Mobilteknologi til videokommunikasjon ved trygghetsalarmer

av

Reidar Nordby

Masteroppgave i
informasjons- og kommunikasjonsteknologi

Høgskolen i Agder
Fakultet for teknologi

Grimstad
mai 2007

Sammendrag:

Denne rapporten behandler bruk av mobiltelefoner som alarmsentral for hjemmeboende brukere. Studien legger vekt på de forskjellige mobile netts egenskaper og begrensninger som alarmbefordrer. Ønske om videotelefoni som alarm behandles og det foreslås løsninger for å ivareta dette uten å gå på akkord med sikkerhet. Juridiske sider med alarmer og videobilder behandles ut fra to ulike scenario avhengig av om hjelpere er offentlige eller private. Studien er gitt som en del av interregIII prosjektet Grensebroen Arena sin satsning innen emnet "Et år til hjemme" rettet mot eldre hjemme- boende.
Prosjektet har spent over et stort område som det har vært nødvendig å innsnevre underveis. Prosjektet berørte i større grad enn ventet juridiske sider ved offentlig hjelp som nødvendiggjorde en radikal omlegging av de opprinnelige ideene som oppgaven var generert ut fra. Disse juridiske aspektene nødvendiggjorde også en todeling av skisserte løsninger slik at prosjektet nå står med en løsning for privat bruk og en for offentlig bruk. Videre førte dette til at det måtte innføres en meldingstjener for å samle inn lovpålagte opplysninger i forbindelse med alarmer som blir behandlet av offentlig helsepersonell. Samtidig er opplysningene som lovverket pålegger innsamlet av sensitiv natur og må sikres.
Prosjektet er gjennomført med tanke på markedsførte enheter med hensyn til mobiltelefoner og dagens eksisterende mobiltelefoninett. Dette betyr at kommende systemer er unntatt behandling med ett unntak. (UMTS rel-4)
Det behandlede alarmsystemet benytter en fallalarm som eksempel gjennom rapporten. Det er imidlertid ingen grunn til ikke å benytte prinsipper og forslag gitt i denne rapporten til alarmsystem for andre markeder eller funksjoner. Felles karakteristika for denne typen alarmsystem er at alarmen blir samlet inn av en Bt-enhet, befordret av en mobiltelefon for så å bli registrert i en meldingstjener som har myndighet til å avgjøre hvor alarmen skal befordres videre. Arkitekturen med tilbakemelding til meldingstjeneren er også generell.

Gjennom prosjektet er det sannsynliggjort at et slikt alarmsystem som skissert i kapittel 5 og 6 lar seg gjennomføre. Videotelefoni over UMTS er ikke egnet som alarmbærer alene, dette gjelder selv om tjenestekvalitet blir innført i UMTS.

Nøkkelord: Eldre, alarmer, mobiltelefoninett, videotelefoni.

Forord:

Denne rapporten er levert som en del av mastergraden i informasjons og kommunikasjonsteknologi ved Høgskolen i Agder, fakultet for teknologi.
Veiledere har vært Rune Fensli og Magne Arild Haglund. Oppgaven er gitt av interregIII prosjektet Grensebroen Arena.
Jeg ønsker å takke mine veiledere Rune Fensli og Magne Arild Haglund for deres gode veiledning, tålmod og forståelse.
Jeg vil også takke oppgavestillerne i Grensebroen Arena: Per-Thomas Huth og Åge T. Johansen for nyttige innspill og støtte. Videre vil jeg takke deltakerne i brukerpanelet: Ann Karin Helgesen, Kjersti L. Jørgensen, Marit Smittil, Safdar Abbas, Tomas Moe og Per Thomas Huth for å stille opp med gode ideer og innspill.

_____

Reidar Nordby

Innhold:

Figurliste

Tabelliste

1 Introduksjon

Denne rapporten omhandler tryggheten ved å benytte det offentlige mobiltelefoninettet i Norge som befordrer av alarmer basert på videobilder. Denne analysen er ansporet av at vår levealder øker og vi blir stadig flere eldre i samfunnet. Som eldre har vi andre behov enn unge og middelaldrende. Et av behovene som blir sterkere er trygghet når kroppen begynner å svikte. Denne rapporten tar opp eldres behov for kommunikasjon med hjelpepersonale ved en ulykke. Dagens mobilteknologi åpner muligheter for helt nye anvendelser av teknologien innen pleie og omsorg. Nye teknologier som video- kommunikasjon og automatisk alarmdeteksjon tilrettelegger for bruk av ny teknologi innen pleie og omsorgsektoren. Ved å utstyre eldre med avansert mobiltelefon med hensiktsmessig programvare oppnås automatisk kontakt mellom forulykkede og hjelpepersonell. Hvis så denne kommunikasjonen også inneholder levende bilder vil man oppnå tettere personlig kontakt med den forulykkede. Er situasjonen slik at den forulykkede ikke kan svare er dette en alarmsituasjon. Ved en slik situasjon vil hjelpepersonellet kunne hente ut ytterligere opplysninger fra systemet. Rapporten tar for seg sikkerheten ved selve alarmveien gjennom det offentlige mobiltelefon-systemet. Videre beskriver rapporten gjennom scenarios et fleksibelt alarmanlegg og mulig realisering av et utvalg alarmer basert på dagens tilbud i telenettet og tilgjengelig mobiltelefon-teknologi. Rapporten gir også en risiko- og sikkerhetsvurdering ved denne type alarmsystemer.

1.1 Rapportens form

Denne rapporten er delt inn i 8 kapitler pluss vedlegg.
Kapittel 1 Introduksjonen tar deg som leser gjennom en kort introduksjon til eldres og pleie-trengendes behov for sikring ved hverdagsulykker.
Kapittel 2 gir bakgrunnen og definisjonen av prosjektet, behov for utstyret og oppdragsgivers bakgrunn. Også tidligere arbeid i tilliggende områder nevnes. Kapitlet definerer også rammene for oppgaven både praktisk og juridisk før forskningsspørsmålene defineres.
Kapittel 3 introduserer leseren til teknologien bak mobile nett og gir bakgrunn for de senere kapitlene. Begrepet Quality of Service behandles og noen abonnementsløsninger og – tilbud legges fram.
Kapittel 4 definerer metoder og framgangsmåter som benyttes i oppgaven.
Kapittel 5 angir prinsipper for planlegging og implementering av alarmanlegg med video som mulig informasjonsbærer. Nødvendige kriterier for alarmsystemer settes.
Kapittel 6 viser de resultater som er kommet fram gjennom oppgaven. Her defineres funksjonsbeskrivelse, det presenteres forslag til implementering av demonstrator samt at det er lagt inn en risikovurdering over foreslått demonstrator.
Kapittel 7 Gjør opp status fra de foregående kapitler i en diskusjon og foreslår videre arbeid.
Kapittel 8 konkluderer over forslag og tilrådninger alarmsystemet.

1.2 Oppgavedefinisjon

Følgende oppgavedefinisjon er lagt til grunn for prosjektet:

Bakgrunn
Prosjektet "Grensebroen Arena" arbeider med problemstillinger rundt teknologi for å øke sikkerheten og tryggheten til hjemmeboende pleietrengende. Grensebroen Arena ønsker en evaluering av alarm -løsninger som benytter videooverføring basert på nyere mobil -telefon teknologi.

Studien
Problemdefinisjon:
Hvordan kan offentlige mobiltelefon-nett og private trådløse nett nyttes til å gi pleietrengende større trygghet og fleksibilitet gjennom bruk av mobile løsninger for overføring av videosignaler. Hvilken grad av sikkerhet og kapasitet kan ulike nett-teknologier og nett-tjenester tilby for å overføre videobaserte alarmer. Hva karakteriserer mobiltelefoner som er egnet for videobaserte alarmer.

Gjennom studien søkes det presentert funksjonsbeskrivelse til et system av mobile enheter for kommunikasjon og overvåkning, herunder videokamera og sensorer, mellom pasient og helseenhet eller pårørende. Aktuelle rammeverk i forhold til personvern utredes.

Det skal skisseres prinsipper for aktuelle løsninger til et funksjonelt system for videobasert trygghetsalarm basert på vurderinger av funksjonsbeskrivelsen med grunnlag i teknologiske muligheter. Ut fra disse prinsipper foreslås en implementering av prioriterte funksjoner i en demonstrator.

Ut fra aktuell risikobetraktning gjennomføres det en teknisk analyse av systemets pålitelighet. Mulige effekter i forhold til trygghet og muligheter for rask oppfølging av pasienter i kritiske situasjoner identifiseres

Om tiden og tilgjengelig teknologi tillater utvikles det en demonstrator basert på funksjonsbeskrivelsen. Demonstratoren ønskes modellert i standard beskrivende modelleringsspråk (UML / XML) og eventuell implementering i JAVA / J2ME.

1.3 Grunnlaget for studien

Studien er initiert av Grensebroen som en del av deres satsning for å oppnå "Et år ekstra hjemme." Studien baseres på nyere mobilteknologi, trådløse videokameraer og sensorer. Ut fra forventet befolkningsvekst vil behovet for effektivisering av pleie og omsorgssektoren bli en nødvendighet, se tabell 1. Ved å forlenge boperioden i eget hjem vil samfunnet kunne spare store ressurser i trygdeboliger og sykehjem. Ved å lette arbeidssituasjonen for hjemmepleiere vil man også kunne spare ressurser per bruker i hjemmepleien. Statistisk sentralbyrå har laget en framskrevet befolkningsstatistikk basert på trender i befolkningsutviklingen [10]. Statistikken viser at vi vil få en dramatisk vekst i antall eldre.

1.4 Behovet for mobile alarmer

Mobile alarmer har den fordelen at de er personlige og kan bæres på kroppen eller i klær / håndveske. De er med brukeren i nær sagt alle situasjoner. Dette betyr at brukeren er fri til å oppholde seg hvor som helst utendørs og allikevel være sikret med et utvalg av sine personlige alarmer.

Ved bruk av trådbaserte systemer er brukeren bundet til det overvåkede området, og sikkerheten alarmsystemet gir eksisterer ikke utenfor dette området.
Innendørs vil utstyr for mobile alarmer ha meget enkel montering som normalt utføres av brukeren selv eller helsepersonell /pårørende. Alarmsystemer basert på mobil videokom-munikasjon er imidlertid ikke så sikre i bruk som trådbundne systemer. Dette kommer først og fremst av tilstandene i mobiltelefonnettet. Avhengig av den lokale tilgangen til mobiltelefonnettet vil man stedvis oppleve at man ikke kan benytte video-kommunikasjon eller kvaliteten på de levende bildene er sterkt forringet. Det er derfor viktig at alarmer som primært ønskes oppsatt med videooverføring også kan frambringes gjennom mobiltelefonnettet med lav båndbredde uten videobilder. Behovet for implementasjonen avspeiles i statistikken for ulykker med dødelig utfall i de senere år hvor bla. fall, landtransport og kvelning dominerer [15]. Se vedlegg 1. Ytterligere motivasjon kan hentes fra artiklene [23, 24, 25].

1.5 Grensebroen

Grensebroen er et prosjekt innen InterregIII satsingen hvor det knyttes sammen ressurser på tvers av nasjonale grenser, i dette tilfellet mellom Sverige og Norge. Grensebroens nettverk ligger i dag i det geografiske området Østfold – Fyrbodal og består av offentlig virksomhet, næringsliv og akademia. Grensebroens overordnede mål er å gjøre regionen til en attraktiv norsk/ svensk arena for brukerstyrt produktutvikling og test av teknologi for helse og omsorg. Under parolen "Et år lengre hjemme." Administrerer grensebroen flere delprosjekt som har dette som vinkling.

1.6 Tidligere arbeid

Liv Berit Fagerli og Per-Gunnar Fyhn utga i 2005 rapporten "Sykepleieres IT kunnskap: en intervjuundersøkelse av sykepleiere i hjemmesykepleien." [6] Konklusjonene fra denne rapporten viser at databruk i hjemmesykepleien var preget av "ad hook" løsninger hvor bruk av enkle programmer for tekstbehandling er dominerende (i år 2003). Sikkerhetsaspekt med personvern og sikring av data synes å være sekundært hvis man ser bort fra at datamaskiner og terminaler var plassert sentralt inne på overvåket område (kontor). Rapporten avslører at sykepleiere generelt er positive til implementering av ny teknologi, men uten å ha dette som hovedinteresse. Rapporten viser også at sykepleiere klager på manglende utstyr og programvare, samt muligheter for tilegning av IT kunnskap. Rapporten nevner i en sammenheng bruk av PDA (Personal Data Assistent) (s.43-44) hvor behovet for direkte adgang til helsedata blir nevnt. Rapporten nevner forøvrig bruk av epost (s.42-43), men kobler ikke dette til PDA eller mobiltelefon. Lotherington et al "Telemedisin i pleie- og omsorgstjenesten: Et nødvendig redskap for utvikling av primærhelsetjenesten? - Sluttrapport fra prosjektet SES@m Tromsø" datert 13.nov. 2006 påviser et stort apparat for å implementere telemedisin ut til hjemmesykepleien i Tromsø kommune [7]. Rapporten dekker historikken, tekniske utfordringer og organisatoriske effekter. Det skal bemerkes at denne rapporten handler mye om hvordan selve integrasjonsprosessen mellom de ulike tekniske løsningene er implementert. Rapporten avdekker også at påtenkte funksjoner i et IKT system blir brukt kreativt til oppgaver som ikke er tiltenkt systemet fra start av. Tidligere masterarbeid ved HiA er også benyttet[13]. Burce et. al [18] har studert bruk av fallsensorer og algoritmer for å skille fall fra normale aktiviteter. Mye av materialet er hentet fra "Mobile Communications" av Jochen Schiller. [17] og fra "The 3rd Generation Partnership Project (3GPP)" [29].

Parallelt arbeid i tid:
Sintef, trådløs framtid v/Abelia, MedCoast Scandinavia og OsloBio v/Oslo teknopol har et større forsknings og utviklingsprosjekt "trådløs pasient" som arbeider med å knytte personlig sensor - nettverk opp mot behandlingsinstitusjoner [39]. EU har eCall på trappene for å spore trafikkulykker [120].

2 Scenario

Utgangspunktet for scenarioet er at de fleste mennesker i dag har en mobiltelefon og er fortrolig med dennes funksjoner. Avanserte mobiltelefoner kan føre videosamtaler mellom personer. I tilegg har de aller fleste mobiltelefoner av i dag muligheten til å bli programmert og derigjennom foreta handlinger basert på omkringliggende forhold. Mobiltelefoner utstyrt med PAN (Personal Area network) har muligheten til å bli tilkoblet forskjellige sensorer. Denne rapportens røde tråd er en alarmenhet som løser ut når en person faller. En slik enhet er gitt som oppgave å konstruere for en gruppe studenter på bachelor nivå, se vedlegg 0. Prinsippet med sensorer i personlig nettverk kan utvides så langt fantasien når.

2.1 Aktører

Scenarioet innbefatter følgende aktører som hver for seg spiller en rolle under alarmutvekslingen:

2.1.1 Brukeren

Brukeren, typisk en eldre hjemmeboende person uten stor interesse eller kunnskap om mobiltelefoner og data. Ofte er personen dårlig til bens og savner sine venner og familie.
Den typiske brukeren vil også ha behov for å kunne bevege seg trygt utenfor hjemmet. Brukeren kan være hendig nok til selv å henge opp lampetter og andre objekter på veggen. Brukeren er i utgangspunktet ikke dement og kan derfor selv styre sitt behov for å bli overvåket. Brukeren kan ha problemer med syn, hørsel, stive og/eller skjelvende fingre.

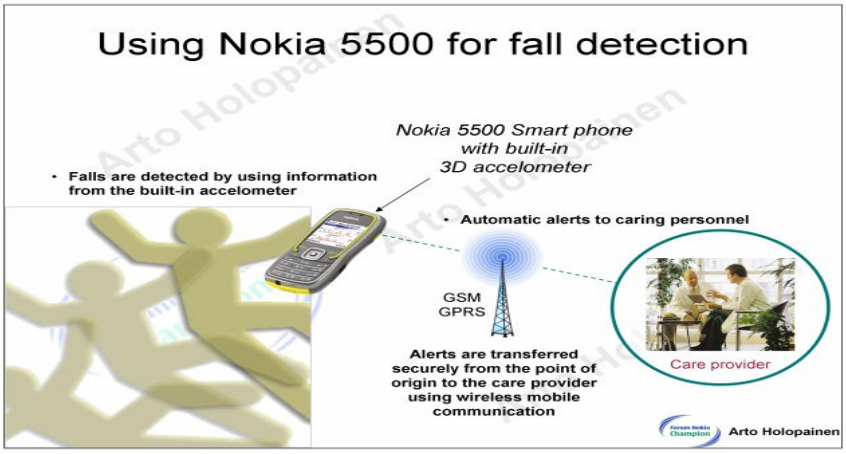
2.1.2 Hjelpepersoner

Hjelpepersoner er av to kategorier: Offentlig ansatt ved institusjon eller pårørende (Slekt og venner.). I første tilfelle vil tjenesten reguleres av en avtale mellom brukeren og institusjonen. I andre tilfelle kreves ingen formell avtale. Den offentlige ansatte hjelpepersonen forventes å ha pleie- og akuttmedisinsk kompetanse. Det forventes også at offentlige hjelpepersoner tørrtrener på bruk av systemet sammen med bruker og pårørende. En pårørende hjelpeperson kan være hvem som helst som har et forhold til brukeren. Det forventes ikke at denne personen har noen spesiell medisinsk kompetanse.

2.1.3 Mobilnettoperatøren

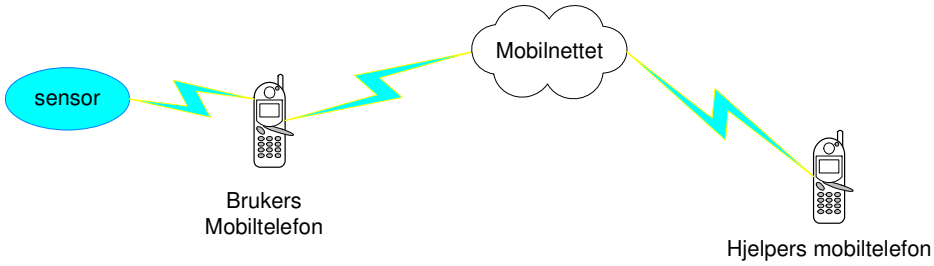
Mobilnettoperatøren knytter sammen mobilabonnentene gjennom nødvendig teknologi. Operatørene knytter sine nett sammen med faste telelinjer som også transporterer andre telesignaler av ymse varianter. Alle telesignaler behandles likt i dette systemet., men det er mulig å gi visse grupper av signaler (samtaler, datastrømmer) bedre forhold, bedre sikkerhet og høyere prioritet enn andre. Mobiloperatørenes tjenestetilbud vil variere. Pr. i dag tilbyr ingen av mobil- telefonoperatørene QoS (Quality of Service) i sine UMTS (Universal Mobile Telecommunication System) mobilnettverk [35, 36].

2.2 Scenario: mobiltelefonen som alarmbefordrer



Figur 1 Mobiltelefon med akselerometer [34]

Figur 1 viser en ide basert på akselerasjons - sensoren i Nokia 5500. I følge [18] bør fallsensoren bæres fastspent på brystet. Det vil være mer praktisk å ha en sensor fastspent på brystet som kommuniserer med mobiltelefonen via Bluetooth (Bt). Sensoren vil generere alarm med eventuelle steds - koordinater til alarmmottaker. (Avhengig av om posisjoneringsdata er tilgjengelig.) Uhellet kan utvikle seg som følger: Brukeren faller. Falldetekotoren registrerer fallet. (Hvordan den registrer er utenfor denne oppgaven, grunnlag i [18].) Falldetektoren sender melding over PAN (Personal Area Network) til mobiltelefonen med beskjed om at fall er inntruffet. Mobiltelefonen gir varsel til brukeren om at den vil tilkalle hjelp. Mobiltelefonen ringer en videosamtale til en forhånds - bestemt institusjon eller pårørende.



Figur 2 Mobiltelefon med videotelefoni og akselerometer utenfor mobiltelefonen.

Samtidig sendes en SMS med hendelsesbeskrivelse, identifikasjon (og eventuell posisjonsangivelse). Er brukeren i stand til å betjene telefonen kan henne eller han bruke telefonens videokamera til å vise skade og omgivelser for hjelpepersonellet. Hvis ikke brukeren er i stand til å betjene telefonen vil videobildet være tilfeldig eller svart. (Fra lomme eller håndveske.) Det er da overveiende sannsynlig at brukeren trenger hjelp. Kravene til applikasjonen er:

- Gjennomkobling av videosamtale skal skje i 99,5 % av anropene.
- Alarm skal ikke kunne stoppes av bruker.
- Mislykkede anrop må følges opp av anrop til andre.
- Dersom ikke videoanrop lykkes skal vanlig taleanrop utføres med opplesing av beskjed.

På veien til hjelpepersonellet passerer videomeldingen hele den rekken av utstyr som det offentlige mobiltelefoninettet består av. Dagens mobilnett består av tre systemer GSM (Global System for Mobile communications), GPRS(General Packet Radio Service) og UMTS (Universal Mobile Telecommunications System). Norske mobiloperatører tilbyr kun videosamtaler i UMTS [41, 43]. Hvorfor dette er tilfelle belyses i kapittel 3. Ved bruk av alle nett typene etableres en forbindelse allerede når brukeren slår på sitt håndsett. Håndsettet blir da enten godkjent eller avvist i mobiltelefonnettet. Samtidig registreres mobiltelefonens kapasiteter av kjernenettet. Som bruker har du liten eller ingen påvirkning på utførelsen av denne prosessen, prosessen blir styrt av det abonnementet du tegnet med operatøren og applikasjonene du har installert i telefonen.

