt EPJ system, og gjennomførte fra august 2002 til januar 2003 et utviklingsprosjekt på dette området. Som en del av et pågående FoU-prosjekt ”Sikkerhet ved trådløse medisinske datanett”, er denne oppgaven en del av dette prosjektet gjennom et studie av det første forsøk i Norge ved anvendelse av mobile dataløsninger i tilknytning til elektronisk pasientjournal.

Etter gjennomførte observasjoner, spørreskjemaundersøkelse med etterfølgende supplerende intervjuer, viste det seg at leger og sykepleiere tok de mobile enhetene lite i bruk. Dette gjelder spesielt PDA og tablet PC som benytter seg av programvaren InfoPack_Helse. Bærbar PC benytter seg derimot av DIPS, som er kjent fra det stasjonære datasystemet og har blitt bedre mottatt. I tillegg til store funksjonelle forskjeller mellom de mobile enhetene, viste det seg at brukerne opplevde stor ustabilitet i det mobile systemet slik det fungerte i utviklingsprosjektet. Det kom frem at de mobile enhetene egnet seg til forskjellige arbeidsoppgaver, så alle tre er ikke direkte konkurrenter. TAM sier at oppfattet nytte og oppfattet enkelhet i bruk påvirker holdning til bruk, og dermed bruk. UAM setter fokus på mer detaljerte elementer, som bør være på plass for å sikre brukeraksept. Disse modellene, sammen med brukererfaringene, belyser hvilke endringer som må til for at mobil EPJ kan innføres mens anvendbarheten blir ivaretatt.

Sikkerhetsmekanismene som ble benyttet i utviklingsprosjektet på SSA, viste seg kun å omfatte bruk av MAC-adresse filtrering og 128-bits WEP-kryptering. Ut fra datatilsynets krav og anbefalinger er dette i svakeste laget. Datatilsynets krav er mulig å tilfredsstille ved bruk av brannmur og sikker autentisering ved hjelp av IPSec og IEEE 802.1x. En slik brannmurløsning vil gjøre det mulig å regulere autorisasjon ved å sentralt definere ressurstilgang for enkelte brukere eller brukergrupper. Videre utvikling av et mobilt datasystem går i retning av smartkort til autentisering av både brukere og utstyr. EAP-SIM er en autentiseringsprotokoll i IEEE 802.1x algoritmen utviklet for autentisering i trådløse LAN mellom en klient og RADIUS server.

Basert på studiet rundt anvendbarhet og sikkerhet er det satt sammen en rekke forslag til utviklingsmuligheter og drøfting av konsekvenser av disse. Blant annet er det viktig at brukergrensesnittet på InfoPack_Helse utvikles mer likt DIPS. Det viste seg å være uheldig for brukerne å ha flere forskjellige datasystemer å forholde seg til. I tillegg savnes hurtigfunksjoner i InfoPack_Helse for å raskere få innsyn i informasjon om bestemte pasienter. Det finnes løsninger på markedet i dag hvor PDA har implementert funksjonalitet for skanning. Dette åpner for muligheten til å skanne en merkelapp på en pasientseng, for raskt å få frem informasjon om pasienten som ligger der. Under utvikling av sikkerhetsløsninger er det vektlagt at disse tiltakene ikke går på bekostning av anvendbarheten.

Forord

Denne rapporten er en avsluttende hovedoppgave i masterutdanningen innenfor informasjon- og kommunikasjonsteknologi (IKT) ved Høgskolen i Agder, avdeling for teknologi i Grimstad. Faget IKT-6400 Hovedoppgave tilsvarer 10 vekttall.

Oppgaven ”Mobil Elektronisk Pasientjournal – Studie av anvendbarhet, sikkerhet og muligheter” ble definert i samarbeid med Rune Fensli, Lars Line og kandidatene. Arbeidet med oppgaven har pågått mellom januar og mai 2003.

Anvendelse av mobile dataenheter for medisinsk bruk er i en rask utvikling. Prosjektet Mobil Elektronisk Pasientjournal ved Sørlandet sykehus HF Arendal er banebrytende i Norge, og er utgangspunktet for en studie i forhold til anvendbarhet, sikkerhet og fremtidsmuligheter ved mobil elektronisk pasientjournal.

Diplomoppgaven er knyttet til et pågående forskningsprogram mellom Høgskolen i Agder, Telenor FoU Agder, Sørlandets Sykehus HF Arendal og Grimstad Kommune med tittelen ”Sikkerhet i trådløse medisinske datanett”, NFR prosjekt nr 153935/320. Oppgaven omhandler en viktig del av dette prosjektet gjennom et studie av det første forsøk i Norge ved anvendelse av mobile dataløsninger i tilknytning til elektronisk pasientjournal, EPJ.

Med utgangspunkt i denne rapporten er det utarbeidet en presentasjon som er akseptert som prosjektpresentasjon under seminaret ”Scandinavian Conference in Health Informatics 2003” som skal avholdes i Arendal 12.-13. juni 2003.

Denne rapporten er skrevet av Vegar Kristensen og Bård Eirik Lyche. Vi vil takke våre veiledere Rune Fensli og Lars Line for råd og hjelp under arbeidet med oppgaven.

Grimstad, 26. mai 2003

Vegar Kristensen Bård Eirik Lyche

Innholdsfortegnelse

Figurliste

Tabelliste

1 Innledning

1.1 Oppgavetekst

Anvendelse av mobile dataenheter for medisinsk bruk er i en rask utvikling. Ved Sørlandet sykehus HF Arendal (SSA) har det vært en begrenset testing av håndholdte systemer beregnet for bruk under legevisitt. Prosjektet Mobil Elektronisk Pasientjournal (Mobil EPJ) ved SSA er banebrytende i Norge, og er utgangspunktet for en studie i forhold til anvendbarhet, sikkerhet og fremtidsmuligheter ved mobil elektronisk pasientjournal.

Gjennom oppgaven skal det gjøres en kartlegging av brukernes erfaringer fra testperioden. Det er nødvendig at trådløse datanettverk for helsesektoren tilfredsstiller lovpålagte krav til datasikkerhet, og en skal evaluere aktuelle sikkerhetsmessige løsninger som kan anvendes. Basert på brukernes erfaringer og sett i forhold til nye teknologiske muligheter, skal det skisseres mulige forbedringsområder og aktuelle funksjoner for et fremtidig mobilt EPJ-system.

1.2 Bakgrunn

SSA innførte i løpet av 2001 elektronisk pasientjournal (EPJ). Nytteverdien av et lignende system er evaluert i rapporten *Nytteverdi af EPJ* [1]. Den nye sykehusloven som trådte i kraft 1.1.2001 tillater bruk av elektronisk lagringsmedium uten bruk av sikkerhetskopier på papir eller mikrofilm. Dette innebærer at mange av de innlagte pasientene har hele den historiske A-journalen elektronisk, papirkopien er makulert.

Straks etter innføringen av EPJ, meldte det seg et behov for å kunne hente opp pasientinformasjon nær pasientens seng under legevisitten. Det er plassert stasjonære PC-er på alle arbeidsrom, behandlingsrom og kontorer, men det er både tungvint og tidkrevende å bruke disse under visitten. På grunn av dette, ble det gjennomført et utviklingsprosjekt med mobil EPJ hos SSA fra august 2002 til januar 2003.

For at et slikt system skal bli akseptert og tatt i bruk av leger og sykepleiere, er det visse kriterier som er nødt til å bli oppfylt [4]. Brukerne må se nytteverdi og oppleve god anvendbarhet for å ta et slikt system i bruk. I dag foreligger det ingen fullstendige evalueringsrapporter på dette området, heller ikke på hvordan et slikt system bør settes opp teknisk for å ivareta en god nok sikkerhet. Under utvikling av sikkerhetsløsninger er det viktig å vektlegge at disse tiltakene ikke går på bekostning av anvendbarheten.

Det ble tatt initiativ til å etablere en prosjektgruppe som hadde til oppgave å administrere det mobile EPJ systemet hos SSA. Denne gruppen er satt sammen av både IT-personale, leger og sykepleiere. Før diplomoppgaven startet, forelå et ønske

fra denne prosjektgruppen om et tett samarbeid. Fra prosjektgruppens side vil dette studiet bidra med råd om hvordan mobil EPJ bør utvikles videre.

1.3 Oppgavebeskrivelse

Tekniske løsninger i et reelt miljø

En trend den siste tiden har vært å føre pasientjournaler på elektronisk form, noe som også fører til at rutinene for å hente ut og lagring av data, endres. Diplomoppgaven tar utgangspunkt i utviklingsprosjektet av mobil EPJ hos SSA, som har strukket seg fra august 2002 til januar 2003. Hensikten med dette mobile systemet, er at leger og sykepleiere skal kunne behandle pasientdata under visitt. Et slikt system kan ikke tas i bruk, dersom sikkerheten ikke er god nok. På den annen side hjelper det ikke at systemet er sikkert, dersom potensielle brukere (her: leger og sykepleiere), ikke vil ta det i bruk.

Diplomoppgaven har som formål å evaluere funksjonalitet, anvendbarhet og nytteverdi ved InfoPack_Helse. Videre vurderes brukernes oppfatning av PDA i forhold til tablet PC og bærbar PC. I denne sammenheng vurderes kvalitet og funksjonalitet på valgte mobile enheter. Dette arbeidet er ment å resultere i forslag til hvilke typer arbeidsprosesser de ulike verktøyene er best egnet til. I tillegg til å evaluere hvilken type informasjon som behandles mest effektivt med de forskjellige verktøyene, er det viktig at det blir frigitt tid til pasientkontakt og behandling.

Trådløse informasjonssystemer kan sies å være spesielt utsatt for avlytting, ettersom en angriper ikke trenger å koble seg opp mot noe fast nett. Alle datasignalene sendes over luften. Dette stiller store sikkerhetskrav i forhold til autentisering, autorisering og kryptering. Diplomoppgaven skal bedømme i hvilken grad sikkerhetsmekanismene i utviklingsprosjektet var tilfredsstillende. Dersom det er mulig å gjøre forbedringer på dette området, skal det presenteres en konkret løsning.

Utviklingsmuligheten som ligger i et slikt mobilt EPJ-system, må fokusere på at visitten skal effektiviseres. I tillegg skal sikkerhetsmekanismene være tilfredsstillende, uten at dette går på bekostning av anvendbarheten.

Begrensninger

Det er ikke ment at oppgaven skal resultere i et ferdig produkt som SSA uten videre skal kunne ta i bruk. Derimot vil resultatet påpeke feil og mangler ved mobil EPJ slik det fungerer i dag, og evaluering av mulige fremtidige løsninger. Det skal ikke testes eller lages nye løsninger eller noen demonstrator. Prosjektet skal søke etter sikre løsninger og metoder for autentisering og meldingsformidling i medisinske nettverk hvor trådløse enheter inngår.

Studiet omfatter ikke strålingsproblematikk og hvordan radiosendere kan være med på å forstyrre annet medisinsk utstyr. Når det gjelder anvendbarhetsstudiet er det heller ikke tatt hensyn til at enkelte brukere eventuelt har motforestillinger mot å arbeide i et strålingsmiljø av helsemessige årsaker.

1.4 Problemstillinger og formål

Bruk av elektroniske journaler er knyttet til sikkerhet på flere nivå. I dette prosjektet fokuseres det på sikkerhet knyttet til sikker trådløs kommunikasjon mellom journalsystemer og mobile enheter. Hvordan kan et mobilt EPJ system utvikles sikkert nok i forhold til krav som stilles fra Datatilsynet? I tillegg er det viktig å få frem om brukerne opplever løsningen som enkel og rask å bruke i sin hverdag. Evalueringsarbeidet vil i hovedsak foregå i tre arbeidsprosesser:

Anvendbarhetsstudie gjennomføres for å kartlegge brukernes erfaringer fra testperioden med mobil EPJ hos SSA. Her fokuseres det på hvordan brukerne ser for seg et velfungerende mobilt EPJ-system. Oppgavens mål er å kartlegge brukernes erfaringer i forhold brukervennlighet, funksjonalitet, behov og eventuelt årsaker til ikke bruk av mobil EPJ hos SSA.

Når det gjelder den tekniske delen av rapporten, skal systemet beskrives. Hvor gode sikkerhetsmekanismer som til nå er valgt, skal evalueres. Det vil være nødvendig med et tett samarbeid med SSA og aktuelle leverandører. Rapporten skal belyse hvilke forbedringsmuligheter det er i forhold til eksisterende sikkerhetsmekanismer.

Oppgaven skal belyse hvilke utviklingsmuligheter som ligger i mobil EPJ-systemer. Resultater fra brukernes synspunkter, egne observasjoner og krav til tekniske løsninger vil være vektleggende faktorer. Studiet av fremtidsmuligheter vil bli den kreative delen hvor nye applikasjoner drøftes i lys av de to foregående kapitlene.

1.5 Rapportens organisering

Både utstyr og infrastruktur rundt det trådløse nettverket hos SSA blir beskrevet slik det fungerte i testperioden. Det tekniske oppsettet er satt opp som en oppfølging til hva som var bakgrunnen og hvilke mål som er ønskelige å oppnå ved en slik innføring.

I anvendbarhetsstudiet utarbeides en rekke hypoteser som det skal evalueres gyldigheten av. I dette arbeidet benyttes observasjon og spørreskjemaer med etterfølgende intervjuer. For å bekrefte eller avvise disse hypotesene benyttes den godt uttestede Technology Acceptance Model (TAM) [4]. I resultatkapittelet er derfor svarene fra spørreundersøkelsen kategorisert i forhold til TAM, slik at det på en oversiktlig måte vises hvordan de ulike elementene er med på å påvirke aksept for systemet.

Sikkerhetsstudiet starter med å gi en innføring i hvilke sikkerhetsmekanismer som var implementert i det mobile EPJ prosjektet hos SSA. For å vurdere om disse sikkerhetsmekanismene er gode nok, blir det tatt hensyn til Datatilsynets krav til sikkerhet. Ut i fra disse kravene, drøftes ulike sikkerhetsmekanismer som eksisterer på markedet i dag og hvilke angrep det er viktig å sikre seg mot. Hele sikkerhetsstudiet ender opp med forslag om tiltak som bør iverksettes for å gjøre et trådløst nettverk sikkert nok i et sykehusmiljø.

Når det gjelder fremtidsmuligheter for et mobilt EPJ system, drøftes anvendbarhet og sikkerhet som de to viktigste parametere. Kravene til disse må i mer eller mindre grad være tilfredsstilt for at systemet skal bli akseptert. Dette arbeidet resulterer i et forslag til forbedringer av systemet slik det har vært frem til nå.

2 Mobil EPJ på SSA

2.1 Bakgrunn

Etter at Sørlandet sykehus HF Arendal innførte elektronisk pasientjournal, meldte det seg et behov for å kunne hente opp pasientinformasjon nær pasientens seng under legevisitten. Selv om det er plassert stasjonære PC-er på alle arbeidsrom, behandlingsrom og kontorer, er det både tungvint og tidkrevende å bruke disse under visitten. Dette ligger til grunn for et arbeid med å innføre mobil tilgang til pasientinformasjon.

Prosjektet mobil EPJ var opprinnelig tenkt som et testprosjekt, men snudde seg etter hvert til å bli et utviklingsprosjekt. Grunnen til dette er at programmet InfoPack_Helse ikke var ferdig utviklet når det ble satt i drift på SSA. I tillegg ble det mange problemer med implementeringen, og flere funksjoner ble ikke implementert. Først etter et par måneders tid økte stabiliteten på systemet.

2.2 Gevinstpotensial ved mobil EPJ

Innføringen av mobil EPJ medfører flere mulige gevinster for SSA [41]. Blant de viktigste gevinstene, kan det nevnes:

- **Optimal utnyttelse av EPJ**
  Innføringen av mobil EPJ kan føre til at utnyttelsen av EPJ-systemet blir optimalisert. Dette er forsøkt oppnådd gjennom et mobilt EPJ-system hvor brukergrensesnittet er utviklet for det medisinske personalets arbeidsoppgaver. Det er lagt vekt på at systemet skal være brukervennlig i tillegg til at de forskjellige arbeidsoppgavene skal kunne løses raskt og enkelt med minst mulig tastetrykk. Systemet er også tilpasset PDA med InfoPack_Helse, kapittel 2.3.6, slik at enhetene skal være lettest mulig å ha med rundt på avdelingen og spare brukerne for mye spasering.

- **Bedret kvalitet på pasientinformasjonen**
  Før innføringen av EPJ ble det papirbaserte journalene tatt med rundt på visitten og arbeidet ble gjort direkte i journalene. Etter innføringen av EPJ ble dette umulig, siden arbeidet måtte gjøres på stasjonær PC. Løsningen fungerte ved at alt ble notert på lapper og i blokker, og at personalet senere måtte skrive inn informasjonene i DIPS etter visitten. Ble det stilt spørsmål visittpersonalet ikke hadde kjennskap til, måtte de gå til nærmeste stasjonære PC og sjekke dette.

  Etter at mobil EPJ er innført, skal personalet unngå å måtte gå til de stasjonære PC-ene. Informasjonen skal leses ut og skrives inn i den elektroniske journalen direkte under visitten ved hjelp av de bærbare, trådløse enhetene. Dette skal redusere behovet for previsitt og fjerne behovet for

ettervisitt. I tillegg fører dette til at hele journalen til enhver tid er oppdatert og tilgjengelig. På denne måten vil også dobbeltarbeid forhindres, og kvaliteten på pasientinformasjonen bedres.

Ettersom pasientinformasjonen alltid er tilgjengelig ved sengen, vil dette også sikre at pasienten får best mulig og riktig behandling. Ved innføringen av mobil EPJ vil også utskriving gå raskere. Legen kan sende all nødvendig informasjon fra enheten til merkantilt personale, slik at de kan begynne å klargjøre papirer under visitten.

I situasjoner der informasjonsflyten går på tvers av yrkesgruppene, eller hvor hver yrkesgruppe har ansvaret for hver sin informasjon, vil mobil EPJ bedre flyten. Informasjonen blir registrert med en gang, og blir raskt tilgjengelig for annet personale som skal bruke informasjonen.

- **Enkle og effektive rutiner med bevart kvalitet og trivsel**
  Mobil EPJ skal sikre bedret informasjon til pasientene. Det legges vekt på at informasjonsbehandlingen skal være både enklere og raskere enn den var med den gamle papirbaserte løsningen. Rutiner kan effektiviseres ved at arbeid kan utføres og tjenester settes i gang ved sengen, med det resultatet at behandlingen går raskere. Mobil EPJ skal ikke gå utover pasientkontakten.

2.3 Utstyret

2.3.1 Aksesspunkt

I prøveprosjektet har SSA benyttet Symbol AP-4121 [6]. Dette er aksesspunkter som støtter 802.11b-standarden med en hastighet på opptil 11 Mbps og tre kanaler. Utover standarden støtter disse aksesspunktene høyhastighets roaming som gjør at de mobile klientene vil velge det aksesspunktet med sterkest signal og minst trafikk til enhver tid.

Sikkerhetsmessig har aksesspunktene støtte for både 128 bits WEP-kryptering og Kerberos V5-kryptering, i tillegg til 40 bits WEP-kryptering som er standard. En kan også benytte kombinasjoner av disse mulighetene. SSA prøvde først med Kerberos V5-kryptering i tillegg til autentisering av kun utvalgte MAC-adresser, men fikk da problemer med at brukerne også måtte bruke Kerberos til å logge seg på de stasjonære PC-ene. Etter en tid ble Kerberos byttet ut med 128 bits WEP-kryptering i kombinasjon med autentisering av utvalgte MAC-adresser.

Sikkerhetsmekanismen *autentisering med utvalgte MAC-adresser* innebærer at aksesspunktene må vite MAC-adressene på alle enhetene som skal ha mulighet for å bruke det trådløse nettet. SSA uttrykte at det var mye jobb å vedlikeholde disse

listene. Aksesspunktene har en mulighet for å hente adresselistene fra en sentral kilde, slik at vedlikehold kun er nødvendig på denne og ikke på hvert enkelt aksesspunkt. SSA benyttet seg ikke av denne muligheten.

SSA har satt opp tre aksesspunkter på kirurgisk avdeling 3D og fem aksesspunkter på medisinsk avdeling UC. På hver avdeling er det også en Power-Over-Ethernet hub fra Symbol som gir strøm til aksesspunktene fra huben gjennom standard Cat5 TP-kabel, slik at separat strømforsyning til aksesspunktene ikke er nødvendig.

Symbol AP-4121 kan leveres med både omnidireksjonal (360°) og direksjonal (20-90°) antenne. SSA har benyttet seg av begge disse.

2.3.2 PDA

Symbols PPT-2846 var i testperioden tilgjengelig for leger og sykepleiere både ved 3D og UC.

Symbol PPT-2846 [5] er en PDA som kombinerer de sterke sidene fra PDA med produktivitetsforbedrende funksjoner. Dette er funksjoner som strekkodeskanning og innebygd trådløs nettverkskommunikasjon basert på 802.11b. Den har en Intel SA 1110 prosessor på 206 MHz og 64 MB RAM. Operativsystemet er Microsoft Pocket PC 2002. Skjermen har ¼ VGA-oppløsning (320 x 240 piksler) med 64 k fargeskjerm.

EPJ-systemet som kjøres på PDA, InfoPack_Helse, er webbasert og den bruker MS Internet Explorer for å få aksess til dataene i DIPS-databasen.

2.3.3 Tablet PC

SSA prøvde også ut en tablet PC. Her valgte de Fujitsu Stylistic LT P-600 [7]. Dette er en tablet PC med 600 MHz Intel Pentium III prosessor. Skjermen er en 8,4'' berøringsskjerm med 800 x 600 pikslers oppløsning og 256 k farger. Operativsystemet er Windows 98 Second Edition med PenX 2.02 programvare for berøringsskjermen.

Ettersom tablet PC-en bare har Ethernet-kort innebygd, ble disse bestykket med Symbol Spektrum24 PCMCIA trådløse nettverkskort.

Tablet PC-en ble i utviklingsprosjektet kjørt med EPJ-systemet InfoPack_Helse, som har webgrensesnitt over MS Internet Explorer slik som PDA. Det var meningen at SSA også skulle prøve tablet PC-en med DIPS over tynnklient slik som den bærbare

PC-en, men det ble i praksis aldri prøvd. DIPS krever minimum 1024 x 768 pikslers oppløsning, og vil derfor ikke fungere på tablet PC.

Utviklingen på markedet rundt tablet PC har vært stor den siste tiden. Et resultat av dette, er at dagens tablet PC har blitt forbedret på flere områder i forhold til de som ble benyttet i utviklingsprosjektet hos SSA, og som er bakgrunn for denne undersøkelsen. De fleste tablet PC-er på markedet i dag har en løsning hvor tastatur likevel er implementert, enten ved at det kan brettes ut eller klikkes på. I tillegg har den stor skjerm med høy nok oppløsning til å kjøre DIPS direkte.

2.3.4 Bærbar PC

Den bærbare PC-en ble utstyrt med det samme trådløse nettverkskortet fra Symbol som tablet PC-en hadde. På denne ble DIPS brukt, i tillegg til Citrix Metaframe tynnklient hvor alle programmer blir kjørt på serveren og ikke i enheten. Her fikk også brukerne nøyaktig samme grensesnitt som på de stasjonære PC-ene, siden disse også kjører tynnklient med samme pålogging.

De største forskjellene på bærbar PC i forhold til de to andre enhetene er hovedsakelig at den bærbare PC-en har prosessorkraft nok og stor nok skjerm til å kjøre DIPS. Dette er absolutt en fordel, siden brukerne da ikke må sette seg inn i et nytt program, men møter et brukergrensesnitt de kjenner godt fra før.

En annen stor forskjell er at den bærbare PC-en har tastatur, noe som gjør at inntasting av data blir mye enklere enn å skrive med penn på skjermen. Dette innebærer også at enheten blir mindre bærbar og må fraktes på tralle.

2.3.5 DIPS

DIPS ASA leverer pasientdatasystemer med mye funksjonalitet. Det er utviklet digitale løsninger for skanning, arbeidsflyt og mobil EPJ. DIPS er et modulært system med funksjoner for digital journal, pasientadministrasjon, radiologi, ventelister, poliklinikk, laboratoriesystem og så videre. DIPS er et åpent system, og over 30 samarbeidspartnere utvikler løsninger som samspiller nært med DIPS, blant annet Medicom med InfoPack_Helse [10].

EPJ-systemet DIPS er et omfattende og kraftig informasjonssystem for sykehus. Systemet er bygd opp av moduler, slik at det kan tilpasses til hver installasjon, samt utvides ved senere anledninger. Det er en tett kobling mellom delsystemene, som gir en helhet og medfører at data registreres og lagres på færrest mulig steder. Samtidig kan data gjenbrukes og presenteres i forskjellige sammenhenger.

Sikkerhetsmessig har DIPS et omfattende system for adgangskontroll. Dette systemet baserer seg på hendelser og kategorisering av data, og gjør at adgangskontrollsystemet er kraftig og fleksibelt. Det kan tilpasses behovene i hver enkelt installasjon. DIPS har adgangskontroll både på funksjons- og datanivå. I tillegg er det mulig å gi kun enkelte brukere tilgang til en pasients data og dermed ha en enda strengere adgangskontroll. Om brukerne må taste inn forskjellige passord flere ganger, øker sannsynligheten for at brukerne noterer ned passord på lapper eller lignende. Dette senker datasikkerheten, derfor kan passordkontrollen i DIPS

integreres i passordkontrollen på nettverket slik at brukerne bare taster inn passordet en gang [10].

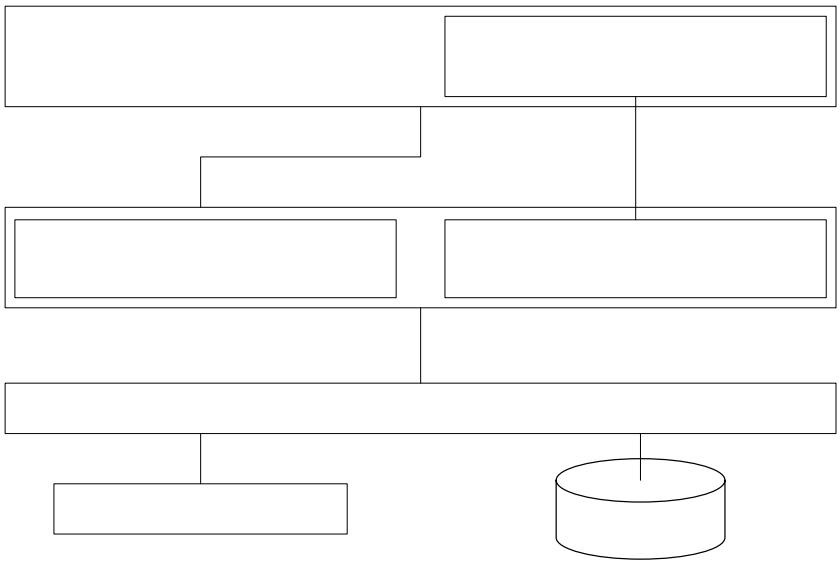
DIPS gir en god kontroll med dataene i systemet. I stedet for å synkronisere data i forskjellige systemer og få alle problemene som følger med det, har man i DIPS valgt å integrere systemene slik at man unngår dobbeltlagring av data. På den måten vil dataene alltid være oppdaterte og korrekte. Det er også automatisk logging av endringer og oppslag i journalopplysningene, slik at man kan spore disse. DIPS har i tillegg en blålysfunksjon som gir mulighet for å omgå sikkerheten ved nød og andre spesielle tilfeller, og på denne måten gi brukeren tilgang til normalt sperrede data. Bruk av denne funksjonen logges spesielt.

DIPS er utviklet for åpen teknologi. Systemene kjøres på standard nettverk og vanlige PC-er. På klientsiden benyttes 32-bits Windows. På databasesiden er det valgt å standardisere på Oracle 8. Gjennom et omfattende sikkerhetssystem kan det integreres funksjonalitet fra tredjeparts leverandører. Det er valgt å benytte Microsofts standard for brukergrensesnitt, noe som gjør at brukere med Windows-erfaring lett lærer seg systemet. Det er ved noen tilfeller lagt inn redundans for å få bedre hastighet. Denne redundansen vedlikeholdes av triggere i databasen. På denne måten vil de redundante data i databasen alltid være konsistente [10].

2.3.6 InfoPack_Helse

InfoPack_Helse er et mobilt informasjonssystem for sykehus utviklet av Medicom AS. Det er den første løsningen i sitt slag på markedet. Medicom AS ble startet i 2000, og fikk en utviklingsavtale med DIPS i april 2001 [11].

InfoPack_Helse er tilpasset DIPS EPJ-system, og selges som en modulbasert påbygging til dette. Systemet er plattformuavhengig, siden det kun avhenger av webleser for å få opp informasjonen [11].



Figur 2-1: Oppbygning av InfoPack_Helse [40]

InfoPack_Helse v1.0 består av InfoPack_Helse Server, InfoPack_Helse Diktafonmodul og InfoPack_Helse Transkripsjonsmodul. Figur 2-1 viser oppbyggingen av InfoPack_Helse. Denne viser at dataene blir presentert som webside og kan lese med en webleser. Dataene som blir sendt over nettet fra serveren til enhetene, er i HTML-format og krever lite ressurser [40].

I tillegg er diktafonmodulet bygd inn med ActiveX og overføring med SOAP til diktafonenheten i serveren, slik at personalet kan diktere pasientjournalen på enheten og sende denne digitalt til skrivestua. Systemet innebærer også en Medicom-server som henter data fra DIPS-serveren og en SQL-server [40].

Det er planlagt at InfoPack_Helse skal bygges ut med flere moduler.

2.4 IEEE 802.11b

Utstyret som har vært i benyttet på SSA har vært basert på 802.11b trådløst nettverk.

2.4.1 Radiogrensesnittet

Frekvensbåndet i 802.11b er 2,4 GHz, nærmere bestemt 2,4000-2,4835 GHz. Overføringshastigheten er maks 11 Mbps på det fysiske laget, men det støtter også 1, 2 og 5,5 Mpbs. 802.11b sender i ISM-båndet (Industrial, Scientific and Medical), populært kalt søppelbåndet. I dette båndet er det ikke noe krav til konsesjon, derfor kan det være mye støy i dette området. Hvis det blir bitfeil på grunn av for mye støy eller for lang avstand mellom den mobile terminalen og aksesspunktet, vil hastigheten automatisk bli justert ned [43].

802.11b er et cellulært system hvor hver celle har en rekkevidde på opptil 100-150 meter i fri sikt. Antall tilkoblede terminaler er i teorien ubegrenset, men de fleste produkter har en begrensning på dette. Standarden definerer også tre kanaler som ligger på hvert sitt frekvensområde, slik at inntil tre celler kan overlappe hverandre [42].

Det er full mobilitet innenfor dekningsområdet til et aksesspunkt. Dersom man beveger seg utenfor dekningsområdet til et aksesspunkt og inn i en ny celle, må forbindelsen settes opp på nytt. Selv om standarden ikke støtter mobilitet, har likevel enkelte produsenter implementert dette i sine produkter. Et eksempel på dette er Symbols utstyr som brukt sammen, støtter høyhastighets roaming for avbruddsfri kommunikasjon ved bytte av aksesspunkt [6].

2.4.2 Tjenestekvalitet

802.11b har forbindelsesløs oppkobling. Det vil si at det ikke settes opp noen fast forbindelse, men at det sendes enkeltstående pakker med hver sine headere ut i nettet. Medium aksess er sørget for av CSMA/CA. CSMA-protokollen gjør at senderen lytter på mediet før den skal sende. Hvis det er opptatt, venter senderen en tilfeldig tid før den prøver på nytt. CA gjør at mottageren kjører en Cyclic Redundary

Check (CRC) på mottatt pakke for å sjekke den for feil. Hvis pakken er feilfri, blir en kvittering (ACK) sendt tilbake [42].

Tabell 2-1: Tekniske data ved IEEE 802.11b

Spektrum	2.4 GHz
Hastighet	11 Mbps (Lag 1)
	5 Mbps (Lag 3)
Svitsjetype	Pakke
Medium aksess	CSMA/CD
Autentisering	Lag 2
Kryptering	40bit RC4 (WEP)
Handover/roaming	Nei
Støtte for faste nett	Ethernet

For å redusere sannsynligheten for feil når lange pakker overføres, blir disse pakkene fragmentert. På mottagersiden blir pakkene refragmentert, sjekket for feil med CRC og kvittering blir sendt. Hvis denne kvitteringen ikke kommer tilbake, vil fragmentet bli sendt på nytt.

802.11b benytter seg av ”best effort”-levering av pakker. Dette betyr at den mobile terminalen kun kan sende pakker, det underliggende nettverket vil da gjøre sitt beste for at disse skal komme frem [42].

2.5 IEEE 802.11a

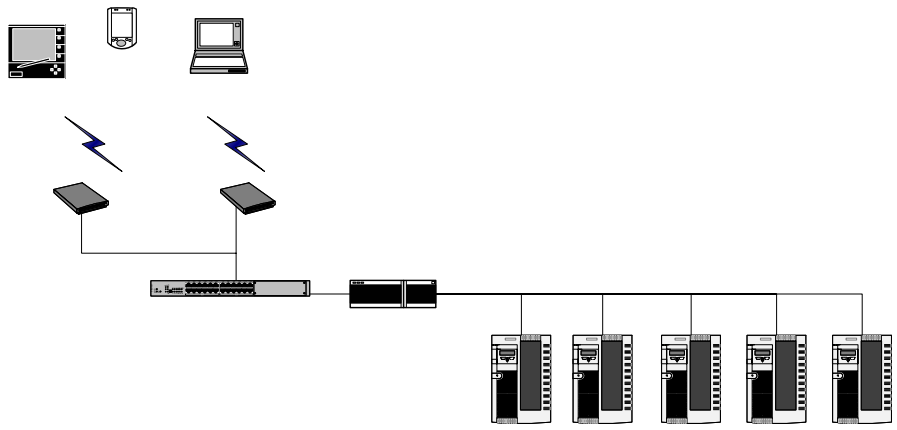
IEEE 802.11a opererer i frekvensområdene 5,15 til 5,25 GHz, 5,25 til 5,35 GHz og 5,725 til 5,825 GHz [8]. Dette forhindrer interferens med Bluetooth og andre produkter som opererer på det velbrukte ISM-båndet, slik som 802.11b. For 802.11a er det allokert 300 MHz for ulisensiert bruk, noe som er seks ganger mer enn for 802.11b. Dette gir mulighet for bitrater opp til 54 Mbps. 802.11a har støtte for både roaming og handover, og åpner for stor mobilitet innenfor det trådløse nettet. Standarden baserer det fysiske laget på Orthogonal Frequency Division Multiplexing (OFDM) [8]. Dette bidrar til en mer stabil forbindelse, ved at flere bærebølger blir benyttet i hver forbindelse. Aksesspunkt som baserer seg på denne standarden, har mulighet til å benytte seg av åtte kanaler. Dette gir mulighet til flere overdekkende celler enn for 802.11b, som har tre kanaler. Sikkerhetsmekanismer som er spesifisert i standarden, er delt nøkkel autentisering og kryptering gjennom WEP-algoritmen. [8]

2.6 Infrastruktur på mobil EPJ på SSA

Prosjektet mobil EPJ innebar at systemet kun skulle settes i drift på to valgte avdelinger. Disse var medisinsk avdeling UC og kirurgisk avdeling 3D.

Figur 2-2 viser hvordan nettarkitekturen på SSA så ut under testperioden av mobil EPJ hos SSA. De trådløse enhetene på avdelingene koblet seg til aksesspunktene som var plassert rundt på de to avdelingene. Alle aksesspunktene var koblet til

Ethernet strømhub, som det er plassert en av på hver avdeling. Disse hub-ene var derfra koblet direkte til den sentrale HP-switchen i nettet. HP-switchen er en lag 3-switch, denne sørger for at de trådløse nettene samles til et VLAN. VLAN-et til det trådløse nettet hadde kun tilgang til EPJ-serveren.



Figur 2-2: Infrastruktur rundt mobil EPJ på SSA

I nett som inneholder sensitiv informasjon, deles disse vanligvis inn i en sikker sone som inneholder de sensitive dataene, og en ikke-sensitiv sone. På denne måten kan det brukes sterkere sikkerhetsmekanismer på den sikre sonen, og resten av nettet unngår sikkerhetsmekanismene. SSA har i motsetning valg å definere hele nettet som sikker sone, slik at alle barrierene hindrer trafikk inn og ut i nettet. Når en først er inne i nettet, er det helt åpent.

Under dette prosjektet ble ikke sikkerheten prioritert, siden det kun er et utviklingsprosjekt. Det ble i starten av prosjektet forsøkt med Kerberos-kryptering, men da dette skapte store problemer, ble det kun kjørt WEP-kryptering med autentisering etter lister med MAC-adresser. Dette er beskrevet nærmere i kapittel 4.1.

PDA

Tablet

Bærb

Aksesspunkt

3 Anvendbarhetsstudie

3.1 Innledning

For å få en oversikt over brukernes synspunkter i forbindelse med aksept av mobil EPJ, har dette studiet kartlagt brukernes erfaringer fra testprosjektet ved avdelingene 3D og UC. Alle data ble samlet inn for å sammenlignes med prosjektets hensikt, som beskrevet i prosjektplanen [19]. Etter samtaler med både IT-drift, sykepleiere og leger ved avdelingene, ble følgende hypoteser formulert:

1. **Mobil EPJ ble lite i bruk i løpet av testperioden**
   Av ulike årsaker virker det som om systemet ikke har blitt anvendt i det omfanget som var ment etter prosjektgruppens ønske da testprosjektet ble innført.

2. **Tekniske årsaker var en viktig årsak til at PDA, tablet PC og bærbar PC ikke ble tatt mer i bruk**
   Både leger og sykepleiere i prosjektgruppen antydet at det har vært en dårlig teknisk kvalitet, og at denne kan være årsaken til at systemet har blitt så lite brukt.

3. **Opplæring og support i forhold til InfoPack_Helse har vært mangelfull i utviklingsprosjektet**
   Som en årsak til den lille bruken av systemet, kan det være at oppfølgingen har vært for dårlig i prosjektgjennomføringen. Dersom brukerne opplever at de ikke vet helt hva mobil EPJ skal brukes til, eller at de ikke får nødvendig hjelp når noe går galt vil dette hemme bruken av systemet.

4. **InfoPack_Helse gir nødvendig informasjon under visittgang**
   Hvorvidt det er enkelt å registrere og hente ut data med InfoPack_Helse, vil i dette tilfellet være avgjørende om leger og sykepleiere tar det i bruk. Det er en problemstilling om PDA oppleves å ha for liten skjerm. I hvor stor grad brukerne verdsetter tastatur i forhold til berøringsskjerm, har også betydning i denne sammenhengen. Det vil her være fokus på om databehandlingen med InfoPack_Helse er så rask, at alt registreringsarbeidet kan gjøres ferdig under visittens raske tempo.

5. **Det eksisterer et behov for mobil tilgang til elektroniske pasientjournaler.**
   Det er behov for å ha med journalene rundt på visitten. Etter innføringen av EPJ har dette vært umulig, ettersom pasientdataene kun har vært tilgjengelige gjennom de stasjonære PC-ene. Det antas at det er et behov for mobil EPJ, slik at den elektroniske journalen kan tas med ved hjelp av en bærbar enhet. Det vil være viktig å få kartlagt hvordan holdningene til mobil EPJ har endret seg i løpet av prosjektperioden.

6. **Mobil EPJ virket forstyrrende i visittpersonalets kommunikasjon med pasientene**
   Det kan antas at brukerne har opplevd at de mobile håndholdte enhetene tok oppmerksomhet fra pasientene. Tilbakemeldinger har gitt indikasjon på at det ble for stor fokus på enhetene. Likevel kan man anta at interessen for å informere pasientene øker, ettersom informasjonen blir tilgjengelig der og da.

7. **Et mobilt EPJ system bør utvides med flere tjenester**
   Når det gjelder utviklingsmuligheter, er det håp om å få frem brukernes egne forutsetninger for å ta systemet i bruk. Et mål her vil være at brukerne selv kartlegger hvilke utviklingsmuligheter det ligger i systemet.

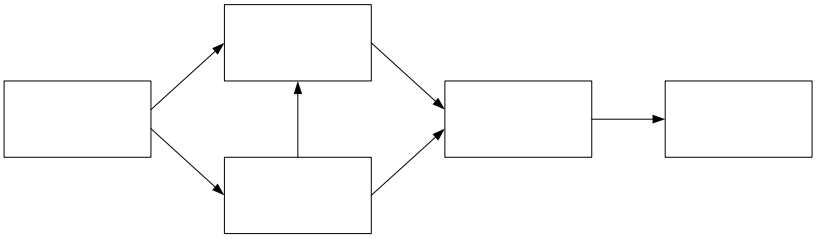
3.2 Teorier

3.2.1 Technology Acceptance Model (TAM)

TAM er en modell som gjennom mange år har blitt godt testet og validert. Denne modellen er først og fremst anvendt til å forklare adapsjonen av teknologi innenfor organisasjoner [3]. Studier har vist at TAM kan bli tatt i bruk til områder som informasjonsteknologi, og kan forklare individers holdninger til ny teknologi [4], [16].

TAM er en adapsjon av Theory of Reasoned Action (TRA) [17], som spesifiserer to viktige faktorer, *oppfattet nytte* og *oppfattet enkelthet ved bruk*, for at IT skal tas i bruk etter intensjonene. I TAM blir formålet fastslått ved å se på holdninger til bruk i tillegg til direkte og indirekte effekter av de nevnte faktorene. Fordelen med denne modellen er at den er både spesifikk og enkel. TAM har etter hvert fått empirisk støtte i informasjonsteknologiske undersøkelser. Studier har vist at TAM kan forutsi intensjoner om bruk av software bedre enn TRA [18].

TAM er ment å bli brukt for å vise sammenheng mellom *oppfattet nytteverdi*, *oppfattet enkelthet ved bruk*, *holdninger til bruk*, *intensjon om bruk* og *faktisk bruk* av mobil EPJ hos SSA.



Figur 3-1: Technology Acceptance Modell, TAM [18]

I TAM er *faktisk bruk* satt opp i modellen som en direkte funksjon av *holdninger til bruk*. Disse vil bekrefte eller avvise hypotesene 1, 2 og 3, som går på bruk og

grunner til lite bruk. *Holdninger til bruk* er en funksjon av *oppfattet nytte* og *oppfattet enkelthet ved bruk*.

Det er i modellen tenkt at *oppfattet enkelthet ved bruk* skal ha en direkte effekt på *oppfattet nytte*. Disse elementene er viktige for å kvalitetssikre resultater av hypotese 3 som omfatter brukeraksept.

Oppfattet nytte er i denne modellen definert som ”i hvilken grad et individ tror at bruk av et bestemt system vil øke hans eller hennes yteevne på arbeidet” [4]. *Oppfattet enkelthet ved bruk* er definert som ”i hvilken grad et individ tror at bruk av et bestemt system vil være fri for fysisk eller mental anstrengelse” [4].

Alle faktorer som ikke eksplisitt er nevnt i modellen, vil gjøre inntrykk enten på intensjoner eller bruk ved å påvirke *oppfattet nytte* og *oppfattet enkelthet ved bruk* [18]. Derfor er det valgt å ta hensyn til *funksjonalitet* under *oppfattet enkelthet ved bruk*, siden tilfredsstillende og logisk funksjonalitet er viktig for å opprettholde enkelthet ved bruk. Funksjonalitet vil også gi et svar på hypotese 6 om at flere tjenester må bli implementert i et slikt system. Under *oppfattet nytte* er det også lagt til *behov*, siden *oppfattet nytte* er avhengig av at det er et behov for systemet. Dette elementet av TAM vil da bekrefte eller avkrefte hypotese 4 som går på at det eksisterer et behov for mobil EPJ.

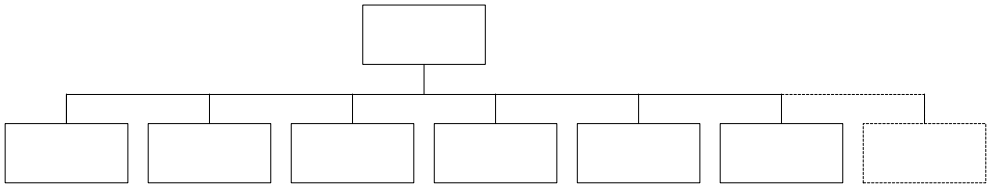
TAM har blitt benyttet til å utvikle hypotesene beskrevet i kapittel 3.1, og til å gruppere forskjellige temaer som har betydning for aksept av det mobile EPJ systemet hos SSA. Ettersom modellen er noe overfladisk, ble både prosjektplanen [19] og Usability Analysis of Man-Machine Interface tatt i bruk for å beskrive anvendbarheten til systemet på et mer detaljert nivå.

3.2.2 Usability Analysis of Man-Machine Interface (UAM)

Hvordan en bruker opplevde brukergrensesnittet til nytt utstyr, er en av de viktigste faktorene i avgjørelsen av aksept. For å gå ned på et mer detaljert nivå under *enkelthet i bruk* i forhold til TAM, benyttes UAM til å få frem hvordan brukerne har opplevd systemets anvendbarhet [2].

UAM er en ny og lite testet modell som er laget spesielt for å vurdere suksess eller fiasko i utvikling av nye produkter. Denne modellen dekker likevel en rekke områder som er av interesse for å vurdere anvendbarhet ved mobil EPJ hos SSA.

Modellen kan regnes som en mer detaljert beskrivelse av *enkelthet i bruk*. Den måler anvendbarhet i forhold til flere attributter som har blitt definert etter datainnsamling fra erfarne brukere.



Figur 3-2: Hierarkisk oppbygning av anvendbarhet

I dette prosjektet er modellen noe forenklet og tilpasset for å passe bedre til testprosjektet hos SSA. Alle hovedgruppene som er vist i modellen ovenfor er med, men en del underpunkter som ikke regnes relevante for mobil EPJ på SSA, er ikke tatt hensyn til. *Enkelthet ved installeringen av systemet* og *muligheter til å erstatte funksjoner i kontrollpanelet* er to eksempler på disse funksjonene. Derimot er det lagt vekt på å beskrive følgende funksjoner mer detaljert:

Under *lærbarhet* er det et ønske å få frem i hvilken grad brukerne opplevde at brukermanual og menyoppsett var presentert på en måte som gjorde systemet tidkrevende og vanskelig å lære seg. Disse problemstillingene er kun aktuelle for tablet PC og PDA som benyttet seg av InfoPack_Helse. Bærbar PC, som benyttet seg av DIPS, er identisk som det stasjonære systemet og førte dermed ikke til behov for opplæring.

Funksjonalitet er en kategori som setter lys på enkelthet ved å registrere og hente ut data med InfoPack_Helse. Det er ønskelig å få frem i hvilken grad dette er med på å redusere arbeidsmengden og effektivisere de ulike arbeidsprosessene rundt visittgang. For alle arbeidsprosessene legges det vekt på å sammenligne med bærbar PC. Denne ble brukt på samme måte som det stasjonære systemet og har dermed samme funksjonalitet, men siden bærbar PC er mer fleksibel, opplevdes den likevel som mer funksjonell.

Hvor *fleksible* de mobile håndholdte enhetene viste seg å være, måles i hvordan brukerne opplever å ha de med seg under visittgang. PDA, tablet PC og bærbar PC er alle ulike i fysisk størrelse, og må derfor behandles forskjellig under bruk. Om de mobile enhetene er ugunstig å ha med seg rundt, vil det være mulig at de stasjonære enhetene foretrekkes til tross for at informasjonsbehandlingen kan gjøres ferdig ute ved pasienten ved bruk av de bærbare enhetene. *Kompakthet* i Figur 3-2 har blitt uthevet, for å vise at dette ikke har så stor betydning for om enhetene blir tatt med på visittgang. Det benyttes trillebord for tablet og bærbar PC, noe som gjør at dette blir et helt annet system enn for PDA som bæres med i lommen.

Når det gjelder *responsevnen* rundt mobil EPJ, er målsetningen å kartlegge hvorvidt dette gir den ønskelige pasientinformasjonen ute hos pasientene. InfoPack_Helse sammenlignes her med DIPS på arbeidsprosessnivå, for å gi en oversikt over hvilke informasjon hver av disse systemene best kan gi. Det er viktig at de mobile enhetene gir nødvendig informasjon raskt nok til å holde følge med visittens raske tempo.

Videre stilles det krav til *leselighet* av informasjonen som skal vises på PDA, tablet og bærbar PC. Uavhengig av responsevnen til InfoPack_Helse og DIPS er det viktig å være klar over at forskjellige typer informasjon egner seg å bli vist på de ulike enhetene. Eksempelvis var ikke røntgenvisning implementert i InfoPack_Helse, fordi skjermstørrelsen på PDA og tablet PC er for liten.

Systemets krav til *vedlikehold* forsøkes å få frem ved å beskrive hvor stabilt systemene virket i utviklingsprosjektet. Dersom det var større stabilitet i DIPS enn InfoPack_Helse eller motsatt, vil dette ha betydning for hvilke system brukerne får størst tillit til og derfor benytter seg av.

Sammen vil alle disse kategoriene ha betydning for oppfattet brukervennlighet og funksjonalitet i TAM. For å kunne drøfte brukeraksept ut fra testprosjektet hos SSA, er det også nødvendig å kartlegge de andre funksjonene i TAM, som beskrevet i kapittel 3.2.1. De nevnte kategoriene ovenfor vil i TAM ha en direkte påvirkning på brukernes oppfattede nytteverdi.

3.3 Metode for anvendbarhetsstudiet

For å samle inn brukererfaringer fra personellet som var involvert i mobil EPJ hos SSA, ble det sendt ut spørreskjema [v1] til disse. Bruk av spørreskjema er en metode som gir kvantitativ informasjon og som kan sendes ut til mange uten store ressurser [35]. Hensikten med spørreundersøkelsen var å få kartlagt den faktiske bruken av mobil EPJ i tillegg til oppfattet nytteverdi, pasientkontakt og holdninger som beskrevet i hypotesene over. Det ble vurdert å legge ut spørreskjemaet på elektronisk form slik av innsamlingsarbeidet skulle gå lettere. Etter drøfting med prosjektgruppen på SSA, ble det bestemt at dette ville kun gi resultater fra de mest datainteresserte. Ettersom denne evalueringen ønsket å ta for seg alle som arbeider på de to avdelingene, ble skjemaene levert i papirform.

Etter innsamlingsarbeidet ble det utviklet et inntastingsskjema i Microsoft Access. Dette skjemaet var spesialtilpasset spørreundersøkelsen, for at det skulle være enkelt å registrere svarene i en database. Videre ble dataene importert til statistikkprogrammet SPSS, som ble tatt i bruk for å vise de innsamlede dataene grafisk, samt se sammenhenger og krysskorrelere ulike temaer i undersøkelsen.

For å supplere spørreskjemaene ble det tatt initiativ til intervjurunde med fire utvalgte personer fra hver avdeling. Dette var for å gi den kvalitative informasjonen som benyttes for å supplere spørreskjemaene hvor de var mangelfulle, samt å finne andre brukererfaringer. Her ble det utviklet en intervjuguide [v3] for å styre intervjuet slik at ønsket informasjon kom frem.

Informasjonsinnsamlingen har blitt gjort i samarbeid med Kurt Birkeland fra Kube Rådgivning AS. Han hadde i oppdrag fra Medicom AS å evaluere mobil EPJ prosjektet hos SSA [34]. Dette samarbeidet med Kube Rådgiving AS ble gjort for å minske bruken av tid for helsepersonellet som fra før er meget opptatte og vil ha minst mulig bry med slike undersøkelser. Dette samarbeidet ga noen fordeler, men var også en ulempe for dette prosjektet, siden Kurt Birkeland hadde i oppdrag å skrive en ren evalueringsrapport og ville vinkle dette annerledes. Løsningen ble å ha et større antall spørsmål både i spørreskjemaet og i intervjuguiden slik at begge vinklinger fikk god dekning. Det var også nødvendig å inngå kompromiss på enkelte punkter. Når det gjelder evalueringsarbeidet, ble dette gjort uavhengig av Kurt Birkelands evaluering.

3.3.1 Observasjon

Observasjon ble i starten gjennomført for å få innsyn hvordan i systemet er ment å virke ved avdelingene. Denne delen ga bakgrunnskunnskap som ble tatt i bruk under bearbeidelse av spørreskjemaene og etter hvert intervjuskjemaene. Under de første

observasjonene og uttestingene var det stor fokus på å trekke ut hypoteser rundt prosjektet. Observasjonen gikk ut på at det ble tatt en runde på avdelingene hvor basestasjoner er plassert, demonstrasjon i bruken av enhetene, samtaler med personalet om deres erfaringer og utprøvning av enhetene.

3.3.2 Spørreskjemaundersøkelse

Utvikling av spørreskjemaene [v1] ble gjort ut fra prosjektplanen med vekt på rutiner under visittgang [19], TAM [4] og UAM [2]. I tillegg ble det tatt hensyn til erfaringer som kom frem etter innføringen av EPJ ved Amtsykehuset i Roskilde [1]. Etter ønske fra prosjektgruppa på SSA, ble det lagt vekt på å holde et mest mulig enkelt og lettforståelig språk. Tilbakemeldingen fra både leger og sykepleiere viste at det til tross for lik programvare, var viktig å skille på PDA og tablet PC. Det forelå en hypotese om at håndteringen av disse skulle være sterkt ulik hverandre, noe som skulle ha betydning for nytteverdien. I tillegg var det av interesse å se på forskjeller i bruk det er i de ulike avdelingene. Arbeidsprosessene er forskjellige, noe som burde resultere i ulike behov.

Ved utformingen av spørreskjemaet ble spørsmålene gruppert i følgende seks kategorier:

A. Om din stilling
Det var et ønske å få samlet data om responderen og dens stilling. Her ble det spurt etter stilling, arbeidssted og arbeidsordning for at det skulle være mulig å se eventuelle sammenhenger mellom bruk og arbeid.

B. Din bruk av mobil EPJ
Her fokuseres det på bruk, tilgjengelighet og hvordan den tekniske stabiliteten har endret seg i løpet av perioden. I tillegg spørres det om holdninger til prosjektet og hvor i tidsperioden brukeren var mest positiv til bruken av mobil EPJ.

C. Informasjon og opplæring
Kartlegging av hvor god brukerne selv mener informasjonen og opplæringen har vært. Spørsmålene gikk på opplæring på de forskjellige enhetene, hvor mye de har gjort selv for å lære seg bruken, forståelighet av brukermanualen for InfoPack_Helse og kvaliteten på informasjon gitt fra IT-avdelingen. Disse temaene vil kunne krysskorreleres med del B for å få frem årsaker til ikke-bruk av mobil EPJ.