2.3 Begrensninger og fokus

2.3.1 Avgrensninger av oppgaven

Siden oppgaven går ut på analyse av det mobile telefonnettet faller det offentlige transportnettet utenfor behandling. IPtelefoni over WLAN (Wireless Local Area Network) blir ikke behandlet. Videre behandles ikke eventuell sammenkobling mellom eksterne kamera og mobiltelefon (via Wi-Fi eller Bt). De enkelte detektorers teknologi vil heller ikke bli behandlet. Oppgaven tar ikke høyde for Bt kvalifisering [83]. Oppgaven tar ikke høyde for bruk av systemet som overvåknings- system når brukeren er dement. Slik bruk reiser medisinske / etiske / juridiske spørsmål som oppgaven ikke behandler selv om grensene mot denne bruken belyses. Det tas ikke høyde for forskrifter i forbindelse med CE merking. Oppgaven belyser heller ikke de organisatoriske forhold som må ligge til rette for å bruke et slikt system i en helseinstitusjon eller hvordan et slikt alarmsystem kan knyttes til eksisterende eller framtidige elektroniske journalsystemer.

2.3.2 Begrensninger i personvern, helselovgivning og CE merking

Scenariene reiser problemer i forhold til personvern, datasikkerhet og privatlivets fred. Innhenting av videobilder uten at alarm er utløst er problematisk hvis systemet brukes av offentlige institusjoner. Dette er derimot ikke noe problem i forbindelse med pårørende. [37] Enheten eller anlegget kommer inn under ”Lov av 11.juni 1976 nr.79 om kontroll med produkter og forbrukertjenester.” Regulert av ”Forskrift av 19. august 1994 om konstruksjon, utforming og produksjon av personlig verneutstyr”[31]. Det kreves CE merking før markedsføring. Falldetektoren er i grenseland til å komme inn under ”Forskrift om elektromedisinsk utstyr”, men gjør ikke dette. I så tilfelle ville også selve mobiltelefonen og mobilnettet gjort dette siden det er hele systemet som behandles [38], og [43] via [44]. Skal enheten brukes i institusjonssammenheng støter man på kravet i Helsepersonellovens [59] § 39 om plikt til å føre journal og § 40 om innholdet i denne. Dette er utdypet i ”Forskrift om pasientjournal” som i seg selv er hjemlet i Helsepersonellovens § 46. § 5 i ”Forskrift om pasientjournal” [60] betinger at lagring av journaldata (bilder) må finne sted og knyttes opp mot en personlig journal for hver pasient. § 9 i forskriften presiserer at video og lydopptak ”er å anse som del av journalen inntil nødvendig informasjon er nedtegnet på forsvarlig måte”. § 14 setter krav til oppbevaring av journalopplysninger i 10 år etter siste innføring. Videre pålegger § 29 i helseregisterloven [3] meldeplikt til datatilsynet ved bruk av elektronisk behandling av helseopplysninger. ”Forskrift om elektronisk kommunikasjon med og i forvaltningen” [61] § 5 forlanger sikring av opplysningene slik at taushetsplikten opprettholdes. § 4 i samme forskrift forlanger at institusjonen gjør tilgjengelig de sikkerhetsmidler som er nødvendig. ”Lov om elektronisk signatur”[62] fastlegger kvalitetskrav til elektroniske signaturer og administrasjon av disse. Loven er grunnlag for og hjemler ”Forskrift om elektronisk kom-munikasjon med og i forvaltningen”. Pasientrettighetslovens [65] § 3-6 verner pasienter mot spredning av personopplysninger, herunder legems- og sykdomsforhold. Paragrafen åpner allikevel for slik spredning etter samtykke. § 3-2 gir pasienten rett til informasjon om hva de enkelte helsehjelp innebærer (risiko). § 3-5 fordrer at informasjonen skal være tilpasset pasientens

forutsetninger. Helsepersonell skal så vidt mulig sikre at pasienten har forstått innhold og betydning av opplysningene. Gitte opplysninger skal nedtegnes i pasientjournalen. § 4-1 presiserer at helsehjelp som hovedregel skal gis på grunnlag av samtykke. § 4-6 og § 4-8 omhandler "*myndige som ikke har samtykkekompetanse*". Samtykkekompetanse er definert i § 4-4.
Personopplysningslovens [1] formål er å beskytte den enkelte person mot krenkelse gjennom behandling av personopplysninger. (Kap. I § 1) Lovens bestemmelser administreres av Datatilsynet [16]. Datatilsynet har blant sine oppgaver å gi råd og veiledning i spørsmål om personvern og sikring av personopplysninger. (Kap. VIII § 42) Personvernnemnda er klageinstans over Datatilsynet. (Kap. VIII § 43) Både Datatilsynet og Personvernnemnda har taushetsplikt etter forvaltningsloven, de kan likevel gi opplysninger til utenlandske tilsynsmyndigheter dersom dette kreves for å kunne treffe vedtak. (Kap. VIII § 45)
Mange av paragrafene i Personopplysningsloven hjemler at kongen kan gi nærmere regler i forskrifter. Disse forskriftene og reglene er samlet i "Personopplysningsforskriften" [2].
I vårt tilfelle så vil videoovervåking av enkeltpersoner komme inn under det som kalles sensitive personopplysninger (Kap I § 2 pkt. 8) siden dette dreier seg om både rasemessig og etnisk bakgrunn samt helseforhold og seksuelle forhold. Loven er svak i det perspektiv at den utfyller andre lover, dvs. at dersom en annen særskilt lov regulerer et forhold så gjelder den særskilte loven. (Kap. I §§ 5-7) Generelt kan personopplysninger bare samles inn dersom den det samles opplysninger om gir sitt samtykke til dette. (Kap. II § 8) Dette er ytterligere skjerpet inn for sensitive opplysninger i § 9. Nødalarmer og vår form for videoovervåkning kommer klart inn under bokstav g så lenge alarmene går til hjelpepersonell med taushetsplikt [12 s. 110] Pårørende må ha skriftlig avtale med bruker der bruker gir samtykke etter bokstav a. §11 bokstav b krever at unødige data ikke samles inn, Bokstav c spesifiserer at data ikke gjenbrukes til annet formål enn det som er hensikten og er samtykket til. I vårt tilfelle er det verdt å legge dette på minne siden dette kan ha med lagring å gjøre. Bokstav e setter krav til at data er korrekte og ikke lagres lengre en nødvendig, dette er videre utdypet nærmere i henholdsvis § 27 og § 28. § 28 gir hjemmel til å lagre anonymiserte historiske data og gir samtidig rett for den registrerte til å kreve sletting av dataene. § 13 pålegger behandlingsansvarlig (som er lovens betegnelse på administrator for et informasjonssystem) å sikre sine data med konfidensialitet, integritet og tilgjengelighet. Dette betyr at det må lages en risikoanalyse for systemet og sikkerhetstiltakene må settes inn etter denne. Dette betyr også at det må benyttes kryptering og autentisering [12 s129]. Overvåkning er underlagt meldeplikt jfr. § 31 og også konsesjonspliktig etter § 33. Imidlertid finnes det unntak for konsesjonsplikt i personopplysningsforskriften § 7-25 og § 7-26 om pasientopplysninger hos helse og sosialpersonell. § 36 definerer fjernsynsovervåkning. § 38 presiserer at kamera som hovedregel ikke skal nyttes der "en begrenset krets av personer ferdes". § 40 pålegger merking av områder der kameraovervåkning finner sted. § 41 åpner for videre forskrifter. Datatilsynet har gitt ut noen veiledninger i tolkning av bestemmelser i samme lov på sine nettsider [15].

Sosial og helsedirektoratet har nylig gitt ut en norm for informasjonssikkerhet i helsesektoren (7. august 2006.) [14]. Denne normen er en bearbeidelse av aktuelle bestemmelser i det Norske lovverket med utfyllende kommentarer og er ment som en sammenfatning av disse. Normen er også ment som en kontrakt mellom de forskjellige aktørene i helsesektoren og kan gjøres juridisk bindende ved avtale. En slik avtale benyttes av Norsk Helsenett AS. Uten avtale fungerer denne normen som et veiledende dokument om informasjonssikkerhet. Til normen er det utgitt en serie faktaark for å belyse de enkelte områdene normen omfatter. Sosial og helsedirektoratet henviser til veiledninger på Datatilsynets hjemmesider [15].

Ved henvendelse til datatilsynet uttrykkes det bekymring for at systemet brukt i institusjons -sammenheng kan bli en tvang og ikke en frivillig sak. I det øyeblikk systemet blir brukt ufrivillig eller blir tvunget på noen er det både melde- og konsesjonspliktig (konsesjon fordi dette gjelder videobilder). Dette gjelder også dersom brukeren blir dement! Forutsetningen for systemet er at brukeren lager skriftlige avtaler med den som skal motta alarmene hvor det går tydelig fram at dette er en frivillig ordning. I praktisk bruk for helseforetak må altså brukeren orienteres med god informasjon om hva dette er før en avtale kan signeres, det skal gå fram av avtalen at ordningen er frivillig og at avtalen ikke gjelder ved demens. Bruk av kontrollsystemer mot demente er i utgangspunktet forbudt idet de mangler samtykkekompetanse etter

Pasientrettighetslovens § 4-3. Fortsatt bruk må da inn under Sosialtjenesteloven bestemmelser om tvangsmidler i kapittel 4A som aktualiserer bruk av § 9 bokstav g [37]. En egen lov ” Lov om rettigheter for og begrensning og kontroll med bruk av tvang m.v. overfor personer med demens” var til høring med høringsfrist 1. desember 2002, men er nå innarbeidet i Sosialtjenesteloven [81, 82]. ”Forskrift om krav til akuttmedisinske tjenester utenfor sykehus.” Nevner i merknadsdelen til § 10 at Legevaktsentralene kan betjene trygghetsalarmer.

2.3.3 Fokus

Denne rapporten søker å analysere om dagens mobiltelefonitjenester innen videooverføring er tilfredsstillende for bruk til alarmformål når alarmen består av en videosamtale. Rapporten forsøker å belyse potensielle problemer forårsaket av varierende servicekvalitet i det offentlige mobiltelefonnettet når dette brukes til å overføre video, og hvilke forbedringer som er mulig å gjennomføre for å øke sikkerheten.

2.4 Forskningsspørsmålene

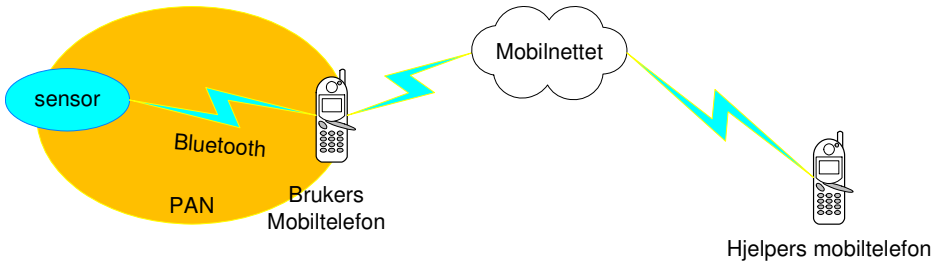
Problemdefinisjonen og scenarioene reiser følgende forskningsspørsmål:

- Hvilke funksjoner bør være med i et system for mobile videoalarmer?
- Hvilke begrensninger setter teknologien i offentlige nett?
- Hvilke begrensninger setter teleoperatørene?
- Hvilke begrensninger setter lovgivningen?
- Hvordan kan mobil videotelefoni utnyttes til alarmformål med dagens mobilnett?

3 Mobile nett, signalveier og struktur

3.1 Personlige nett

3.1.1 Bluetooth



Figur 3 Fokusområde Bluetooth

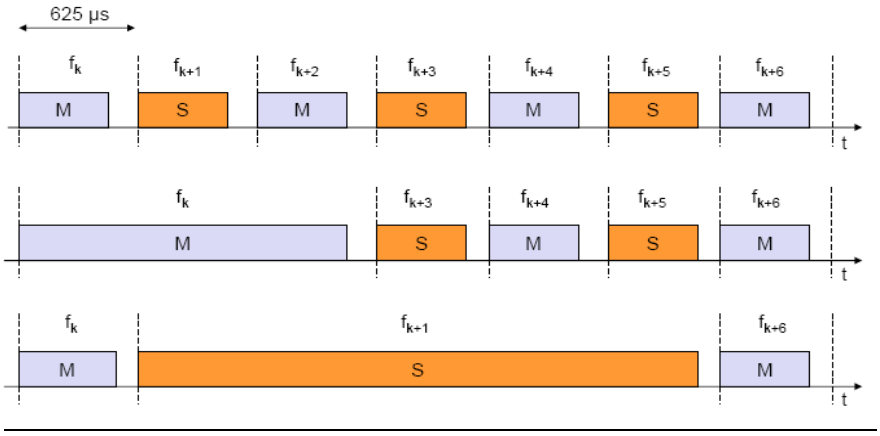
Bluetooth (tidligere Blåtann, forkortes Bt) er en kommunikasjonsteknologi primært utviklet for å erstatte signalkabler mellom periferiutstyr. Mobiltelefonfabrikantene fant konseptet nyttig og en av pådriverne i utviklingen har vært Ericsson [40,66]. Figur 3 kan antyde at mobiltelefonen har forbindelse med sensoren og mobiltelefonnettet samtidig. Dette er ikke tilfelle i vår applikasjon. Sensoren initierer en melding via Bt, mobiltelefonen kan tolke meldingen og utføre handling deretter. Sentrale meldinger over Bt i dette prosjektet er alarm og batteristatus. Bt kommunikasjon er delt i tre klasser etter utstrålt effekt og dermed rekkevidde.

Tabell 1 Effektklasser i Bt [68]

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

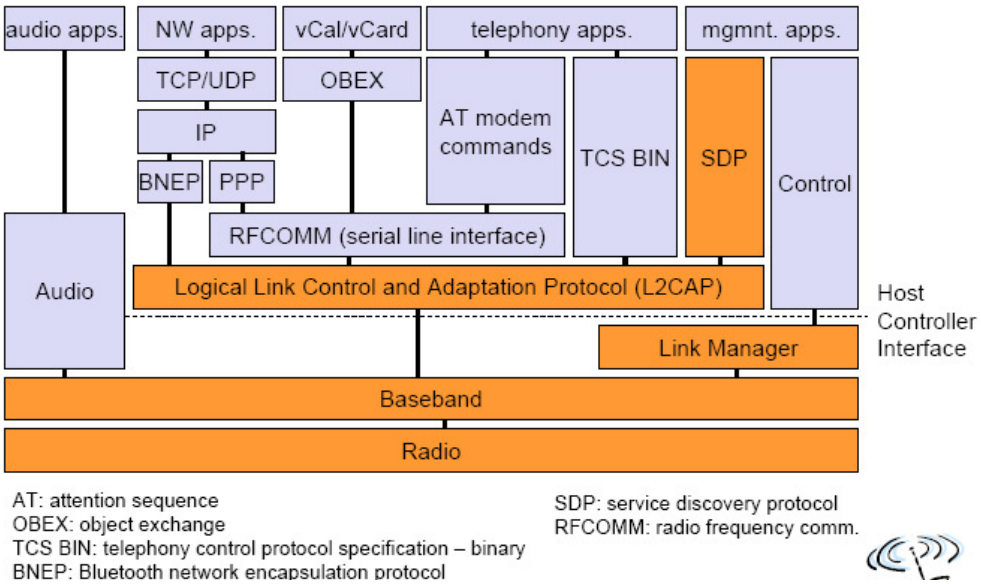
I praksis når signalene i klasse 1 i størrelsesorden 100 meter, klasse 2 i størrelsesorden 10 meter og klasse 3 ca. 1 meter, tallene gjelder i fri luft [67]. For å nå rundt i en leilighet med vegger og etasjeskiller må vi altså benytte klasse 1. For sensor og mobiltelefon båret på kroppen eller i klær vil klasse 2 være tilstrekkelig. Klasse 3 er for kommunikasjon hvor utstyret ligger side om side f.eks. på et bord. I alt kan åtte Bt-enheter være aktive samtidig i et piconett, i tillegg kan flere enn 200 være tilknyttet (parkert) og klare til å aktiveres [40]. En av enhetene betegnes master og styrer kommunikasjonen i nettet mens resten av enhetene gis betegnelsen slave. En slave kan opptre som master i et annet piconett og dermed danne et scatternet. På denne måten kan Bt-enhetene operere som reléstasjoner og til sammen dekke et område større enn radiorekkevidden til hver enkelt enhet [40]. Bt benytter frekvenshopp [40 s.59] (1600 hopp / sek) innen

ISM (Industrial Science and Medical band) båndet 2,4 til 2,485 MHz. Det hoppes mellom opptil 79 frekvenser i dette båndet. Hoppmønstret avgjøres i utgangspunktet av master sitt serienummer og klokketilstand [67]. Samtidig med at Bt benytter frekvenshopp deles også tiden mellom enhetene, TDD (Time Division Duplex), med tidsluker tilsvarende intervallene mellom frekvenshoppene (625 µS), master sender i alle tidsluker med like nummer, slavene sender i tidsluker med ulike-. Det er definert sendetider av varighet. 1, 3 og 5 tidsluker. Både master og slave kan benytte seg av disse. Frekvensskiftingen stopper når en lang sendetid benyttes og frekvensene som skulle brukes hoppes over slik at det opprinnelige hoppmønstret holdes vedlike.
Figur 4 vises tidsinndelingen mellom master og slaver, f_i er fortløpende frekvens og tidsluke. S kan være hvilken som helst slave som master M har anropt.



Figur 4 Tidsdelt dupleks [17]

ISM båndet er som navnet tilsier i utgangspunktet et "skittent" radiobånd hvor mye forskjellig elektromagnetisk stråling tillates, blant annet fra mikrobølgeovner[40]. Derfor er det beskrevet en mekanisme, AFH (Adaptive Frequency Hopping) [76] for å unngå de verste støyområdene innen bandet. AFH virker ved at de aktuelle frekvensene Bt bruker testes av en av enhetene i nettet for støy. Støybefengte frekvenser utelukkes fra hoppmønsteret [68]. Modulasjonen innen hver bærefrekvens er GFSK (Gaussian Frequency Shift Keying).
Bt benytter seg av lagdelt modell for kommunikasjonsfunksjonene, se Figur 5. Nederste nivå betegner det fysiske laget hvor maskinvare befinner seg. Lagene over betegner implementasjoner av standardiserte funksjoner. Overgang mellom to lag betegner (standardiserte) mellomkoblinger.
I Bt består spesifikasjonene av to deler; kjernespesifikasjoner (core specification) og profilspesifikasjoner (profile specification) [40]. Kjernespesifikasjonene dekker minimum av hva som skal til for å få definert andre protokoller, i Figur 5 markert med okerfarge. Radio laget består av radioforbindelse og radioutstyr, tabellen over med effekter hører for eksempel hjemme i dette laget. Baseband laget styrer radioforbindelsen, grupperer datastrømmen etter type og iverksetter kommandoer fra Link Manager som i sin tur administrerer ressursene i radioforbindelsesutstyret, sørger bl.a. for kryptering, QoS og strømsparingsfunksjoner. I praksis vil den fysiske implementasjonen stoppe ved dette nivået. Lagene over dette vil dermed bestå av funksjoner i programvare.



Figur 5 Bt sin protokollstakk [17]

Laget L2CAP (Logical Link Control And Adaption Protocol) Definerer forskjellige kommunikasjonsmodi og deres grad av QoS. Oppretter logiske kanaler og spesifiserer sikkerheten til hver kanal den oppretter. Se videre i avsnitt om sikkerhet i Bt. SDP (Service Discovery Protocol) er en funksjon som finner andre Bt-enheter innen rekkevidde og kan annonsere sin tilstedeværelse mot andre enheter [40]. Når så to Bt-enheter skal opprette en forbindelse må de gjennom en autentisering. Dette gjennomføres ved en paring (pairing) hvor de involverte enhetene beregner og utveksler autentiseringsnøkler. Like nøkler må sendes fra begge sider. Enheter uten tastatur benytter faste nøkler som eventuelt må tastes inn på motparten. Etter en vellykket paring lagres nøklene for senere bruk. Neste trinn er autorisering denne er ikke obligatorisk og kan utelates. Etter paring og eventuell autorisering blir enhetene ovenfor hverandre ”trusted devices” som utveksler informasjon seg imellom. Neste trinn er å enes om en krypteringsnøkkel. Datakommunikasjon i Bt kan foregå enten som forbindelsesorientert (SCO, Synchronus Connection Oriented) eller forbindelsesløs (ACL Asynchonous ConectionLess) hvor førstnevnte er egnet for lyd og bildeforbindelser, mens forbindelsesløs kommunikasjon egner seg for datatrafikk der formålet er å sende meldinger. Hver datapakke består av en 72 bit lang access code, en header på 54 bit og nyttemeldingen som kan bestå av alt fra 0 till 2745 bit. I kontrollpakker kan bestå av kun access code eller access code og header [83]. Nyttelasten kan bestå av forskjellig kodede data, det finnes syv definerte nyttelastpakker se Tabell 2. I vårt tilfelle er hastighet uinteressant siden datamengdene er svært små. Derimot så er det interessant med robusthet mot påvirkning av signalet. Vi er derfor interessert i en høy FEC (Forward Error Correction) rate for å unngå å måtte sende meldingen på nytt. Et logisk valg er derfor DM1 som kun trenger en tidsluke og har feilkorreksjon.