D. Funksjonalitet og brukervennlighet
Her ble det satt opp en del påstander angående funksjonalitet og brukervennlighet på PDA og tablet PC, som responderne sa seg enig eller uenig i. Det ble belyst hvorvidt brukerne foretrekker skjermstørrelsen på PDA eller tablet PC. Videre ble det fokusert på enkelthet og hurtighet i forhold til å registrere og finne frem data med de mobile håndholdte enhetene.

E. Arbeidsprosesser

Arbeidsprosessene ble vurdert i forhold til effektivisering ved bruk av PDA, tablet PC og bærbar PC. Å skille på de forskjellige enhetene ble gjort for å få tilbakemelding om hvilke av disse som egnet seg til de ulike arbeidsprosesser. Deretter fulgte en rekke påstander angående effektiviteten rundt bruken av de mobile enhetene. I denne sammenhengen ble det sortert på tidsforbruk i forhold til visittgang og tilgjengelighet av pasientinformasjon. Det var også ment å få frem hvordan brukerne mente de ulike mobile håndholdte enhetene egnet seg for å ha med under visitt. Det ble også registrert i hvilken grad PDA, tablet PC eller bærbar PC virket forstyrrende i brukernes kommunikasjon med pasientene.

F. Mobil EPJ i fremtiden

For å registrere hvordan brukerne så for seg et velfungerende system, ble det spurt etter forbedringsområder. Det ble sortert på om systemet burde være enklere eller raskere i bruk for PDA eller tablet PC. Brukerne ble i tillegg oppfordret å komme med egne forslag til forbedringer og nye funksjoner ved bruk av mobil EPJ. I tillegg ble det registrert hvor viktig teknisk stabilitet i systemet var for brukerne.

I de fleste påstandene ble det brukt svaralternativene *helt enig*, *litt enig*, *litt uenig* og *helt uenig* i tillegg *vet ikke* for å gi en jevn skalering hvor alle skulle finne et alternativ de følte var riktig. Det viste seg i ettertid at de to alternativene *litt enig* og *litt uenig* var noe uklare, siden en responder kan være både litt enig og litt uenig i en påstand, og at det dermed ble noe tilfeldig hva svaret blir. Dette ble derfor tatt hensyn til ved vurdering av resultatene.

3.3.3 Intervju

Intervjurunden ble iverksatt med mål for å supplere spørreskjemaene på områder hvor disse var mangelfulle. Prosjektgruppen ble engasjert for å velge ut to leger og to sykepleiere ved hver avdeling. Kriteriene for dette utvalget, var at de hadde kjennskap til og benyttet seg av mobil EPJ ved SSA. Det ble påpekt at man ikke skulle foreta utvalget ut fra deres interesse og engasjement for systemet, og at det ikke utelukkende skulle velges såkalte ”superbrukere”.

Det ble i arbeidet utviklet en intervjuguide, vedlegg [v3]. Arbeidet med utviklingen av intervjuguiden startet da resultatene fra spørreskjemaet forelå, slik at intervjurunden kunne utdype de områder hvor det var mangler, i tillegg til å gi annen kvantitativ informasjon.

Intervjuskjemaet ble satt opp ut i fra tre hovedbolker som var interessante for prosjektet:

1. **Intervjuobjektets stilling og rolle**
   Her ble det spurt om hvilke enheter som har vært brukt, motivasjon og om de tror at dette prosjektet har noe for seg generelt. Både hvorfor de selv har benyttet de mobile enhetene, og hvorfor de tror det generelt har vært liten bruk, vil være nyttig supplement til spørreskjemaene.

2. **Intervjuobjektets erfaringer**
   Dette punktet gikk mer ut på hvilke erfaringer intervjuobjektene har dannet seg i løpet av testperioden, og hvilke problemer de har opplevd. Det har vært et ønske å fokusere på hva som har stimulert og hindret bruken av systemet. Det ble også forsøkt å finne større forskjeller både på de mobile enhetene og programvaren.

3. **Intervjuobjektets syn på fremtidsmuligheter**
   Her ble det kartlagt hvilke krav som ble satt til fremtidige, lignende forsøk og forslag til forbedringer, nye funksjoner eller annet som kunne være med å løfte produktet.

På spørsmål om funksjonalitet, ga intervjurundene detaljert tilbakemelding. Det var dermed lettere å forstå hvordan brukerne på de ulike avdelingene opplevde å ha de forskjellige enhetene med seg. Det var også ønskelig å få belyst flere konkrete årsaker til at skjermstørrelsen synes å være for liten.

Betydningen ved å bruke tastatur eller berøringsskjerm ble ikke belyst tilfredsstillende under spørreskjemaene, noe som førte til at dette fikk plass under intervjuene. Om manøvrering i menysystem, var det viktig med kvalitativ informasjon. Det ble valgt å ta dette opp på intervjurunden, slik at dette kunne diskuteres med brukerne selv. Her var det også ønskelig å få en sammenligning med DIPS, siden en overfladisk gjennomgang av spørreskjemaene antydet at brukerne ønsket et grensesnitt mest mulig likt DIPS.

3.4 Resultater fra spørreskjemaer

Under gjengis de mest interesante resultatene fra spørreundersøkelsen. Besvarelsen i sin helhet er lagt med som vedlegg [v2].

3.4.1 Svarprosent

Det ble delt ut til sammen 81 spørreskjemaer hvorav 39 ble utfylt og returnert. Ved beregning av svarprosenten er det ikke tatt hensyn til eventuelt sykefravær, permisjoner eller lignende. Svarprosenten delt på de to avdelingene var som følger:

Tabell 3-1: Svarprosent

	UC	3D
Utdelte skjemaer	44	37
Besvarte skjemaer	20	19
Svarprosent	45 %	51 %

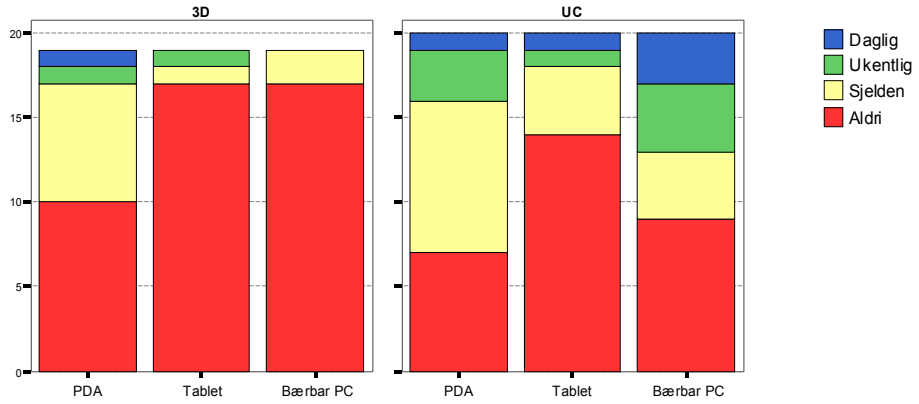
Avdelingslederne fortalte at henholdsvis 8 og 11 personer ved 3D og UC som fikk utdelt spørreskjemaer, ikke hadde noen kjennskap til mobil EPJ hos SSA. Dette var på grunn av permisjon eller sykemelding. Disse burde i utgangspunktet ikke fått

utdelt skjemaer, som fører til en mer riktig svarprosent på 60 % ved UC og 65 % ved 3D.

Det registreres at ingen leger fra UC har svart på spørreskjemaene. Derimot har kommentarer fra disse blitt tatt i betraktning fra intervjuene, se kapittel 3.5.

3.4.2 Bruk

Følgende graf skisserer bruken av mobil EPJ i testperioden. 14 personer svarte at de aldri hadde brukt noen av hjelpemidlene. Av disse var det 5 personer som hadde kvelds- eller nattstilling, der det ikke ble gått visitt. 25 personer brukte minst ett av hjelpemidlene, 15 på UC og 10 på 3D. Av de 25 brukerne brukte 22 PDA, 8 brukte tablet PC og 13 brukte bærbar PC. Tallene innebærer altså at flere benyttet mer enn ett hjelpemiddel.



Figur 3-3: Bruken av PDA, tablet og bærbar PC på avdelingene 3D og UC

Samlet sett var det kun 27 % av brukerne av PDA som benyttet enheten daglig eller ukentlig. Når det gjelder bærbar PC, er den tilsvarende beregningen 64 %.

Som Figur 3-3 viser, har ikke bærbar PC vært tilgjengelig på UC.

3.4.3 Informasjon og opplæring

I Tabell 3-2 kartlegges brukernes oppfatninger angående opplæring og informasjon gitt fra ledelsen og IT avdelingen. Det kommer tydelig frem av svarene at de aller fleste kjente til at mobil EPJ var i bruk i avdelingen. Dette stemmer godt med påstander fra prosjektgruppen og IT-avdelingen på SSA, som sa at alle ansatte på de to avdelingene fikk tilbud om opplæring. Derimot viste det seg at leger og sykepleiere stort sett mente at opplæringen på PDA og tablet PC var dårlig. Til tross for den dårlige opplæringen, opplevde flesteparten at brukermanualen var enkel å forstå. Det viste seg også at brukerne selv mente de hadde brukt lite tid på å lære seg å anvende de forskjellige enhetene.

Tabell 3-2: Informasjon og opplæring rundt PDA, tablet PC og InfoPack_Helse

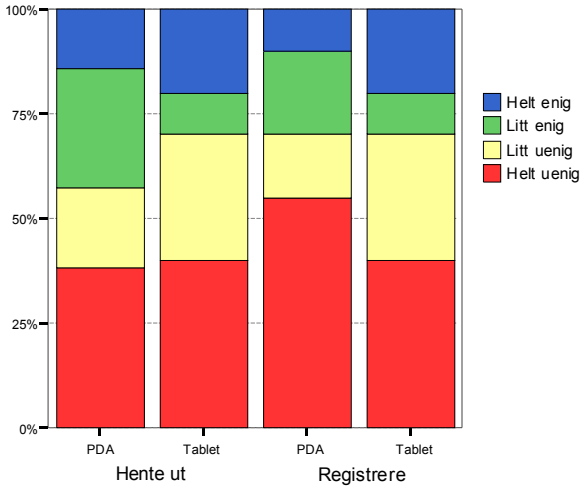
Påstand	Vet ikke	Helt uenig	Litt uenig	Litt enig	Helt enig
Du kjenner godt til at mobil EPJ er i bruk i avdelingen	6	3	0	2	28
Du har fått god opplæring i bruk av PDA	4	16	3	11	5
Du har fått god opplæring i bruk av tablet PC	6	23	4	5	1
Du har brukt mye tid på å lære deg PDA på egenhånd	3	14	5	11	6
Du har brukt mye tid på å lære deg tablet PC på egenhånd	5	21	7	5	1
Brukermanualen for InfoPack_Helse er oversiktlig og enkel å forstå	21	3	4	9	2
Du må få bedre informasjon om hva InfoPack_Helse skal brukes til	11	3	1	11	13
Du har fått større vilje og interesse for bruk av data i løpet av testperioden for mobil EPJ	7	9	10	4	9
Mobil EPJ har gitt deg bedre IT-kompetanse	8	20	3	6	4

Det bør legges merke til at så mange som 61 % av de spurte, ønsker mer informasjon om hva InfoPack_Helse skulle benyttes til.

3.4.4 Brukervennlighet og funksjonalitet

Registrere og hente ut pasientdata ved bruk av InfoPack_Helse

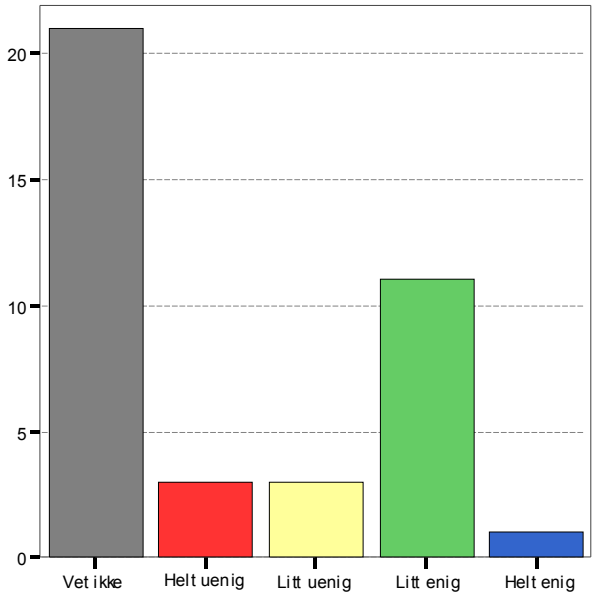
På påstand om at det var enkelt å hente ut og registrere data på henholdsvis PDA og tablet PC, hadde brukerne erfaringer som vist i Figur 3-4. Her ble bærbar PC utelatt, siden denne kjører DIPS programvare. Av disse dataene virket det som om det var omtrent like enkelt å registrere som å hente ut data ved bruk av de to enhetene. Det bør noteres at det var 50 % ved PDA og 75 % ved tablet PC som svarte *vet ikke*. Disse hadde ingen formening om registreringsarbeidet, og er derfor ikke av interesse for undersøkelsen.



Figur 3-4: Enkelthet ved å registrere og hente ut data med InfoPack_Helse

Begrepsforvirring

Følgende fordeling var tilbakemeldingen på påstanden om at InfoPack_Helse inneholdt vanskelige eller misvisende begreper. Av de som brukte systemet, og derfor hadde en formening om spørsmålet, viste det seg å være en stor spredning i svarene.



Figur 3-5: Opplevd begrepsforvirring rundt InfoPack_Helse

Skjermstørrelse

Tabellen under viser hvilke meninger legene og sykepleierne hadde i forhold til om skjermstørrelsen er stor nok på PDA og tablet PC.

Tabell 3-3: Skjermstørrelse ved PDA og tablet PC

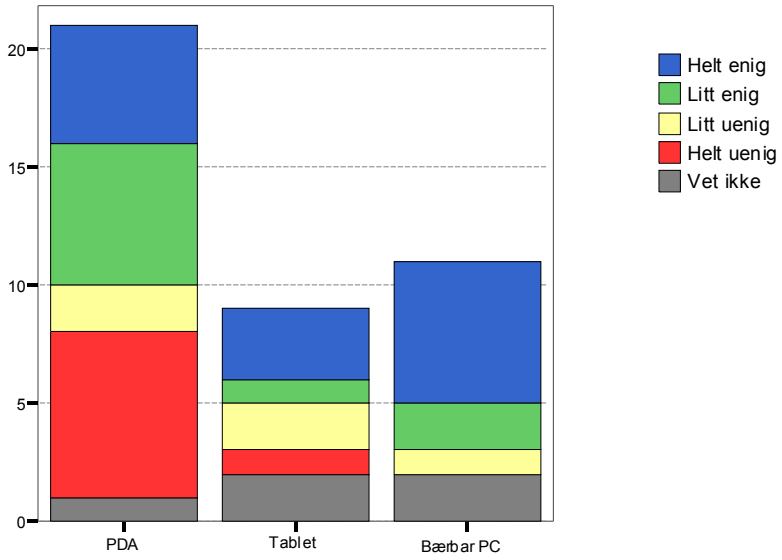
Av de som har benyttet henholdsvis PDA og tablet PC					
	Helt enig	**Litt enig**	**Litt uenig**	**Helt uenig**	**Vet ikke**
Skjermen på PDA er stor nok	14 %	23 %	14 %	35 %	14 %
Skjermen på tablet PC er stor nok	38 %	50 %	0 %	12 %	0 %

Av de som ikke har benyttet henholdsvis PDA og tablet PC					
	Helt enig	**Litt enig**	**Litt uenig**	**Helt uenig**	**Vet ikke**
Skjermen på PDA er stor nok	6 %	6 %	6 %	6 %	76 %
Skjermen på tablet PC er stor nok	0 %	0 %	3 %	3 %	94 %

Tabellen viser stor spredning i oppfatningen om skjermstørrelsen var stor nok på PDA. Når det gjelder tablet PC, var det en overvekt blant brukerne som syntes at skjermstørrelsen var stor nok, hele 88 % av de spurte var enig i dette. Av de som ikke tok de mobile håndholdte enhetene i bruk, viste det seg at de aller fleste ikke hadde noen oppfatning til spørsmålet. Dette avkrefter at skjermen var en klar grunn til at disse personene ikke har tatt i bruk verken PDA eller tablet PC.

Fleksibilitet

Responsen på påstand om at de forskjellige enhetene var fleksible å ha med seg på visitt, vises i figuren under. Bærbar PC skilte seg ut som den best egnede, PDA følger like etter, mens tablet PC ikke er så godt egnet.

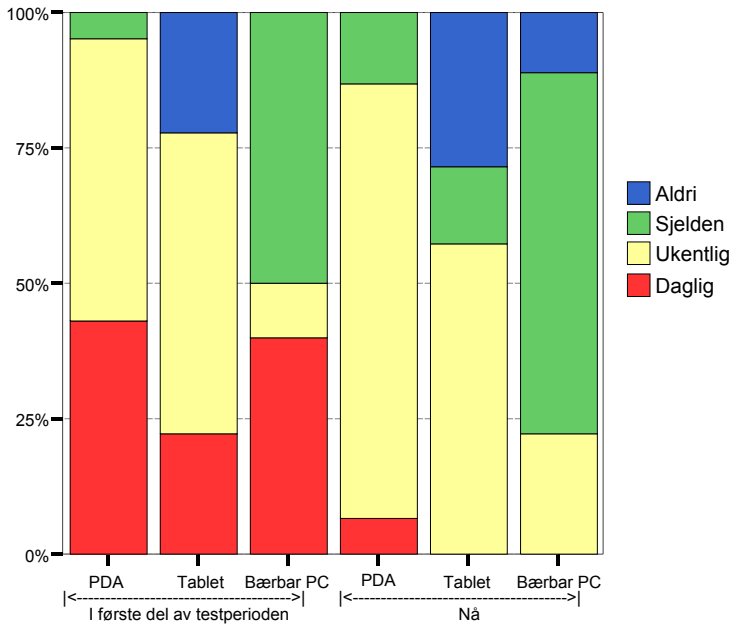


Figur 3-6: Hvor fleksible PDA, tablet PC og bærbar PC er til å ha med på visitt

Kun de som benyttet seg av de enkelte av enhetene, er med i denne oversikten. Dette for at uttalelsene skal bygge på erfaringer, og ikke antagelse, på hvor godt egnet enhetene var å ha med seg under visittgang.

Teknisk kvalitet

Under er en oversikt over hvor ofte brukerne opplevde at de mobile enhetene ikke fungerte. 69,7 % svarte *vet ikke*, et alternativ som er fjernet, siden disse ikke hadde kjennskap til den tekniske stabiliteten. Bærbar PC viste seg som den mest stabile av enhetene.

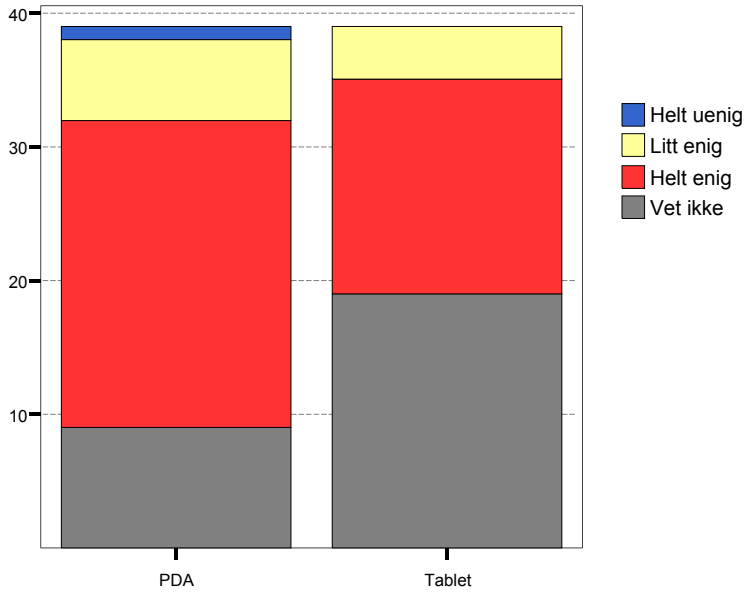


Figur 3-7: Oppfattet teknisk stabilitet for PDA, tablet PC og bærbar PC

Her er det viktig å merke seg at det var mye tekniske problemer med systemet i begynnelsen av testperioden, også ifølge IT-avdelingen. Disse problemene bedret seg etter ca. 2 måneders tid. Da hadde mange brukere allerede gitt opp å bruke systemet og opplevde ikke at systemet etter hvert ble mer stabilt.

Registrere og hente ut data

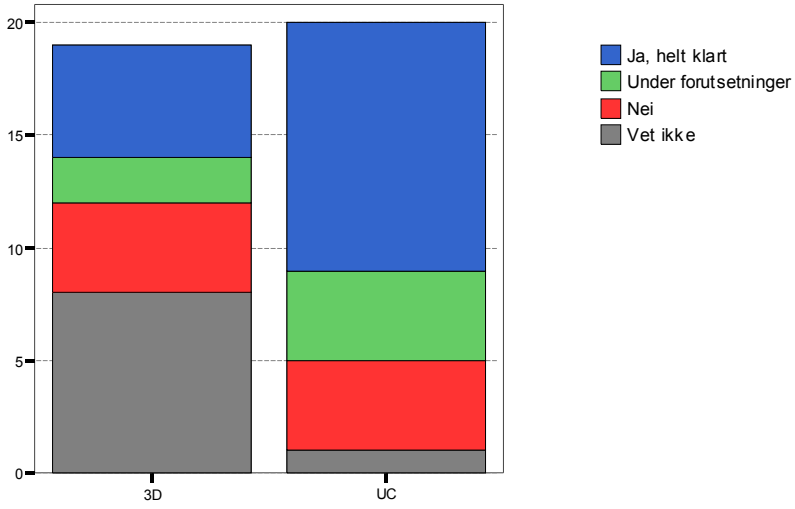
Under vises svarene på påstanden om at PDA og tablet PC må være enklere eller raskere å bruke. Her ligger det en utfordring for systemutviklerne, ettersom så godt som alle mente at InfoPack_Helse må bli raskere og enklere å bruke.



Figur 3-8: Om PDA og tablet PC må være enklere eller raskere å bruke

3.4.5 Nytteverdi og behov

Brukernes svar på påstanden om at det fortsatt er behov for mobil EPJ, er gjengitt i Figur 3-9. Resultatene viser at brukerne mente at det er behov for mobil EPJ ved avdelingen UC. På 3D var det en stor usikkerhet på dette området.



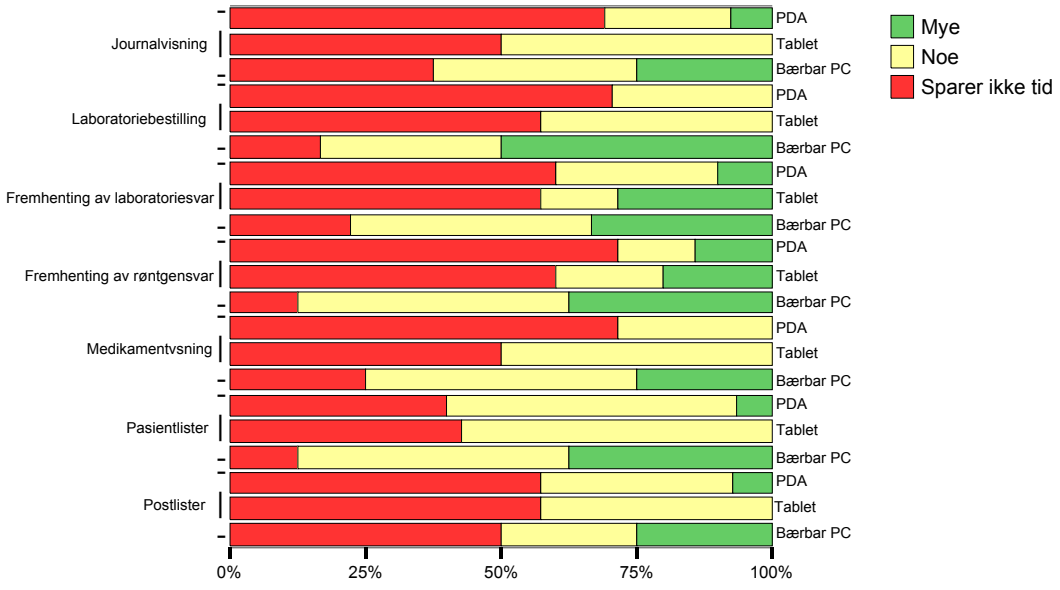
Figur 3-9: Oppfattet behov for mobil EPJ ved avdelingene 3D og UC

Det viste seg å være liten forskjell mellom hjelpemidlene, men ”troen på” bærbar PC og PDA var noe større enn på tablet PC. Det er seks personer som mente det finnes behov under følgende forutsetninger:

- At systemet jobber like raskt mobilt som på det stasjonære systemet.
- At systemet er "oppe" til enhver tid.
- Kun behov på dagtid, ikke om kvelden. Dette er fordi det vanligvis ikke gjennomføres visittrunder på kvelds- og nattevakter.
- På store sengeposter, med stor pasientutskifting og pasienter med enkle problemstillinger. På post (UC) med flere langtidsliggere og god kontinuitet mellom pasienter og lege, er det mindre behov.
- Når det er kø ved datamaskinene, og vi sitter og skriver rapport. På noen områder ved visittgang. Liten gevinst i henhold til kostnadene.
- Kan være OK i forhold til å kunne svare på spørsmål fra pasienten under visitten.
- For å minske tid til previsitt, lettere tilgang til informasjon på pasientrommene under visitt.

Tidsbesparelse ved arbeidsprosessene

Når det gjelder tidsbesparelse ved bruk av mobil EPJ til de ulike arbeidsprosessene, ble svarene som vist i Figur 3-10. Totalt 81,5 % av alle svarene viste at de ikke hadde brukt noen av de mobile håndholdte enhetene til arbeidsprosessene. Ettersom disse dataene ikke kan si noe som helst angående tidsbesparelse, er disse dataene fjernet. Det betyr i praksis at det er kun svarene fra de som har brukt den aktuelle enheten som er tatt med.



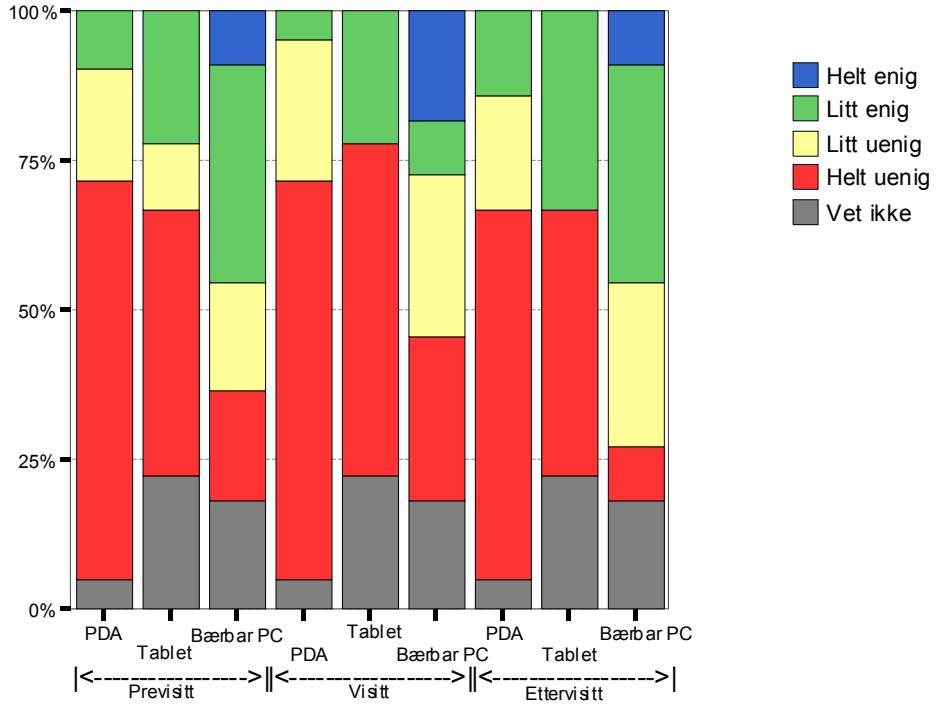
Figur 3-10: Tidsbesparelse ved arbeidsprosesser sortert på PDA, tablet PC og bærbar PC

Om man gir *mye* verdien 1, *noe* verdien 2 og *sparer ikke tid* verdien 3, vil gjennomsnittet av alle arbeidsprosessene ligge på 2,37. Det vil si at alle brukerne samlet mener noe midt imellom *noe* og *sparer ikke tid* på spørsmålet om tidsbesparelse av arbeidsprosessene ved bruk av mobil EPJ.

En viktig årsak til at bærbar PC opplevdes mer tidsbesparende enn de to andre enhetene, er at bærbar PC kjører DIPS programvare.

Tidsbesparelse under visittgang

Brukernes respons på påstand om at PDA, tablet PC og bærbar PC opplevdes som tidsbesparende i forhold til previsitt, visitt eller ettervisitt. En typisk oppfatning her er at bærbar PC var mest tidsbesparende, mens henholdsvis tablet PC og PDA følger som mindre effektive til visittgang.

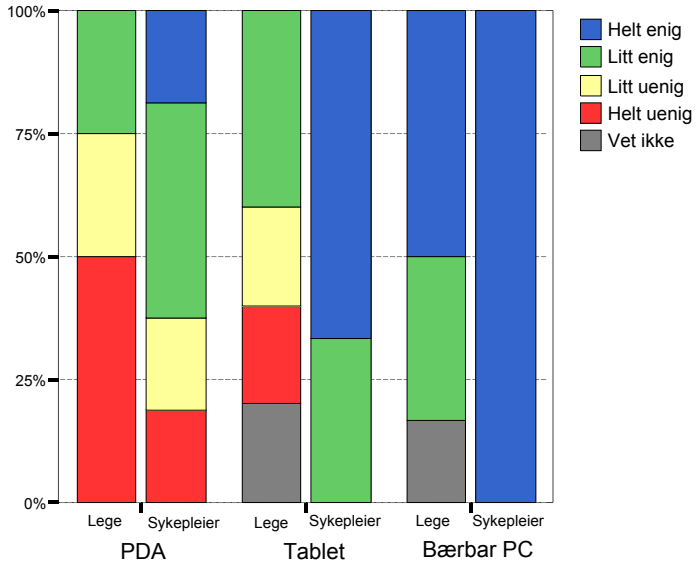


Figur 3-11: Tidsbesparelse ved previsitt, visitt og ettervisitt ved bruk av de mobile enhetene

Også her er det viktig å legge merke til at det ble kjørt DIPS på de bærbare PC-ene, og at dette er et program som ble implementert for to år siden. Brukerne er derfor godt kjent med dette programmet, noe som gjør at arbeidet går fortere og lettere enn med InfoPack_Helse.

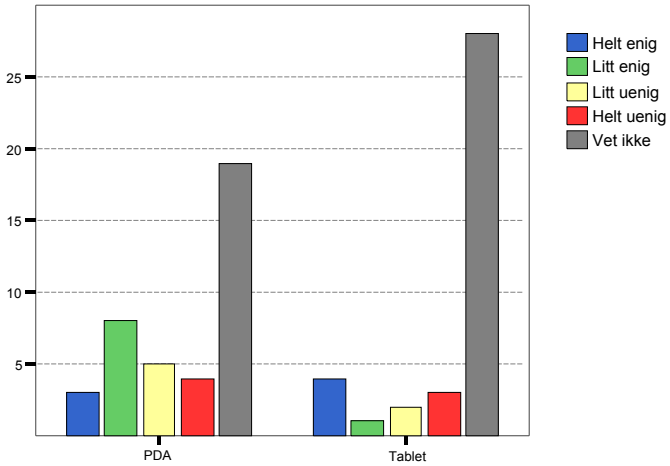
Informasjonstilgjengelighet

Brukernes respons på påstand om at pasientinformasjonen ble mer tilgjengelig ved bruk av mobil EPJ under visitten vises i Figur 3-12. Her vises kun svarene fra leger og sykepleiere, ettersom alt annet personale svarte kun *vet ikke*. Det bør legges merke til at PDA kom dårligst ut, tablet PC ble oppfattet noe bedre, mens flest av brukerne mente at pasientinformasjonen ble mer tilgjengelig ved bruk av bærbar PC.



Figur 3-12: Mobil EPJ fører til at pasientinformasjonen blir mer tilgjengelig under visitten

Her vises responsen på påstand om at InfoPack_Helse ga en den pasientinformasjonen en trengte i det daglige arbeidet. Her er ikke bærbar PC tatt med, siden DIPS ble kjørt på disse enhetene. Av de som hadde en formening om dette spørsmålet, viste det seg at bare halvparten av brukerne synes InfoPack_Helse ga nødvendig pasientinformasjon.

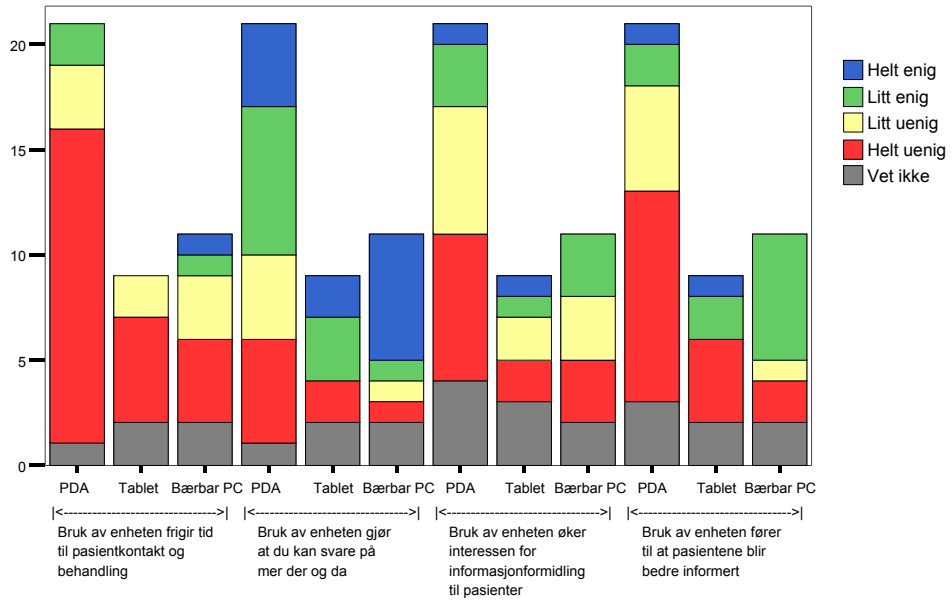


Figur 3-13: InfoPack_Helse gir nødvendig pasientinformasjon

Pasientkontakt og informasjon til pasientene

I Figur 3-14 vises legers og sykepleieres opplevelser i forhold til kontakt og informasjon med pasientene. Det bør her legges merke til at ingen av brukerne sa seg enig i at tablet PC frigjorde tid til pasientkontakt og behandling. Resultatet er litt mer positivt for PDA og bærbar PC, hvor et par stykker sa seg enig i påstanden. Nært opp mot halvparten av de spurte svarte at bruk av mobil EPJ førte til at man kunne svare pasientene på mer der og da. Her opplevdes PDA og tablet PC så godt som likeverdige, mens brukerne var noe mer positive til bærbar PC.

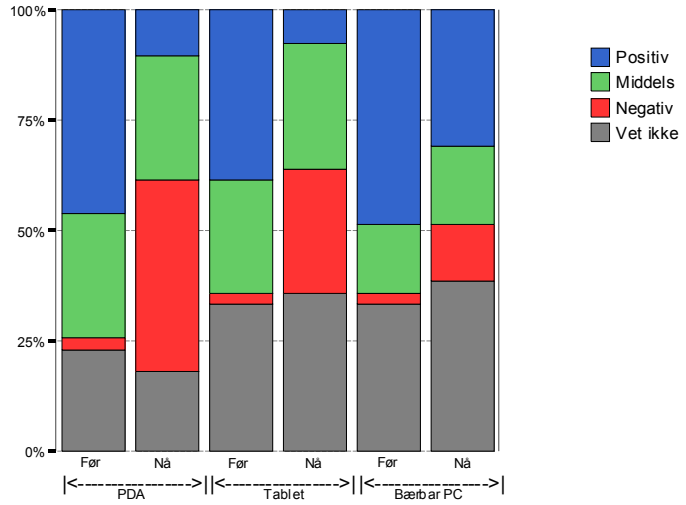
Derimot er det kun 20-25 % av brukerne som svarte at interessen for informasjonsformidling til pasientene økte, til tross for at så mange svarte at informasjonen ble mer tilgjengelig. Slik systemet fungerte, var halvparten av de spurte enig i at bærbar PC førte til at pasientene ble bedre informert, mens tallene er mindre positive med PDA og tablet PC. Generelt viser figuren at mobil EPJ hadde en negativ påvirkning i forhold til pasientkontakt og informasjon til pasientene.



Figur 3-14: Kontakt og informasjon til pasientene under bruk av PDA, tablet PC og bærbar PC

3.4.6 Endring av holdninger til mobil EPJ i løpet av testperioden

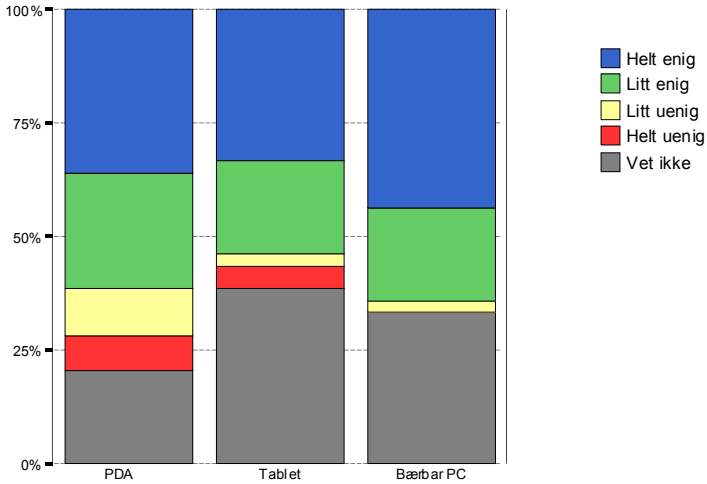
Spørsmålet om hvilke holdninger brukerne hadde i forhold til mobil EPJ ble besvart slik Figur 3-15 viser. Denne fremstillingen viser tydelig at holdningene endret seg i negativ retning, spesielt for PDA og tablet PC. For bærbar PC viser det seg at holdningene var mest positive og endret seg minst i negativ retning. Figuren viser også at holdningene til de forskjellige enhetene er relativt like, slik at utgangspunktet er det samme.



Figur 3-15: Endring av holdninger til PDA, tablet PC og bærbar PC i løpet av testperioden

3.4.7 Utviklingsmuligheter

Under vises hvorvidt brukerne tror mobil EPJ har noen hensikt, dersom systemet fungerer slik det er ment. Dette gir et klart signal om at leger og sykepleiere stiller seg positive til mobil EPJ. Av brukerne som har en formening om spørsmålet er kun 5 % negative ved bruk av PDA, 2 % negative ved bruk av tablet PC og 1 % negative ved bruk av bærbar PC.



Figur 3-16: Om mobil EPJ har noen hensikt dersom det fungerer etter hensikten

Etter å ha gjort seg opp en formening hvordan mobil EPJ har fungert under testperioden, ga brukerne følgende forslag til forbedringer av systemet:

- PDA og tablet PC må kunne kjøre DIPS
- Strekkode skanning
- Enklere system
- Systemet må bli raskere
- PDA og tablet PC bør ha større og mer oversiktlige skjermer.
- Hurtigfunksjon for å finne pasienter raskere.

3.5 Resultater fra intervjuer

Intervjurunden på avdelingene 3D og UC av både leger og sykepleiere belyste brukererfaringer som er gjengitt under. Besvarelsene kan i sin helhet leses i vedlegg [v4].

3.5.1 Årsaker til liten bruk

Alle de spurte hadde tekniske problemer som hovedårsak til liten bruk av mobil EPJ. Det legges til at stabiliteten var dårligere på PDA og tablet PC som har benyttet seg av InfoPack_Helse, enn på bærbar PC som bruker DIPS. Flere leger og sykepleiere la vekt på at de ikke er interessert i mobil EPJ for teknologien sin skyld, men at det må ha nytte for dem personlig for at de skal bli tatt i bruk. Systemet må gjøre at arbeidet blir mer effektivt enn de stasjonære PC-ene. Følgende punkter gikk igjen:

- Problemer med å få logget seg inn.
- Det tar for lang tid å få hjelp fra IT-avdelingen ved problemer.
- Vanskelig å gjøre unna registreringsarbeidet under visittens høye tempo, spesielt med PDA og tablet PC som benytter seg av det lite innarbeidede InfoPack_Helse.
- For dårlig tid på avdelingene til å teste ut nye applikasjoner.
- Vanskelig å finne fram i menysystemet
- For treg respons

Om man oppsummerer for PDA, ble det ofte nevnt for liten skjerm, dårlig oppetid, ikke god nok programvare, samt dårlig flyt i den logiske oppbyggingen. Bortsett fra skjermstørrelsen, var utsagnene de samme i forhold til tablet PC. Det kom frem at PDA med den lille skjermstørrelsen muligens kunne passet for sykepleiere. For leger, som i motsetning er avhengig av å behandle større mengder informasjon, var ikke PDA noe godt alternativ.

Spesielt legene mente det beste er å forberede seg til møte med pasientene før visittgang, slik at de husker all pasientinformasjonen under visittgang. Det eksisterte derfor ikke et ønske om å ha med seg datautstyr rundt. Likevel syntes samtlige at det var greit å finne frem ønskelige data når noen spurte. Man slapp da å gå til en stasjonær maskin og komme tilbake senere.

3.5.2 Hvordan det har vært å sette seg inn i InfoPack_Helse

Uttestingen av InfoPack_Helse førte til at leger og sykepleiere har fikk nok et elektronisk informasjonssystem å sette seg inn i, ved siden av DIPS. Flere la vekt på at det var kompliserende å ha to forskjellige systemer å forholde seg til. Følgende punkter gikk igjen når det gjaldt brukererfaringer av InfoPack_Helse:

- Siden det er så stor forskjell mellom InfoPack_Helse, føles det for mange tungt å ha to forskjellige systemer.
- Programvaren er for lite tilpasset arbeidsprosessene slik at programmet føles ulogisk. Programvaren bør tilpasses arbeidsprosessene, ikke omvendt

Til tross for disse punktene, mente de fleste at InfoPack_Helse ikke var vanskelig å sette seg inn i og forstå. Brukerne etterlyste en bedre dialog med systemutviklerne, slik at programvaren blir bedre tilrettelagt for arbeidsprosessene. Flere brukere mente at programmererne burde være med rundt da arbeidet gjøres, og tilpasse brukergrensesnittet etter disse behovene.

3.5.3 Opplæring og brukerstøtte fra IT-avdelingen

Fra brukerne var det stor variasjon i oppfatningen om hvor effektiv brukerstøtten var. Denne spredningen gjengis i sitatene under:

- ”IT-avdelingen var positiv og motiverende, men det tar lang tid før det kommer hjelp, opptil et par dager.”
- ”Brukerstøtten var ikke spesielt bra, måtte ringe og mase når noe gikk galt.”
- ”Oppfølgingen må bli bedre dersom et lignende system skal settes i drift.”

Andre hadde en annen oppfatning:

- ”Når vi ringte, og det gjorde vi ofte, fikk vi veldig fort assistanse.”

Ut i prosjektet var det enkelte som ikke lenger ville bruke tid på å få de mobile enhetene til å fungere, og la de heller vekk.

Når det gjelder opplæringen, ble brukerne fortalt hvordan InfoPack_Helse var ment å fungere og alle funksjonene som skulle komme. Dette gjaldt også applikasjoner som ikke var ferdig implementert under testprosjektet hos SSA. Dette viste seg å bidra til frustrasjon, da flere var motivert for å gå løs på oppgaver som ikke fungerte da de skulle prøve det ut selv.

Brukerne nevnte også at det ved implementering av nye datasystemer burde settes av mer opplæringstid i mindre grupper enn hva som var tilfellet på SSA.

3.5.4 Hva som har stimulert til bruk av mobil EPJ

Etter hvert som man skal utvikle informasjonssystemene i et sykehusmiljø til å bli papirløst, øker behovet for mobil datatilgang. Dette behovet var alle de spurte klar over, og hadde som bakgrunn for motivasjon for å benytte seg av dette.

De vanligste faktorene som har stimulert til bruk er:

- Ønske om lettere tilgang til data
- Håp om å spare tid til previsitt og postvisitt
- Motivasjon fra ledelse
- Bedre informasjon til brukerne
- At systemet er nytt og at det er et testforsøk hvor avdelingen er en foregangsavdeling

Det kom fram at sykepleierne som gikk visitt med leger som var motivert for mobil EPJ, fikk økt motivasjonen av disse. På en annen side fikk flere sykepleiere motivasjon redusert av leger som ikke ønsket å ta mobil EPJ i bruk.

3.5.5 Hva har hindret bruken av mobil EPJ

Mange opplevde å bruke mye tid på å finne frem informasjon ute hos pasientene, spesielt med PDA og tablet PC som de ikke var så godt kjent med. Dette opplevdes som frustrerende for brukerne, og kommentaren som gikk igjen var:

- ”Datautstyr ute hos pasienten stjeler oppmerksomhet fra pasienten.”

Ettersom hele innføringen av mobil EPJ var et pålegg fra ledelsen og få ble forespurt om hva de ønsket seg av et slikt system, følte flere av brukerne seg overkjørt av IT-avdelingen. Det kom ofte frem i denne sammenhengen, at InfoPack_Helse må tilpasses bedre til arbeidsprosessene og ikke motsatt.

Det er vanlig at leger ikke har tid til å være med på previsitt. Med innføringen av mobil EPJ skulle det være mulig å gjøre unna dette arbeidet sammen med lege under visitten. PDA og tablet PC med sine svakheter gjorde det umulig å henge med i det raske tempoet, noe som gjorde disse uegnet. Bærbar PC med full DIPS funksjonalitet og tastatur opplevdes å være mer egnet. Det legges til i denne sammenheng, at det er en del opplysninger som utveksles mellom lege og sykepleier under visitt, som ikke passer å snakke om på foran pasientene.

3.5.6 InfoPack_Helse kontra DIPS

PDA med InfoPack_Helse viste seg å være egnet til andre oppgaver enn DIPS, og at disse ikke er konkurrenter i et mobilt system. Begge kan eksistere, men med forskjellige funksjoner implementert. På en annen side ble det kommentert at det er uheldig å ha flere enheter å forholde seg til.

- Tastatur fungerer bedre og er kjappere enn berøringsskjerm
- DIPS er enklere å bruke
- InfoPack_Helse er ulogisk oppbygd i forhold til DIPS
- Det er lett å bli forvirret når det er benyttet forskjellige begreper i InfoPack_Helse i forhold til DIPS

InfoPack_Helse benytter seg mye av lister, for eksempel over pasienter, prøver og så videre. Disse listene viste seg å være tidkrevende. Dersom en pasient hadde tatt mange blodprøver, tok det lang tid å finne frem den siste.

3.5.7 Sammenligning av PDA, tablet PC og bærbar PC

Kommentarer som gikk igjen er at de fleste leger og sykepleiere velger å benytte seg av datasystemer de er kjent med. I og med at programvaren DIPS hadde vært i bruk over lengre tid, førte dette til at PDA og tablet PC ofte ble liggende igjen, til fordel for den bærbare PC-en.

Alle de spurte mente at PDA hadde for liten skjerm til å behandle pasientjournaler og andre dokumenter hvor det er mye tekst. Brukernes synspunkter på forskjellen mellom PDA og tablet PC var følgende:

- PDA har for liten skjerm
- Tablet PC er stor nok, men den er tung å ha med seg på visitten

I utviklingsprosjektet var den medisinske kurven papirbasert. Da måtte legene ha med seg både kurvepermen, enheten og andre lapper. Siden dette er for mye å bære, måtte de ha med seg en tralle, og når tralla først skulle med, synes brukerne at det var bedre å ha med seg en bærbar PC på grunn av større skjerm, full DIPS tilgang og tastatur.

3.5.8 Teknisk kvalitet

Brukerne opplevde at IT-avdelingen mente de overdrev problemene som var med de mobile enhetene. En rekke av feilene som brukerne mente var av teknisk karakter, mente IT-avdelingen bestemt var forårsaket av brukerfeil. Det var en del startproblemer med InfoPack_Helse sin server, som har forårsaket en del nedetid for PDA og tablet PC. Da dette ble bedret, hadde flere leger og sykepleiere sluttet å bruke enhetene på grunn av problemene.

Alle de spurte var enige i at mobil EPJ ikke vil bli tatt i bruk og akseptert før den tekniske stabiliteten blir betydelig bedre enn hva som var tilfellet under utviklingsprosjektet.

- ”Datasystemet må fungere like sikkert som om det er summetone i telefonen.”

3.5.9 Forslag til nye bruksområder for InfoPack_Helse

Følgende forslag til nye bruksområder for enhetene og InfoPack_Helse ble nevnt i intervjuene:

- Føre inn temperaturer
- Kvittere for medisiner
- Skanne inn pasienter for raskt å få frem pasientinformasjon
- Erstatte løse lapper med diktafontjeneste og elektroniske beskjeder som sendes direkte til kontoret

3.6 Drøfting

3.6.1 Hypoteser

Mobil EPJ ble lite i bruk i løpet av testperioden

Enhetene var generelt i liten bruk, spesielt ved avdeling 3D hvor ikke engang bærbar PC var tilgjengelig. Figur 3-3 viser at PDA ble benyttet av flest, på både på 3D og UC. Derimot viste det seg at disse brukerne ikke anvendte PDA like flittig som brukerne av tablet PC og bærbar PC. Av de som har benyttet seg av bærbar PC, benyttet 64 % enheten ukentlig eller daglig. For PDA var tilfellet 27 %. Dette sier noe om at brukerne av PDA raskt ga opp bruken, mens de som prøvde bærbar PC, fortsatte å bruke den. Siden enhetene var tenkt brukt til visitten, og denne kun gjennomføres på dagtid, ble det mindre bruk på kveld- og natteskiftene. De som jobber fast som nattevakt, vil derfor ha mindre bruk for mobil EPJ.

Tekniske årsaker var en viktig årsak til at PDA, tablet PC og bærbar PC ikke ble tatt mer i bruk

Det vises av Figur 3-7 at det mobile systemet som benyttet seg av DIPS, var under testperioden noe mer stabilt enn systemet som benyttet seg av Medicom sin InfoPack_Helse server.

Den tekniske kvaliteten for InfoPack_Helse endret seg, og ble mer stabil mot slutten av testperioden. Den tilsynelatende bedre driftssikkerheten i slutten av perioden, må i noen grad sees i sammenheng med at bruken avtok. Det legges her til grunn at de mest interesserte og datakyndige brukerne var de som benyttet de mobile håndholdte enhetene gjennom hele testperioden.

Tilbakemelding fra IT-avdelingen sa at mange brukere ga de mobile håndholdte enhetene eller nettverket skylden når noe gikk galt, selv om det var personlig feilbruk som var den reelle årsaken.

Opplæring og support i forhold til InfoPack_Helse har vært mangelfull i utviklingsprosjektet

Resultatene fra spørreskjemaet, Figur 3-15, viser at det var stor interesse for å sette seg inn i mobil EPJ ved prosjektstart. 77 % av brukerne som besvarte spørreskjemaene, mente at de kjente godt til at mobil EPJ ble testet ut ved avdelingene. Når allikevel det store flertallet av brukerne (61 %) mente de burde hatt bedre informasjon om hva InfoPack_Helse kunne brukes til, indikerer dette at informasjonen ikke ble gitt på en tilfredsstillende måte. Dette viser at mange brukere mener de ble for dårlig informert av IT-avdelingen i løpet av testperioden.

En del funksjoner i InfoPack_Helse, som fra prosjektplanen [19] var ment å fungere, fungerte ikke i det hele tatt under testperioden. En klar årsak til at så mange brukere oppfattet opplæringen for dårlig, forklarte de i intervjuene med at de ble fortalt hvordan systemet var ment å fungere, men da de skulle benytte systemet på egenhånd, fungerte det ikke slik. Dette kunne vært unngått om produktet hadde vært

mer modent før det ble satt ut i prøvedrift. IT-avdelingen burde også ha informert om dette, slik at brukernes forventninger ikke var så store.

Prosjektledelsen opplevde mye fravær når opplæringen ble gitt. Fra intervjuene viste dette seg å komme av at kursene har foregått på tidspunkt hvor de ansatte har hatt vakter. Opplæringen ble også vanskeliggjort av de tekniske problemene i nettet den første delen av prosjektperioden.

54 % svarte *vet ikke* på påstanden om at brukermanualen for InfoPack_Helse er oversiktlig og enkel å forstå, fra Figur 3-5. Dette kan bety at mange ikke brukte brukermanualen noe særlig eller at denne var lite tilgjengelig. Av de som har gjort seg opp med en formening, var de fleste litt enige eller helt enige i denne påstanden. Det virker derfor som om de som brukte tid på å lese brukermanualen synes den er lettforståelig.

InfoPack_Helse gir ikke nødvendig informasjon under visittgang

Figur 3-13 viser hva responderne svarte på påstand om at InfoPack_Helse ga nødvendig pasientinformasjon. Nesten halvparten av de som benyttet systemet, sa seg helt eller litt uenig i at InfoPack_Helse ga nødvendig informasjon. For at innføringen skulle kunne betegnes som vellykket, burde dette resultatet vært mer positivt. Et av hovedmålene med hele prosjektet var nemlig å gi brukerne nødvendig informasjon, så dette var en kritisk suksessfaktor. Hvis dette kravet ikke var tilfredsstilt, ville aldri InfoPack_Helse bli tatt i bruk. På grunn av liten skjermstørrelse på PDA og menyoppsettet i InfoPack_Helse, burde denne enheten bli benyttet til andre arbeidsprosesser enn bærbar PC med DIPS. PDA viste seg å være best egnet for behandling av mindre dokumenter og enkle registreringer.