Tabell 2 Nyttelasttyper i Bt med FEC koder [83]

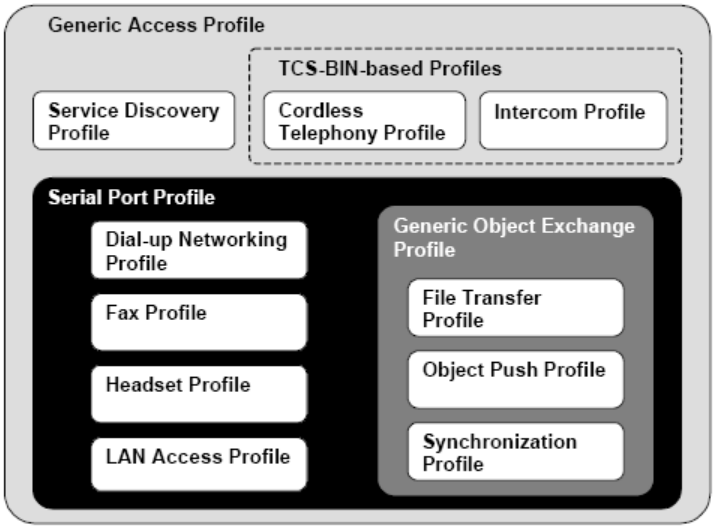
Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
AUX1	1	0-29	no	no	185.6	185.6	185.6

En Bt- oppkobling starter alltid fra master og kan starte med kjent eller ukjent adresse. For kjente adresser starter oppkoblingen med en anropsmelding (page message) som sendes på 32 definerte frekvenser. Slaver i standby (det vil si påslått men ikke innført i nettverket) modus "våkner opp" og lytter hvert 1.28 sekund for å lytte etter meldinger. Maksimal tid for å gjøre en oppkobling er 2,56 sekunder[83]. Dersom master ikke kjenner adressen til slaven må den spørre med en forespørselsmelding (inquiry message), noe som nærmes kan sammenlignes med å rope " Hvem der? ". Slavene vil da svare med adresser og klokkestatus. Master kan da sende en vanlig anropsmelding for å knytte til seg en slave. Når slaven er tilkoblet kan den ha en av fire modi i sin tilkobling; Aktiv, sniff, hold og parkert. Aktiv modus (Active mode) deltar slaven aktivt på radiolinken og sender og mottar datapakker hele tiden. Denne tilknyttningsmodusen er den beste ut fra tidsperspektiv, men resulterer i et høyt strømforbruk. I Sniff modus blir slaven lagt til å "sove" for en viss tid om gangen slik at forbindelse med master opprettholdes til bestemte tider. Denne modusen sparer energi fordi radiomottakeren i slaven kan slås av i perioder, og slaven slipper å sende bekreftelse på pakker fra master når den er lagt i søvn. Hold modus er nyttig når slaven skal gjøre andre oppgaver og er opptatt med dette. Park modus benyttes når man har et nett som består av mer enn syv enheter. Alle Bt-enheter for salg skal kvalitetssikres gjennom institusjoner som har BQTF (Bluetooth Qualified Test Facility). For å oppnå denne testen brukes en programvare "Profile Tuning Suite" fra Bluetooth.org. Ved å benytte dette verktøyet vil prisen for godkjenning være 7500 USD [84]. Dette er ikke aktuelt på første prototypen, men ved produksjonsprototype.
Det finnes en rekke protokoller avsatt for spesielle formål. Disse benyttes av profiler som er standardiserte kommunikasjonsoppsett for utstyr.

Tabell 3 Øvrige protokoller i Bt [79]

Akronym	Full tittel	Beskrivelse
AVCTP	Audio / Video Control Transport Protocol	Transportmekanismer for kontroll av audio / video enheter.
AVDTP	Audio / Video Distribution Transport	Forhandling, etablering og overføring av audio / video strømmer.
BNEP	Bluetooth Network Encapsulation Protocol	Generell databærer for PAN og IP. Følger IEEE 802.3 Bærer for PAN benytter direkte L2CAP
RFCOMM		Emulering av seriekabel gjennom Bt. Benytter L2CAP Bygger delvis på ETSI TS 07.10 standarden.
SDP	Service Discovery Protocol	Protokoll for annonsering og avdekking av tjenester i Bt nettverk. Annonserer og registrerer UUID(Universally Unique IDentifier)

Profilene bygger på hverandre slik at noen danner grunnlag for andre. Dette illustreres med følgende illustrasjon hentet fra Bluetooth SIG [114].



Figur 6 Avhengighetsforhold mellom profiler i Bt [114]

En liste over profiler i Bt med mulige anvendelser og roller er gitt under.

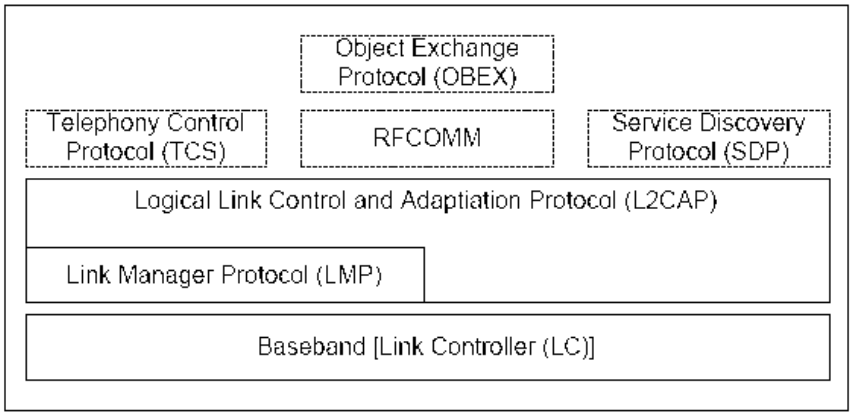
Tabell 4 Bt profiler omarbeidet fra [79]

Akronym	Full tittel	Beskrivelse	Roller
A2DP	Advanced Audio Distribution Profile	For overføring av stereolyd mellom kilde og mottaker. Benytter GAVDP støtter formatet SBC og kan støtte MPEG-1og -2 Audio, MPEG-2 og -4, AAC og ATRAC. Typisk anvendelse er ”walkman”.	Source, Sink
AVRCP	Audio / Video Remote Control Profile	Fjernkontroll av audiovisuelt utstyr. RF fjernkontroll via mobiltelefon.	
BIP	Basic Imaging Profile	Kontroll av bildeutstyr inklusive printere, skjermer og lagringsenheter samt digitale kamera.	
BPP	Basic Printing Profile	Generell for printere, ingen drivere i sendeenhet.	Sender Printer
CIP	Common ISDN access Profile	ISDN signalering og dataoverføring.	
CTP	Common Telephony Profile	Mobiltelefonen som trådløs telefon via Bt transponder koblet til fasttelefon, eller bruk av trådløs telefon gjennom mobiltelefonapparat.	
DUN	Dial Up Networking profile	Oppkobling mot internett og andre telenett, eks. bærbare maskiner via mobiltelefon mot internett. Etterlever ETSI 07.07 og PPP Baseres på SPP som bærer. Transparent.	
ESDP	Extended Service Discovery Profile	Standardisere Plug and Play over Bt.	
FAX	FAX Profile	Emulerer FAX maskin mot telenettet. Eks. Ved å benytte en datamaskin med Fax programvare og en mobiltelefon for oppkobling. Etterlever ITU T.31 og ITU T.31 AT kommandoer.	
FTP	File Transfer Protocol	Oppkobling mot FTP servere via Bt. Bygger OBEX og baseres på GOEP	Server client

GAP	Generic Access Profile	Grunnprofilen for all kommunikasjon, må implementeres i alle Bt-enheter, inneholder rutinene for søk og oppkobling mot andre BT-enheter.	
GAVDP	General Audio / Video Distribution Profile	Oppkobling av audiovisuelt utstyr og etablering av koblinger. Eksempel er kobling mellom hodesett og Musikkspiller (walkman).	Initiator Acceptor
GOEP	Generic Object Exchange Profile	Overføring av objekter mellom enheter. Bærer for OPP, FTP og SYNC	Server Client
HFP	Hands-Free Profile	Ringe fra og til mobiltelefon via håndsett, og mellom mobiltelefon og bilstereo.	
HCRP	Hard Copy Cable Replacement Profile	For printere som har behov for drivere installert i den sendende enheten.	Server Client
HSP	Headset Profile	For hodesett benytter SCO og AT kommandoer fra GSM 07.07	
HID	Human Interface Device	For tastaturer, pekeenheter (mus), spillkontrollere og sensorer.	
ICP	Intercom Profile	Mobiltelefoner innen Bt rekkevidde som interkomm uten å benytte mobiltelefonnettet. Benytter SCO til lydtransporten og TCS binary. Walkie Talkie.	
OBEX	Object Exchange	Definerer dataobjekter og kommunikasjonsprotokoll med ressursavhengighet og ressursstyring. Også for IRDA overføring. Bygger på RFCOMM. Basis for SYNC, FTP og OPP.	Server Client
OPP	Object Push Profile	For overføring av hele objekter fra slave til master. Bygger på GOEP.	Server Client
PAN	Personal Area Networking Profile	Ad–Hoc Nettverksfunksjoner for å lage ad-hoc nettverk og strukturerte nettverk.	
SDAP	Service Dicovery Application Profile	Beskriver bruken av SDP for å annonsere tjenester, registrere tjenester og avregistrere tjenester. Bygger på SDP og GAP. Obligatorisk i alle Bt implementasjoner.	
SAP	Sim Access Profile	For å kunne nyttegjøre seg SIM modulen i en hånd- holdt mobiltelefon for en annen mobiltelefon, eks en fastmontert biltelefon.	
SPP	Serial Port Profile	Erstatning for RS-232 seriekabel, beskriver hvordan man setter opp virtuelle serieporter gjennom Bt forbindelser. Opp til 128 kbit/s. Benytter RFCOMM og GAP. Bærer for DUN, FAX, HSP og LAN	
SYNC	SYNChronization profile	For synkronisering av kalender, adresser og filer. Beskriver generelle synkroniseringsmekanismer over Bt.	Server Client
TCS binay / TCP	Telephony Control Spesification	Beskriver hvordan et Bt utstyrt mobilapparat kan sømløst overføres til en Bt node koblet til fasttelefon. Basert på ITU-T Q.913. Benytter L2CAP.	
VDP	Video Distribution Profile	Beskriver videooverføring til og fra Bt enheter. Danner grunnlag for overføring i standardene H263 profile 3 og 8 og MPEG-4 simple profile.	
WAP	WAP over Bt profile	Beskriver overføring av WAP informasjon gjennom Bt. Tenkt brukt for eksempel til lokale informasjonskiosker og lignende.	Server client

Av profilene så er det tre som utmerker seg til vårt formål; Serial Port Profile (SPP) fordi den fungerer som en RS232 kabelerstatter. Human interface device (HID) fordi den tar høyde for sensordata. Også profilen OPP kan tenkes å dekke vårt formål. Denne profilen fordrer imidlertid også GEOP og krever mer prosessorkraft i sensoren, noe som i sin tur går ut over batterikapasiteten. (Profilen VDP kan nyttes til et

utvidet kameraanlegg som ikke behandles i denne rapporten.) Figur 6 viser at disse profilene er avhengige av ”Generic Access Profile” (GAP). Denne spesifikasjonen finner vi sammen med ”Core specification” [68] volume 3, part C, seksjon 2.4.3 og ikke sammen med de andre profilene. Teksten i det følgende avsnittet er basert på disse publikasjonene.



Figur 7 GAP's profilstakk [68]

Figur 7 viser protokollstakken til GAP. Denne bør sammenholdes med Figur 5 for å få et bilde av hvor de forskjellige funksjonene og protokollene befinner seg i hierokratiet. Figuren inkluderer de protokollene som GAP helt og delvis baserer seg på. GAP baserer seg helt på LC og LMP ,de andre inntegnede protokollene er med for å illustrere bruken av sikkerhetsfunksjonene i GAP. [68 s. 1161] Det er definert at Bt-enheter som ikke benytter noen annen profil skal benytte GAP. Profilens formål er å introdusere og møte felles behov som oppstår ved aksess og overførings-modi. Spesielt er gitt til avsløring (Discovery), kommunikasjonsetablering (link establishment) , og sikkerhetsprosedyrer (security procedures). Gjennom profilen defineres to roller A-party og B-party hvor A-party er initiativtaker til oppkoblingen og kommunikasjonen. Det defineres variale for oppkoblingen ut fra følgende tabell:

Tabell 5 Faste variable brukt i GAP, omarbeidet fra [68]

Kjent som	Navn	BaseBand -nivå	Brukernivå	Hensikt	Kommentar
BD_ADDR	Bt Device Address	48 Bit	12 x Hex typer	Gjennkjenne Bt- enheter	
Bt Device Name	Brukervennlig navn	Max 248 bytes	Max 248 tegn	Gi Bt-enheten et forståelig navn	Det er ikke forventet at enheter kan håndtere mer enn 40 karakterer eller vise mer enn 20 av dem.
Bt-Pin	Bluetooth passkey	PINBB 16 x Hex 0x00-0x7F	PINUI Max 16 tegn	Godkjenne nye Bt-enheter for hverandre.	Kan lagres i enheter som ikke har tastatur ! Da forlanges bruk av kun siffer !
Class of Device	Bt Device Class major Bt Device Class minor Bt Service Type	Beskrives i[115]	Fri	Presentere Enhetens tjeneste	3 felt i beskrivelsen

GAP er også ansvarlig for ”Pairing” av Bt-enhetene som skal kobles sammen. Hensikten med dette er å etablere en sikker kryptert radioforbindelse mellom enhetene. Dette kan gjøre på to måter; på initiativ fra brukeren eller på initiativ av Bt systemet. Termen som brukes om første tilfelle er ”bonding” i andre tilfelle

”autenticate using the passkey” I alle tilfelle må brukeren taste inn enhetens passord for å utføre paringen. Profilen definerer forskjellige modus for sammenkoblingen av enhetene.

Tabell 6 Samsvar mellom modi og krav [68]

Procedure	Ref.	Support
Discoverability modes:	4.1	
Non-discoverable mode		C1
Limited discoverable mode		O
General discoverable mode		O
Connectability modes:	4.1.3.3	
Non-connectable mode		O
Connectable mode		M
Pairing modes:	4.2.2.2	
Non-pairable mode		O
Pairable mode		C2
C1: If limited discoverable mode is supported, non-discoverable mode is mandatory, otherwise optional.		
C2: If the bonding procedure is supported, support for pairable mode is mandatory, otherwise optional.		

O = Option = valgfritt , M = Mandatory = Obligatorisk

Når en Bt-enhet vil undersøke sine omgivelser for andre Bt-enheter sender den en inqiry (søk) melding, enheter som er i modus ”General discoverage mode” vil da svare og presentere seg for enheten som spør. Enheter som enten blir hindret fra å oppfatte inquiry meldingen eller er i ”Non discoverable mode” svarer ikke og kalles ”stille enhet” (silent device). Om ”Limited discoverage mode” sier standarden at enheten skal kun befinne seg i denne tilstanden i en begrenset tid for å kunne respondere på ”limited inquiry” kommandoen. En Bt enhet kan enten være i”non-connectable” eller i ”connectable” modus. Enheter i ”non-connectable” modus skal ikke foreta søk for å se etter andre enheter. Enheter i ”connectable” modus skal periodevis foreta søk for å annonsere sin tilstedeværelse. Søk kan foretas på flere måter for å oppnå forbindelse.

Tabell 7 Søketider og metoder i Bt [68]

Scenario	Page Scan Interval	Page Scan Window	Scan Type
R0 (1.28s)	$T_{GAP}(107)$	$T_{GAP}(107)$	Normal scan
Fast R1 (100ms)	$T_{GAP}(106)$	$T_{GAP}(101)$	Interlaced scan
Medium R1 (1.28s)	$T_{GAP}(107)$	$T_{GAP}(101)$	Interlaced scan
Slow R1 (1.28s)	$T_{GAP}(107)$	$T_{GAP}(101)$	Normal scan
Fast R2 (2.56s)	$T_{GAP}(108)$	$T_{GAP}(101)$	Interlaced scan
Slow R2 (2.56s)	$T_{GAP}(108)$	$T_{GAP}(101)$	Normal scan

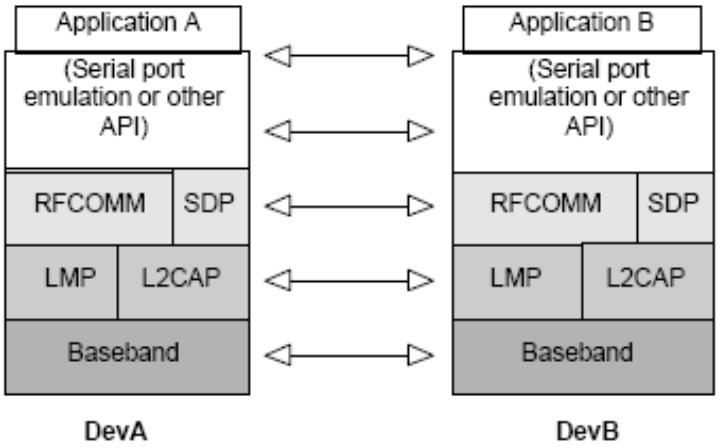
Tabell 7 viser mulige søketider ut fra søkefrekvenser og timerinnstillinger. I vår applikasjon er rask søketid nødvendig for å sette ned responstiden til systemet. Det er derfor uaktuelt å benytte de lengste søketidene. For å gi et perspektiv om timertidene er Tabell 8 tatt med.

Tabell 8 Timertider i GAP [68]

Timer name	Recommended value	Description	Comment
$T_{GAP}(100)$	10.24 s	Normal time span that a Bluetooth device performs inquiry.	Used during inquiry and device discovery.
$T_{GAP}(101)$	10.625 ms	Minimum time in INQUIRY_SCAN.	A discoverable Bluetooth device enters INQUIRY_SCAN for at least $T_{GAP}(101)$ every $T_{GAP}(102)$.
$T_{GAP}(102)$	2.56 s	Maximum time between repeated INQUIRY_SCAN enterings.	Maximum value of the inquiry scan interval, $T_{inquiry\ scan}$.
$T_{GAP}(103)$	30.72 s	A Bluetooth device shall not be in a discoverable mode less than $T_{GAP}(103)$.	Minimum time to be discoverable.
$T_{GAP}(104)$	1 min.	A Bluetooth device should not be in limited discoverable mode more than $T_{GAP}(104)$.	Recommended upper limit.
$T_{GAP}(105)$	100ms	Maximum time between INQUIRY_SCAN enterings	Recommended value
$T_{GAP}(106)$	100ms	Maximum time between PAGE_SCAN enterings	Recommended value
$T_{GAP}(107)$	1.28s	Maximum time between PAGE_SCAN enterings (R1 page scan)	Recommended value
$T_{GAP}(108)$	2.56s	Maximum time between PAGE_SCAN enterings (R2 page scan)	Recommended value

Enheter kan være åpne for videre paring eller ikke, en enhet som ikke kan pares sammen med andre skal returnere ”pairing not allowed” når den mottar en forespørsel om paring (LMP_in_rand på BB nivå), brukernivå beskjed skal være ”non bondable mode” eller ”does not accept bonding”. Hvis enheten aksepterer paring skal den akseptere (LPM_accepted alternativt LMP_in_rand) Hvis enheten har fast PIN skal den som svar selv forespørre en paring. Konsekvensen er altså at minst en av enhetene ikke kan ha fast PIN.
GAP styrer sikkerhetsmekanismene i Bt. Profilen definerer tre sikkerhetsmodi, med stigende sikkerhet, ikke sikker(non-secure), tjenestebasert sikkerhet (service level enforced security) og Linkbasert sikkerhet (link level enforced security). Ikke sikker er som navnet sier en helt åpen link som uten videre kan avlyttes med dertil egnet utstyr. Utstyret som benytter dette nivået er også forhindret fra å forespørre om sikkerhet eller foreta søk. Tjenestebasert sikkerhet benyttes når applikasjonen krever autorisasjon, autentifikasjon og kryptering. Linkbasert sikkerhet forhindrer ny paring med andre enheter. Profilen beskriver videre mekanismer for link, kanal og forbindelsesetablering.

De andre profilene kan nås fra nettsiden [79] og en av disse er ”Serial Port Profile (SPP)” fra 22-Feb-2001. [114] profilens formål er å erstatte RS232 kabler mellom enheter. Profilen er i utgangspunktet begrenset til en tidsluke i Bt overføringen og dermed kapasitetsbegrenset til 128 kbit/s. Imidlertid kan profilen kjøres i flere instanser parallelt mellom samme enheter eller mot andre.



Figur 8 Protokollmodel for SSP [114]

I Figur 8 tilhører LMP, L2CAP samt Baseband tilhører OSI(Open Systems Interconnection Basic Reference Modell) lagene 1 og 2 mens RFCOMM er Bt- varianten av GSM TS 07.10. SDP (Service Discovery Protocol) sørger for sammenkobling av enhetene (benytter GAP behandlet i forrige avsnitt). SSP benytter seg av følgende roller; Device A og Device B, hvor Device A er initiativtaker til sambandet mellom enhetene. Ut over dette er enhetene likestilte. Profilen tilbyr alle sikkerhetsmodi, men ingen av dem er obligatoriske. Oppsett av en virtuell kanal følger følgende mønster:

Tabell 9 Sekvens for oppretting av virtuell seriekanal, omarbeidet fra [114]

	Aktivitet	**Bruker**
1	Utfør søk etter RFCOMM Server kanal nummer med rett applikasjon	SDP
2	Krev autentisering av motparten	
3	Etterspør ny L2CAP kanal fra RFCOMM	RFCOMM
4	Initier en RFCOMM sesjon på den nye L2CAP kanalen	
5	Start en ny datalink forbindelse på RFCOMM med nummeret fra pkt.1	RFCOMM

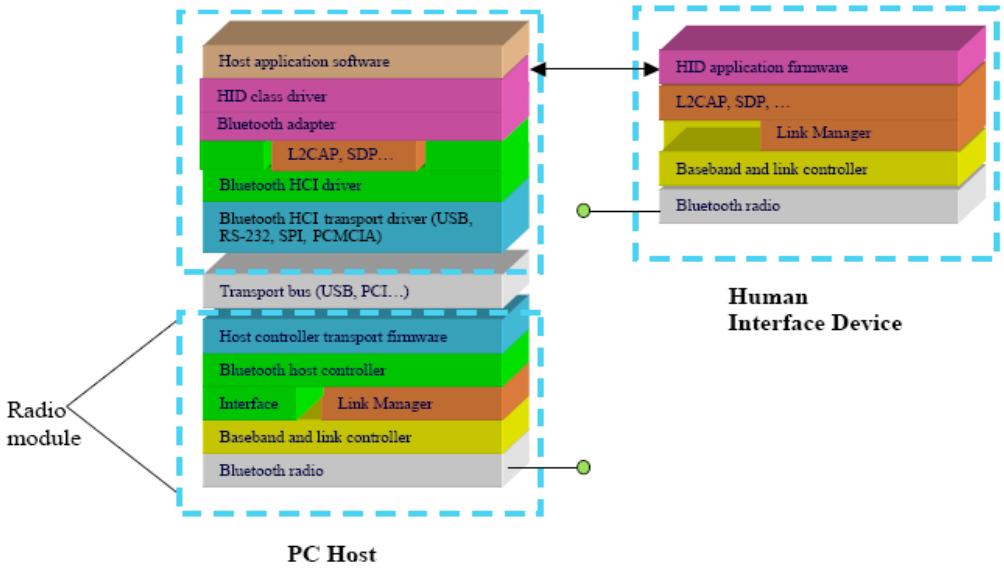
Merknad til Tabell 9: Trinn 3 og 4 utelates hvis det allerede eksisterer en sesjon mellom enheten.
Det er Device A som er ansvarlig for opprettingen av kanal (initiativtakeren).
Neste hovedaktivitet er aksepten av link og den virtuelle seriekommunikasjonen. Dette er det Device B (den anropte) som har ansvaret for.

Tabell 10 Akseptering av link og seriell forbindelse, omarbeidet fra [114]

1	Hvis forspurt, ta del i autentisering, og eventuell kryptering	
2	Aksepter ny kanal	L2CAP
3	Aksepter en RFCOMM forbindelse på denne kanalen	L2CAP
4	Aksepter en ny datalink forbindelse, aksepter eventuelle forespørsler om autentisering og kryptering	RFCOMM

Kommentar: trinn 1 og 4 kan betraktes som isolert hendelser dersom det eksisterer en sesjon fra tidligere.
Neste steg er å registrere tjenesten i SDP databasen over forbindelser i den enkelte enhet.
Profilen beskriver til slutt nødvendige krav som settes for andre protokoller i modellen (Interoperability) mot RFCOMM, L2CAP, SDP Link Manager og Link Controller.

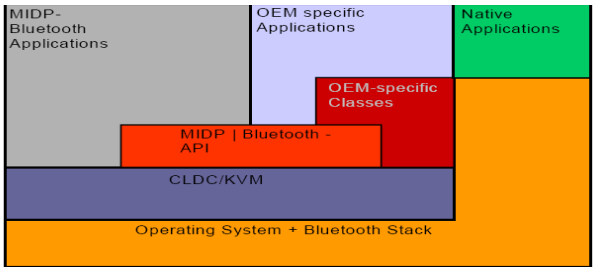
Profilen HID (Human Interface Device) profil som passer for vårt tilfelle med en enkel alarm for overføring av enkle statusdata, profilen benytter L2CAP [79]. Teknisk beskrivelse av denne profilen finnes i [80] et 120 siders dokument fra Bluetooth SIG (Special Interest Group).
Protokollstakken i HID er vist i Figur 9. Vi finner igjen Link Manager, L2CAP og SDP fra Figur 5. HID stakken vist tar høyde for at det finnes en Bt USB enhet koblet til en dataenhet (eks. en PC), derfor lagene ”Host controller transport firmvare”, ”Transport bus” og ”Bluetooth HCI transport driver”. Allikevel, denne profilen er spesielt tatt fram for kommunikasjon over USB. Denne tas derfor med her som et hint om mulig tilkobling av sensor til stasjonære PC’er eller dedikerte datamaskiner.



Figur 9 Protokollstakken i HID profilen [80]

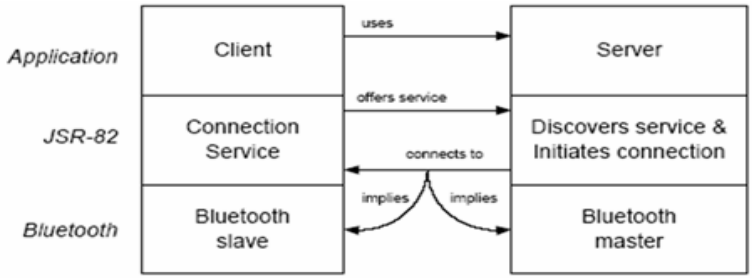
3.1.2 Bt og Java 2ME

Til J2ME (Java 2 Micro Edition) er utgitt et bibliotek ("Java ™ APIs for Bluetooth™ Wireless Technology (JSR 82)")[116] som ivaretar protokollene L2CAP, RFCOMM,SDP og OBEX. OBEX er en egen pakke sidestilt med Bluetooth pakken og dermed fullstendig selvstendig enhet som kun benytter Bluetooth som en virtuell kommunikasjon. Videre støtter J2ME disse profilene; GAP, SDAP, SPP og GOEP. Biblioteket støtter ikke audio og / eller telefonikontroll. Til biblioteket hører også to verktøy "Technology compatibility kits (TCK) for test av ferdige applikasjoner med hensyn til formelle Bt parametre.



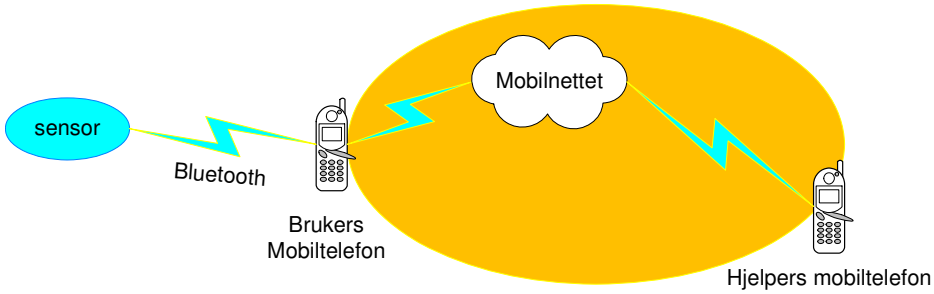
Figur 10 Bt applikasjons og referansemodellmodell i J2ME [116]

Figur 10 viser modellen for Bt applikasjoner i J2ME. Noen forklaringer; CLDC (Connected Limited Device Configuration) er javabiblioteket i mobiltelefonen KVM refererer til K Virtuell Maskin [117] som er selve javatolken. MIDP (Mobile Information Devicd Profile) [118] er applikasjonskallbiblioteket til java for CLDC / KVM her utvidet med Bt API. OEM er et begrep for Original Equipment Manufacturer, og betegner her ekstra programvare "medsent" av produsenten, importør, distribitør, .., .
Biblioteket inneholder alle de nødvendige funksjoner for datakommunikasjon over Bt i vårt tilfelle. Nokia Forum har laget en demo for kommunikasjon mellom client server [119] som er et godt utgangspunkt for videre programmering.



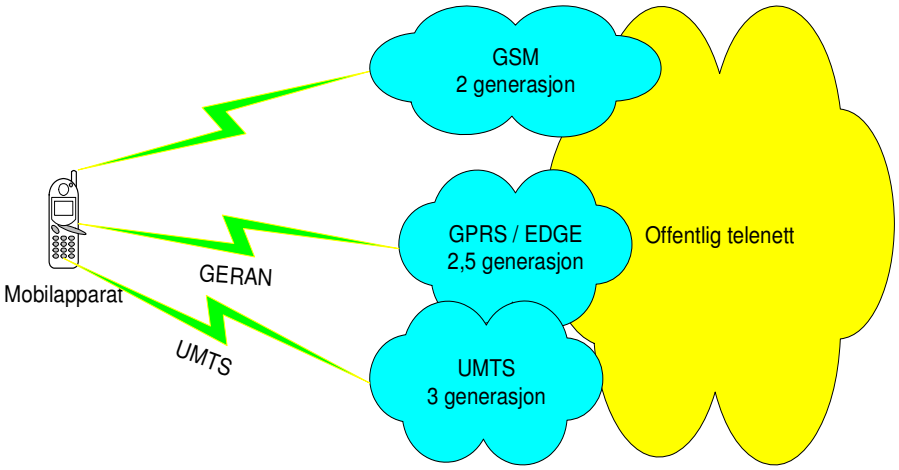
Figur 11 Kommunikasjon mellom klient og server [119]

3.2 Det offentlige mobilnettet, struktur



Figur 12 Fokusområde mobiltelefoninett

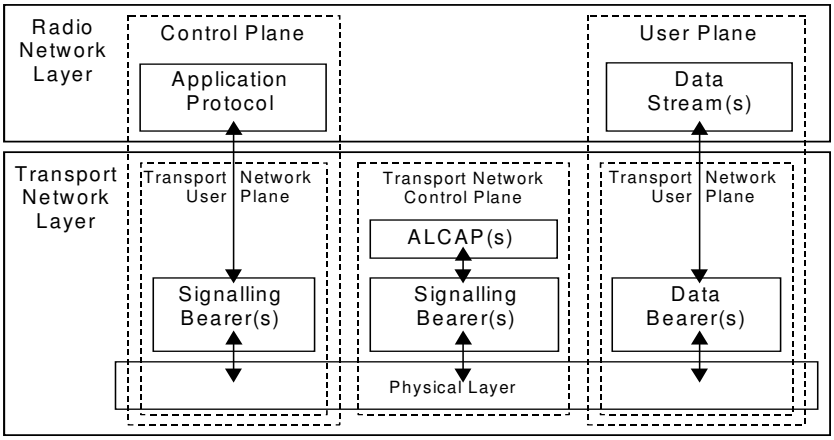
Det offentlige mobilnettet består i Norge i dag av tre nettstandarder. GSM, GPRS og UMTS. GSM og GPRS betegnes som et annengenerasjons mobiltelefoninett(2G) GPRS utvidet med EDGE (Enhanced Data rates for Global Evolution) betegnes 2,5G mens UMTS er 3 generasjon (3G). Vær oppmerksom at videotelefoni i dag kun tilbys i UMTS [41, 42]. Skal EDGE benyttes til videotelefoni må dette følgelig skje med en applikasjon som maskerer videobildene som datakommunikasjon.



Figur 13 Konseptuel oppbygging av dagens mobiltelefoninett i Norge

Figur 13 viser konseptuelt de forskjellige teknologiene i mobiltelefoninettet i Norge. Generasjonene 2G, 2.5G og 3G er allment kjent. Mindre kjent er at 3G passer inn i et rammeverk definert av ETSI (European Telecommunications Standard Institute) i midten av nittiårene, kalt Global Multimedia Mobility (GMM), UMTS er et av flere 3G konsepter [40 s.136]. UMTS benytter Radiosystemet UTRA (Universal Terrestrial Radio Access) Når dette kobles sammen til nett får vi UTRAN (Universal Terrestrial Radio Access Network). Tilsvarende benytter ikke oppdaterte GSM og GPRS/EDGE-systemer radiosystemet PLMN (GSM Public Land Mobile Network). Oppdaterte systemer benytter GERAN (GSM EDGE Radio Access

Network). GERAN er definert av 3GPP (3rd Generation Partnership Project) [29, 51]. UMTS overlapper GPRS /EDGE i felles bruk av kjernenettkomponenter (Gjelder UMTS rel-3 og rel-4).
Som det framgår av figuren over møtes de tre teknologiene først i kjernenettet, hvilket utstyr som blir brukt i kjernenettet avhenger av tjenesten som mobilnettet formidler. For at et telesystem skal fungere må de enkelte komponentene i systemet kunne avtale og styre informasjonsstrømmen mellom seg [40, 30]. Dette gjøres i hva som kalles kontrollplan, som består av signaleringsutstyr og dedikerte logiske kanaler i telesystemet. Figur 14 viser en modell av sammenhengen mellom kontrollplan, brukerplan, hva som er radionett og transportnett. Kontrollplanet har som oppgave å administrere teleutstyret slik at brukerens datakommunikasjon kan foregå med forventet hastighet og kvalitet. Kontrollplanet sørger blant annet for summetonen, at telefonen ringer, at veien gjennom telefonsystemet blir klargjort til riktig tid og med riktige parametere samt at du blir taksert riktig. Denne funksjonaliteten er sentral i oppgaven siden kontrollplanet tar seg av selve gjennom-koblingen av alarmer i telenettet.

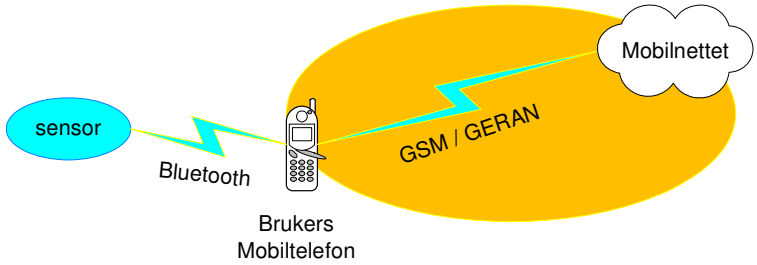


Figur 14 Generell protokollmodell for UTRAN med mellomkoblinger. [30]

Selve signal- befordringen tar brukerplanet seg av. Her forgår selve den voluminøse transporten av informasjon mellom brukerne. Eneste unntak er meldinger som i noen tilfeller benytter kontrollplanet. Figur 14 illustrerer forholdet mellom de forskjellige plan og laginndelingen i UTRAN. Lagene opptrer som en sortering mellom radiodelen og kjernenettet i mobilsystemet. Mellom blokkene går kommunikasjonen i standardiserte mellomkoblinger[30]. Denne rapporten skiller ikke eksklusivt ut kontrollplanet som emne, men leseren bør ha i minne at all styring av enhetene i telekommunikasjons - systemet skjer over egne logiske kommunikasjonskanaler og enheter dedikert til dette formålet [40].

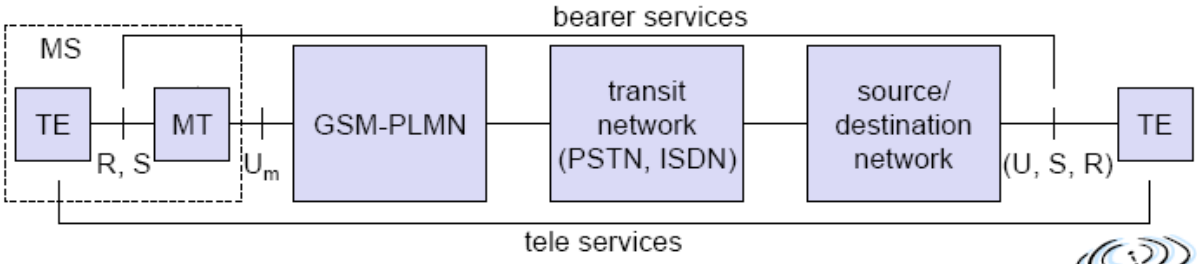
3.3 Det offentlige mobilnettet, Signalveier

3.3.1 GSM



Figur 15 Fokusområde GSM

La oss først se på GSM nettet som en bakgrunn for UMTS nettet i neste avsnitt. GSM ble introdusert i Norge i 15. jan 1993 med prøvedrift, ordinær drift fra 1. mai samme år! [45] Kun Sverige hadde da tatt i bruk systemet. Dette systemet var det første heldigitale mobiltelefonsystem i Europa og har i dag ca. 70 % markedsandel på verdensbasis. [40] Teknologien i GSM stammer delvis fra ISDN (Integrated Services Data Network) og noe forenklet kan man si at GSM er den mobile varianten av ISDN. Motivasjonen for å presentere GSM er at GPRS, UMTS og GSM har store likheter i kontrollplan.



MS = Mobilstasjon, TE = terminalustyr, eks. talekvantifisering MT = Mobil terminering, radiodelen av mobilstasjonen GSM-PLMN = Det offentlige landmobile nettet. PSTN = offentlig linjesvitsjet nett. Datatjenester benytter "bearer services" mens telesamtaler, sms og faks benytter "tele- services"

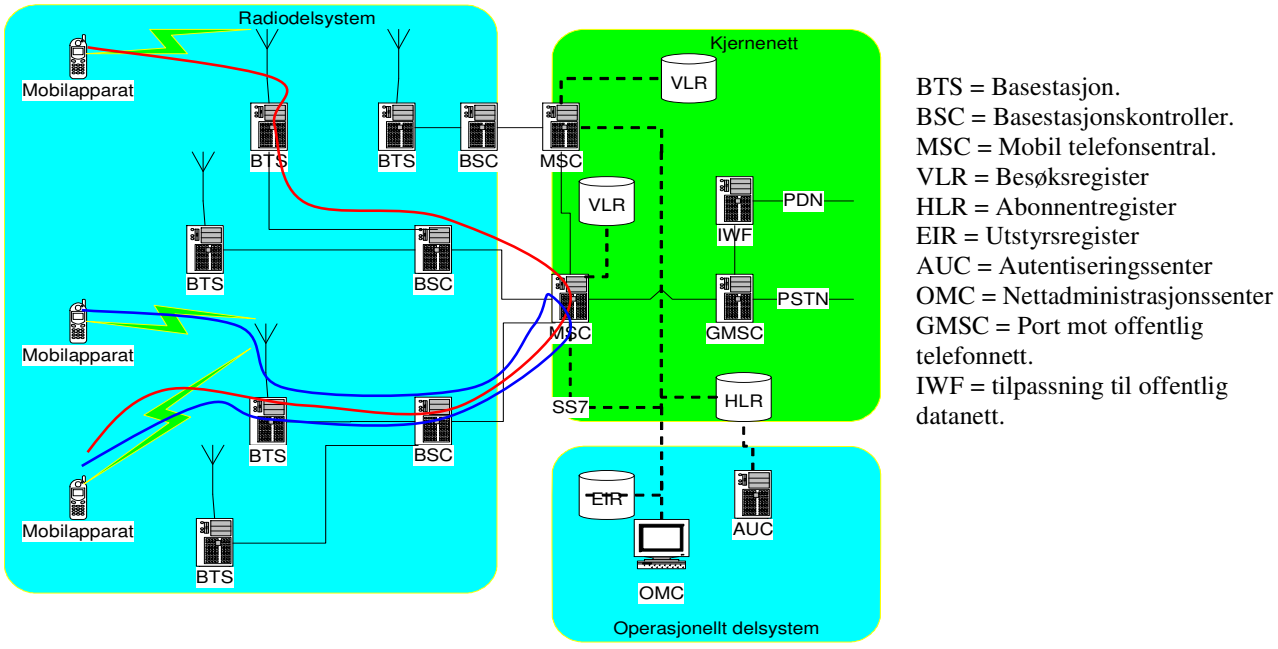
Figur 16 Referansemodell for tjenester i GSM. [17]

GSM benytter seg av ende til ende gjennomkobling. I det originale GSM oppsettet er denne gjennomkoblingen linjesvitsjet. Linjesvitsjet (circuit-switched) skjer ved at bruker sender og mottar informasjon om sin samtale (eller dataoverføring) repeterende (hver 577 µS) til en bestemt tid i syklusen. Brukeren opptar altså like stor plass ($t_{tidsluke}$ * frekvens) gjennom systemet uavhengig av om brukeren har data å sende eller ikke. (Begrepet linjesvitsj stammer fra teleteknikken og betegner at man har periodisk fysisk gjennomkobling med samtalepartner. Varigheten av kontakten er uten betydning, bare man har kontakt ofte nok. Stikkord; samplingsteorem[47])
En talesamtale kan deles inn i følgende faser [47]:

- Oppkobling av utstyr mot nettet.
- Autentisering av utstyr og bruker.
- Samtaleinitiering, gjennomkobling.

- Samtale.
- Nedkobling, registrering.

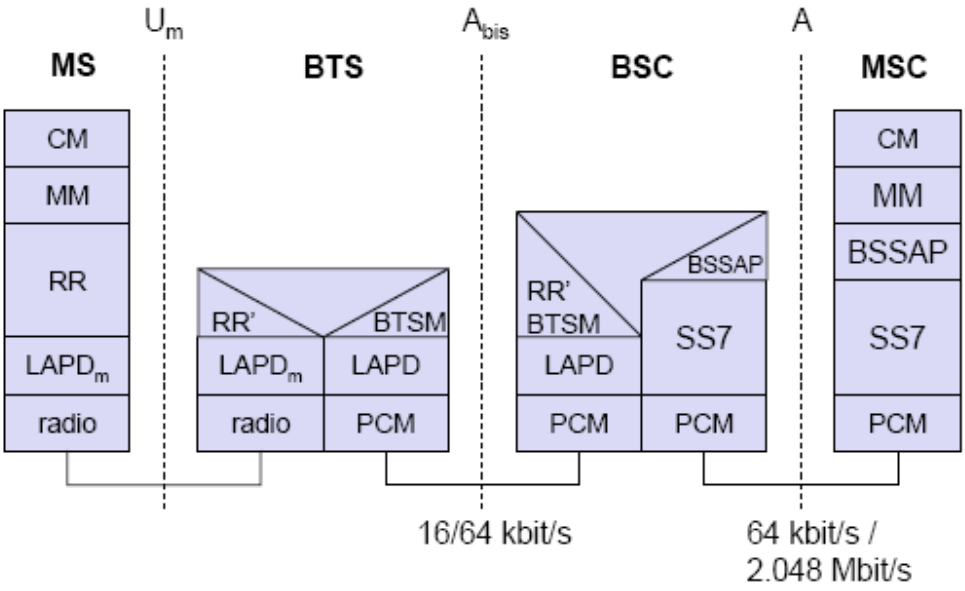
Figur 17 illustrerer oppbygningen av GSM nettet med de viktigste komponentene. De kortstiplede linjene viser også de forskjellige mellomkoblingene mellom de forskjellige enhetene. Langstiplede linjer viser meldingsruter, mens heltrukne linjer markerer gjennomkoblingsveier. Tegningen og ikke minst forkortelsene vil være nyttige i den videre teksten i dette avsnittet.
Oppkobling av mobiltelefonen skjer når utstyret blir satt idrift ved påslag. Mobiltelefonen vil da lytte etter en bestemt tidsperiode i kommandokanalen og sende en foreløpig forespørsel om å få sende. (Og om dette er nødanrop til 110, 112, 113). Mobiltelefonen får da forhåpentlig lov å sende på en gitt frekvens til en gitt relativ tid. Mobiltelefonen vil deretter presentere seg for systemet før den presenterer SIM (Subskriber Identity Module) kortets identitet. SIM kortet er brukerens identitet på mobiltelefonnettet og inneholder alle relevante data om brukeren. Mobiltelefonen blir sjekket opp mot EIR (Equipement Identity Register) registret for sjekk om den er svartelistet (meldt stjålet). SIM kortet blir sjekket mot HLR (Home Location Register) for type av abonnement, for kontoopplysninger, krypteringskodepeker samt behandlet videre i AuC (Authentication Center) Dette er skilt ut fra HLR av sikkerhetshensyn. De aktuelle parametrene blir midlertidig lagret i VLR (Visitor Location Register) så lenge mobilapparatet er påslått og beholder forbindelsen til MSC. (Mobile Servicing switching Center). HLR vil også registrere informasjon om hvilken VLR og MSC mobiltelefonen er tilknyttet samt at mobiltelefonen er aktiv og i samtale. Dersom mobilapparatet ikke er registrert i den lokale mobiltelefonsentralens HLR vil den kontakte andre mobiltelefonsentraler operatøren eier eller har roamingavtale med for å finne informasjon knyttet til SIM kortet.