Kort sagt kan en si at InfoPack_Helse opplevdes verken enkelt eller raskt
Dette samsvarer godt med inntrykket fra intervjuene der det var enighet i at det var tungvint og tidkrevende å navigere i menysystemene ved bruk av ukjent menyoppsett og berøringsskjerm. Figur 3-8 viser at både PDA og tablet PC må bli enklere og raskere å bruke slik at enhetene skal fungere tilfredsstillende. Spesielt oppsto det problemer når sykepleiere ikke rakk å gjøre de nødvendige registreringer under visittens raske tempo.

Det eksisterer et behov for mobil tilgang til elektroniske pasientjournaler.

Mobil EPJ var i testperioden kun ment å bli tatt i bruk under visittgang. Det eksisterte derfor kun behov på dagtid, ikke om kvelden. Brukerne uttrykte at behovet for mobil EPJ er der, spesielt ved avdeling UC hvor over halvparten av de spurte svarte at det eksisterer et behov for denne tjenesten, Figur 3-9.

Mange svarte at det kun eksisterer behov under visse forutsetninger. Det mest vanlige fra både spørreskjemaene og intervjuene var at systemet må være teknisk stabilt og minst like raskt som det stasjonære systemet å bruke.

Det registreres at det var liten forskjell på holdningene til hjelpemidlene, men ”troen” på bærbar PC og PDA er noe større enn på tablet PC. Holdningskurven endret seg mest i negativ retning for PDA og tablet PC. Brukerne endret seg minst i negativ

retning for bærbar PC, noe som indikerer at forventningene er best svart i forhold til denne enheten.

Mobil EPJ virket forstyrrende i visittpersonalets kommunikasjon med pasientene.

Som vist i Figur 3-14, synes over halvparten av de spurte legene og sykepleierne at de kunne svare pasientene mer der og da når de brukte PDA sammenlignet med kun et stasjonært datasystem.

Fra Figur 3-14 kommer det frem at bærbar PC skilte seg ut som den mobile håndholdte enheten som frigjorde mest tid til pasientkontakt og behandling. Brukerne av de to andre enhetene følte at enhetene i mindre grad var tidsbesparende, noe som frigjorde mindre tid til pasientkontakt. På påstand om at pasientene blir bedre informert, var legene og sykepleierne mest enig ved bruk av bærbar PC. Slik systemet fungerte i utviklingsprosjektet, var det kun bærbar PC som ble brukt til å vise skannede journaler.

Tilbakemeldingene fra leger under intervjurunden, var at de fleste ønsker å forberede seg før man møter pasientene. Dette ble begrunnet ved at de ville ha fokus på pasientene når de er på visittrunden. Det legges til at det er viktig at de mobile håndholdte enhetene blir tilpasset arbeidsrutinene, og ikke motsatt. For denne gruppen, eksisterer det ikke noe behov for systemet,

Generelt kan det sies at brukerne oppfattet tablet PC som mest ødeleggende i forhold til pasientkontakt og informasjonstilgjengelighet for pasientene. Dette gjenspeiler tilbakemeldingene om at enheten var tungvint å ha med seg, det tok lang tid å navigere i menysystemet til InfoPack_Helse, registreringsarbeidet tok lengre tid med berøringsskjerm enn tastatur og at de tekniske problemene tok mye av oppmerksomheten fra pasientene. Den tekniske stabiliteten var nemlig dårligst på PDA og tablet PC, som vist i Figur 3-7.

Et mobilt EPJ system bør utvides med flere tjenester

I kapittel 3.4.7 vises brukernes egne meninger angående utviklingsmuligheter for det mobile EPJ systemet som har vært uttestet hos SSA. Blant annet er det foreslått å implementere DIPS på PDA, noe som er umulig på grunn av skjermstørrelsen. Derimot på dagens tablet PC-er, vil dette være mulig. Dette gjør at egenskapene til tablet PC-en er betydelig mer like egenskapene på bærbar PC, enn hva som var tilfellet i utviklingsprosjektet. Hvordan forslagene kan implementeres i et fremtidig system, er grundig beskrevet i kapittel 5.

3.6.2 TAM og UAM

I følge TAM, vil *oppfattet enkelthet ved bruk* direkte påvirke oppfattet nytte. Det gjelder for et mobilt EPJ system, ettersom både enkelthet ved bruk og høy funksjonalitet gjør at nytten av dette systemet vil øke. I intervjuene kom det frem at den viktigste årsaken til den lave bruken, er elementer i UAM [2] som sorterer under oppfattet enkelthet ved bruk i TAM [4].

Det kom i kapittel 3.4.5 tydelig frem at det eksisterer et behov for mobil EPJ, også etter utviklingsprosjektet er gjennomført. Fra Figur 3-14 vises også at et slikt system bidrar til at helsepersonellet kan svare på mer ute hos pasientene. Ser vi dette resultatet opp mot TAM, burde det motivere til større bruk av mobil EPJ enn hva som var tilfellet blant disse brukerne. Denne uoverensstemmelsen kan forklares ved at flesteparten ikke merket at interessen for å informere pasientene økte når informasjonen ble mer tilgjengelig.

Dersom det senere blir innført flere funksjoner i InfoPack_Helse, vil dette medføre at brukerne lettere forstår nytten av produktet. Dersom brukerne ser denne økte nytten, vil behovet for produktet øke. Et eksempel på denne påvirkningen, kan sees i prosjektet ved at brukerne etter opplæringen ikke oppfattet InfoPack_Helse som et enkelt produkt å bruke. Ved oppstart av prosjektet fant de ut at mye av funksjonene som skulle være der, manglet. Når denne funksjonaliteten ikke kom på plass i løpet av en tid, falt både den oppfattede nytten og behovet bort.

Ettersom PDA og tablet PC opplevdes som for tregt å bruke under visittgang, viser TAM at både oppfattet nytte og derfor den faktiske bruken reduseres. Systemet må bli raskere på visittens arbeidsprosesser, om det skal kunne benyttes i arbeidets raske tempo. Fra TAM kan man se at alt dette vil svekke oppfattet nytteverdi av tjenesten. På 3D førte dette til at de praktisk talt sluttet å bruke mobil EPJ før prøveperioden ble avsluttet.

3.6.3 InfoPack_Helse kontra DIPS

Under testprosjektet for mobil EPJ hos SSA, ble det registrert en rekke samsvarende brukererfaringer for PDA og tablet PC. Dette er naturlig, ettersom begge enhetene benyttet seg av den samme programvaren, InfoPack_Helse [11]. Betjeningen av disse enhetene var derfor den samme. Programvaren DIPS, har vært i drift siden 2001, og brukerne har rukket å bli godt kjent med dette systemet. De følte de seg derfor mer komfortable med bruken av DIPS fremfor InfoPack_Helse. I intervjurunden gikk det fram at brukerne også ved implementering av DIPS var skeptiske og negative, men de har blitt svært avhengig av systemet etter hvert, og føler nå at de sparer mye tid på å bruke det. Dette åpner muligheten for at tidsbesparelsene ville økt dersom systemet hadde vært brukt i en lengre periode.

I tillegg var ikke alle ønskelige funksjonene implementert, noe som gjorde at brukerne likevel var nødt til å benytte DIPS for å få tilgang til den nødvendige pasientinformasjonen. En rekke tilbakemeldinger på dette området, sa at nytteverdien vil øke proporsjonalt med antall nyttige fungerende funksjoner som kan implementeres i samme system [20].

Alle var enige i at det tok lang tid å finne frem pasientene med InfoPack_Helse. Man måtte bla i lange navnelister. I denne forbindelse savnet brukerne hurtigfunksjoner for raskere å finne frem pasientene. DIPS er derimot mer basert på direkteknapper i stedet for rullegardinmenyer slik som i InfoPack_Helse. Grundig opplæring kunne redusert denne forskjellen, ettersom brukerne ville ha blitt raskere i bruken av rullegardinmenyene. Det er på grunn av tilpasning til de små skjermene at InfoPack_Helse er mer basert på rullegardinmenyer.

Under demonstrasjon av hele mobil EPJ-systemet og intervjurunden ble det gitt uttrykk for at det var en del begreper i InfoPack_Helse som ikke stemte overens med begrepene i DIPS eller begrepene som ble brukt blant de ansatte. Spørreundersøkelsen viste derimot at det var stor spredning i oppfatningen om dette, men at det er uhensiktsmessig å ha flere datasystemer å sette seg inn i, oppfattes negativt av alle spurte. Flere brukere sa de helst ville at PDA og tablet PC skulle kjørt DIPS, og om man ikke kunne det, burde i alle fall InfoPack_Helse ligne mer på DIPS enn det gjør i dag.

3.6.4 PDA,Tablet PC og bærbar PC

En av de viktigste grunnene for å implementere mobil EPJ, var tidsbesparelse ved arbeidsprosessene [19]. Dette skulle skje ved at all informasjonsbearbeiding ble gjort ferdig ute hos pasientene. Som vist i Figur 3-10 ser man at på de aller fleste arbeidsprosessene ble det spart mest tid med bærbar PC, litt mindre tid med tablet PC og minst tid med PDA. Det er også verdt å merke seg at ingen sa seg helt enig i at PDA eller tablet PC var tidsbesparende.

Bærbar PC skilte seg ut som den enheten som i størst grad sikret informasjonstilgjengelighet. Dette er naturlig ettersom bærbar PC benytter DIPS, en mer komplett programvare enn InfoPack_Helse. PDA og tablet PC opplevdes mer tidkrevende når det gjaldt å få innsyn i den ønskelige pasientinformasjonen enn ved bruk av bærbar PC. Brukerne så da ikke PDA og tablet PC som nyttige nok. Godt over halvparten av de spurte mente det var vanskelig å registrere eller hente ut data ved hjelp av PDA og tablet PC.

PDA viste seg å være minst tidsbesparende til de fleste av arbeidsprosessene, både under previsitt, selve visitten og under ettervisitt, som vist i Figur 3-10. Begrunnelsene som gikk igjen, er at man brukte lang tid på å navigere i journaler, ettersom linjelengden ikke fikk plass horisontalt på skjermen. Dette førte til at bildet måtte navigeres i to retninger for hver linje som ble lest, en enkel feil som burde vært løst før systemet ble satt i drift.

Resultatene fra spørreundersøkelsen viser at det er stor spredning i oppfattelsen av om skjermstørrelsen på PDA er stor nok. Fra Tabell 3-3 kommer det frem at blant de som brukte PDA, er omtrent halvparten fornøyd med skjermstørrelsen. Dette blandede resultatet, viser at enkelte arbeidsprosesser er uegnet ved bruk av PDA. I utviklingsprosjektet hos SSA var det lagt opp til at de samme oppgaver som skulle gjøres med tablet PC, også skulle gjøres med PDA. Skjermstørrelsen til PDA viste seg å være i minste laget ved for eksempel journalvisning, og det gikk heller ikke å se på de skannede journalene. Av de som benyttet seg av tablet PC, mente flertallet (88 %) at skjermstørrelsen var stor nok. I motsetning til PDA, var skjermstørrelsen på tablet PC stor nok til å vise hele setninger i skjermbildet, slik at en slapp å navigere i horisontalt i teksten. De som ikke benyttet tablet PC, hadde ikke gjort seg opp med noen mening om spørsmålet. Dette betyr at skjermstørrelsen mest sannsynlig ikke var den avgjørende årsaken til at brukerne ikke tok enheten i bruk.

PDA viste seg å være den eneste av de mobile enhetene som egnet seg å bære med seg i hånden eller lommen. Dette åpner for at PDA egner seg godt til enkelte arbeidsprosesser. Blant annet vil en sykepleier som har med seg PDA, raskt kunne få opp pasientlister, oversikt over hvilke medisiner som har blitt gitt til bestemte pasienter, foreta medikamentbestillinger og diktafontjenester. Når det gjelder egnethet i forhold til å ha med de mobile enhetene til visittgang, kom tablet PC dårligst ut. Under 50 % av brukerne var enig i at tablet PC var enkel å ha med seg under visittgang. Fra intervjurunden kom det frem at tablet PC var så stor og klumpete, at den ble enklest transportert på en tralle. Og når trallen allikevel skulle benyttes, syntes de fleste det var bedre med bærbar PC, på grunn av større skjerm, tastatur og flere funksjoner i DIPS enn InfoPack_Helse. Derfor svarte nesten 80 % av brukerne at bærbar PC var grei å ha med seg rundt. Når de hadde med seg tralle, kunne også den medisinske kurven fraktes på tralla, slik at leger og sykepleiere kunne ha hendene fri.

Bærbar PC viste seg å være den enheten som tilfredsstilte brukernes forventninger i størst grad, som vist i Figur 3-15. Dette systemet fungerte på samme måte som det stasjonære datasystemet ved avdelingene. Den eneste forskjellen var at brukerne kunne gjøre ferdig all databehandling ute ved pasientene. Bærbar PC var også den eneste av de mobile enhetene som hadde tastatur. Registreringen av pasientinformasjonen opplevdes raskere enn med berøringsskjerm, slik som med PDA og tablet PC.

Brukernes holdninger endret seg mest i negativ retning i forhold til PDA og tablet PC, som begge benyttet seg av InfoPack_Helse. Intervjuene bekreftet i denne sammenhengen at PDA og tablet PC opplevdes som mindre stabilt enn bærbar PC som benyttet seg av DIPS.

3.7 Konklusjon

Etter hvert som all pasientinformasjon har blitt digitalisert, har det utvilsomt oppstått et behov for tilgang til disse dataene der pasientene er. Likevel avdekker denne analysen at den tekniske stabiliteten er nødt til å forbedres om det skal være rom for mobil EPJ i et aktivt sykehusmiljø.

Det har vist seg gjennom utviklingsprosjektet hos SSA at de ulike håndholdte enhetene egner seg til forskjellige arbeidsprosesser. PDA bør benyttes til enkle registreringer både skriftlige og over diktafon. Dessuten egner den seg til å gi ut små mengder pasientinformasjon som for eksempel hvilke medisiner som har vært gitt til bestemte pasienter og laboratoriesvar. Ettersom skjermstørrelsen er for liten for vanlig DIPS er InfoPack_Helse det eneste alternativet. Fremtidig utvikling av dette produktet bør fokusere mer på at enheter med liten skjerm er uegnet til å behandle store mengder informasjon. Eksempelvis er det for tungvint å navigere i dokumenter når det bare er plass til noen få ord i hver linje.

Tablet PC-er som finnes på markedet i dag, ligner mer på en bærbar PC enn hva som var tilfellet under utviklingsprosjektet hos SSA. Skjermstørrelsene på de nye tablet PC-ene er nå så gode, at det er mulig å benytte DIPS på disse. Ettersom tablet

PC er for stor for brukerne å bære med seg sammen med den medisinske kurven, må trillebord benyttes inntil kurven også kommer på elektronisk form. Fram til det, kan brukerne like gjerne ta med seg en fullverdig bærbar PC, som er både raskere og har større skjerm.

PDA med InfoPack_Helse bør benyttes til enkelte arbeidsprosesser, ettersom den er enkel å bære med seg. Tablet PC vil på alle områder tape kampen mot bærbar PC, ettersom de ansees som like mobile.

4 Sikkerhet

4.1 Sikkerhet i mobil EPJ på SSA

Det er vanlig å definere trådløse informasjonssystemer som usikre nett [21]. Dette gjøres fordi slike typer nett har vist seg å være svært utsatt for angrep, ettersom informasjonen sendes i luften. En angriper trenger ikke å koble seg opp mot et fast nett, og heller være inne i bygningen hvor det er et trådløst nett.

Driftingen av et slikt nett må, av sikkerhetsmessige hensyn, ta for seg temaer som autentisering, autorisasjon, konfidensialitet og dataintegritet [39]. Disse sikkerhetstjenestene må sikre nettets tilgjengelighet, uten at funksjonaliteten svekkes. Et trådløst LAN må sikres mot å være en inngang til resten av nettet for en angriper. Dette åpner for en rekke spørsmål, blant annet hvordan bekrefte en brukers identitet før det gis tilgang videre inn i nettet. Det bør også legges vekt på å kontrollere hvilke ressurser en bruker skal få tilgang til. På toppen av alt dette, har en systemutvikler mulighet til å sikre konfidensialitet og dataintegritet.

Sikkerheten i mobil EPJ hos SSA i testperioden tok for seg tilgangskontroll ved at personalet måtte logge seg på med brukernavn og passord. All brukerinformasjon var lagret i en Active Directory (AD)-server som var på samme segment som journalserverne. Så snart brukerne av tablet PC eller PDA ble godkjente av AD-serveren, fikk de tilgang til tjenester som Medicoms server tilbyr. Bærbar PC hadde tilgang direkte mot DIPS.

Dersom en lege eller sykepleier forlot en ferdig innlogget dataenhet, var det av sikkerhetsmessige hensyn en timerstyrt mekanisme for automatisk avlogging. Dette var likt som på det stasjonære trådbundne systemet, men det er lettere å bære med seg en trådløs enhet og dermed lettere for en angriper å ta med seg en trådløs enhet og sitte for seg selv innenfor det trådløse nettets dekningsområde.

For at en eventuell angriper ikke skal kunne lese meldingene som går over radiogrensesnittet, ble det hos SSA blitt tatt i bruk kryptering av signalene. Krypteringsnøkkelen var på 128 bit i WEP-algoritmen. Disse krypteringsnøklene er relativt enkle å knekke med lett tilgjengelig verktøy, som beskrevet i kapittel 4.5. Det ble også gjort et mislykket forsøk på å ta Kerberoskryptering i bruk under testperioden. Ettersom dette førte til at informasjonssystemet ble tregt og ikke ville fungere slik det var tenkt som beskrevet i kapittel 4.4.2, valgte IT-avdelingen å fjerne denne krypteringen.

I tillegg til dette, var det implementert autentisering på MAC-adresse nivå. Da var det bare de MAC-adressene som var registrert i aksesspunktene, som fikk tilgang til nettet. Ved bruk av en sentralt plassert RADIUS-server, kunne registreringen av de gyldige MAC-adressene skje sentralt for alle aksesspunktene. Slik systemet fungerte hos SSA i utviklingsprosjektet, ble de gyldige MAC-adressene programmert i hvert eneste aksesspunkt. Dette førte til at systemet var lite fleksibelt. MAC-adresser kan

forfalskes, men er vanskelig å gjette for utenforstående. Man er nødt til å benytte seg av metoder som er beskrevet i kapittel 4.5, for å få innsyn i andres MAC-adresser.

Det trådløse systemet på SSA var basert på WLAN-teknologien IEEE 802.11b. I kapittel 4.3 beskrives sikkerhetsmekanismene til denne teknologien, hvor det er gitt en fyldig beskrivelse av autentisering og kryptering som har vært benyttet hos SSA.

4.2 Krav til sikkerhet

Datatilsynet definerer at trådløse nettverk i utgangspunktet er å beskrive som usikre, på samme måte som Internett. Slike informasjonssystemer som i tillegg inneholder sensitive personopplysninger, stiller ekstra krav til autentisering og kryptering. Dette er funnet ut fra datatilsynets rapport *Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger* [21]. I denne rapporten oppfordres det til å opprette soner med forskjellig grad av tilgangskontroll. Et enkelt utdrag fra denne rapporten som er relevant for SSA gjengis som følger:

Tilgang til sone med sensitive personopplysninger
Soner skal etableres etter behovet for tilgang og dataoverføring mellom enkelte i informasjonssystemet. Rutinene skal minst inneholde retningslinjer for:

- Etablering og revurdering av soneinndeling
- Opprette soner med angivelse av teknisk sikkerhetsløsning, eksempelvis ruter
- Ekstern tilgang med krav om at den del av informasjonssystemet som benyttes for ekstern tilgang, etableres i egen sone
- Å registrere forsøk på uautorisert tilgang
- Beskrivelse av ansvar og myndighet

Tilgang til sensitive personopplysninger
Det skal etableres rutine for kontroll med tilgang til data og program som benyttes for behandling av sensitive personopplysninger. Rutinene skal minst inneholde retningslinjer for:

- Tildeling og tilbaketrekking av autorisasjon for tilgang med krav om entydig kobling mellom brukeridentitet og fysisk bruker
- Periodisk revurdering av den enkelte medarbeiders behov for tilgang
- Identifisering og autorisering av medarbeidere
- Automatisk avstenging av utstyr som ikke er i bruk

Datatilsynet stiller i skrivende stund konkrete krav til DES-kryptering med minst 128 bits nøkkel. I tillegg er det viktig at et informasjonssystem som skal distribuere sensitiv informasjon, må sikres av to barrierer [26]. Det må finnes en form for løsning for sikker autentisering av brukerne. Dette er nødt til å resultere i at nettverket blir sikret for uautorisert tilgang.

4.3 Sikkerhetsmekanismer i IEEE 802.11b

Følgende kapittel er basert på [42] og [43].

Sikkerhetsmekanismer i 802.11b er autentisering og kryptering. Autentisering skjer mellom et aksesspunkt og hver enkelt node. Slik autentisering kan være enten *åpent system-* eller *delt nøkkel*-autentisering. I åpne systemer kan man autentisere etter lister i aksesspunktet over MAC-adresser for tillatte noder. Delt nøkkel-systemet baserer seg på en kjent kryptert *secret key*. Delt nøkkel-systemet kan kun brukes der det trådløse LAN-et støtter kryptering (siden *secret key* er kryptert).

Wired Equivalent Privacy bruker RC4 PRNG og er krypteringsmetoden for BSS med den opsjonen.

4.3.1 Autentisering

802.11b definerer to undergrupper av autentiseringstjenester; *åpent system* og *delt nøkkel (shared key)*. Hvilken undergruppe som blir brukt i hvert tilfelle, blir identifisert fra authentication management-pakkene, siden disse er selvidentifiserende med hensyn til autentiseringsalgoritmen.

Etter en vellykket autentiseringsprosess er det et gjensidig autentiseringsforhold mellom to stasjoner. Autentisering kan brukes mellom en mobil terminal og et aksesspunkt.

Åpent system autentisering

Åpent system autentisering er den enkleste formen av autentiseringsalgoritmer. Det er en nullautentiseringsalgoritme. Med andre ord vil hvilken som helst terminal som ønsker å bli autentisert, bli autentisert dersom det mottagende aksesspunktet er programmert til åpent system autentisering. Klienten må allikevel sende med riktig SSID (Service Set Identifier). 802.11b-utstyr leveres med åpent system autentisering som standardverdi.

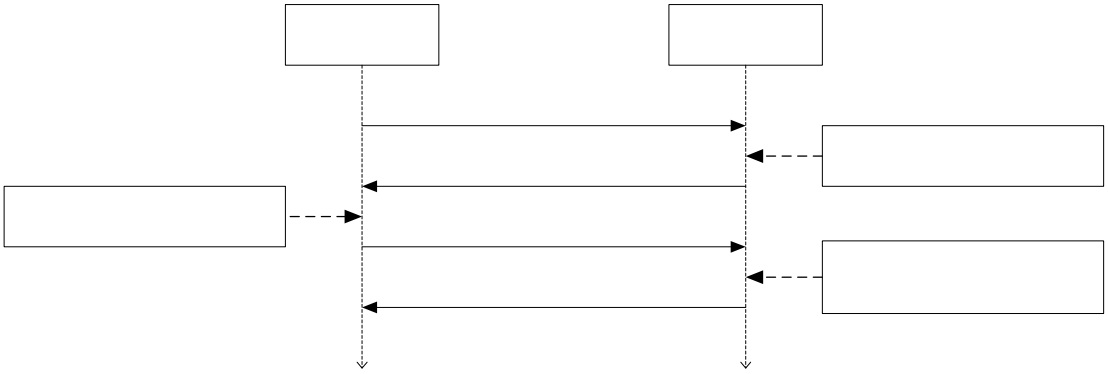
Åpent system autentisering innebærer en tostegs autentiseringsprosess. I det første steget vil en mobil terminal påstå en identitet og spørre etter en autentisering for denne identiteten. I det andre steget vil aksesspunktet sende en autentiseringsrespons hvor svaret er enten suksessfullt eller ikke.

Figur 4-1: Åpent system autentisering

I åpne systemer kan man også velge å autentisere etter lister i aksesspunktet, for eksempel lister over tillatte noders MAC-adresser.

Delt nøkkel-autentisering

Delt nøkkel-autentisering er en *challenge-response* autentisering. Denne autentiseringsmetoden går ut på at begge parter kjenner til den delte hemmelige nøkkelen. Det antas at denne er delt ut til de deltagende nodene via en sikker kanal, som er uavhengig av 802.11b. Delt nøkkel-autentisering gjennomfører autentiseringen uten behov for å overføre nøkkelen i åpenhet, ved å bruke WEP-algoritmen. Derfor må WEP-algoritmen være implementert i både aksesspunktet og den mobile terminalen for at delt nøkkel autentisering skal kunne fungere.



Figur 4-2: Delt nøkkel autentisering

Delt nøkkel-autentisering innebærer en firestegs autentiseringsprosess. Det første og siste steget er like de to stegene i åpent system autentisering. Det vil si at det første steget er en autentiseringsforespørsel fra terminalen til aksesspunktet, mens det fjerde steget er en autentiseringsrespons tilbake til terminalen.

Etter å ha mottatt forespørselen fra terminalen, genererer aksesspunktet et tilfeldig tall og sender dette tallet som en utfordring til terminalen. Den mobile terminalen bruker den hemmelige nøkkelen og WEP-algoritmen til å kryptere dette tallet, og sender det kryptert tilbake til aksesspunktet. Aksesspunktet dekrypterer og sammenligner med den opprinnelige utfordringen som ble sendt. Hvis disse er like, blir den mobile terminalen autentisert og en autentiseringsrespons blir sendt tilbake til denne.

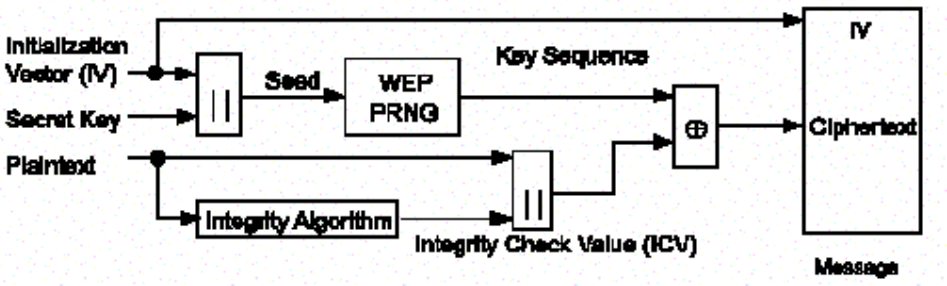
4.3.2 Kryptering

Wired Equivalent Privacy (WEP) algoritmen

Brukere av trådløse systemer er ofte kjent med problemet med avlytting av dataoverføringen. Trådbundne nettverk har i seg selv en sikkerhetsfunksjon ved at man fysisk må koble seg på nettet med nettverkskabel, men denne finnes ikke i trådløse LAN hvor signalene kan gå gjennom både vegger og vinduer. 802.11b spesifiserer en algoritme som gjør at trådløst LAN blir ekvivalent med vanlig LAN når det gjelder datakonfidensialitet. WEP-algoritmen skal beskytte autoriserte brukere av trådløst LAN mot avlytting. Datakonfidensialitet er avhengig av en ekstern *key*

management-tjeneste som distribuerer ciphering- og decipheringnøkler. WEP-algoritmen kan implementeres i både maskinvare og programvare. Det er en symmetrisk algoritme, det vil si at hver node har en felles, hemmelig nøkkel. Hvordan denne nøkkelen blir distribuert, fremgår ikke av spesifikasjonene til 802.11b.

WEP-algoritmen betegnes som en svak algoritme [9]. Sikkerheten som denne algoritmen gir, avhenger av hvor vanskelig det er å finne den hemmelige nøkkelen. Dette avhenger igjen av lengden på nøkkelen og hvor ofte den byttes. Algoritmen har også hyppig bytting av initialiseringsvektoren (IV), slik at angrep av *rå styrke*-metoden blir vanskelig. WEP bruker opprinnelig 40 bit RSA RC4 PRNG algoritme, men nøkkelen har etter hvert blitt utvidet til 128 bit og helt i det siste opp til 256 bit.



Figur 4-3: WEP-generering av ciphertext

For å få konfidensialitet på datakanalen, blir dataene kryptert til ciphertekst. Initialiseringsvektoren og den hemmelige nøkkelen gir grunnlaget for et *seed* som WEP PRNG bruker for å generere en nøkkelsekvens. Denne nøkkelsekvensen blir så XOR-et med plaintext, det vil si dataene som skal sendes, til ciphertext. Deretter vil denne ciphertexten blir sendt over kanalen sammen med initialiseringsvektoren. På den andre siden vil ciphertexten bli XOR-et med den eksakt samme nøkkelsekvensen, og plaintext vil komme ut. Nøkkelsekvensen blir generert på samme måte og med den samme initialiseringsvektoren som hos avsender. Når kryptering med WEP-algoritmen er i bruk, beskyttes kun pakkens nyttedata, slik at headeren er åpen for alle andre noder i nettverket. Dermed kan alle nodene lese headerdata som brukes til å administrere nettverket.

4.4 Mulige sikkerhetsmekanismer for trådløse LAN

4.4.1 Service Set Identifier (SSID)

Vanligvis vil aksesspunktene med faste tidsintervall kringkaste en melding som inneholder SSID, for å opplyse eventuelle terminaler i nærheten om sin eksistens. SSID er aksesspunktets identifikasjon. Om kringkasting av SSID er skrudd av i et aksesspunkt, må alle terminaler som ønsker å koble seg til dette aksesspunktet på forhånd kjenne til dets SSID [9].

SSID er en vilkårlig datastreng som er *navnet* til et eller flere aksesspunkt. Standardoppsettet fungerer slik at alle aksesspunktene kringkaster sin

tilstedeværelse. Hensikten med dette, er å identifisere trådløst LAN til klientene. SSID hindrer at en klient kobler seg opp mot feil aksesspunkt, men støtter ingen andre spørsmål i forbindelse med sikkerhet. Dermed forhindres ikke en angriper å sette opp falske aksesspunkter.

Det er mulig å skru av annonseringene av SSID for å gjøre den vanskeligere å oppdage, men den synliggjøres ved etterspørsel fra en mobil terminal. Ettersom alle managementpakkene i 802.11b blir sendt ukryptert, er det lett for en angriper å lytte til disse meldingene og plukke opp aksesspunktets SSID, selv om dette ikke blir kringkastet. Derfor bør denne metoden kun benyttes i forbindelse med delt nøkkel-autentisering for å oppnå maksimal sikkerhet.

4.4.2 Kerberos autentisering

Kerberos er en autentiseringsprotokoll som ble forsøkt benyttet på SSA i utviklingsprosjektet med mobil EPJ. Hensikten med dette systemet, er at brukerne kan få tilgang til alle servere på nettverket på en sikker måte, uten å måtte la passordet gå over nettverket ukryptert. Kerberos kan bli benyttet for gjensidig autentisering og nøkkelgenerering [33].

Metoden fungerer ved at to parter som skal autentiseres mot hverandre, ikke vet noe om hverandre. Det blir da tatt i bruk en tredjepart for å hjelpe til med nøkkelutvekslingen i denne prosessen. En slik tredjepart blir ofte kalt en autentikasjonsserver. Protokollen som benyttes i denne nøkkelutvekslingen kan variere, men er oftest basert på TCP/IP.

Kerberos involverer følgende tre servere:

- *Autentikasjonsserver (AS)* - Verifiserer brukere gjennom innlogging.
- *Ticket Giving Server (TGS)* - Leverer bevis av identitetsbilletter.
- *Filserver* – Serveren som gjør jobben brukeren vil autentiseres mot.

Kerberos virkemåte:

1. Brukeren skriver sitt navn som sendes til AS i klartekst
2. Sesjonsnøkkel og billett sendes tilbake etter å ha blitt kryptert med brukerens offentlige nøkkel.
3. Når melding 2 mottas, spør arbeidsstasjonen etter brukerens passord. Dette passordet brukes så til å dekryptere melding 2. Arbeidsstasjonen overskriver brukerens passord for å forsikre seg at det kun befinner seg i arbeidsstasjonen i noen millisekunder.
4. Brukeren forteller arbeidsstasjonen at det ønskes kontakt med filserveren. Arbeidsstasjonen sender en forespørsel til TGS om billett for å bruke filserveren. Denne meldingen er kryptert med TGS sin offentlige nøkkel, og blir benyttet som bevis for at brukeren er den han/hun utgir seg for å være.
5. TGS lager en ny sesjonsnøkkel (K_{AB}) som sendes til arbeidsstasjonen i to eksemplarer. Den første er kryptert med sesjonsnøkkelen fra melding 2 så bare brukeren skal lese meldingen, mens den andre er kryptert med filserveren sin offentlige nøkkel. Det legges også med et tidsstempel som ikke

er mulig å forandre av noen som ikke har kjennskap til sesjonsnøkkelen som brukes mellom TGS og brukeren.

6. Brukeren sender K_{AB} og t for å opprette en forbindelse med filserveren. Nå vil kommunikasjonen opprettholdes under beskyttelse av K_{AB}.

Dersom brukeren etter hvert vil kommunisere med en annen server, gjentas meldingene fra nummer 3 mot TGS.

Et vanlig problem med Kerberos implementeringer, er et krav om fast IP-adresse for klienten som vil koble seg opp mot nettet. Vanligvis tildeles IP-adressene av DHCP-serveren etter at klienten har blitt autentisert. Det vil hos SSA, hvor det kun er et fast antall dataenheter, være mulig å registrere faste IP-adresser på klientene for å unngå dette problemet.

Under testprosjektet hos SSA, viste det seg å være et problem med oppsettet for Kerberos under autentiseringen med AD-serveren. Under dette oppsettet, krevde AD at alle klienter benytter seg av Kerberos, også de stasjonære PC-ene. Resultatet ble at Kerberosserveren ble overbelastet og store deler av sykehuset fikk problemer med autentiseringen. Disse problemene førte igjen til at Kerberos ikke ble brukt under testprosjektet for mobil EPJ. Dagens mest solide krypteringsmekanismer tilbys av brannmur med VPN-funksjonalitet

4.4.3 Public Key Infrastructure (PKI)

PKI innebærer alle elementene som kreves for å implementere offentlig nøkkel kryptering. Dette inkluderer nøkkelpar, Certificate Authority (CA), sertifikat mottaker og alle andre programvare- og maskinvarekomponenter.

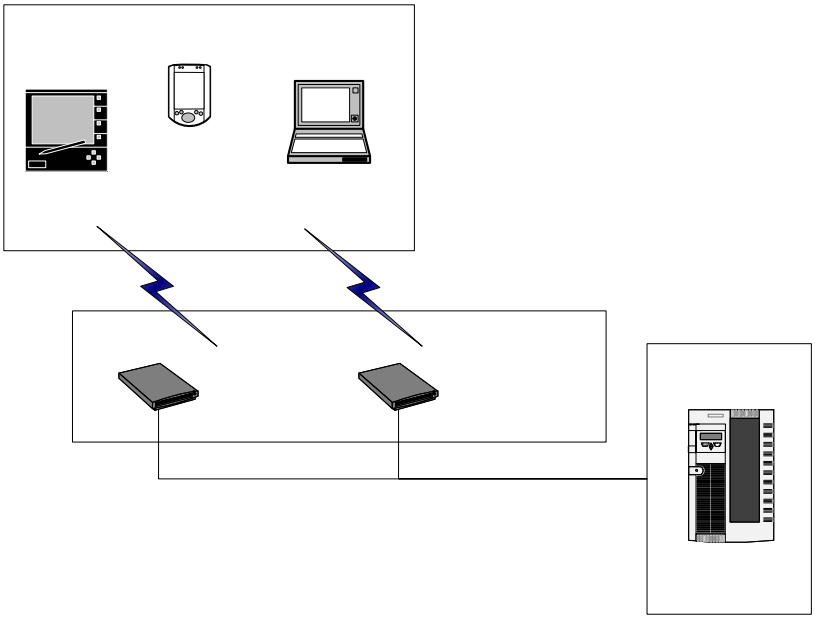
Et nøkkelpar er bestående av et par matematisk assosierte, kryptografiske nøkler, en offentlig og en privat. Den offentlige nøkkelen kan fritt distribueres til alle og brukes ved kryptering, mens den private nøkkelen er hemmelig og benyttes til å dekryptere informasjonen. Hvordan denne mekanismen fungerer, er beskrevet i kapittel 4.3. Den store fordelen er at både avsender og mottaker ikke behøver å kjenne til begge krypteringsnøklene, kun den offentlige. Dermed unngår man å sende private krypteringsnøkler over usikrede linjer, som for eksempel Internet.

PKI kan brukes i forbindelse med digitale signaturer, elektronisk handel via Internet og så videre. En PKI-løsning innebærer også distribusjon av offentlige nøkler via digitale sertifikater som utstedes av CA. PKI tilbyr også meldingsintegritet som forsikrer at meldingen ikke har blitt endret. Disse mekanismene er detaljert beskrevet i [27].

4.4.4 802.1x autentisering

802.1x er en autentiseringsdialog mellom en klient som trenger tjenester fra et nettverk, og nettverket, slik som illustrert i Figur 4-4. Dialogen benytter seg av IETF sin autentiseringsprotokoll *Extensible Authentication Protocol (EAP)* og *Remote Authentication Dial-In User Service (RADIUS)* for å autentisere klienter og distribuere nøkler [12].

Metoden benytter seg av protokollen EAP over LAN (EAPOL) for dialogen mellom søkeren om autentisering og aksesspunktet. Mellom aksesspunktet og autentiseringsserveren bæres EAP meldingene over RADIUS-protokollen slik som illustrert i Figur 4-4. Hovedfunksjonen til autentikatordelen, er å fungere som en EAP-proxy mellom søkeren om autentisering og AAA-serveren (AS).



Figur 4-4: Autentisering med IEEE 802.1x

EAP velger ingen spesifikk autentikasjonsmekanisme i link kontroll fasen, men utsetter dette til autentiseringsfasen. Dette gjør det mulig for autentikatoren å spørre etter mer informasjon før den determinerer autentiseringsmekanismen [14]. Eksempler på autentikasjonsalgoritmer som blir støttet av EAP er MD5, Engangpassord, digital ID og så videre.

802.1x standard autentiseringsdialog:

1 Aksesspunktet spør etter identitet fra den mobile klienten ved hjelp av EAPOL.
2 Klienten sender sin identitet til aksesspunktet
3 Aksesspunktet videresender denne identitet til AS via EAP over RADIUS
4 AS og klienten har en EAP-dialog om autorisering
5 Dersom dialogen er vellykket, vil klienten og AS dele en sesjonsnøkkel
6 AS sender sesjonsnøkkelen til aksesspunktet i en RADIUS attributt som en del av RADIUS accept-melding.
7 Aksesspunktet setter i stand sin kontrollerte port for klienten sin MAC-adresse, og lager valgfritt en WEP-nøkkel ved hjelp av EAPOL nøkkel-pakken.

Det finnes ulike EAP-metoder som har blitt tilført i IETF sitt Internettbibliotek. Flere av disse er godt beskrevet i *Wireless LAN Access Control and Authentication* [12], [14].

Tablet

For å unngå falske aksesspunkter som beskrevet i kapittel 4.5, bør et trådløst LAN utvikles med støtte for toveis autentikasjon.

I sin enkleste form er standarden designet for link-lags (OSI-lag 2) autentisering, og er dermed basert på klientens MAC-adresse. Autentikatoren har ingen andre måter å identifisere en klient eller dens pakker uten høyere lags autentiseringsmekanismer. Denne metoden har ingen funksjonalitet for autentisering på IP-laget og kontrollerer ikke hvilke tjenester brukeren er autorisert til å bruke.

EAP-Transport Layer Security (TLS)

EAP-TLS er den mest brukte og tilgjengelige protokollen for EAP. Klienten må i dette tilfellet gi et digitalt sertifikat som AS kan validere. På samme måte må AS ha et sertifikat som klienten validerer. En forutsetning for at en eksplisitt gjensidig autentisering skal fungere, er at sertifikatene tilbys av en Certificate Authority (CA). EAP-TLS krever kompleksiteten til PKI for å støtte autentisering av klienten. En sterkt autentiseringsmetode med bruker ID og passord, er en mer praktisk autentikasjon i mange bedrifter.

EAP-TLS er robust mot man-in-the-middle angrep, se kapittel 4.5. Det spiller ingen rolle om en angriper klarer å avlytte datatrafikken. EAP-TLS klarer uansett å motstå slike angrep.

Autentiseringen baserer seg på X.509 standarden som er en standard struktur for sertifikater [28]. Komponenter som benytter seg av denne standarden garanterer:

- Navnet til entiteten som skal bli sertifisert
- Entitetens offentlige nøkkel
- Navnet til sertifikat autoriteten
- En digital signatur

X.509 sertifikater kan benytte seg av flere forskjellige digitale signaturalgoritmer, så sertifikatet må spesifisere hvilken algoritme det bruker. X.509 versjon 3 støtter offentlig nøkkel autentisering, mens versjon 2 støtter CRL. Sertifikater kan fritt bli kopiert og distribuert. For å bevise at man eier navnet som oppgis i sertifikatet, må det bevises at den private nøkkelen brukeren innehar, korresponderer den offentlige som sertifikatet inneholder [28].

4.4.5 Remote Authentication Dial in User Service (RADIUS)

RADIUS er en industristandard for sentralisert *authentication*, *authorization* og *accounting* (AAA) for brukere som skal koble seg til nettverket [26].

- *Authentication* er prosessen som bestemmer om en bruker skal godkjennes som den brukeren utgir seg for å være.
- *Authorization* er systemet som kontrollerer hvilke tjenester en bruker skal få tilgang til i nettverket.
- *Accounting* er prosessen som genererer log-filer som beskriver hver forbindelse. Dette kan hos SSA bli brukt til arbeidet med system diagnose og brukerplanlegging.

RADIUS er en server som inneholder informasjon om brukerne som skal bli autentisert og tilgang videre i nettverket. Plasseringen bør være mellom aksesspunktet og det trådbundne LAN. Standarden er en nødvendighet for sikker IEEE 802.1x autentisering og er derfor kompatibel med forskjellige EAP protokoller som nevnt i kapittel 4.4.4.

Aksesspunktene (AP) har mulighet til å etterspørre MAC-adressene til de mobile klientene som vil koble seg opp mot nettet. Dette åpner for muligheten til kun å gi nettaksess til de MAC-adressene som er forhåndslagret. Listen over de MAC-adresser som skal få tilgang, kan bli lagret i langtidsminnet hos AP eller hos en sentral RADIUS server. Ved sistnevnte starter AP autentiseringsprosessen ved å sende en RADIUS-forespørsel med MAC-adresssen som bruker ID og et *null passord* til en sentral RADIUS server som vil sjekke i sin liste. RADIUS-løsningen er spesielt bra egnet dersom MAC-adressen skal brukes til forskjellige AP. Man slipper da å forhåndsprogrammere gyldige MAC-adresser i alle AP. For en hacker er det mulig å forandre en MAC-adresse, noe som gir dette en lav grad av sikkerhet. En angriper kan avlytte trafikken og plukke opp en godkjent MAC-adresse, og så oppgi seg for å være denne godkjente brukeren.

RADIUS inneholder funksjonalitet som muliggjør fleksible og robuste VPN-tjenester, som beskrevet i kapittel 4.4.7.

4.4.6 Smartkort

Smartkort er et kort med minne for å lagre viktige data om en persons identitet. Privat nøkkel, digitale sertifikater og annen personlig informasjon blir sikkert lagret på kortet for å hindre misbruk av elektronisk identitet.

På markedet i dag finnes det flere modeller av bærbar PC og tablet PC med innebygd smartkortleser.

Figur 4-5: Smartkortleser for PDA [38]

Det er mulig å benytte smartkort teknologien sammen med VPN [15]. Selve VPN-sertifikatene blir da lagret på kortet. Flere produsenter tilbyr smartkortløsninger med støtte for IPSec-kompatible VPN. Dette er nærmere beskrevet i kapittel 4.4.7.

Et smartkort som mistes, skal ikke kunne bli tatt i bruk av andre. Det finnes derfor mekanismer for at en bruker må taste inn en PIN-kode som smartkortet benytter for autentisere brukeren. Det vil også inneholde de nødvendige nøkler for krypteringen. Ved bruk av denne metoden behøver ikke systemutviklerne bekymre seg over at digitale sertifikater må beskyttes på noen harddisker. Selve nøklene ligger inne på kortet [15].

I en vanlig IEEE 802.11-kommunikasjon, er det vanlig å benytte seg av 802.1x autentisering som beskrevet i kapittel 4.4.4. Ved bruk av smartkort, vil autentiseringsprosessen foregå på samme måte som EAP-TLS, men den mobile enhetens identitet blir hentet fra smartkortet og ikke MAC-adressen [29].

EAP-SIM

En autentiseringsprosess som støttes av IEEE 802.1x, er EAP-SIM. Dette er en metode, som i prinsippet er lik EAP-TLS, som er beskrevet i kapittel 4.4.4.

1. En 802.11-kommunikasjon starter med en uautentisert klient som ønsker forbindelse med et aksesspunkt. Aksesspunktet er koblet opp mot en autentiseringsserver.
2. Når klienten trigger EAP-protokollen i autentiseringsserveren, svarer serveren med å be om klientens ID som finnes på dens smartkort.
3. Autentiseringsserveren inneholder autentiseringsmateriell som sammenlignes med ID fra klientens smartkort. I tillegg utvinnes de delte hemmelighetene: klientautentiseringsnøkkel, nettverksautentiseringsnøkkel og en mastersesjonsnøkkel.
4. Ved gjensidig autentisering foretas de samme beregningene hos klienten og en klassisk challenge-response protokollflyt.
5. Når autentiseringen er vellykket, vil mastersesjonsnøkkelen bli benyttet for å beskytte dataene mellom klienten og aksesspunktet.

Opprinnelig er denne EAP utviklet for IEEE 808.11 og GSM, hvor autentiseringsmaterialet blir hentet av fra HLR/AuC. Dersom dette materialet ligger inne hos autentiseringsserveren, vil det være mulig å foreta 802.1x autentisering uten bruk av MAC-adresse som EAP-TLS.

4.4.7 Virtual Private Network (VPN)

VPN er en metode for bruk av kryptering og tunnelering for sikkert å forbinde to brukere over et offentlig nettverk. Ved å plassere en VPN port rett bak aksesspunktene vil kommunikasjonen som går over eteren være beskyttet.

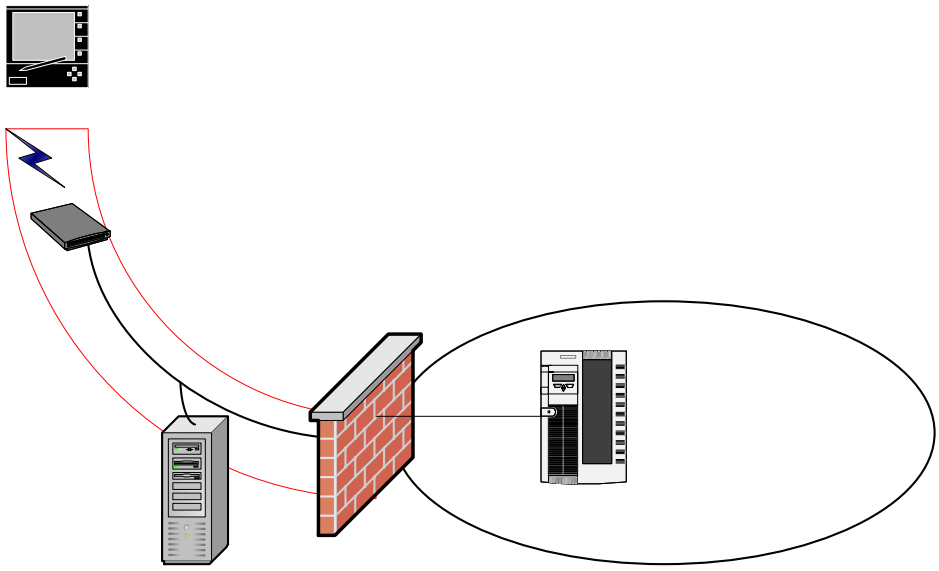
Denne teknologien er utviklet for å eliminere sikkerhetsrisikoen ved å sende ukryptert data over offentlige nett. I et trådløst LAN, vil datakrypteringen gå hele veien til VPN-serveren, og ikke bare til aksesspunktet.

Et VPN benytter seg av en rekke metoder for å holde forbindelsen og dataene sikre. Teknikken støtter både autentisering og kryptering av data.

Et fundament for VPN-sikkerhet er Internet Key Exchange (IKE). Pakker kan her beskyttes ved hjelp av forhåndsdelte hemmelige nøkler mellom to parter eller bruk av standard offentlig nøkkel-kryptering. IKE støtter også digitale sertifikater som gir støtte for et helt annet nivå av konfidensialitet [13].

Alle VPN krever konfigurering av klienter som det skal gis tilgang til i nettet. Når VPN blir tatt i bruk sammen med sterk autentisering, hindrer dette angripere å koble seg opp mot nettet, selv om de var i stand til å finne en VPN-sesjon.

VPN-produktene kan sorteres i maskinvarebaserte systemer, selvstendige applikasjoner og brannmurbaserte systemer. De to førstnevnte løsningene er meget enkle å sette opp og administrere, i tillegg til at de regnes som sikre løsninger. Disse løsningene regnes for å være best egnet dersom ikke begge endepunktene er kontrollert av samme selskap [28]. I SSA sitt tilfelle, vil det være mest aktuelt å se på et brannmurbasert system. Denne metoden er den mest trygge, fordi den drar fordel av sikkerhetsmekanismene som finnes i en brannmur.



Figur 4-6: VPN forbindelse i det trådløse LAN-et hos SSA

Det kan settes opp en brannmur mellom aksesspunktet og nettverket, som bare tillater autentisert VPN tilgang og kan beskytte nettverket mot angrep, slik Figur 4-6 viser. På grunn av svakheter ved WEP-algoritmen, er det en fordel at VPN støtter blant annet DES, 3DES eller Advanced Encryption Standard (AES). VPN beskytter bare trafikken som blir rutet gjennom tunnelen, og ikke selve klienten eller nettverket.

I motsetning til 802.1x, som kun gir støtte for autentisering på link-lags nivå i OSI-modellen, vil det være mulig å sette opp VPN-forbindelser på nettverksnivå ved bruk av IPSec. Dette gir mulighet for å kontrollere trafikken basert på hvilke tjenester

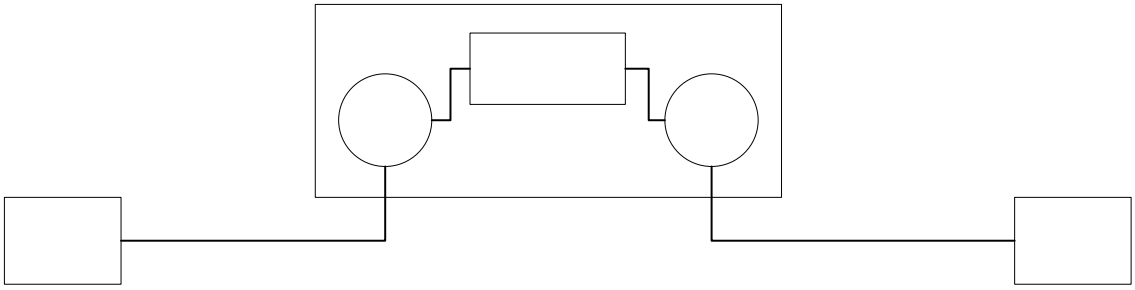
bestemte brukere eller brukergrupper skal få tilgang til [15]. Dagens kombinerte VPN/brannmur løsninger har også støtte for smartkort.

4.4.8 Brannmur

En brannmur er en spesielt programmert ruter som er plassert slik at alle som skal inn i en sikret sone, må gjennom denne, slik som beskrevet i Figur 4-6.

Det finnes to typer brannmurer, nemlig filter-baserte og proxy-baserte [28]:

- *Filter-baserte* brannmurer kontrollerer datatrafikken mellom to nettverk og kan kaste eller videresende pakker basert på klienters IP-adresse og TCP/UDP portnummer.
- *Proxy-baserte* brannmurer derimot setter opp en FTP/TCP forbindelse mot klienten på den ene siden og en identisk forbindelse mot serveren som vist i Figur 4-7. Denne løsningen gjør det mulig å kontrollere at en bruker eller en brukergruppe er autorisert til forskjellige tjenester i det beskyttede nettet.



Figur 4-7: Brannmur med proxyfunksjonalitet, pakkefiltre og applikasjonsgateway

Ved integrering av brannmurteknologi med VPN-utstyr, blir sikkerheten og drifting av systemet forbedret i forhold til å ha separate brannmurer [14]. Tidligere har det vist seg at konfigurering av begge disse systemene slik at brannmuren ikke skal blokkere VPN-trafikk, har vært vanskelig.

4.4.9 IPSec

IPSec er et rammeverk for å tilby ulike sikkerhetsmekanismer, og er bestående av Authentication Header (AH) og Encapsulating Security Payload (ESP) [28]. AH tilbyr tilgangskontroll, autentikasjon og forbindelsesløs meldingsintegritet. ESP støtter de samme tjenestene i tillegg til konfidensialitet. De kan begge brukes alene eller sammen for å tilby en god blanding av sikkerhetstjenester som passer for brukerne. Sammenkoblingen av disse to gjøres ved hjelp av en Security Association (SA).

IPSec krever liten kunnskap fra klientene, ettersom autentiseringen ikke er brukerbasert. Isteden kommer sikkerheten fra arbeidsstasjonens IP-adresse eller dens sertifikat for å etablere brukerens identitet og forsikre integritet av nettverket. En IPSec-tunnel opererer på nettverkslaget og beskytter alle pakkene, uavhengig av applikasjon.

Hvordan IPSec kan benyttes sammen med VPN-teknologi er nærmere beskrevet i [15]. IPSec baserte VPN gjør det mulig for en administrator å definere en liste med spesifikke nettverk og applikasjoner som kan bli aksessert.

En ulempe med IPSec-kompatible produkter, er at de kun tilbyr aksesskontroll over tilgangskontroll på nettverks- og transportlaget. Det blir derfor ikke mulig å regulere tilgang til individuelle ressurser. Det er behov for sterkere, mer selektive kontrollmekanismer for å være sikker på at brukerne bare kan aksessere den informasjonen de er autorisert til å se. Denne typen selektive løsninger i et VPN er tilgjengelig gjennom enkelte ikke-IPSec løsninger som for eksempel SOCKSv5 [44].

Det finnes i dag enkeltstående enigheter som gir støtte for både IPSec baserte VPN løsninger, med integrert støtte for IEEE 802.1x autentisering med RADIUS-funksjonalitet, og brannmur. Et eksempel på et slikt produkt er SonicWall GX650.