Figur 17 GSM nettet oppbygging og funksjon og mulige signalveier ved samtale.

Mobilapparatet rapporterer styrke og feilrate til BSC (Base Station Controller) via BTS (Base Tranreceiver Station). Disse målingene omfattere ikke bare den kanalen som er i bruk men også visse andre kanaler i nærliggende celler. BTS rapporterer egne målinger av mobilapparatets nærhet, styrke og feilrate til BSC. BSC sammenligner målingene fra mobilapparatet fra BTS og vurderer å flytte mobil-apparatet over till annen BSC alternativt overlate mobilapparatet til en annen BSC via MSC.

Neste aktivitet er når brukeren slår et telefonnummer for å ringe. BSC kan da avvise samtalen dersom den eller BTS er i ferd med å bli overlastet. Den kan også legge mobiltelefonen over til en annen BTS dersom dette er formålstjenelig på grunn av kapasitet. Samtidig som telefonnummeret blir oversendt MSC for analyse. Finnes nummeret i operatørens HLR, mottakerens mobilapparat er markert aktiv og nettverket har kapasitet til samtalen reserverer MSC de nødvendige ressursene (frekvenser og tid) og mottakerapparatet blir satt til å ringe. Finnes ikke telefonnummeret i operatørens HLR vil det søkes i HLR tilknyttet andre operatører som mobiloperatøren eier eller har roamingavtale med.
Når nummeret er funnet i et HLR blir telefonnummeret assosiert med vedkommende mobil-apparat og mobilapparatet blir satt til å ringe dersom det mottaende systemet har kapasitet. I tilfelle at abonnenten det ringes til ikke er en mobilabonnent, går nummerforespørselen gjennom nettverksporten til det offentlige telefonnettet. Har dette nettet kapasitet vil mottakerapparatet bli satt til å ringe. I alle tilfelle vil gjennomkobling skje når abonnenten det ringes til aksepterer samtalen.
Når samtalen er slutt vil oppdatert kontoinformasjon bli lagret i HLR samtidig som alle ressurser samtalen opptok blir frigjort.



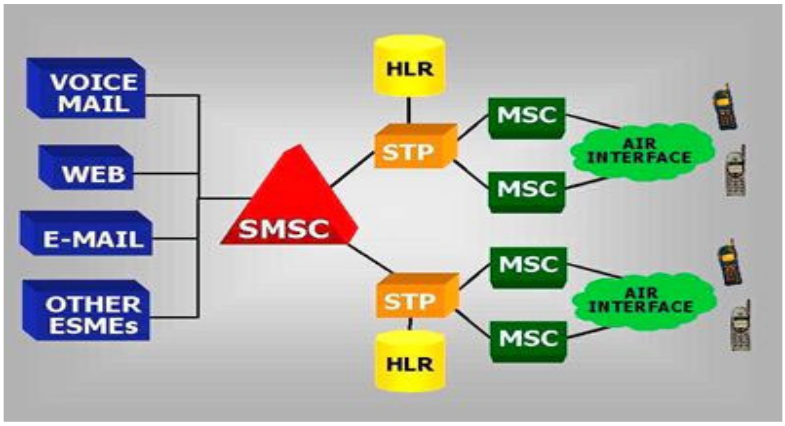
Figur 18 Signaleringsprotokollene i GSM [17]

Figur 18 viser signaleringsprotokollene som GSM benytter. De samme protokollene benyttes i R99. Det laveste laget viser den fysiske signalbæreren. Lagene over viser funksjonalitet innbakt på hvert nivå i systemet. For å begynne med forbindelsen mellom mobilapparatet og basestasjonen: Radioprotokollen i bunnen er den fysiske radioen med sine radiotekniske funksjoner; synkronisering (med ”frame advance”), monitorering av radiokvalitet og kryptering / dekryptering inklusive FEC (Forward Error Correction). Neste nivå Link Access Procedure for D channel mobile (LAPDm) tilbyr virtuell sikker forbindelse mellom de sammenkoblede høyere lagene. Blant funksjoner dette laget benytter er retransmittering av pakker med feil, fragmentering og sammensetting av hele beskjeder, LAPDm er ”arvet” fra ISDN og tilpasset, derfor m. Radio Resource management laget sørger for at radioressursene blir riktig anvendt (Legg merke til at dette er delt mellom base - stasjonen og basestasjonskontrolleren med BTSM (BTS Management) som formidler mellom disse.) Oppgaven her er å sette opp, vedlikeholde og avslutte radiokanaler. Dette skjer typisk ved oppringing, endring av radio- og trafikkforhold og ved overgang mellom basestasjoner (handover). Mobility Management (MM) foretar registrering, identifisering, autentisering og lokalisering samt skjuler brukerens identitet på nettet. Call Management (CM) tilbyr mobilsystemets tjenester til

brukeren. Forbindelsen mellom basestasjonen og basestasjonskontrolleren og i kjernenettet baserer seg på PCM (Pules-Code Modulation) som protokollbærer [40].

3.3.2 SMS.

SMS følger stort sett samme mønster som tale. Det er likevel en vesentlig forskjell. Tale og datakommunikasjon foregår i egne transmisjonskanaler som er transparente gjennom nettet, og nettet behandler disse som direkte gjennomkobling. Meldingene utnytter derimot ledig kapasitet i selve signaleringskanalene til og fra mobiltelefonen. Dermed kan meldinger sendes parallelt med en pågående talesamtale eller dataoverføring. Dette betyr også at meldinger faller inn under samme kategori som administrasjonsmeldinger og i utgangspunktet på samme nivå som styringen av mobilkommunikasjonen mellom mobilapparat og MSC. Meldinger sendes via en (leverandør-) uavhengig meldingstjener i mobilnettverket. SMS er også den eneste muligheten mobiltelefonnettet har til å nå fram til mobilapparatet for å kunne styre dette [17]. Ref. Figur 16 Bearer services. Dette fordi nettopp hastigheten mellom enhetene må tilpasses og dermed bufres.
Fysisk var tjenesten ofte lokalisert til samme lokaler som MSC og HLR, men er nå overlatt til frie operatører og har en fri plassering i nettet [48].

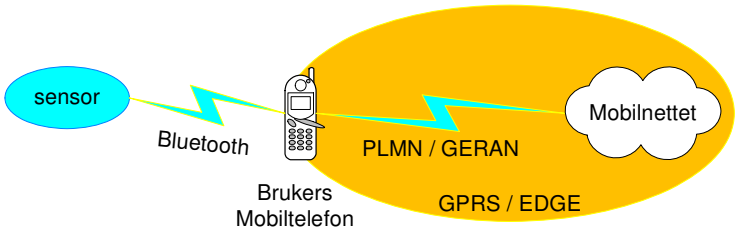


SMCS = Short Message Service Center. STP = Signal Transfer Point.

Figur 19 Meldingssystemer i GSM. [48]

Merk at det ikke er noen leveringsrammer angående tid, det er imidlertid mulig å gi meldingene prioritet. Det er også mulig å spesifisere kvittering av meldingene. Meldingene blir lagret til mobilapparatet blir slått på eller det ligger teknisk til rette å sende dem til mobil-apparatet. Relasjoner til GSM, GPRS og UMTS er beskrevet i [128]. Det er verd å merke seg at ved bruk av UMTS overføres SMS som datatrafikk på egne kanaler uten prioritering i dagens mobilnett, men med prioritering i mobilapparatet. [128].

3.3.3 GPRS/EDGE



Figur 20 Fokusområde GPRS / EDGE

Standardiserte videosamtaler over mobiltelefonnettet benytter en av standardene H.263 (RFC2190) [21] eller H.264 [20] (ISO/IEC 14496-10 [19]. Disse standardene fordrer minimum 64 kbit/s. Skal dette være mulig i begge retninger uten å benytte UMTS må GSM utvides til EDGE (Enhanced Data for Global Evolution). Med EDGE kan man maksimalt oppnå 384 kb/sekund. Tilsvarende hastighet som dagens UMTS. Utbyggingen mot EDGE har gått trinnvis. Grunnlaget for EDGE ble lagt med GPRS nettet som var en utbygging av GSM nettverket for å understøtte pakkeorientert datakom-munikasjon. Med pakkeorientert kommunikasjon menes at informasjonen deles opp i bolker (pakker) som adresseres og sendes ut på nettet [47] s.4. Utstyr i nettet (rutere) sørger for at datapakka kommer fram til adressaten. GPRS tillater hastigheter opp til 171.2 kbit/s. Dessverre er det ingen håndapparater som utnytter denne hastigheten begge veier. Klassifiseringen av mobilapparater stopper på 85.6 kbit/s en vei og 21.4 kbit/s i motsatt retning (CS-4 class 12 se Tabell 12). Dette setter en effektiv stopper for videosamtaler over GPRS. Eventuelle levende videobilder kan dermed bare sendes en vei.

Tabell 11 Brukerhastigheter i GPRS i forhold til kodeskjema [17]

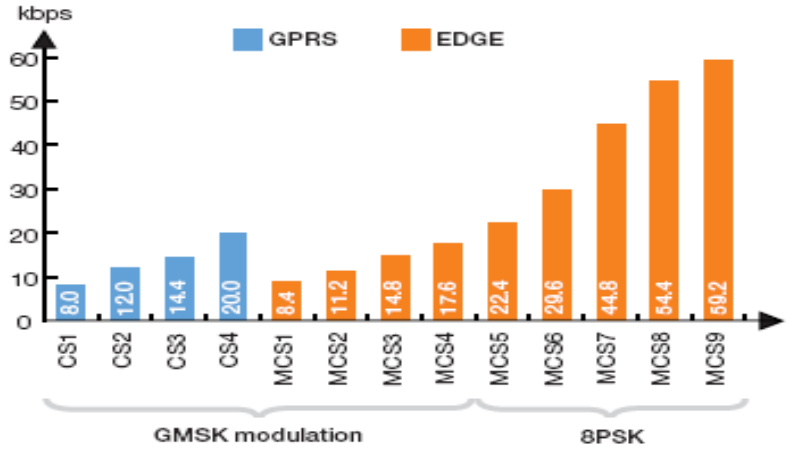
Coding scheme	1 slot	2 slots	3 slots	4 slots	5 slots	6 slots	7 slots	8 slots
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

Det skal nevnes at GPRS har forskjellige kodeskjema som gir varierende datahastighet. CS1 har meget høy datasikkerhet (redundans), mens CS-4 sender rå data uten redundans. For levende bilder betyr ikke enkeltfeil noe rolle. Øyet vil maskere vekk mye feil, det er viktigere å holde bildetakten og oppdateringen av bildene vedlike. Dermed vil videobilder være egnet for full hastighet uten FEC. (Forward Error Correction.)

Tabell 12 GPRS klassifiseringen av utstyr [17]

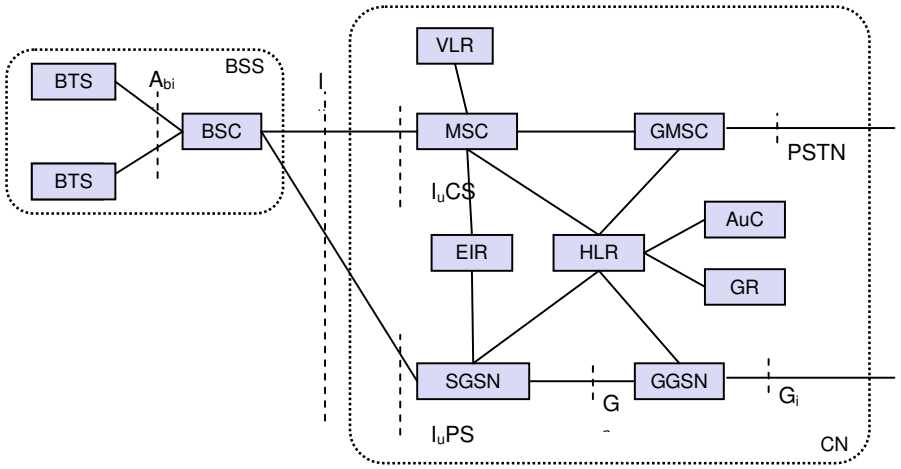
Class	Receiving slots	Sending slots	Maximum number of slots
1	1	1	2
2	2	1	3
3	2	2	3
5	2	2	4
8	4	1	5
10	4	2	5
12	4	4	5

Med innføringen av EDGE kom nye modulasjonsformer (8PSK) og nye kodeskjema som typisk økte hastigheten pr. tidsluke med en faktor i underkant 3. Ikke 4 som man skulle tro ved å gå fra en bit koding til tre. Grunnen er at man benytter større overhead i andre kodeskjema. Samtidig beholdt man GMSK modulasjonen fra GPRS i fire kodeskjemaer for å kunne dra nytte av denne modulasjonsformens fordeler under dårlige radioforhold. Man byttet imidlertid ut protokollen som GPRS benyttet for å få til en retransmisjons-mekanisme som tillot reformatering og overføring av enkeltpakker i andre kodeskjemaer.



Figur 21 GPRS og EDGE, hastigheter pr. tidsluke og kodeskjemaer. [22]

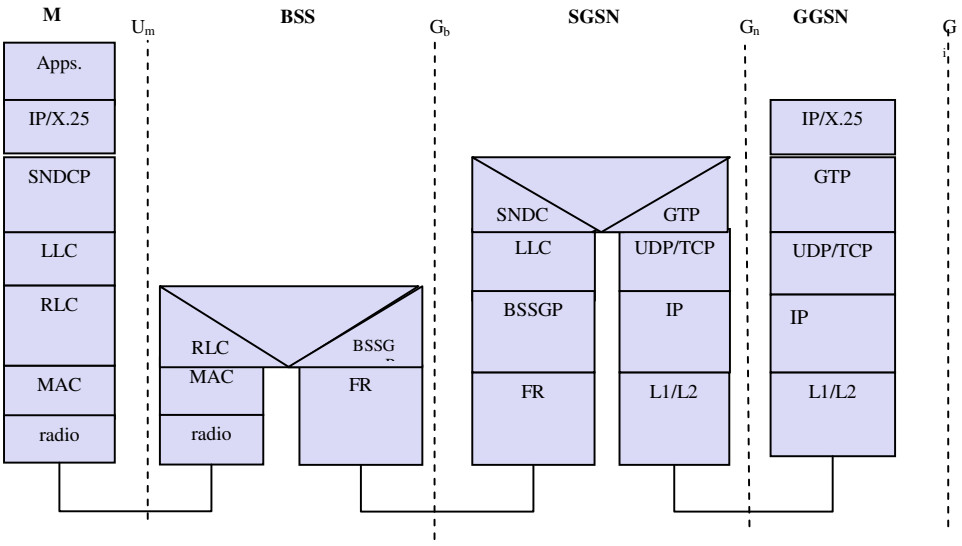
Dette betyr at man kan benytte videokommunikasjon formatert med H.263 med to tidsrammer i hver kommunikasjonsretning. En slik løsning har flere problemer. Et problem er den lave utnyttelsen av kanalene. En annen er at GPRS er pakkeorientert. I praksis vil det si at det blir større overhead på pakkene og at pakkenes ankomst til mottakeren ikke nødvendigvis skjer til rett tid. Det er derfor ingen operatører i Norge som tilbyr dette [37,38]. Skal man sende videobilder må disse altså sendes som datafiler og sanntidsapektet går tapt.



Et blandet GSM/ GPRS offentlig mobiltelefonnett vist uten håndapparat. Håndapparatet kommuniserer med BTS. PSTN er det tradisjonelle linjesvitsjede telefonisystemet. G_i er betegnelsen på tilkoblingen til det offentlige pakkeorienterte datanettet.

Figur 22 GSM/GPRS nett uten håndapparat. [omarbeidet etter 40]

Figur 22 viser et kombinert GSM/GPRS nett før GERAN. I forhold til GSM er det innført tre nye noder i kjernenettet; SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support Node) og GR (GPRS Register). SGSN tilsvarer MSC i GSM og sørger for adressering av datapakkene og routing av disse videre i nettverket. (Eller, i tilfelle lokalforbindelse, routing til samtalepartner.) GGSN tilpasser og router datastrømmen til og fra det offentlige datanettet.
GR inneholder abonnement – opplysninger nødvendige i GPRS nettet.
GPRS nettet tilbyr to typer gjennomkobling, en forbindelsesorientert punkt til punkt tjeneste (PTP-CONS) og en punkt til punkt forbindelsesløs tjeneste (PTP- CLNS), i første tilfelle fungerer nettet som en virtuell gjennomkobling, i andre tilfelle som dagens internett. Som det framgår av Figur 23 benytter GPRS / EDGE IP- adressering. Dette fremstår som et problem hva angår sikkerheten for nettet fordi IP adressene tildeles dynamisk og dermed fordrer en URL (Uniform Resource Locator) (i praksis mobiltelefonnummer) som således må registreres og spres over navnetjenernettverket, i tillegg er IP- adresser for tiden en knapphetsressurs. Mobiloperatørene kan tilby faste IP adresser til spesielle applikasjoner for å omgå problemet[37]. Denne blir i så tilfelle lagret permanent i GR (GPRS Register) [40] Se Figur 22.

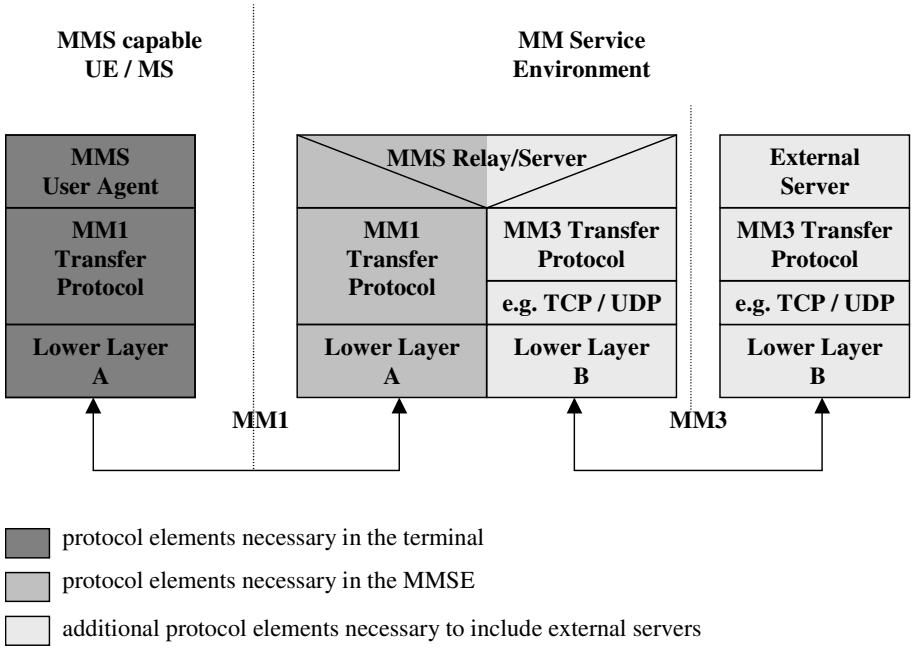


Figur 23 Protokollstakkene i GPRS [17]

Figur 23 viser protokollene som blir brukt i GPRS. Verdt å merke seg er bruken av IP og UDP / TCP(User Datagram Protocoll / Transmission Control Protocol), kjent fra datakommunikasjon.
Protokollen GTP (GPRS Tunnelling Protocol) tilbyr ende til ende virtuell forbindelse, enten til andre GPRS nett (mellom GGSN) eller til det offentlige datanettet gjennom grensesnittet G_i. For de øvrige protokollene henvises til relevant litteratur for eksempel kilden [40] eller definisjonene utgitt av ETSI [33].

3.3.4 MMS

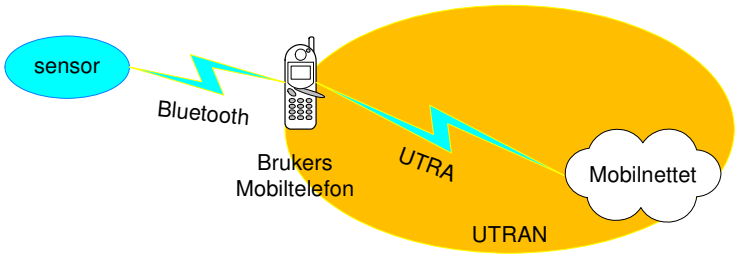
MMS (Multimedia Message Service) er en tjeneste levert av mobiltelefonoperatørene til mobiltelefoner støtter MMS terminal (Programvare: MMS User Agent). Tjenesten er definer i standarden TS 23.140 fra 3GPP med forskjellige versjoner. Siste skudd på stammen er i skrivende stund V6,13.0 fra 2006-06 [55]. Tjenesten benytter pakkeorientert kommunikasjon til oversendelse av tekst, bilder og videosignaler. MMS kan settes opp til å gi bekreftelse på at meldingen er levert og kan prioriteres i GPRS nettet. (Prioritering av melding er ikke tilbudt av Telenor mobil eller NetCom, NetCom tilbyr bekreftende meldinger [96]) Tjenesten er på samme måte som SMS koblet opp mot en uavhengig server. Denne serveren kan igjen knyttes til andre servere [55]. Tjenesten er også tilgjengelig på PC'er med oppkobling mot samme server via internett [52]. Tjenesten kan enten overføres med PTP-CONS eller PTP-CLNS, men dette avhenger ofte av telefonens implementasjon av MMS terminalen [52]. Systemet består av Terminalprogrammet i mobiltelefonen (MMS User Agent). Serveren som også er router (MMS Relay / Server senere i teksten kalt MMSC) og eksterne servere.



Figur 24 Protokollene i MMS [55]

Figur 24 Viser protokollene brukt til MMS. Man ser at MMS systemet benytter to egne protokoller: MM1 mellom mobilenheten og serveren (som kommer på toppen av protokollene i Figur 23) og MM3 som benyttes mellom de forskjellige serverne [55].

3.3.5 UMTS



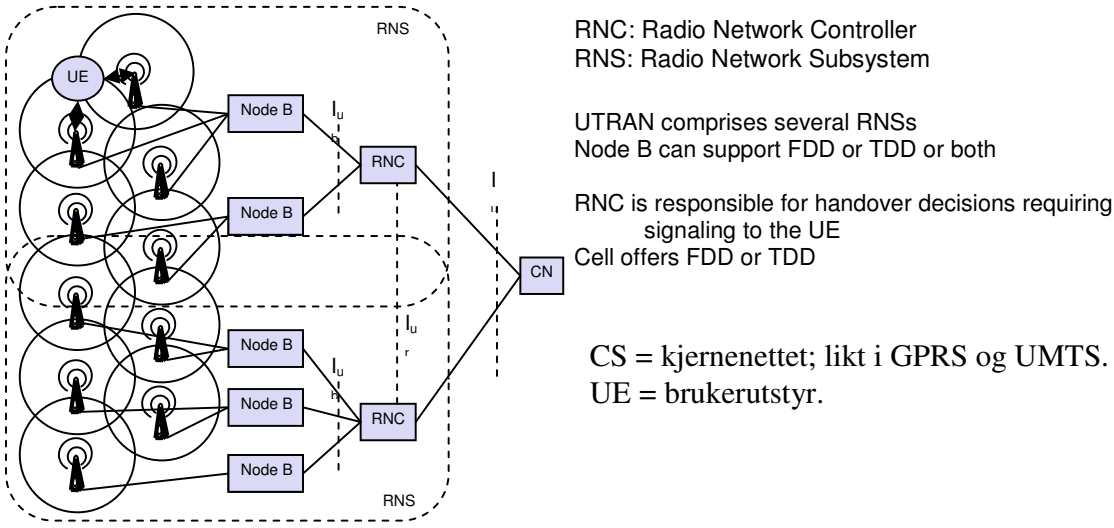
Figur 25 Fokusområde UMTS

Utbyggingen av UMTS i Norge skal i følge konsesjonsvilkårene til NetCom [54] og Telenor Mobil være ferdig i mars 2007. Da skal alle tettsteder med over 200 innbyggere være dekket [53].
Dekningskart finnes tilgjengelig på [48] og [49]. Ved henvendelse til Post og teletilsynet [89] kan opplyse om at det er tre konsesjonsholdere for UMTS i Norge: Telenor mobil, Netcom og ”3”. Den sistnevnte har ikke til nå kommet i gang med å bygge ut nett. En konsesjon er stadig ledig.
UMTS kan med overføre alle kommunikasjonsformer som distribueres av GSM og GPRS / EDGE. Det er også drivkraften bak introduksjonen å avlaste GSM og da spesielt radiooverføringen i PLMN-RAN.
Alt fra starten av med R99 (Release -99 senere omdøpt til Rel-3) hadde UMTS linjesvitsjet 64 Kb/s med henblikk på videotelefoni, det er også denne utgaven av UMTS som fram til i dag er blitt brukt i Norge.
Med fastsettelsen av Release 4 i mars 2001 ble det innført normer for QoS (Quality of Service). Disse normene er motivert nettopp ut fra behovet for å skille forskjellige tjenesteformer fra hverandre.

Tabell 13 Tjenesteprofilene i UMTS Rel-4 [17]

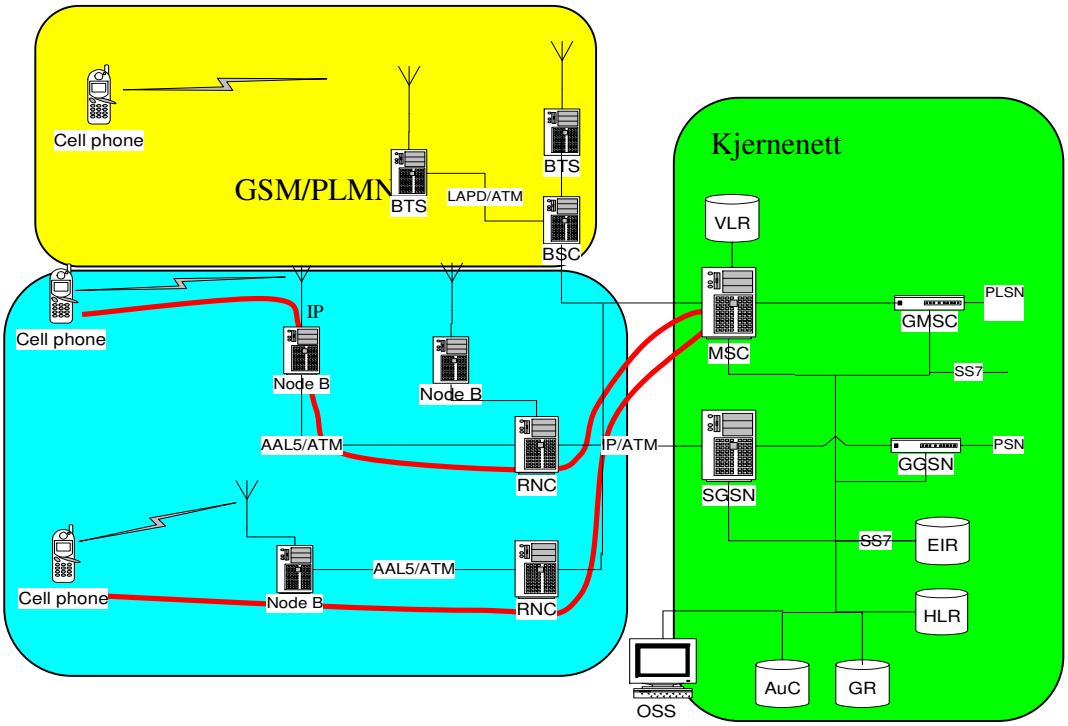
Service Profile	Bandwidth	Transport mode	
High Interactive MM	128 kbit/s	Circuit switched	Bidirectional, video telephone
High MM	2 Mbit/s	Packet switched	Low coverage, max. 6 km/h
Medium MM	384 kbit/s	Circuit switched	asymmetrical, MM, downloads
Switched Data	14.4 kbit/s	Circuit switched	
Simple Messaging	14.4 kbit/s	Packet switched	SMS successor, E-Mail
Voice	16 kbit/s	Circuit switched	

Tabell 13 viser de aktuelle tjenesteprofilene som ble innført med Rel-4 og deres hastigheter. Som det framgår av tabellen vil videotelefoni benytte profilen "High Interactive MultiMedia".
Figuren under viser forenklet radionettet i UMTS (UTRAN). Kjernenettet i UMTS R99 er likt med kjernenettet i GSM/GPRS med noe utvidede tjenester (programvare) i nodene [40].



Figur 26 UTRAN [17]

UMTS utgivelsen R99 er nevnt. UMTS bygges ut gradvis. Inngangsbiletten er radio- systemet UTRAN. Dette systemet ble beskrevet i 3GPP publikasjonen TS 25.401 V3.10.1 (R99 senere betegnet Rel-3). Senere kom det til Rel-4 (mars 2001) som bla. innførte QoS, Rel-5 (mars 2002) innfører nytt kjernenett basert på IP som bæremekanisme i tillegg til nye radiokodeskjema (HSDPA) som øker hastigheten til mobiltelefon opp til teoretiske 14.4 Mbps. [56].
Sett fra brukerens ståsted merkes det i dag liten forskjell på EDGE og UMTS i praktisk bruk til datakommunikasjon, enkelte steder oppnår UMTS høyere datahastighet. UTRAN og UMTS er imidlertid bygd for større datahastigheter og billigere handtering av dataene. UMTS er enda et relativt nytt system og fremdeles i utvikling [57].



Figur 27 Mulig signalvei for videosamtaler i UMTS ved lokalsamtaler.

Figur 27 er laget ut fra opplysninger i [40] viser mest sannsynlig signalvei for mobil videosamtale i et lokalsamfunn. Tabellen under utdyper de enkelte enhetenes oppgaver.

Tabell 14 Aktive enheter i UMTS nettet ved en videosamtale, omarbeidet fra [40]

UMTS/ Kjernenett	Enhet/ nr	Funksjon	Kobler til
UMTS	Node B 1	Radiomellomkobling Kobler sammen radio delen med den trådbundene infrastrukturen i UTRAN	Mobilapparat RNC
UMTS	RNC 2	Administrerer Node B i sitt distrikt. Viderebefordrer pakkedata til SGSN og taledata til MSC. Sørger for handover innen distriktet.	Node B Andre RNC SGSN MSC
Kjernenett	MSC 3	Koblingssenter i linjesvitsjet mobilt nett. Sørger for signalering til og fra mobilapparat, tilordning av ressurser (Herunder QoS og hastighet) oppretting av kommunikasjon mot offentlig linjesvitsjet nett via GMSC. (andre mobiltelefon-nett og operatører)	GMSC Andre MSC VLR EIR HLR RNC
Kjernenett	GMSC 4	Porten mot det offentlige linjesvitsjede nettet. (PSTN). Sørger for avvisning eller innkobling av innkommende samtaler fra PSTN til mobilnettet.	MSC HLR PSTN
Kjernenett	EIR 5	Database over brukerutstyr; stjålet, kapasitet, fungerer, meldt feil.	GGSN MSC

Kjernenett	HLR 6	Database over SIM kort, abonnementsinfo (herunder telefonnr., krypteringsnøkkel-peker,) posisjon, taksering, autentisering via AuC og GR. Kan inneholde fast IP adresse.	SGSN MSC GGSN GMSC AuC GR DHCP
Kjernenett	AuC 7	Autentiserer SIM kortet, styrer kryptering av forbindelsen gjennom UTRAN.	HLR
Kjernenett	VLR 8	Database over aktive mobilapparater i området til MSC	MSC

For å få til en gjennomkobling med videokommunikasjon må man gjennom flere ledd. Se Tabell 14 for en oversikt over enheter som involveres i videosamtaler i det offentlige mobilnettet. Tabellen omhandler kun ett mobilsystem. Dersom man oppretter en videosamtale med en bruker utenfor eget kjernenett bruker man dobbelt opp av utstyret nevnt i tabellen i tillegg til transportnettet i det offentlige telenettet. Systemet vil alltid forsøke å velge korteste vei gjennom systemet. Allikevel er korteste vei ikke kortere enn at signalet når fram til MSC. Dermed er korteste vei UMTS har den som er beskrevet i Figur 27.
Viktig å merke seg er at hvis man er tilsluttet UMTS nettet vil tale og datatrafikk inkludert MMS bli sendt over dette radiogrensesnittet.

3.3.6 Andre 3G nett

Det finnes en utbygger av 3G nett som bruker CDMA2000 teknologi i 450 MHz båndet; Nordisk Mobiltelefon Norway AS med varemerket ICE. I skrivende stund tilbyr ikke ICE håndterminaler med mellomkobling [90].

3.4 QoS

Begrepet QoS (Quality of Service, Norsk; tjenestekvalitet) er en samlebetegnelse på levert kvalitet til sluttbruker. Begrepet tallfester variabler som overføringstid, svingninger i overføringstid, overførings-kapasitet, feil og tap. I vårt scenario passerer signalene gjennom Bt, mobiltelefonen, det offentlige mobilnettet og tilbake til en mobiltelefon. Frode Sørensen definerer begrepet for pakkedata i [46 s.170] til ”*Tjenestekvalitet er et nettverks evne til å oppfylle bestemte grenser for båndbredde, pakketap, tidsforsinkelse og variasjon i tidsforsinkelse (jitter) for dataoverføringen.*” Post og telesystemet har kommet med en ”Norsk veiledning for rapportering av tjenestekvalitet”[63]. Denne har et avsnitt om ”Alternative, indirekte parametrer” som bygger på ETSI EG 202 057-2 [64]. Denne standarden definerer ”*Quality of Service (QoS): collective effect of service performance which determines the degree of satisfaction of a user of the service”*
Denne gjelder for dataoverføringer med modemer og SMS.

3.4.1 QoS i Bt

I Bt har man allerede fra konstruksjonen tatt hensyn til QoS, ikke minst av hensyn til det som er nevnt foran om at ISM båndet er utsatt for mye ukjent radiostråling.

Tabell 15 Innbygde QoS mekanismer i Bt.

Teknikk	Lokalisert	Utfører	Resultat
Frekvenshopping	Baseband laget	Sprer nytteinformasjonen over flere frekvenser.	Unnviker at all informasjon går tapt ved blokkering av en frekvens.
FEC	Baseband laget	Gjentar informasjonen og gjør signalene overføringsvennlige [91].	Gjør informasjonen tilgjengelig selv om deler av forbindelsen går tapt.
Paring	Link Manager Protocol	Autentiserer sammenkoblede parter.	Hindrer mottak fra ukjente enheter.
CRC	Link Manager Protocol	Sjekker datastrømmen for feil.	Kaster åpenbart feil data.
Kryptering	Link Manager Protocol	"Anonymiserer" datastrømmen.	Gjør avlytting meningsløst.

Tabell 15 gir en oversikt over QoS mekanismene i Bt, som det framgår finner vi disse mekanismene samlet i to lag i protokollstakken. Problemene med de beskrevne tiltakene er at Bt-enheter ofte lider og at kryptering utføres med enklest mulig nøkler og algoritmer [40 s.287-288]. Motivet for dette varierer, men liten datakraft og ønske om å spare strøm i enhetene er nærliggende.
Manglende QoS egenskaper i grunnsystemer kan kompenseres med innbygging av QoS i de applikasjonene som ligger øverst i protokollstakken. Problemet er da at disse er overlatt hver enkelt applikasjonsutvikler å implementere.

3.4.2 QoS i offentlige mobilnettet

GSM bygger på streng linjesvitsjing implementert for tale og er enkelt i sin oppbygging. QoS har derfor her stort sett gått på talekvalitet. Sikkerhet for brudd er god. SMS benytter kontrollplanet som meldings-befordrer og må betraktes som enda sikrere.
Figur 14 og Figur 27 viser en signalvei for videosamtaler når man ringer "lokalt". Er mobil-apparatet det ringes til utenfor regionen må man også innom transportnettet for fasttelefoni. ETSI (European Telecommunication Standardization Institute) har laget "3GPP TS 23.107 version 4.6.0 Release 4" [26] Denne standarden tar for seg QoS i GPRS og UMTS. At disse teknologiene skal være like med hensyn til QoS ble vedtatt av 3GPP TSGN WG1 GSM-UMTS Interworking and MM to UMTS Ad-hoc meeting 22-24.11.1999 Oulu, Finland. [28] I det følgende vil det som sies om UMTS også gjelde for GPRS. Dessverre er det ingen av mobiloperatørene i Norge som har innført denne standarden i sine nett. I stedet benyttes "best effort" i UMTS og GPRS. Krav til QoS ble definert i standarden EN 301 344 [33] fra september 2000. Standarden omhandler mye annet også, men ett delkapittel (15.2) omhandler QoS. Standarden innfører tre prioritetsklasser; høy, normal og lav. Standarden innfører også fire delay- klasser; 1 til 4 hvor 4 er betegnet "best effort". Det er imidlertid ikke noe krav om at andre delayklasser benyttes enn "best effort". Den kanskje viktigste er innføringen av pålitelighetsklassene (Reliability Classes) som beskriver bruken av overføringsprotokollene. (GTP, LCC og RLC) til forskjellige typer overføring.

Tabell 16 Pålitelighetsklassene i følge EN 301 344 Kilde [33]

Reliability Class	GTP Mode	LLC Frame Mode	LLC Data Protection	RLC Block Mode	Traffic Type
1	Acknowledged	Acknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that cannot cope with data loss.
2	Unacknowledged	Acknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that can cope with infrequent data loss.
3	Unacknowledged	Unacknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that can cope with data loss, GMM/SM, and SMS.
4	Unacknowledged	Unacknowledged	Protected	Unacknowledged	Real-time traffic, error-sensitive application that can cope with data loss.
5	Unacknowledged	Unacknowledged	Unprotected	Unacknowledged	Real-time traffic, error non-sensitive application that can cope with data loss.
NOTE: For real-time traffic, the QoS profile also requires appropriate settings for delay and throughput.					

Videre defineres to tabeller med overføringshastigheter den ene definerer topphastigheter mens den andre definerer gjennomsnittshastigheter
QoS parametrene ble ytterligere konkretisert i standarden EN 301 113 fra november 2000, som utfyller og delvis erstatter EN 301 344, tallfester nivået av QoS.

Tabell 17 Pålitelighetsklassene i følge EN 301 113 Kilde [34]

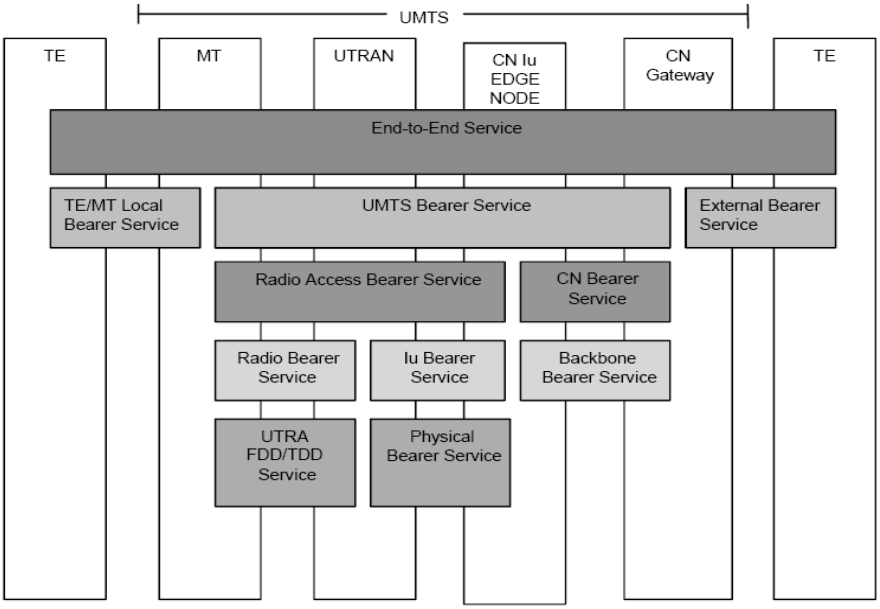
Reliability class	Lost SDU probability (a)	Duplicate SDU probability	Out of Sequence SDU probability	Corrupt SDU probability (b)	Example of application characteristics.
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}	Error sensitive, no error correction capability, limited error tolerance capability.
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}	Error sensitive, limited error correction capability, good error tolerance capability.
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}	Not error sensitive, error correction capability and/or very good error tolerance capability.

Sammenlignes disse tallene i Tabell 17 med anbefalingene i TS 123.107 ser man at klasse 1 gir for god leveringskvalitet, klasse 2 og 3 dekker så vidt kravene til videokommunikasjon hvor klasse 3 vil hakke i videobildet (på grunn av høyt pakkebortfall). Alle klassene er egnet for tale. Videre defineres maksimale delaytider i standarden. Delaytider er av stor viktighet når det gjelder kommunikasjon mennesker imellom (slippe å vente).

Tabell 18 Delaytider i EN 301 113 Kilde [33]

Delay Class	Delay (maximum values)			
	SDU size: 128 octets		SDU size: 1024 octets	
	Mean Transfer Delay (sec)	95 percentile Delay (sec)	Mean Transfer Delay (sec)	95 percentile Delay (sec)
1. (Predictive)	< 0.5	< 1.5	< 2	< 7
2. (Predictive)	< 5	< 25	< 15	< 75
3. (Predictive)	< 50	< 250	< 75	< 375
4. (Best Effort)	Unspecified			

Tabell 18 med delaytider viser at GPRS er dårlig egnet til direkte menneske - menneske kommunikasjon på grunn av de lange delaytidene. En sammenligning av verdiene anbefalt i TS 123.107 vedlegg A.2 viser dette. Her anbefales delaytiden for tale 0,1 sek. maks. ende til ende og for video 0,4 sek. maks. ende til ende.
Figur 28 under er hentet nettopp fra TS 123.107 og illustrerer de forskjellige områdene innen QoS i UMTS. Figuren avspeiler en gjensidig tjeneste / transportforhold i oppbyggingen av mobiltelefonnettet. Essens av figuren må leses slik: Kunden opplever ”end-to-end” service. Av dette er kunden selv ansvarlig for transporten i ”TE/MT local bearer service” siden dette er brukerens eget utstyr. (I vårt scenario inngår Bt-forbindelsen mellom sensorer og mobiltelefonen samt selve mobiltelefonen her.) Mobiltelefonoperatøren er ansvarlig for transporten i ”UMTS bearer service” siden dette er mobiltelefonnettet. Mobiltelefonoperatøren kan derimot ikke være ansvarlig for hva som skjer utenfor sitt nett (”External Bearer Service”).



Figur 28 UMTS QoS Arkitektur [26]

Siden mobiltelefonnettet er komplekst og kan modelleres i flere komponenter avspeiles disse i figuren. Radiodelen med styring og mellomkoblinger tas ut som en egen komponent under navnet ”Radio access bearer service”. Denne deles så i to mellom radio-utstyret (Radio Bearer Service) og mellomkoblingen til kjernenettet (CN) (Iu Bearer Service). ”Radio bearer service” bygger direkte på transporten i UTRA (radiosystemet i UMTS). Iu Bearer service bygger direkte på behandlingen i den fysiske mellomkoblingen. ”CN Bearer Service” betegner tjenestene kjernenettet tilbyr og bygger på transporttjenestene i kjernenettet. Behandlingen her i dette avsnittet avspeiler det som i figur 14. er betegnet ”UMTS bearer Service”. I den utstrekning fastnettet blir behandlet er dette i formål av sammenligning.
3GPP definerte i TS 23.107 fire tjenesteklasser for UMTS, hver med spesielle egenskaper for tiltenkt bruk.