4.4.10 Tynnklient

Mobilitet omfatter også datautstyr som ikke er bærbart. Med tynnklient er det mulig å logge seg på forskjellige datamaskiner, og få den samme arbeidsflaten slik den var da brukeren sist logget seg ut.

Det kan også ligge sensitive data lagret på de trådløse klientene. Disse kan havne i hendene på feil personer dersom datautstyret havner på avveie. For å unngå dette er det vanlig å benytte seg av tynnklient. Alle sensitive data blir da værende på de sikre serverne. Hos SSA har Citrix Metaframe (Citrix MF) blitt benyttet i testprosjektet [37].

Tynnklient gir støtte for serverbasert databehandling. Produkter finnes i dag på markedet som plattform- og maskinuavhengig programvare. All administrasjon kan gjøres sentralt. Nyere XP-versjoner av Citrix MF har støtte både for smartkortløsninger, RSA og SSL.

4.5 Angrep på trådløse LAN

4.5.1 Sniffing

Trådløse nettverk åpner for avlytting fra hvilken som helst radiomottaker innenfor senderens rekkevidde. Ved bruk av antenne med forsterkning, kan avlyttingen skje langt utenfor veggene til den bygningen hvor det trådløse LAN benyttes. En angriper som avlytter trafikken kan få innsyn i enkelte brukernavn og passord, i tillegg til data som brukes i forbindelse med autentikasjon. Ethereal [22] gjør det mulig å overvåke datatrafikken som går i et nett eller overvåke data som er lagret på en klient. Disse dataene kan angriperen ta i bruk senere til andre typer angrep.

Når en angriper har fått vite hvordan man kan få tilgang til nettet, kan han/hun ta i bruk en gyldig brukers identitet. Ved avlytting kan en angriper få greie på en gyldig brukers MAC-adresse, som benyttes for å ta over brukerens posisjon i nettet. Prismdump [32] er et gratis program som kan benyttes til å fange opp alle

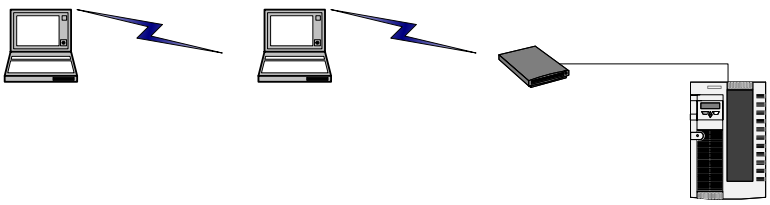
nettverkspakker som er i luften. Dataene kan så lagres på angriperens harddisk for senere analyse av dataene.

Kryptert data mellom klient og aksesspunkt reduserer muligheten for avlytting av brukerdata. WEP-kryptering som ble benyttet i utviklingsprosjektet hos SSA har vist seg å være enkel å knekke ved hjelp av pakkesniffere. Airsnort [23] er et WiFi-verktøy som gjenvinner krypterte nøkler fra WEP [31]. Programmet opererer ved å passivt monitorere transmisjoner, og beregner krypteringsnøkkelen når nok pakker er samlet. Typisk kan dette være en datamengde på mellom 100 Mb til 1 Gb [25].

For å hindre faren for sniffing, må de mobile enhetene og aksesspunktene ha støtte for meldingsintegritet. Med dette menes at hver melding må signeres ved hjelp av en nøkkel som er delt mellom de mobile enhetene og aksesspunktene

4.5.2 Man-in-the-Middle angrep

En angriper utgir seg for å være det trådløse aksesspunktet og får en klient til å sende seg informasjon. Dataene blir så avlyttet før de sendes videre i begge retninger [14].

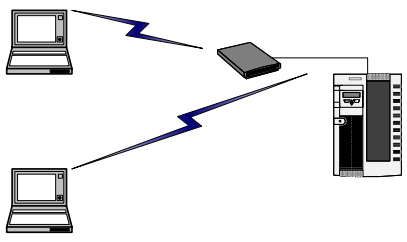


Figur 4-8: Man-in-the-middle angrep

Link-lags autentikasjon stopper en utenforstående i å gjennomføre disse angrepene. Tilstrekkelige sikkerhetsmekanismer på nettverkslaget stopper en insider fra å gjennomføre disse angrepene. Slike mekanismer er bedre beskrevet i kapittel 4.4.7.

4.5.3 Session-Hijacking angrep

En angriper kan avlytte forbindelser satt opp av en gyldig klient. Serveren tror den sender data tilbake til klienten, men dataene blir avlyttet før de når klienten [14].



Figur 4-9: Session-Hijacking angrep

4.5.4 Falske aksesspunkt

Aksesspunktene for IEEE 802.11b-standarden selges i dag for rundt 1000 kroner, og er tilgjengelig hos de fleste forhandlere av datautstyr. Arbeidstakerne kan derfor selv sette opp slike basestasjoner. Dersom det ikke blir gitt beskjed om dette til IT-avdelingen og sikkerheten ikke er satt opp på tilstrekkelig god måte, vil dette utgjøre en stor sikkerhetsrisiko. Dette aksesspunktet vil være som en åpen dør inn i nettet.

For en inntrenger vil det også være mulig å plassere ut en basestasjon for å få den ønskelige tilgangen til sykehusnettverket. Sykehuset, som er stort og uoversiktlig, kan gjøre det mulig for en basestasjon å stå utplassert over en periode, uten å bli oppdaget. For å forhindre at dette skjer, kan man innføre noen form for sentraliserte autentiseringsmekanismer.

4.5.5 Denial of Service angrep (DoS angrep)

Denial of Service-angrep mot trådløse LAN kan omfatte alt fra enkle radiointerferens-angrep til mer spissfindige angrep som mot en mobil enhet eller et aksesspunkt. En trådløs klient kan for eksempel oversvømme en annen klient med pakker slik at den drukner i informasjonsoverfloden.

Det blir regnet som umulig å sette opp et nettverk som ikke kan være utsatt for noen DoS-angrep. Det gjelder bare å være klar over at de eksisterer for å redusere skadene og være i stand til å gjenkjenne og spore de tilbake til kilden.

4.6 Drøfting

Trådløse nettverk er mer enn noe annet nett, avhengig av gode mekanismer for autentisering, kryptering, dataintegritet og konfidensialitet. Det vil i alle trådløse LAN være mulig å avlytte de signalene som sendes i luften. Her vil kryptering spille en sentral rolle for at en angriper ikke skal få innsyn i lesbare data etter avlytting. Et trådløst nett vil aldri bli 100 % sikkert, men det finnes en rekke sikkerhetstiltak man kan benytte seg av for å hindre at sensitive data havner på avveie. I tillegg til radiogrensesnittet, vil det være mulig for en angriper å bryte seg inn hos en trådløs klient, et aksesspunkt eller rett og slett koble seg opp mot det sikrede nettet hvor sensitive personopplysninger lagres hos SSA.

IT-avdelingen ved SSA definerer hele sitt datanettverk som sikkert, også det trådløse nettet. Dette står i sterk kontrast til Datatilsynet som mener at trådløse LAN er i utgangspunktet å regne som usikre nett. Slik det er vist i kapittel 4.5 kan både MAC-adresse autentisering og 128-bits WEP-kryptering knekkes av en angriper på en enkel måte. For at mobil EPJ hos SSA skal kunne regnes som sikkert nok, bør krav fra Datatilsynet tilfredsstilles. En kombinasjon av sikkerhetsmekanismene som drøftes under, vil være en forutsetning for at det trådløse nettverket kan bli sett på som en utvidelse til det sikre nettet, slik Figur 4-10 viser.

En måte å trenge seg inn i et trådløst nettverk uten å bruke tekniske hjelpemidler, er rett og slett å stjele en trådløs enhet tilhørende nettverket. I et hektisk sykehusmiljø hender det ofte at datautstyr forlates innlogget. Det hjelper da ikke hvor gode

sikkerhetsmekanismer nettet er satt opp med, når en angriper får fri tilgang til systemet. Dersom de ansatte ved SSA hadde fått hvert sitt smartkort som måtte brukes til innlogging i datasystemet, måtte brukerne vært tilstede når datautstyret brukes.

En datamaskin vil normalt inneholde en del data, og bør av denne grunn ikke komme på avveie. Ved bruk av tynnklient, vil det ikke bli lagret noe data hos klienten slik at denne faren blir eliminert. På markedet i dag eksisterer det programvareløsninger som er lite ressurskrevende, og som kan implementeres på både PDA, tablet PC og bærbar PC.

For å hindre en angriper å koble seg opp mot et aksesspunkt, kan man deaktivere annonseringen av et aksesspunkts SSID. En eventuell angriper må da vite SSID for å finne aksesspunktet. Ettersom man kan snappe disse dataene enkelt med gratis avlyttingsprogrammer fra en gyldig forbindelse, må denne løsningen sees på som et svakt sikkerhetstiltak. I alle fall må man kombinere dette tiltaket med sikker kryptering, som gjør SSID vanskeligere å få avlyttet.

Dersom en avlogget klient kommer på avveie, vil en angriper kunne skaffe seg gyldig brukernavn og passord ved å bruke et pakkesnifferprogram som for eksempel Ethereal, beskrevet i kapittel 4.5. For å hindre angripere i å få innsyn i data som sendes i luften, er det nødvendig å kryptere datatrafikken. Det viser seg å være stor variasjon i kvaliteten på de krypteringsmetodene som finnes. WEP-kryptering har vist seg å være blant de svakeste teknikkene, selv om sikkerheten øker proporsjonalt med nøkkellengden. Ved 128-bits nøkkel må det samles mye data, og det tar litt tid å knekke koden som er beskrevet i kapittel 4.5. I utviklingsprosjektet hos SSA ble det forsøkt med Kerberoskryptering, men konfigureringsproblemer har ført til at denne metoden sees på som lite fleksibel og derfor uegnet. Derimot finnes det i dag IPSec-baserte VPN-løsninger, som er enkle å konfigurere.

Blant de sterkeste krypteringsmetodene som finnes på markedet i dag, er mekanismer som er implementert i ulike VPN-standarder. Slik Figur 4-10 viser, vil det være mulig å sette opp en VPN-forbindelse mellom klientene og brannmuren inn mot det sikre systemet. Et VPN basert på IPSec vil støtte kryptering på nettverkslaget i OSI-modellen.

802.1x autentisering, ved hjelp av en AAA-server som RADIUS, er i sin enkleste form basert på link-lags autentisering. Svakheten til denne metoden vil være MAC-adressen som kan forfalskes av angripere. Dersom man baserer denne prosessen på EAP-TLS, vil man i tillegg benytte seg av sikkerhetsmekanismer som finnes på transportlaget. Ved innføring av smartkort vil autentiseringen foretas basert på elektronisk ID som er lagret på kortet. Smartkort eliminerer behovet for å sende ID over nettet. Ettersom det digitale sertifikatet må finnes i fysisk form hos klienten, vil det ikke være mulig for en angriper å lage en kopi som forklart i kapittel 4.4.5. Det finnes i dag gode metoder både for at brukeren skal kunne autoriseres mot en dataenhet og at dataenheten skal autentiseres mot nettet. Sistnevnte kan gjennomføres ved hjelp av EAP-SIM som opprinnelig er en standard for WiFi-autentisering for GSM [29]. Dersom autentiseringsdataene ligger på en lokal

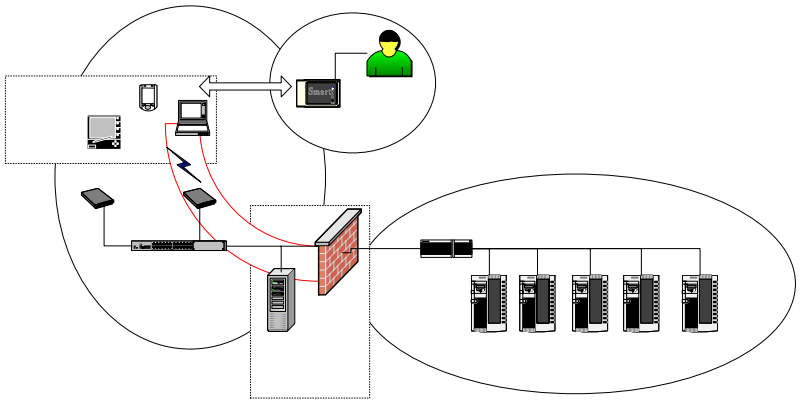
autentiseringsserver isteden for HLR/AuC, vil det med denne algoritmen være mulig å sikre tilgang på lokale servere.

Datatilsynet stiller konkrete krav til at informasjonssystemer som inneholder sensitive personopplysninger, skal sikres gjennom minst to barrierer. Dersom sikker autentisering kan sies å være den ene, vil en brannmur sikre for den andre. Ved å benytte seg av brannmur, kan man godkjenne visse forbindelser inn i et sikret nett, for eksempel VPN-forbindelser. Man kan konfigurere slik at bestemte brukere eller brukergrupper kun får tilgang til de data de er autorisert til å få innsyn i. For å hindre angrep direkte mot de mobile enhetene, kan disse sikres med personlig brannmur. Dersom man skal kombinere brannmur med VPN-løsning, vil kryptering og dekryptering være ressurskrevende for prosessorene. Denne løsningen vil dermed gå tregt og er derfor uegnet hos klientene.

4.7 Sikkerhetsmessige løsninger for et trådløst helsenett

Det vil i et trådløst nett på et sykehusmiljø være viktig å ta hensyn til autentisering, autorisasjon, konfidensialitet, dataintegritet og angrep på de mobile enhetene.

Som et resultat av evalueringen i kapittel 4.6, viser Figur 4-10 hvordan nettverket på SSA kan utvides for å øke sikkerheten rundt mobil EPJ hos SSA. Ut fra Datatilsynets krav er det viktig å utarbeide ulike soner med forskjellige sikkerhetsnivåer og tiltak.



Figur 4-10: Nettverksstruktur rundt trådløse LAN hos SSA utvidet med sikkerhetselementer

For å kontrollere trafikken inn i det sikrede nettet, anbefales bruk av brannmurteknologi for å kontrollere tilgangen fra den trådløse sonen. En solid AAA-server, for eksempel RADIUS, bør benyttes for autentisering før man får tilgang gjennom brannmuren. Basert på denne sikre autentiseringen, settes det opp VPN-forbindelse mellom en brannmur og en mobil klient. Det vil sikre en meget god kryptering av datatrafikken i det trådløse nettet. På klientsiden betyr dette at det må installeres en VPN-klient programvare. Inn mot nettverket derimot kan det settes opp et enkeltstående produkt med integrert løsning for RADIUS, IPSec basert VPN og

brannmur. Et eksempel på et slikt produkt er SonicWall GX650 FireWall som er passende i store selskap hvor mye data skal håndteres.

Smartkortløsningen som anbefales brukt i et fremtidig system, benyttes både for å autentisere en bruker mot en PDA, tablet PC eller bærbar PC. I tillegg finnes det algoritmer som sikrer autentisering av de mobile enhetene mot nettet.

I et stort og uoversiktlig sykehusmiljø vil det være store muligheter for at noen av de mobile klientene havner på avveie. For å forhindre at sensitive data samtidig blir borte, anbefales bruk av tynnklient, som beskrevet i kapittel 4.4.10 for å hindre at data lagres på en PDA, tablet PC eller en bærbar PC. Dersom dette blir kombinert med personlige smartkort, vil det være utilstrekkelig for en angriper å snappe opp en brukers passord, for kortet må også være tilstede. Sistnevnte hindrer i tillegg faren som foreligger når datautstyret forlates ferdig innlogget.

5 Utviklingsmuligheter for mobil EPJ i et helsemiljø

5.1 Funksjonelle utviklingsmuligheter

I spørreundersøkelsen og intervjuene kom det tydelig frem at brukerne mente det var flere forbedringer som kunne gjøres på systemet for at det skulle bli bedre og lettere å bruke. Flere av forbedringene som ble påpekt, er rene feil i systemet, mens andre gikk på manglende funksjonalitet eller at denne kunne forbedres. Forbedringer som ble foreslått av leger og sykepleiere etter at utviklingsprosjektet ble avsluttet, er gjengitt i kapittel 3.4.7 og 3.5.9. Basert på disse tilbakemeldingene, er det under foreslått mulige utviklingsmuligheter for mobil EPJ i et sykehusmiljø.

Lettere å finne frem pasienter med InfoPack_Helse

InfoPack_Helse har allerede en funksjon for raskt å finne frem pasientene ved at brukerne kan bruke en ”Gå visitt”-funksjon, som gjør at pasienter fra riktig avdeling eller seksjon kan velges direkte fra en egen nedtrekksliste. En ulempe med denne funksjonen, er at nedtrekkslisten vil forsvinne om brukeren navigerer vekk fra de pasientrelaterte sidene.

En måte å løse dette på, vil være å benytte seg av strekkodeleseren som finnes på PDA-ene, slik at brukeren kun skanner en strekkode og får all informasjon om den pasienten opp på skjermen automatisk. Strekkoden kan for ekspempel plasseres på pasientens armbånd, men brukerne tror pasientene fort kan føle ubehag med dette og føle seg som en vare. Det vil da være mer etisk riktig å plassere strekkoden vekk fra pasienten, for eksempel på sengen, slik at skanningen foregår på avstand fra pasienten.

Få den medisinske kurven på elektronisk form

Av både spørreundersøkelsen og intervjurunden, går det fram at både leger og sykepleiere mener at å få pasientenes medisinske kurve på elektronisk form, vil gjøre at mobil EPJ blir mer nyttig. På den måten slipper de å ha med seg både papirbasert og elektronisk informasjon rundt på visitten. Kurven brukes mye, noe som fører til at det kan spares mye tid på registreringsarbeidet om denne kommer på elektronisk form. Leger og sykepleiere kan registrere informasjon direkte på enheten, og informasjonen vil i det samme øyeblikket være tilgjengelig for alle.

Om kurven hadde vært på elektronisk form, kunne også sykepleiere lagt temperatur-, puls- og blodtrykksmålinger direkte inn i systemet ved hjelp av de bærbare enhetene, slik at også disse ble digitalisert.

Å ha den medisinske kurven på elektronisk form, krever en oppetid på 100 % siden denne er sentral i all behandling av pasienten. Uten kurven vil ikke leger eller sykepleiere ha noe informasjon om pasienten, og pasientbehandlingen hindres.

Få brukergrensesnittet på InfoPack_Helse mest mulig likt DIPS

Brukerne av EPJ og mobil EPJ har forskjellige forutsetninger for daglig bruk av IT. Det varierer både i alder og interesse, og spenner fra ivrige brukere som fort lærer seg nye ting, til eldre mennesker som ofte ikke er vant til å bruke datamaskiner. Det er viktig at programvaren blir lagt til rette for alle brukerne, også de minst erfarne. Bruk av DIPS har etter en tid kommet godt inn i arbeidsrutinene, og de fleste føler seg komfortable med bruken av det. Ved innføringen av InfoPack_Helse, følte flere av brukerne at det ble for mye å lære seg.

En utfordring på dette området er å utvikle InfoPack_Helse til å ligne mer på DIPS i oppsett og begreper. På den måten vil brukerne få en følelse av at de har noe kjennskap til programmet fra før. Den logiske oppbygningen bør også være lik DIPS.

Programvare må baseres mest mulig på direkteknapper i stedet for menyer

For å spare plass på skjermen, har man i InfoPack_Helse valgt å bruke rullegardinmenyer i stedet for direkteknapper for hver funksjon slik som i DIPS. Flere brukere har ønsket at InfoPack_Helse også skal benytte disse direkteknappene i større grad, fordi de føler at det er for tungvint og tregt å måtte gå inn i hovedmenyen for hver enkelt funksjon en skal hente opp. Problemet er at direkteknapper i stor nok størrelse vil ta mye plass på skjermen, og med en PDA som fra før har begrenset skjermplass, vil dette føre til at plassen å bruke, blir mindre. Hvis en på PDA skulle hatt like mange direkteknapper som i DIPS, ville det forminske plassen til videre bruk.

En annen mulighet vil være å benytte en kombinasjon av direkteknapper og rullegardinmenyer ved å ha noen få og dynamiske direkteknapper for de utvalgte og mest brukte funksjonene, og i tillegg ha godt tilpassede rullegardinmenyer for å bruke de andre funksjonene. På denne måten vil de funksjonene som brukes mest, alltid være lett tilgjengelig, mens de andre funksjonene vil ligge tilgjengelig på den tilpassede rullegardinmenyen.

Under utviklingsprosjektet ble det benyttet en gammel modell av tablet PC som benyttet InfoPack_Helse. Ved bruk av nyere utgaver av tablet PC, vil det være mer aktuelt å benytte seg av DIPS. Det vil av denne grunn være mer aktuelt å sammenligne tablet PC med bærbar PC. Størrelsen på skjermen er likevel ikke på nivå med en bærbar PC.

Digital diktering

Modulet for digital diktering i InfoPack_Helse eksisterer og er implementert i installasjonen på SSA. Det var meningen at diktafonen skulle bli brukt på PDA, men ettersom lydkvaliteten ikke var god nok, ble ikke tjenesten tatt i bruk. Digital diktering er en funksjon som brukerne føler er viktig, og som bør være i drift i et ferdig utviklet system. Personalet er avhengig av å kunne diktere, og om dette ikke er implementert i mobil EPJ, vil brukerne likevel gå rundt med en vanlig diktafon. Mangel på digital diktering har ført til at brukerne har sett mindre nytteverdi ved bruk av PDA.

Selve problemet med lydkvaliteten er det en enkel løsning på. For å få tilfredsstillende lydkvalitet på opptaket, må det tas i bruk en ekstern mikrofon. En

mulighet vil være at det brukes en bærbar handsfree ved bruk av diktafon, slik at man også kan høre på opptaket hvis man ønsker.

Det var ikke planlagt i prosjektet at tablet PC-ene skulle brukes til diktering. Dette er likevel teknisk mulig, og ved bruk av bærbar handsfree vil dette være en fullgod løsning. På den bærbare PC-en er det ikke like lett. Denne kjører DIPS programvare, og digital diktering har ikke vært implementert i DIPS på SSA. For å kunne bruke digital diktering på den bærbare PC-en, må SSA oppgradere sin versjon av DIPS til en nyere versjon om inneholder modul for digital diktering.

Fra mange av sykepleierne ble det ytret ønske om å kunne lese inn korte beskjeder i diktafonen, og sende disse til kontoret i stedet for skrivestua, i tillegg til å skrive inn korte beskjeder og sende til kontoret. På denne måten kan man unngå at beskjedene blir skrevet på små lapper som blir liggende i lommer og kan mistes, eller flyter rundt på vaktrommene. En kan også sende disse beskjedene under visittrunden, slik at kontorpersonalet kan komme raskere i gang med arbeidet, for eksempel ved utskrivning av en pasient.

Bedre system for medikamentstyring

Det er ønskelig med et elektronisk system for å holde orden på medisinene. Funksjoner i medikamentstyringen vil dreie seg om både å styre medisinlager og beholdning, samt medisinering av pasienter.

I første omgang vil det være aktuelt å benytte PDA til å registrere hvilke medisiner som er gitt til de forskjellige pasientene. Man vil dermed få en kvittering på at riktig medisin er gitt til riktig pasient.

Etter hvert bør det også bli mulig å benytte systemet til å registrere medisiner inn og ut fra lageret. Det blir dermed lettere å holde oversikt over medisinbeholdningen. Systemet må da inneholde informasjon om medisineringen til hver pasient og en liste over alle medisiners strekkode og egenskaper.

Ved innlogging må man komme direkte inn der man var ved forrige utlogging

Ved en hektisk hverdag på sykehuset, er man avhengig av at systemet fungerer effektivt og raskt. Det er viktig at effektiviteten opprettholdes eller økes etter innføringen av mobil EPJ. For at brukerne skal slippe å bruke mye tid på innlogging, er det derfor viktig at når de logger inn, kommer de direkte inn i systemet der de var ved forrige utlogging. På denne måten vil ikke innlogging etter brudd i dekning eller en uønsket avstengning av enheten ta så mye tid.

Systemet må også være basert på en rutine som gjør at brukeren kun trenger å logge seg inn en gang. En bruker skal kun logge seg på nettverket, og bør etter det ha tilgang til alle programmer og tjenester uten å måtte logge seg inn spesifikt på disse.

Sykepleiedokumentasjon

Det har til nå ikke vært mulighet for å lagre sykepleiedokumentasjon direkte i DIPS eller InfoPack_Helse. For å frigjøre seg fra papirbaserte systemer og få alt digitalisert, er dette viktig. På den måten har brukerne kun de mobile enhetene og de

stasjonære PC-ene å forholde seg til. Denne funksjonen er i midlertidig klar i nye versjoner av DIPS, og InfoPack_Helse bør også utvides til å inkludere dette.

5.2 Konsekvenser av tilfredsstillende sikkerhetsmekanismer

Det er viktig at de økte sikkerhetsmekanismene som følger med installasjonen av et trådløst nettverk, ikke medfører mer kompliserte og tidkrevende rutiner for brukerne. Ingen av sikkerhetsmekanismene som er foreslått i kapittel 4.7 vil ha noen negativ påvirkning på anvendbarheten av det mobile EPJ systemet, men enkelte tiltak vil føre til et endret bruksmønster i forhold til datasystemene i et sykehusmiljø.

Smartkort

Innføring av smartkort i forbindelse med autentisering er i følge intervjuobjektene en god og enkel løsning. På denne måten kan de ha dette kortet med og sette det inn i en kortleser i enheten ved pålogging. Her ser brukerne for seg at de skal bli logget inn direkte ved innsetting av smartkortet og være i gang uten noen form for passordinntasting, men det vil i praksis bli implementert med en kode for å aksessere nøkkelen som ligger i smartkortet. Innføring av smartkort bør også gjelde det stasjonære datasystemet og låsekortene til de ansatte. Det bør nemlig fokuseres på at det skal bli færrest mulig forskjellige kort å ha med seg rundt.

Ved bruk av smartkort kan det lange og komplekse passordet byttes ut med en kortere og enklere PIN-kode som er enklere å huske. Denne innføringen bidrar dermed til å redusere faren for at passord blir notert ned på lett tilgjengelige steder, for eksempel en lapp klistret til skjermen.

I tillegg hindrer smartkortløsningen at ferdig innloggede dataenheter forlates i et hektisk sykehusmiljø, siden kortene følger brukerne fra maskin til maskin.

Autorisering og gode rutiner for pålogging

Uansett hva slags påloggingsmekanismer som blir tatt i bruk, er det viktig at systemet støtter felles innlogging, slik at brukerne kun logger seg på nettet en gang og får med det tilgang til alle applikasjoner han/hun er autorisert til å bruke. Denne typen rollebasert aksesskontroll sikres best ved hjelp av sikkerhetsmekanismer basert på digital ID. Dette er viktig for å opprettholde effektiviteten, og med brukernes arbeidsrutiner med korte oppslag og lange inaktive perioder, blir det ofte tidsavbrudd. Ved innlogging må brukeren også komme direkte inn der han/hun var ved utlogging. Med slike mekanismer vil det være mulig å korte ned tiden for tidsavbrudd for påloggingen, slik at sikkerheten økes ytterligere. Det vil ved full implementasjon bli mange enheter, følgende vil en del enheter til enhver tid bli liggende uten tilsyn.