Tabell 19 UMTS QoS klassene [26]

Traffic class	**Conversational class** conversational RT	**Streaming class** streaming RT	**Interactive class** Interactive best effort	**Background** Background best effort
Fundamental characteristics	- Preserve time relation (variation) between information entities of the stream Conversational pattern (stringent and low delay)	- Preserve time relation (variation) between information entities of the stream	Request response pattern Preserve payload content	Destination is not expecting the data within a certain time Preserve payload content
Example of the application	- voice	- streaming video	- Web browsing	- background download of emails

For bruk i vårt system er det tjenesteklassen ”Conversational” som kommer til anvendelse. Denne klassen betegner tjenester som trenger rask og presis levering av data i tid, men hvor dataene kan være beheftet med noen feil. De forskjellige parametrene som brukes for å styre samtalekvaliteten i klassen ”conversational” er:

Tabell 20 Parametrene i tjenesteklasse "Conversational" omarbeidet etter ETSI TS 123 107

Betegnelse	**Beskriver / formål**	**Enhet/kommentar**
Maximum bitrate	Den maksimale hastigheten som datastrømmen vil ha. /Beskytter utstyret mot for høye datahastigheter.	Kbps /Benyttes til beregning av pakkehastighet i transparent modus
Delivery order	Er det viktig at dataene kommer ordnet i riktig rekkefølge? /Ikke nødvendig ved ren filoverføring	Ja/Nei /Viktig ved taleoverføring.
Maximum SDU size	Den maksimale størrelsen av en datablokk (pakke) /Bestemmer hva nettverket må dimensjonere for.	Byte (oktett) Angis som alternativ til SDU format information
SDU format information	Presis informasjon om størrelsen på datapakkene dersom disse har bestemt størrelse. (som i videokommunikasjon) / Fast datablokkstørrelse kan overføres enkelt og billig.	Bits Bør tilpasses størrelsen på UTRAN pakkene i transparent modus. Angis som alternativ til Maximum SDU size.
SDU error ratio	Tillatt feilrate i overførte datapakker. / Benyttes til å beregne kodeskjema, protokoller og algoritmer for radiooverføringen.	
Residual bit error ratio	Forskjellige deler av overføringen kan ha forskjellig følsomhet for feil. / Benyttes til å beregne kodeskjema, algoritmer og protokoller for radiooverføringen.	Tale maks. 10^{-4} for klasse 1 pr. bit. Tale maks. 10^{-3} for klasse 2 pr. bit. Video: 10^{-6} – ingen synlig forringelse 10^{-5} – lite synlig forringelse 10^{-4} – noe synlig forringelse 10^{-3} – grense for praktisk bruk
Delivery of erroneous SDUs	Dersom pakker med feil ikke kan brukes er det ingen grunn til å sende dem over en link med dårlig	Yes: pakker med feil merkes og leveres. No: pakker med feil leveres ikke. ”-”: ingen feilsjekk, alle pakker leveres.

	kapasitet.	
Transfer delay	Maksimal tillatt forsinkelse gjennom nettet på 95 % av pakkene. / Beskriver om overføringstiden er viktig for opplevd kvalitet.	Viktig for tale og videokommunikasjon. Tale : 0.1 sek. Maks. ende til ende. Video : 0.4 sek. Maks. ende til ende.
Guaranteed bit rate	Minimum dataflyt som applikasjonen krever. Alle andre karakteristikker blir vedlikeholdt på dette nivået. / Brukes til kapasitetsreservasjoner i nettet.	
Allocation/ Retention priority	Samtaleprioritet. Settes av nettet.	Denne variabelen kan være nøkkelen i alarmsammenheng.
Source statistics descriptor	Trafikk beskrivende av tale./ tale har en velbeskrevet profil av data.	Speech / unknown

Legg merke til attributten ”Allocation / Retention priority” som er lagt inn for å gi gjennom-koblingen prioritet. I vårt scenario med alarmer kan dette være nøkkelen for å oppnå en sikker gjennomkobling. Det skal nevnes at i V4.6.0 er denne attributten er gitt en bemerkning om at ”The addition of a user-controlled Allocation / Retention Priority attribute is for further study in future releases.” Note 4 i [26]. Denne merknaden er beholdt i Rel 5.d.0 og Rel 6.4.0 pr. mars 2006, men med påskrift om at dette er en abonnement - variabel.
Interessant kan det være å se hvilke innvirkninger feil har på bildekvaliteten av videobilder. Flere enn en av tusen bit feil gjør videobildet ubrukelig [26]: vedlegg 2. Forklaringen på dette er at bildet er komprimert av codecen og pakket etter den aktuelle videooverføringsstandarden. (H263, H263L, H264AVC)

3.5 Muligheter for å øke sikkerheten i mobilnett

Sikkerhet kan deles inn i to. På den ene siden sikkerhet for at meldinger kommer fram, at samtaler blir gjennomkoblet og at ikke samtaler brytes. På den andre siden handler sikkerhet om dataintegritet, at samtalen eller meldingen kommer uskadet og uavlyttet fram. Tiltak for å bedre framkommelighet går på å gi prioritet og å kutte ned på antall utførelsesledd. Tiltak for å bedre dataintegritet går på kryptering.

3.5.1 Påvirkning av sikkerhet i Bt

Sikkerhetsnivået ved Bt tilkobling kan velges i tre kategorier, se tabell.

Tabell 21 Strategier for sikring av Bt etter [88]

Sikkerhetsmodus 1	Ikke sikker
Sikkerhetsmodus 2	Sikkerhet på tjenestenivå
Sikkerhetsmodus 3	Sikkerhet på linknivå

For Bt-enhetene gjelder valget mellom ”trusted” og ”untrusted” ved paring. ”Trusted” åpner opp for alle tjenester i enheten. Når det gjelder tjenestene i Bt har disse tre sikkerhetsnivåer:
Autentisering og autorisasjon, autentisering alene og åpen. Ikke alle mobilprodusenter har tatt sikkerhet i Bt like alvorlig [88]. Som nevnt tidligere har mange Bt-enheter liten datakraft, muligens motivert av lavt strømforbruk. Bluetooth SIG foreslår å benytte åtte karakterer eller lengre PIN koder for å generere sikkerhetsnøkkelen mellom enhetene, og å sette enhetene til ikke – avslørbar (non discoverable) [88].

3.5.2 Påvirkning av sikkerhet i offentlige mobilnett

For GPRS (og dagens UMTS) finnes som påpekt tidligere muligheten for å benytte faste IP-adresser (se Figur 23). Dette er imidlertid et tveegget sverd siden dette svekker datasikkerheten[85]. Fordelen er at man kutter ut to fjerntliggende operasjoner (DHCP tildeling og DNS oppslag) [46 s348].
I tilfellet UMTS så ventes det sterk forbedring innen kort tid med at mobiltelefonioperatørene innfører Release 4 med QoS. Dette vil gi muligheter til å kjøpe seg prioriterte samtaler og meldingstjeneste gjennom abonnementet [35, 36]. Rel-4 splitter også kjernenettet i kontrollplan og transportplan for å kunne kontrollere og dermed tilby tjenestekvalitet. Som kunde er du helt i mobiltelefonoperatørens hender når du har valgt abonnement. I GPRS er det ikke kjent at noen av operatørene kommer til å gi prioritet etter EN 301 344 eller EN 301 113. Både Telenor mobil og NetCom AS tilbyr faste IP adresser i sine nett i noen av sine tilbud [102,103]. Telenor indirekte ved at de tilbyr kunden å sette opp IP adressene via egen DHCP. NetCom ved å sette adressene fast i egen DHCP.

3.6 Abonnementløsninger

3.6.1 Tilknyttingsteknologier for tjenermaskiner

Ved alle data tilknyttinger til kjernenettet tilbys sikrede IP Tunneler (VPN Virtual Private Network) som førstevalg. Telenor har hatt tilbud om X.25 datapak, men faser ut dette [100] fra 2004. For SMS og MMS finnes ferdige løsninger for å motta og sende SMS gjennom en direkte tunnellering i internett til SMSC. Telenor tilbyr disse tjenestene under navnet SMS Bedrift og SMS Aksess. NetCom tilbyr dette som tjenesten telemetri og M2M [103,104]

3.6.2 Innholdstjenesteleverandører

Innholdstjenesteleverandører (CPA: Content Provider Access) er tjenestetilbydere som tar betaling for leverte tjenester eller varer (ringetoner, musikk, video, dataoppslag osv) via brukerens mobilabonnement. Det finnes mange tilbydere av tjenestene innen SMS og noen på MMS. Her er situasjonen at en leverandør har rettigheter til å dele sin aksess med flere andre (videresalg), dette er en absolutt mulighet for kommuner og mindre bedrifter. Imidlertid gjør vilkårene for bruk av denne tjenesten det vanskelig å bruke den til alarmformål. Bla. må brukeren bekrefte betaling før tjenesten er tillatt igangsatt og skal strykes fra kundelister ved innaktivitet i 60 dager [98, 101]. Ved en implementasjon må da applikasjonsprogrammet automatisk finne, lese og så automatisk svare på en SMS på brukerens vegne. Dette reiser problemer både av etisk og juridisk art.

3.6.3 Telenor

Telenor kan tilby et utvalg tilknytninger til meldingstjeneste og mobiltelefoni. Tjenestene varierer i pris og kundebredde.

Tabell 22 Abonnenttyper tilbudt av Telenor Mobil omarbeidet etter [97]

Abonnement / Applikasjon	Type	Betingelser	Pris / volum / betingelser
SMS Bedrift Outlock + gratis app.	Direkte kommunikasjon med SMSC gjennom internet m. kryptert VPN Tidligere datapak fases ut [100].	Abonnement på mobilapparater må være innen samme bedrift. + SDSL abonnement	Etablering kr. 7500 Månedspris kr. 750 Opp til 2500 SMS / mnd.
SMS Access	Direkte kommunikasjon med SMSC gjennom	Abonnement på mobilapparater behøver ikke være innen samme	Etablering kr. 7500 Månedlig kr. 6000

Outlock + gratis app.	internet m. kryptert VPN Tidligere datapak fases ut [100]. Femsifret telefonnummer	bedrift. + SDSL abonnement	Max 22000 SMS/ mnd sendt fra server til Telenorkunder [97].
SMS Access Med MMS Outlock + gratis app.	Direkte kommunikasjon med SMSC gjennom internett og kryptert VPN Tidligere datapak fases ut [100]. Femsifret telefonnummer	Abonnement på mobilapparater behøver ikke være innen samme bedrift. + SDSL abonnement	Etablering kr. 9500 Månedlig kr. 6500 Max 22000 SMS / mnd sendt fra server og 700 MMS sendt fra server til Telenorkunder [97].
Mobil Data Aksess Krever egen applikasjon.	Generell data-kommunikasjon over GPRS med kryptert IPtunnel til GGSN. Kryptert IP Tunnel i internett mellom server og GGSN.	Abonnement på mobilapparater behøver ikke være innen samme bedrift. + SDSL abonnement	Etablering kr. 15000 Månedlig kr. 2000 [99]
CPA Krever egen applikasjon i server.	Direkte kommunikasjon med SMSC gjennom Internett m. kryptert VPN.	Abonnement på mobil- apparater behøver ikke være innen samme bedrift. Innholdsleveransestjenester for fri avbenyttelse i mobilnett. + SDSL abonnement	Første Etablering kr. 50000 Tilleggs etablering Kr 20000 Månedlig Kr. 3000 Tillegg ut over første kr.1000 [98] Innholdsleverandører kan selge videre tjenester til andre virksomheter.
Mobilabonnement Bedrift	 Bedrift Bedrift Basis Bedrift Netto	 Mindre enn 15 min tale pr dag Mindre enn 5 minutter daglig Uten subsidiering av utstyr Daglig bruk er samtale utenfor bedriften. Interne samtaler (tale) minuttpris kr 0,- kun startpris.	Etablering kr 150,- Månedspris / minutt / start 119,- / 0,59 / 0,48 49,- / 0,99 / 0,59 59,- / 0,59 / 0,59 SMS kr 0,59 MMS kr 1,59 Tale tilegg andre operatører enn Telenor kr 0,38 * min
Mobilabonnement Bedrift	Bedrift Proff	Mer enn 15 minutter daglig utenom bedriften. Interne samtaler (tale) minuttpris kr 0,- kun startpris. Ingen tilegg for telefoni til andre operatører	Etablering kr 150,- Tale kr 0,39 * min Start kr 0,59 SMS kr 0,59 MMS kr 1,59
Mobilabonnement Privat / Bedrift	GSM Alarm	Lav trafikk < 2,4 MB pr. måned Støtter : SMS, MMS, videotelefoni, GPRS, EDGE, UMTS og CSD	Etablering kr 100,- Månedspris kr 16,- SMS kr 1,59 MMS kr 1,59 Startpris Tale 0,49 Tale kr 4,50 / min

3.6.4 NetCom AS

Også NetCom AS tilbyr lignende løsninger som Telenor mobil. De har en litt annen profil på tjenestene og fakturerer pr tjeneste i stedet for pr. pakke.

Tabell 23 Abonnenttyper tilbudt av NetCom omarbeidet etter [105, 106]

Abonnent / applikasjon	Type	Betingelser	Pris / volum
Telemetri	Dataforbindelse direkte til SMSC / MMSC over internett. Innebefatter generell dataoverføring. INGEN VPN	Autentisering må skje hos bedriften	Etablering kr 100 Månedsavgift kr 25 Pr SMS kr. 0,81 GPRS pr MB kr 16 [105] GSM oppstart kr 0,39 GSM til NetC kr 4.02 /m GSM til Fastlinje 4,02 / m GSM til Telenor 4,02/m
M2M VPN	Dataforbindelse direkte til SMSC med kryptert VPN over internett. [108]	Private IP adresser Forutsetter Telemetri	Etablering kr 10000 Månedspris kr 2000 Fast IP kr.29 pr. SIM [106]
M2M Basic	Dataforbindelse med fast IP på håndapparat og brannmur mot kunde [107] INGEN VPN	Kunde er ansvarlig for autentisering og autorisering. Forutsetter Telemetri	Etablering kr 0 Månedspris kr 89 pr SIM [106]
Business Talk	Mellom mobilabonnenter	Bedriftsabonnement med en faktura. Subsidierte telefoner.	Etablering kr 161,30 Månedspris Pr. apparat kr 125 Internt i bedrift Kr 0 Ringepris kr 0,69 /min Startpris kr. 0.48 SMS kr 0,59 MMS kr 1,59
Business Talk Basic	Mellom mobilabonnenter	Bedriftsabonnement med en faktura. Ikke subsidierte telefoner.	Etablering kr 161,30 Månedspris Pr. apparat kr 59,00 Internt i bedrift Kr 0 Ringepris kr 0,59 /min Startpris kr. 0,48 SMS kr 0,59 MMS kr 1,59
FamilyBusiness	Familietilbud til ansatte i bedrift hvor det finnes bedriftsavtale.	Familiemedlemmer har ikke intern ringepris.	Etablering kr 161,30 Månedspris Pr. apparat kr 55.65 Ringepris kr 1,36 /min Startpris kr. 0.48 SMS kr 0,56 MMS kr 1,59

4 Metoder

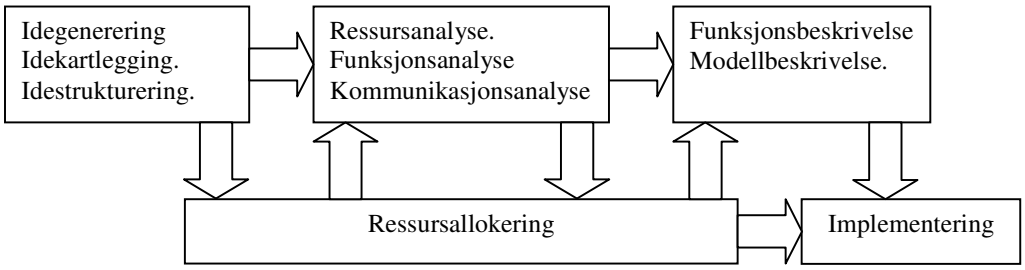
4.1 Tillempning av kontekstuell design og brukerdesign

For å ha et utgangspunkt er det ønskelig å lage en brukerbeskrivelse for slike system som vi diskuterer. En metode som kan benyttes er å kombinere kontekstuell design med en metode for brukerdesign benevnt "Focus Group" [11s 267]. Samtidig må metoden tilpasses et presset tidsskjema. Dette tenkes gjort på den måten at det samles et brukerpanel bestående av en håndfull personer med forskjellig bakgrunn innen geriatri og teknologi. Det må finnes nok kompetanse i et slikt brukerpanel til å gi normative utsagn til prosjektet. Grensebroen Arena besitter en del kontakter som skal kunne inneha nødvendig kompetanse. Tillempet metode er beskrevet i vedlegg 0.
En tillempning er nødvendig ut fra hensynet til brukerpanelets størrelse og sammensetning. Kontekstuell design [58] består vanligvis av 7 lenkede aktiviteter som spenner fra observasjon og kartlegging av eksisterende (arbeids-) metoder via sikring, analyse og restrukturering til ny sikring og implementering sammen med brukerne. Dette faller godt sammen med brukerdesignmetoden "Focus Group", som bygger på samme metode, men har et annet fokus. Forskjellen kan grovt oppsummeres til at kontekstuell design har kjent utgangspunkt og ender opp i ukjent system mens man i brukerorientert design ofte ikke har noe konkret kjent utgangspunkt, men vet hva man vil ha.

4.2 Metoder for utvikling av mobiltelefonapplikasjoner

4.2.1 UML diagrammer og modellering

Forut for en implementering må følge en planlegging av hvordan det tenkte objektet skal fungere. Dette gjelder uansett om konstruksjonen er et byggverk, mekanikk, elektronikk eller programvare. Meget grovt og meget generelt sett følger all byggevirksomhet følgende aktiviteter:



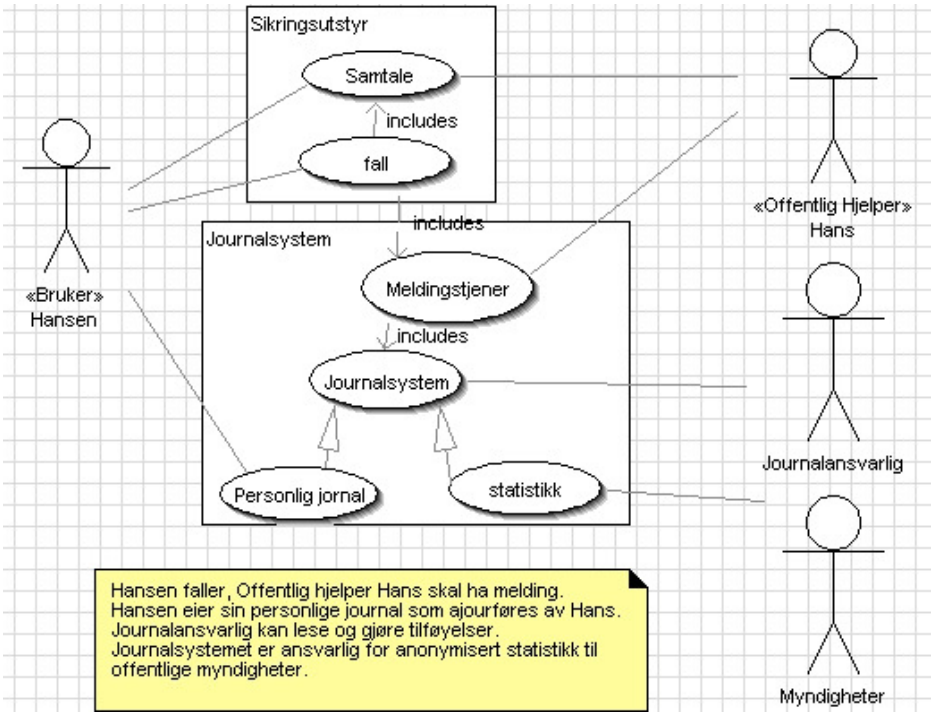
Figur 29 Generell aktivitetsplan

Universal Modelling Language; (UML®) [8] har sitt utspring i data- sammenslutningen Object Management Group (OMG) som står for spesifikasjonen og leder an i arbeidet med å standardisere symbolspråket. OMG eier også varemerket UML. At de flere disipliner har fellestrekk innen utvikling har ledet til at språket har fått tilhengere innen flere bransjer, ikke bare databransjen. Modeller kan finnes på flere nivå, fra de mest konkrete (og i noen tilfelle kjørbare) applikasjoner, til metamodeller (MOF: Meta Object Facility) som gir grunnlaget for tolkningen av modellspråket i seg selv [109]. Målet er å gjøre applikasjoner og data uavhengige av maskinvare og programmeringsspråk ved å definere data og

applikasjon sammen i et beskrivende språk som beskriver nødvendig applikasjon slik at applikasjonen kan genereres automatisk via Modell Driven Architecture [109].
UML består i to deler; infrastruktur og ”superstructure” tilknyttet disse er et tredje språk : Object Constrain Language (OCL). Infrastruktur [110] beskriver de grunnleggende komponentene i UML og definerer UML som språk (meta-metamodell) mens ”superstructure” [111] beskriver brukermetodene; kilde [112].
UML beskriver til sammen tretten forskjellige skjemaer i tre forskjellige kategorier: Struktur, oppførsel (behavior) og samarbeid (Interaction). De mest brukte diagrammene er i struktur- kategorien; klassediagram og objektdiagram. I oppførsel finner vi Use-Case diagram, aktivitetsdiagram og tilstandsdiagram. I samarbeidskategorien finner vi bl.a. timing diagram.
Det er gjort store anstrengelser for å gjøre symboler og tegn så intuitive som mulig. Jeg vil derfor kun introdusere diagramtypene som følger i senere kapittel.
Det finnes flere verktøy hvor det er mulig å bruke UML. Det mest nærliggende er å benytte verktøyer basert på åpen kildekode. Både fordi verktøyene er billige (i visse tilfelle gratis) og fordi de ofte holder en brukbar kvalitet. Omondo er et slikt verktøy [112] som fungerer til vårt formål. Sammen med CarbideJ fra Nokia for programmering av Nokia mobiltelefoner vil vi kunne dokumentere og kode javaprogrammer. Omondo bygger på programmeringsplattformen eclipse som igjen kjører ved hjelp av java virtuell maskin (JVM). Det hele koker ned til at du trenger en litt kraftig datamaskin som kan kjøre JVM for å drive programutvikling.