VPN og brannmur

For å hindre avlytting av data, er det anbefalt å sette opp en kryptert VPN-tunnel fra brannmuren i nettet og helt ut til klientene. Selve tunnelen har ingen konsekvens for brukerne av de mobile enhetene, men det er klienten selv og brannmuren som må ta seg av kryptering og dekryptering. Ved kombinert personlig brannmur og VPN ute hos klientene, vil kryptering og dekryptering være ressurskrevende. For brukerne

oppleves dette ved at systemet går tregt. I et fremtidig system, anbefales derfor ikke klienten å benytte seg av personlig brannmur.

Tynnklient

I et hektisk sykehusmiljø kan de mobile enhetene fort bli liggende uten tilsyn, noe som kan føre til at noen av disse blir stjålet. Bruk av tynnklient medfører at ingen data blir lagret på enhetene. Sensitiv informasjon havner med dette ikke direkte i hendene på den som har stjålet en av de mobile enhetene. Dette vil ikke medføre noen stor betydning for brukerne av enhetene, men ved bruk av tynnklient vil alle prosesser og applikasjoner bli kjørt på serveren. Prosesseringen på enhetene vil da bli minimal, og vil kompensere for den tapte prosessorkraften som går med til kryptering og dekryptering av VPN-tunnelen. Rutiner for å sikre at det mobile utstyret ikke havner på avveie, er uansett et av de viktigste tiltakene.

Ny trådløs LAN teknologi

Dersom et mobilt EPJ system skal settes i drift i dag, bør man gå videre fra IEEE 802.11b, som var brukt i utviklingsprosjektet hos SSA, til IEEE 802.11a [8]. Rent sikkerhetsmessig vil ikke denne overgangen føre til noen endringer. Tilfredsstillende sikkerhetstiltak bør baseres på metoder som illustrert i kapittel 4.7. Derimot gir den nye standarden støtte for roaming og handover, noe som gir brukerne større bevegelsesfrihet. I tillegg øker antall kanaler fra tre til åtte, slik at man kan ha flere overlappende soner med flere tilkoblede brukere, noe som gjør at kanalplanlegging ved full installasjon blir enklere.

Brukere opplevde at det enkelte ganger tok lang tid å laste sidene. Fordi systemet blir mye benyttet under visittiden, er det derfor viktig at det trådløse nettet er overdimensjonert i forhold til vanlig bruk. Ved en overgang, vil hastigheten blir økt fra 11 Mbps til 54 Mbps.

5.3 Drøfting av utviklingsmuligheter

Behov og ønsker i forhold til informasjonsbehandlingen, har vist seg å være veldig ulike hos de ulike brukergruppene ved SSA. Basert på stilling og avdeling, er det forskjellige oppgaver som skal utføres. I tillegg vil alder og interesse for data være med på å styre motivasjonen for nye datasystemer. PDA, tablet PC og bærbar PC har vist seg å være egnet til forskjellige arbeidsoppgaver og derfor også til forskjellige brukergrupper ved sykehuset.

Spørreundersøkelse og intervjuer viser at PDA i større grad dekker sykepleiernes behov for informasjonsbehandling enn legenes behov, Figur 3-12. Sykepleierne skulle helst hatt DIPS direkte på PDA, men ettersom skjermstørrelsen gjør dette umulig, må InfoPack_Helse benyttes som et grensesnitt mot informasjonen i DIPS-databasen.

Mange brukere av PDA mente at denne fungerte best til små oppslag i lister og bestilling av prøver, kapittel 3.5.1. PDA er hendig å ha med seg, og er godt egnet til bestilling og avlesning av resultater fra prøver. Muligens er PDA et verktøy for sykepleiere som kan bringe den med seg til behandling av mindre datamengder.

Dersom den medisinske kurven blir lagt inn på elektronisk form, kan PDA være et nyttig hjelpemiddel for å registrere for eksempel blodtrykk, puls, væskeregnskap og så videre, i systemet.

Forslaget i denne rapporten går ut på å satse på denne bruken for PDA, i tillegg til å utvide bruken når sykepleiedokumentasjon og den medisinske kurven blir elektronisk. Da vil PDA bli et godt hjelpemiddel til å registrere måleresultater og anmerkninger. Diktafonmodulet i InfoPack_Helse bør også tilpasses slik at PDA kan brukes for å sende digitale beskjeder til kontoret.

PDA har allerede digital diktering, med denne har ikke vært i bruk på grunn av for dårlig lydkvalitet, og PDA må derfor utstyres med handsfree. Dikteringsfunksjonen er bygd inn i nye versjoner av DIPS, og kan derfor også etter hvert bli benyttet ved bruk av bærbar PC.

For å få en generell bedring av brukervennligheten på PDA og i InfoPack_Helse, bør disse også utvides til å kunne skanne strekkoder på pasientens seng for raskt å komme inn i pasientens data. På denne måten kan arbeidsrutinene effektiviseres. For lett å finne pasienter når sengen ikke er tilgjengelig, bør også pasientlistene få bedre filtrering, slik at pasientene blir lettere å finne. Listene kan for eksempel filtrere på avdeling, gruppe eller rom. For begge systemene er det viktig med en felles innlogging for alle applikasjoner, slik at det kun er nødvendig å logge inn en gang.

Det blir ved innføringen av et fremtidig system viktig med bra og godt organisert opplæring slik at alle blir trygge på bruken av InfoPack_Helse. De største forbedringsmulighetene er å gjøre programmet enklere å bruke, samt å tilpasse produktet til de arbeidsprosessene som er egnet seg for PDA. Systemutviklerne må også følge visittpersonalet, og utvikle programmet etter deres behov. Etter innføringen, bør det gjøres tilpasninger til de ulike avdelingene.

Flere av legene som ble intervjuet, uttrykte tydelig at PDA var lite egnet til deres bruk, og at bærbar PC var det riktige verktøyet for dem. Bærbar PC hadde større skjerm, kjørte DIPS og hadde tastatur. De synes heller ikke at tablet PC var egnet ettersom denne kjørte InfoPack_Helse og hadde dette programmets begrensninger i tillegg til berøringsskjerm. Dagens tablet PC-er har gjennomgått en betydelig utvikling, og ligner derfor mer på den bærbare PC-en som ble benyttet i utviklingsprosjektet.

I denne rapporten er det i fremtiden satset på to enheter til hvert sitt bruk. Sykepleierne skal ha med seg PDA store deler av tiden, og benytte denne til korte oppslag og registreringer. Bærbar PC skal brukes til å gå visitt. Ulempen med denne løsningen er at brukerne fortsatt må bruke to forskjellige programmer, InfoPack_Helse på PDA og DIPS på bærbar PC.

I DIPS bør en funksjon for full medikamentstyring legges til, slik at medikamentinformasjon, medikamentlogistikk og pasienters medisinering kan registreres og kontrolleres ved hjelp av de bærbare enhetene. Kapittel 5.1 beskriver noen utviklingsmuligheter som bør tilpasses i DIPS. Blant annet bør den medisinske kurven komme på elektronisk form. For brukerne betyr dette at det kun vil være behov for å ha med seg en av de mobile enhetene under visittgang.

De nye tablet PC-ene som finnes i dag er kraftige og har dessuten god nok oppløsning til å kjøre DIPS og PACS over Citrix Metaframe slik den bærbare PC-en har gjort i utviklingsprosjektet. De bærbare PC-ene er fortsatt kraftigere med bedre skjerm enn tablet PC-ene, men det er ventet at denne forskjellen vil jevne seg ut. For de brukerne som vil anvende tastatur, har de fleste nye tablet PC-ene som leveres i dag, mulighet for å klikke på eller brette ut et tastatur. Dersom den medisinske kurven kommer på elektronisk form, vil det kun være behov for å ha med seg en av enhetene, og ikke papirbasert materiell. I et slikt fremtidig system vil tablet PC-en komme ut som den mest egnede. Dette åpner for muligheten til å kun bære med seg denne, i stedet for bruk av bærbar PC på trillebord. Dette gir også mulighet til å velge mellom bruk av tastatur, eller å skrive rett på skjermen med skriftgjenkjenningsprogramvare, slik at håndskriften kommer på skjermen som tekst.

6 Drøfting

Utviklingsprosjektet på SSA ble gjennomført på en måte som stilte store krav til de som skal drive prosjektet videre, både når det gjelder applikasjonsutvikling og sikkerhet. Ideen bak prosjektet var god, og gjennom spørreskjemaer og intervjuer viser det seg å eksistere et behov for et slikt system.

128-bits WEP-kryptering kan enkelt knekkes ved hjelp av gratis sniffe programmer som er tilgjengelig på Internett [31]. Klarer man klarer å knekke koden, vil man kunne lese datastrømmer som går i luften. Gyldige brukeres MAC-adresser vil da komme frem i klartekst, og en angriper vil kunne forfalske sin egen MAC-adresse. Dersom MAC-adresse filtrering er eneste tilgangskontroll, må nettet av nevnte grunner regnes for usikkert.

For å beskytte seg mot direkte angrep på de mobile håndholdte enhetene, vil det være mulig å ta i bruk personlig brannmurløsning på klientsiden.
Kryptering og dekryptering er meget ressurskrevende når brannmur benyttes sammen med VPN. For at datatrafikken ikke skal gå tregt, anbefales det å kutte ut brannmurløsningen på klientsiden. VPN regnes blant de sikreste krypteringsteknikkene som finnes for trådløse LAN. Denne mekanismen bør heller benyttes sammen med tynnklient for å hindre at data lagres på de mobile klientene. På nettverkssiden, finnes det integrerte VPN/brannmurløsninger som kan basere seg på IPSec. Denne løsningen er fleksibel og enkel å konfigurere. Dersom man i tillegg baserer det trådløse nettverket på en form for sikker autentisering av både brukere og utstyr, kan systemet regnes som sikkert nok i forhold til krav som stilles fra Datatilsynet. Det finnes flere sentraliserte autentiseringsalgoritmer som støttes av blant annet RADIUS og Kerberos. På høyeste nivå av sikkerhet for autentisering, anbefales bruk av smartkort eller digital ID.

Det er viktig for innføringsprosessen av et mobilt EPJ system at sikkerhetsmekanismene ikke går på bekostning av anvendbarheten eller funksjonaliteten til systemet. Det er også viktig at systemet er utviklet med formål om å sikre nytteverdi for brukerne. Under utviklingsprosjektet viste det seg at InfoPack_Helse ikke opplevdes å være godt nok utviklet på områder som var viktig for å sikre brukeraksept [4]. En svakhet ved spørreundersøkelsen og utviklingsprosjektet hos SSA, er at det var liten bruk av de mobile enhetene. Dette resulterte i at hovedtyngden av tilbakemeldingene, kom fra de mest interesserte og motiverte brukerne. Det vil være naturlig å anta at de som ikke benyttet seg av systemet, heller ikke opplevde like stor nytteverdi som de hyppige brukerne.

Ved innføring av et lignende system, vil det være viktig med en tettere oppfølging fra systemutviklerne. Når uerfarne brukere i et hektisk arbeidsmiljø opplever at systemet ikke fungerer slik de hadde ventet seg, reduseres motivasjonen raskt. Det er tydelig at systemet må tilpasses arbeidsprosessene, og ikke motsatt. I tillegg må systemet virke raskere enn hva de er vant med. Leger og sykepleiere er nemlig ikke interessert i nye datasystemer for teknologiens skyld. Det vil være mulig å sette i drift en rekke nye applikasjoner i et mobilt EPJ system, men det er viktig å skille på hvilke

arbeidsprosesser som er best egnet for PDA, tablet PC eller bærbar PC. Eksempelvis vil PDA egne seg best til enkle registreringer og gi innsyn i små mengder data, mens tablet PC og bærbar PC konkurrerer om å bli tatt i bruk til mer omfattende oppgaver som å lese større dokumenter.

7 Konklusjon

Innføring av mobil EPJ i et sykehusmiljø gjør det mulig for helsepersonell å registrere og få innsyn i pasientinformasjon hvor pasientene befinner seg, gjerne under visitt. I et sykehusmiljø hvor papirbaserte pasientjournaler erstattes med journaler i elektronisk form, har det vist seg å være et behov for mobil tilgang til disse dataene ute ved pasientene. Ved å gjøre all databehandling ute hos pasienten, kan man i et hektisk sykehusmiljø spare mye tid. Et slikt system er nødt til å tilpasses visittpersonalets arbeidsprosesser for at det skal bli benyttet. Hovedutfordringene for innføringen ligger hos IT-avdelingen, som både må ta hensyn til anvendbarhet, sikkerhet og stabilitet.

Anvendbarhetskapittelet i denne rapporten, viste årsaker til liten bruk av mobil EPJ under utviklingsprosjektet hos SSA. Resultater fra spørreundersøkelse og intervjuer belyste elementer i TAM-modellen som ikke er oppfylt i tilstrekkelig grad til å sikre bruk. Spesielt gjelder dette funksjonalitet og enkelthet ved bruk. Ved å sammenligne resultatdataene med elementer fra UAM-modellen viser rapporten, på et mer detaljert nivå, i hvilken grad ulike funksjoner oppfattes å ha fungert. På dette nivået ble det avdekket en rekke forskjeller på PDA, tablet PC og bærbar PC, noe som gjorde det mulig å avdekke hvilken enhet som er best egnet til ulike funksjoner.

Prosjektet avdekket at PDA og bærbar PC bør benyttes til ulike formål, og at disse enhetene ikke på noen måte konkurrerer om aksept hos brukerne. Tablet PC har derimot vist seg å være for vanskelig å bringe med seg, sammenlignet med PDA. Samtidig taper tablet PC kampen mot bærbar PC, ettersom den har mindre skjerm og mangler både tastatur og nyttige funksjoner i DIPS. PDA bør benyttes til enkle registreringer og behandling av små mengder data. På grunn av liten størrelse på enhetene, vil disse være egnet for sykepleiere å bringe med seg også utenom visitten. Bærbar PC må derimot transporteres på trillebord, og er derfor best egnet til visittgang. De medisinske kurvene må over på elektronisk form for at det skal ha noen hensikt å benytte tablet PC. Det blir for tungvint å bære med seg både tablet PC og papirdokumenter på visitt. Dagens størrelse og yteevne på tablet PC, gjør det mulig å benytte seg av DIPS og tastatur.

Sikkerhetsmekanismene som har vært implementert under utviklingsprosjektet, kan ut fra Datatilsynets anbefalinger vurderes til å være i svakeste laget. Prosjektet avdekket godt tilgjengelig utstyr, som kunne gitt en angriper innsyn i sensitive data gjennom det trådløse nettet i utviklingsprosjektet på SSA. Bruk av brannmurteknologi inn mot sikker sone sammen med solid autentisering av både av bruker og utstyr, vil sikre Datatilsynets krav til to barrierer. Det anbefales i tillegg bruk av integrert brannmur med VPN-funksjonalitet og sikker autentisering basert på IPSec og IEEE 802.1x. Sistnevnte åpner muligheter for enda sikrere autentisering i et fremtidig datasystem, basert på smartkort. Arbeidet som gjenstår med innføringen av smartkort er omfattende, og vil i stor grad påvirke sykehusansattes hverdag. Smartkortløsningen bør ved innføringen også omfatte det stasjonære datasystemet.

Referanser

Datoene i klammeparentes viser datoen linken sist er aksessert.

[1] Amtsygehuset i Roskilde, DSI Institut for Sundhetsvæsen, KMD Dialog
Nytteværdi af EPJ, oktober 2001

[2] Hidenori Shinno, Hitoshi Hashizume, Hayato Yoshioka og Kenji Itoh
Product development methodology for machine tools (Usability analysis of man-machine linterface)
JSME international journal nr. 3, 2002

[3] Shirley Taylor og Peter A. Todd
Understanding information technology usage: A test of competing models
Information systems research, juni 1995

[4] Fred D. Davis
User acceptance of information technology: System characteristics, user perceptions and behavioral impacts
Internation journal of man-machine studies, 1993, 475-487

[5] Symbol
Portable Pen Terminal 2800 Series technical specifications
http://www.symbol.com/products/mobile_computers/mobile_ppc_ppt2800.html [19. mars 2003]

[6] Symbol
Access Point 4121 technical specifications
http://www.symbol.com/products/wireless/ap_4121_11.html
[19. mars 2003]

[7] Fujitsu
Stylistic LT P-600 tablet PC technical specifications
http://www.fujitsu-siemens.com/rl/products/pentablets/stylisticltp600.html
[19. mars 2003]

[8] DCM Technologies
White paper on IEEE 802.11a
http://www.dcmtech.com/802-11aTechnology.pdf [20. mars 2003]

[9] Internet Security Systems
Wireless LAN Security, 2001
http://documents.iss.net/whitepapers/wireless_LAN_security.pdf
[20. mars 2003]

[10] DIPS ASA
http://www.dips.no [3. april 2003]

[11] Medicom AS
www.medicom.no [3.april 2003]

[12] Interlink Networks, John Vollbrecht Founder
Wireless LAN access control and authentication, 2000
http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf [4. april 2003]

[13] Intel Information Technology
VPN and WEP, januar 2003
http://www.intel.com/eBusiness/pdf/it/wp021306.pdf [4. april 2003]

[14] NetScreen Technologies Inc.
Securing wireless LANs, januar 2003
http://www.netscreen.com/techpubs/pdf/wp_Securing_Wireless_LANs_with_NetScreen_final_1_21_03.pdf [4. april 2003]

[15] TeleChoice
IPSec VPNs-Ready for prime time, september 2002
http://www.switchlink.be/Security/pdf/IPSec_VPN.pdf [4. april 2003]

[16] Fred D. Davis, Richard Bagozzi & Paul Warshaw
User acceptance of computer technology: A comparison of two theoretical models, Management Science, 1989

[17] Martin Fishbein & Icek Ajzen
Belief, attitude, intention and behavior: An introduction to theory and research, Addison-Wesley, 1975

[18] Fred D. Davis
Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly, 1989

[19] Gerd Gulstad
Prosjektplan: Mobil EPJ i rutiner rundt visittgang, Aust-Agder sykehus HF, 28. april 2002

[20] Knut Lundeby (Ed.)
Knowmobile: Knowledge access in distributed training, mobile opportunities for medical students, University of Oslo, 2002
http://www.intermedia.uio.no/prosjekter/knowmobile/ [28. april 2003]

[21] Datatilsynet 07.98
Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger
http://www.datatilsynet.no/dtweb/attachment/786/TR100_98.pdf
[28. april 2003]

[22] Ethereal
http://www.ethereal.com [30. april 2003]

[23] Airsnort
http://airsnort.shmoo.com/ [30. april 2003]

[24] Kurt Lekanger
Mitt dataleksikon, IDG Norge Books, 2001
http://www.pcworld.no/dataleksikon [30. april 2003]

[25] Mpirical
Companion version 5.1 reference guide
http://www.mpirical.com/companion/mpirical_companion.html [1. mai 2003]

[26] Rune Fensli, HiA
Wireless Local Area Network (WLAN) og sikkerhet, 2003
http://fag.grm.hia.no/runef/DAT2950/Uke_14/WLAN_sikkerhet.zip

[27] Articsoft
Introduction to Public Key Infrastructure, 2003
http://www.articsoft.com/wp.pki_intro.htm [19. mai 2003]

[28] Carry L.Peterson & Bruce S.Davie
Computer networks a system approach, 2000, s. 570-616
Morgan Kaufmann, San Francisco USA

[29] Gemplus
Secure WLAN solutions for enterprice mobility, 2002

[30] What is a VPN? Explaining Virtual Private Networks
http://findvpn.com/articles/what.php [19.mai 2003]

[31] Sandvik, Andenæs, Valle, Søiland, Aadland & Vaaland, 2001
WLAN IEEE 802.11b

[32] AXIS Communications
Prismdump
http://developer.axis.com/software/tools/ [19. mai 2003]

[33] Andrew S. Tanenbaum
Computer Networks, 1999
Prentice Hall PTR

[34] Kurt Birkeland, Kube Rådgiving
Erfaringer med Mobil EPJ i rutiner rundt visittgang, 2003
Medicom AS

[35] Johannessen, A. og Tufte, P.A.

Introduksjon til samfunnsvitenskapelig metode, 2002
Abstrakt forlag, Oslo.

[36] Medicom AS
InfoPack_Helse Brukermanual, versjon 1.0.1, november 2002

[37] Citrix
Citrix MetaframeXP Presentation Server for Windows, 2003
http://www.citrix.com/site/resources/dynamic/salesDocs/MetaFrame_XP_Features_Overview_4_03.pdf [19. mai 2003]

[38] Proactive
http://www.pro-active.fr/products/springcard-cf/ [19. mai 2003]

[39] Fensli, R., Torstensen, H.
Security aspects of wireless medical computer networks. A proposal of combined security actions, 2003
Scandinavian Conference in Health Informatics, 12. juni, Arendal, Norway

[40] Medicom
Presentasjon Sørlandets Kompetansefond, oktober 2002

[41] Tom Hemming Karlsen & Vivian Eikestad
Organisasjonsutvikling og gevinstrealisering knyttet til elektronisk pasientjournal ved medisinsk avdeling, Aust-Agder sykehus HF, april 2002
Sosial- og Helsedepartementet
http://kvalis.ntnu.no/PublicDocs/OGASA [20. mai 2003]

[42] Institute of Electrical and Electronics Engineers, Inc.
Specific requirements P802.11 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999

[43] Breeze Wireless Communications Ltd.
IEEE 802.11 Technical Tutorial
http://www.breezecom.com [20. mai 2003]

[44] The Internet Engineering Task Force
SOCKS Protocol Version 5, 1996
http://www.ietf.org/rfc/rfc1928.txt [22. mai 2003]

Liste over forkortelser med forklaring

3DES	*Triple Data Encryption Standard*	Bruker DES til kryptere, dekryptere og kryptere med tre forskjellige nøkler.
AAA	*Authentication, Authorization and Accounting*	System for å sikkert bestemme identitet og rettigheter til en bruker, samt å logge brukerens aktiviteten.
ACK	*Acknowledge*	Et tegn som bekrefter en forespørsel.
AD	*Active Directory*	Tjeneste for sentralt å behandle og dele informasjon om brukere og nettverksressurser, samt være en sentral autoritet for nettverkssikkerhet.
AES	*Advanced Encryption Standard*	Standard for symmetrisk kryptering av data.
AH	*Authentication Header*	Ekstraheader i IP-pakken brukt i IPSec.
AP	*AksessPunkt*	Punkt for sammenkobling av trådløst og trådbundet LAN.
AS	*Authentication Server*	Verifiserer brukere gjennom login i ved bruk av Kerberos.
BSS	*Basic Service Set*	En samling stasjoner som kan kommunisere over 802.11 trådløst LAN.
CA	*Certificate Agent*	Tiltrodd tredjepart som bekrefter validiteten og identiteten av enheter i en offentlig nøkkel-utveksling.
CRC	*Cyclic Redundancy Check*	En metode til å oppdage feil i en overført datablokk.
CSMA/CA	*Carrier Sense Multiple Access/ Collision Avoidance*	En metode for å aksessere et nettverksmedium.

DES	*Data Encryption Standard*	Metode for kryptering av dokumenter.
DHCP	*Dynamic Host Control Protocol*	Protokoll for distribusjon av nettverksinformasjon til noder.
EAP	*Extensible Authentication Protocol*	Autentiseringsprotokoll som gjør at klienter kan autentisere seg mot en sentral autentiseringsserver.
EAPOL	*EAP Over LAN*	Protokoll for overføring av EAP-pakker mellom klient og aksesspunkt.
EAP-TLS	*EAP-Transport Layer Security*	En variant av EAP. Bruker digitale sertifikater for både klient- og serverautentisering.
EPJ	*Elektronisk Pasient Journal*	System for å lagre og behandle pasientjournaler elektronisk.
ESP	*Encapsulating Security Payload*	Ekstraheader til IP-pakken som inneholder sikkerhetsparameter.
ESS	*Extended Service Set*	En samling BSS som overlapper hverandre og gir begrenset mobilitet.
FTP	*File Transfer Protocol*	Internettgrensesnitt som via TCP/IP gir tilgang til filer og kataloger på en maskin.
HTML	*HyperText Markup Language*	Språk for koding av hjemmesider.
IEEE	*Institute of Electrical and Electronic Engineers*	Forening som står bak utviklingen av en rekke standarder innen data- og elektronikkindustrien.
IETF	*Internet Engineering Task Force*	Den viktigste standardiseringsorganisasjonen for Internett.
IP	*Internet Protocol*	Protokoll på nettverkslaget for kommunikasjon i datanett.
IPSec	*IP Security*	Protokoll designet for å gi IP sikkerhetstjenester.

ISM-bånd	*Industrial, Scientific and Medical-bånd*	Betegnelse for det lisensfrie 2,4 GHz båndet.
LAN	*Local Area Network*	Lokalnett, begrensede datanett.
LEAP	*Lightweight EAP*	En variant av EAP. Autentisering baserer seg på en felles hemmelighet mellom klient og nett, for eksempel brukerens passord.
MAC	*Media Access Control*	Ett av to sub-lag til datalink-laget i OSI-modellen.
MT	*Mobil Terminal*	Enhet med trådløs tilkobling til datanettet.
PAE	*Port Access Identity*	Tjeneste under 802.1x implementert i klienter og aksesspunkt.
PDA	*Personlig Digital Assistent*	Liten håndholdt datamaskin.
PKI	*Public Key Infrastructure*	En asymmetrisk krypteringsmetode.
PRNG	*Pseudo Random Number Generator*	Algoritme som genererer et tilfeldig nummer.
RADIUS	*Remote Authentication Dial In User Service*	Protokoll for sikker autentisering.
RSA	*Rivest Shamir & Adleman*	Offentlig nøkkel-algoritme.
SA	*Security Association*	Involverer utveksling av hemmelige nøkler, samt administrasjon, levetid og utbytte av nøklene.
SQL	*Structured Query Language*	Standard språk for å søke/hente informasjon fra en database.
SSID	*Service Set Identifier*	Aksesspunktets ID i trådløst LAN.
SSL	*Secure Sockets Layer*	Sikkerhetsprotokoll som kjører på TCP/IP.
TAM	*Technology Acceptance Model*	Teoretisk modell.
TCP	*Transport Control Protocol*	En forbindelsesavhengig protokoll for kommunikasjon på datanett.

TGS	*Ticket Giving Server*	Leverer bevis av identitetsbilletter.
TRA	*Theory of Reasoned Action*	Teoretisk modell.
UAM	*Usability Analysis of Man-Machine Interface*	Teoretisk modell.
UDP	*User Datagram Protocol*	UDP er en forbindelsesuavhengig del av TCP/IP-protokoll-suiten.
VLAN	*Virtual Local Area Network*	Det å dele inn ett fysisk nettverk i flere virtuelle nettverk, slik at de opptrer som om de var ulike fysiske nettverk.
VPN	*Virtual Private Network*	Noder som kommuniserer og benytter krypteringsteknologi slik at datene ikke kan leses av uautoriserte brukere.
WEP	*Wired Equivalent Privacy*	En krypteringsteknikk for trådløse nettverk.
WIFI	*Wireless Fidelity*	Standard som garanterer interoperabilitet mellom produkter fra forskjellige leverandører.
WLAN	*Wireless Local Area Network*	Et lokalnettverk (LAN) hvor data overføres trådløst, vanligvis via radiosignaler.

Vedlegg

[v1] Spørreundersøkelse om bruk av mobil EPJ

[v2] Resultater fra spørreundersøkelse om bruk av mobil EPJ

[v3] Intervjuguide om brukererfaringer av mobil EPJ

[v4] Resultater fra intervjuer om brukererfaringer av mobil EPJ