4.2.2 Use-Case diagram

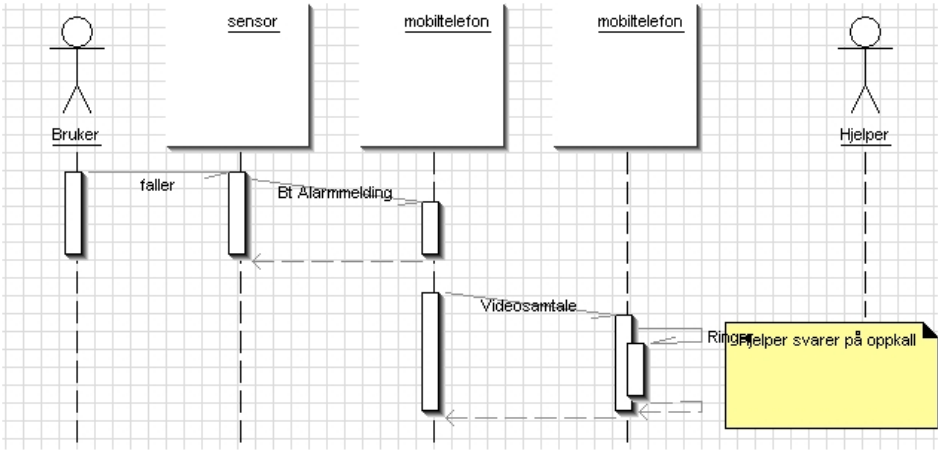
Under vises et use-case diagram som uttrykker prinsippet i løsning med offentlig bruk: 5.1.4.
Brukeren har en relasjon til sikringsutstyr som trer i virksomhet ved aktiviteten ”fall”.
Utstyret benytter journalsystemet for å få en relasjon til Hans som er på jobb i det aktuelle øyeblikket.
Hansen har en relasjon til sin personlige journal som er en del av journalføringen som Hans må utføre.
Journalsystemet inneholder også en statistikk som inngår i den generelle journalføringen.



Figur 30 Use-Case diagram

4.2.3 Sekvensdiagram

Sekvensdiagrammer benyttes for å poengtere årsak virkningseffekter og hendelseskjeder. Et eksempel er diagrammet under som forenklet er ment å illustrere tilfellet med privat hjelper.
Brukeren faller, sensoren oppdager fallet, sensoren sender melding til telefonen til brukeren. Brukerens mobiltelefon ringer videosamtale til hjelperens mobiltelefon.



Figur 31 Sekvensdiagram

De enkelte symbolene i diagrammet forstås slik: Tidsakse er nedover i figuren, rektangler i markeringslinje betyr aktivitet i vedkommende objekt. Aktiviteter som starter andre aktiviteter kan ikke avsluttes før barn-prosessen er fullført. Pil betegner en hendelsesstart (som også kan være start på avslutning), Pil tilbake til utgangspunkt er ventefunksjon.

4.3 Symbian og Java™

4.3.1 Verktøyet Carbide.J

Nokia har utgitt et programmeringsverktøy for sine mobiltelefoner for programmering i Java™ 2 ME. Verktøyet finnes i fem versjoner; frittstående, for integrering med eclipse, for integrering med Borland JBuilder, NetBeans og IBM® WebSphere Studio Device Developer. Programmeringsverktøyet kan karakteriseres som en mellomting mellom fullt programmeringsmiljø og programmeringsverktøy. Verktøyet har en simpel form for UML støtte. Verktøyet inneholder et sett med emulatorer for hver hovedtype av Nokia mobiltelefoner integrert i verktøyet er også støtte for overføring av programmer til fysiske mobiltelefoner.

4.3.2 Sanntids videostreaming og Java™

Videostreaming fra mobiltelefonen kan kun skje etter at videoen er tatt opp [124]. Applikasjonsutvikling med Java på Symbian S60 og sanntids video- streaming er ”ikke anbefalt” i henhold til denne kilden, men foreslår å benytte Symbian C++ isteden se Tabell 24.

Tabell 24 Muligheter i Java™ contra Symbian C++ [124]

Video Use Case	Symbian C++ Support	Java™ Support
Play a local file or RTSP stream using the S60 Media Player and RealPlayer engine	Use AppArc APIs (RApaLsSession) to launch the S60 Media Player application	Use MIDlet.platformRequest to launch the platform Media Player
Play a local file or RTSP stream using a custom UI and RealPlayer engine	Create your own UI and use the CVideoPlayerUtility API to play and control a file or URL	Use JSR-135
Play a local file with your own player	Create your own player. Use CMdaAudioOutputStream for audio rendering (1) and CDirectScreenAccess APIs for video rendering	Not recommended
Stream video content using your own player	Use network APIs (RSocketServ, RConnection, RSocket) to connect to the network (2). Then use CMdaAudioOutputStream for audio rendering (1) and CDirectScreenAccess APIs for video rendering.	Not recommended
Implement a custom MMF plug-in	Use MMF APIs (CMMFController, CMMFCodec, etc.)	Not possible

(1) CMdaAudioOutputStream can decode some formats on some devices, if a DevSound codecs for the respective formats are present on that device.
(2) The high-level streaming protocols (e.g. RTSP, RTP, RTCP, SDP) have to be implemented by the application.

4.3.3 Programverifisering, signing i Symbian

Symbian Software Limited (Symbian) tilbyr en programverifiserings rutine med det formål å kvalitetssikre programmer mot Symbians vedtatte regler, under foretningsprogrammet Symbian Signed. Programmet tilbys til applikasjoner som er utviklet under Symbian OS v9 og senere. Sentralt i programmet står symbians nettsider [127] hvor man må registrere sitt medlemskap og bli tildelt identifikasjoner og signeringsnøkler. Prosessen består i at man benytter et sett ”pre-signing test tools” for å avdekke uoverenstemmelser med Symbians programmeringsregler (Som også er listet som ”Symbian Signed Test Criteria” på samme nettsted) Videre sendes applikasjonen signert med privat nøkkel sammen med sertifikat til Symbian for testing i et tilknyttet testhus. Hvis applikasjonen passerer vil denne bli signert på nytt med VeriSign sitt sertifikat og bli registrert i VeriSign sitt arkiv. Symbian utgir en lukket katalog over applikasjoner for distributører hvor applikasjonen blir registrert. For å få tildelt en signeringsnøkkel må man registrere et firma, registreringsavgift er for tiden USD 350 årlig. For privatpersoner som ønsker å utgi programvare må man gå gjennom ”Publisher Certifiers”, firmaer godkjent av Symbian til å pre-teste og sende inn applikasjoner på vegne av andre.

5 Prinsipper for løsning

5.1 Systemarkitektur

5.1.1 Bt forbindelsen

Bt forbindelsen vil være et svakt punkt i alarmsystemet. Derfor er det viktig om varsling til bruker og alarmsentral dersom denne forbindelsen er ute av funksjon. Selve forbindelsen kan realiseres med profilen SSP for enkel implementasjon i java. Av nyttesignaler som må overføres er selve alarmen og batteritilstand.

Tabell 25 Bt meldinger

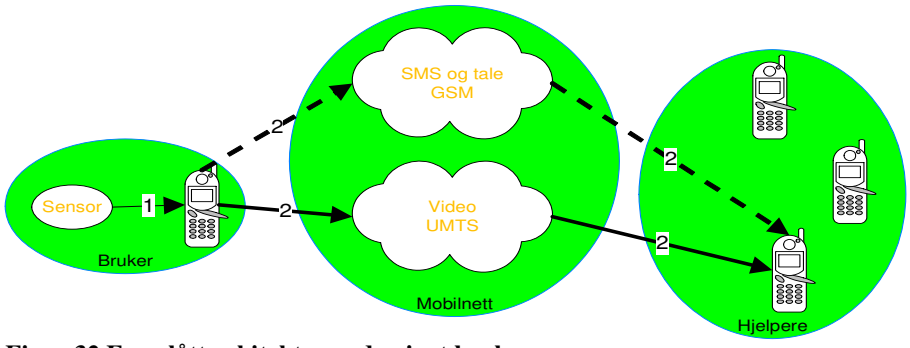
Melding fra mobiltelefon	Respons	Varighet til neste	Utløser	Kommentar
søk	søk		Bonding	Sensor har fast PIN
Paring	Paring	Kun en gang	Sikret forbindelse	
Polling status	Status ev. med alarm	1 sekund	Hvis alarm, SMS Alarm	Sensor er slave
Polling status med batteri tilstand	Batteristatus + ev alarm	Hvert 1024 polling tilsvarer 17 min. 4 sek.	Talemelding i mobiltelefon dersom batteristatus er lav. Display av batteristatus. SMS Alarm dersom dette er indikert	Tilstrekkelig med når batterikapasiteten er såpass stor som minimum fem døgn.

5.1.2 Videooverføring

Som vist i 4.3.2 tillater ikke kombinasjonen utvikling i JavaTM og Symbian S60 sanntidsoverføring av videobilder fra kamera på noen annen måte en videotelefoni. (”ikke anbefalt” i veiledningen [124]) Dette setter en effektiv stopper for bruk av eksterne kamera på telefonen. Imidlertid finnes muligheter ved bruk av Symbian C++. Vi er dermed henvist til å benytte mobiltelefonens innebygde programvare for videotelefoni og mobiltelefonens kamera for videotelefoni.

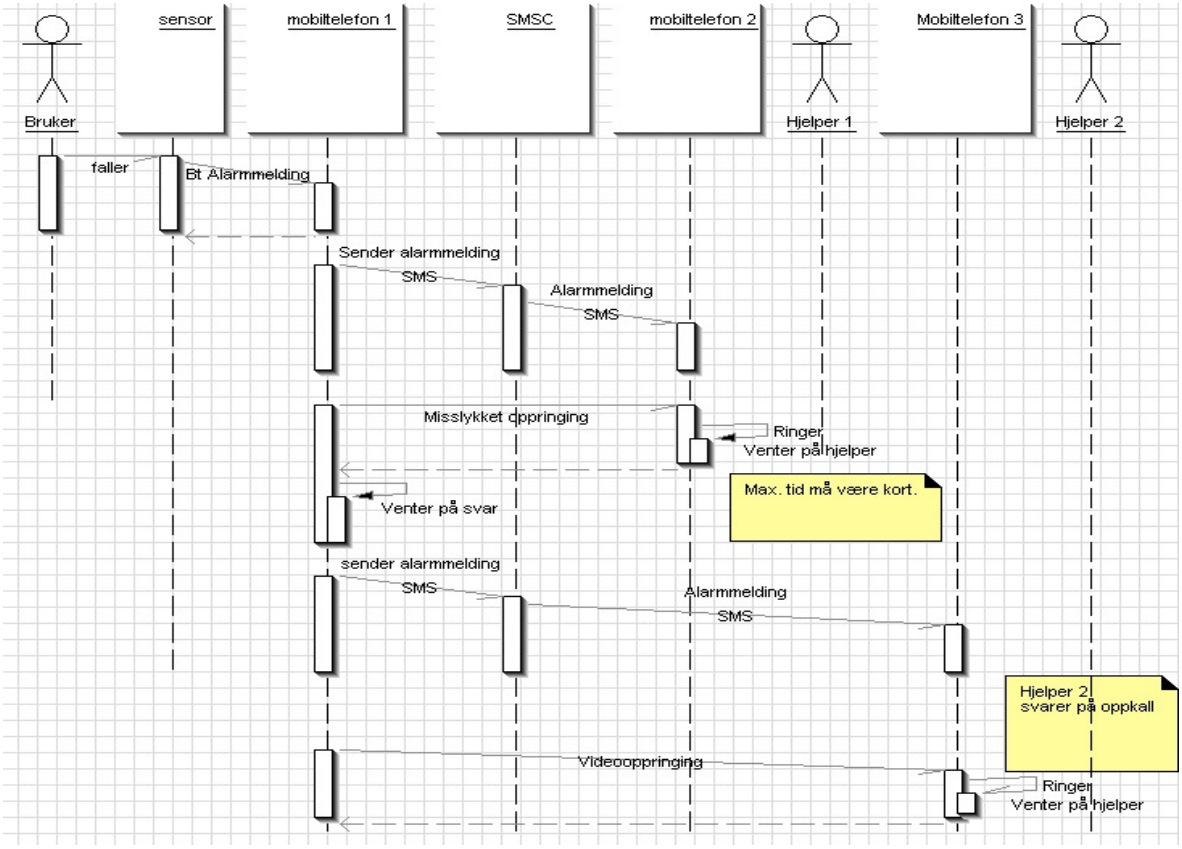
5.1.3 Privat bruk

Som det framgår av innledningen må det skilles mellom privat og offentlig bruk av systemet. Ved privat bruk vil alle krav til journalføring og lagring falle bort. Det er da tilstrekkelig med en enkel oppringing mot den private hjelperen. Siden det ikke kan garanteres dekning i UMTS og dermed pålitelig videoforbindelse må oppringningsrutinene dekkes opp av SMS og taleoppringing.



Figur 32 Foreslått arkitektur ved privat bruk.

Som det framgår av Figur 32 vil en sensor gi melding til mobiltelefonen. En SMS melding syntetiseres og sendes hjelperen. Mobilapparatet må avgjøre om det har mulighet til å ringe videosamtaler, hvis ikke dette er mulig må vanlig talesamtale benyttes. Mobiltelefonen vil da ringe en samtale til 1. hjelper. Dersom det ikke oppnås svar bør mobiltelefonen gjenta prosedyren mot en annen hjelper.
Dette fordrer en kontaktliste i mobilapplikasjonen. Skal systemet ha noen mening må det finnes flere hjelpere. Brukerpanelet var meget klar på at hjelp i ulykkestilfelle ikke er noen privatoppgave, men en del av det offentliges ansvarsområde. Figur 33 viser sekvensen som applikasjonen bør arbeide etter.

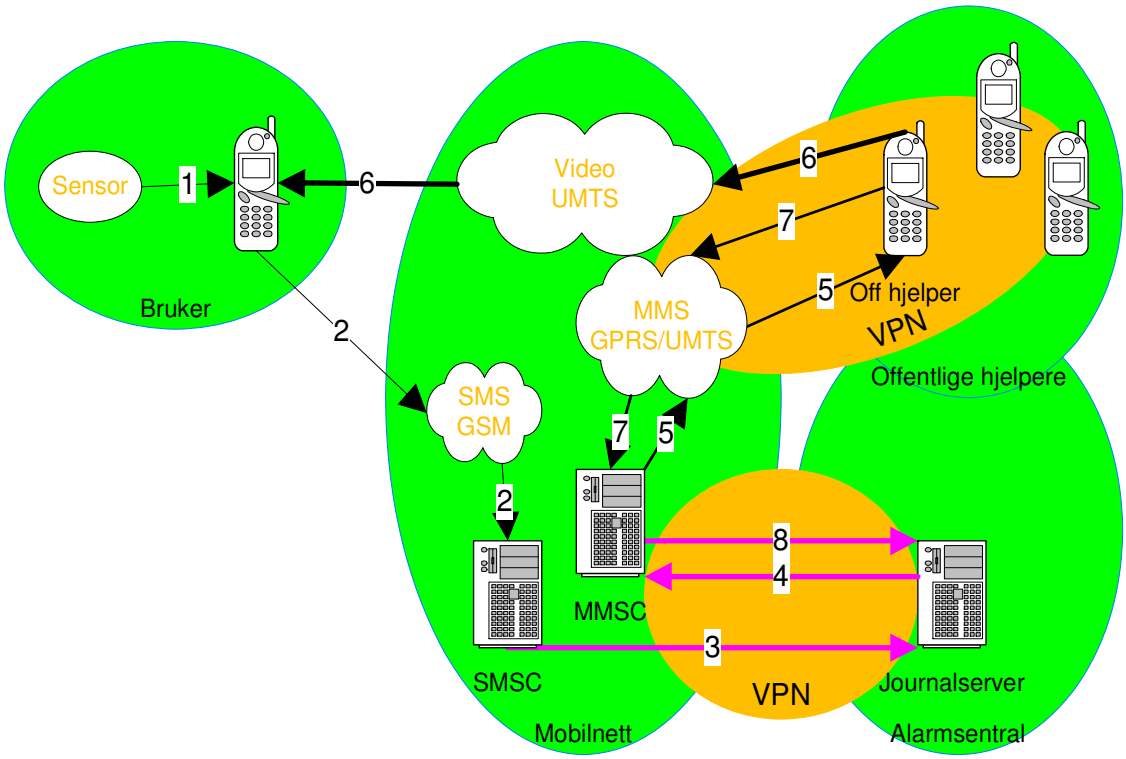


Figur 33 Alarmoppringning, sekvens for privat bruk

Kommentar til Figur 33 er at telefonsamtalen høyst sannsynlig vil nå hjelperen før SMS meldingen fordi SMS meldingen buffres i SMSC.

5.1.4 Offentlig bruk

Ved offentlig bruk må helselovgivning og forskrifter omhandlet i 2.3.2 følges. Dette innebærer bl.a. Journalføring og sikring av journaldata. Det foreslås derfor at selve alarmmeldingen overføres med SMS for å bli registrert i en meldingstjener som registrer alarmen for så å sende alarmen videre til en offentlig hjelper med ny MMS melding. Hjelperen må da ringe opp brukeren med videosamtale hvis dette er mulig, hvis ikke må talesamtale benyttes. Det er mulig og anbefales å automatisere denne oppringningen. På samme måte som for private hjelpere må ubekreftede meldinger føre til ny MMS melding til en annen hjelper. MMS anbefales fordi den gir mulighet for automatisk kvittering.



1 Alarmmelding fra sensor over Bt.
2 SMS til SMSC over kontrollplan i GSM.
3 SMS Alarmmelding fra SMSC til Journalserver over internett VPN. Journalserver sender kvittering til brukerapplikasjonen.
4 – 5 MMS Alarm til hjelper via MMSC og VPN. Gjentas til andre hjelpere ved manglende kvittering.
6 MMS Hjelper ringer, bruker fortrinnsvis videosamtale.
7 – 8 Hjelper avkvitterer i journal.

Figur 34 Foreslått arkitektur og meldingskjede ved offentlig bruk.

Den foreslåtte arkitekturen bygger på følgende erkjennelser:

- UMTS vil ikke bli utbygd til å dekke alle lokasjoner.
- UMTS er mer utsatt for radioskygger enn GSM / GPRS inne i bygninger.
- GPRS gir ingen ekstra verdi for korte meldinger utenom mulighet for kvitteringsmelding.
- SMS har sikkerhets og trafikkfordeler i radiosystemet fordi det følger kontrollplanet til GSM. Dette gjelder kun dersom UMTS er utilgjengelig.
- Alle meldinger må bekreftes av applikasjonen / hjelper.

Føreste erkjennelse bygger på det faktum at konsesjonsvilkårene for UMTS slår fast at utbygging skal dekke alle tettsteder med over 200 innbyggere. Dette betyr at landsbygd, utmark og skog- områder vil være uten dekning. Dette betyr for vårt system at mobiliteten til brukeren blir svært svekket dersom det forlanges videosamtale.
Andre erkjennelse innebærer at brukeren kanskje ikke har UMTS dekning på toalettet selv om det er dekning i stua. Brukeren vil da ikke kunne stole på systemet inne i sin egen boenhet. SMS er da et bedre valg siden denne tjenesten også dekkes av GSM nettet med forventet større gjennomtrengningsevne.
Tredje erkjennelse går på at GPRS ikke har noen nytteverdi dersom video eller bilde ikke kan rettes mot interessante objekt. Ved et fall er nytteverdien av informasjonen i et bilde svært begrenset dersom bildet blir tatt i ei lomme eller veske. Det er først når samtalen starter at videobilder kan gi verdifull informasjon.
Denne og neste erkjennelse åpner muligheten for å benytte enkel og sikker SMS som alarmbærer.
Siste erkjennelse går på at meldinger må bekreftes av hva eller hvem som tolker meldingene. Dette sikrer at innholdet i meldingene blir forstått og handling blir utført. Det er derfor logisk å sende bekreftelse på melding først etter at resultathandling er utført.

5.1.5 Applikasjonen i mobiltelefonen til brukeren

Prinsippene over indikerer at følgende funksjoner må utføres av mobiltelefonapplikasjonen:

- ved privat bruk:
- Oppkobling og vedlikehold av Bt-forbindelse til sensor.
- Generering av SMS - alarmmelding og sending.
- Sette mobiltelefon i håndfri modus med høyttaler aktivert. Spille av talemelding.
- Oppringing av hjelper, fortrinnsvis som videosamtale.

- Ved offentlig bruk:
- Oppkobling og vedlikehold av Bt-forbindelse til sensor.
- Generering av kryptert SMS -alarmmelding og sending.
- Overvåkning av bekreftelse på alarmmelding.
- Eventuelt gjenta alarmmelding.
- Klargjøring for alarmsamtale: sette mobiltelefonen i håndfri modus for automatisk svar og med håndfri høyttaler aktivert. Spille av talemelding.

5.1.6 Applikasjonen i hjelpers mobiltelefon

Ved privat bruk er det ikke nødvendig med applikasjon i hjelpers mobiltelefon ut over at mobiltelefonen må støtte SMS og videotelefoni.
Ved offentlig bruk bør telefonen inneholde applikasjon som:

- Hurtigvalg for sending av kvitteringsmelding og oppkobling til bruker, fortrinnsvis som videosamtale.

- Påminnelse om journalføring etter alarm. Det bør likevel sendes påminnelse fra meldingstjener dersom journalføring uteblir.

5.1.7 Serverapplikasjon

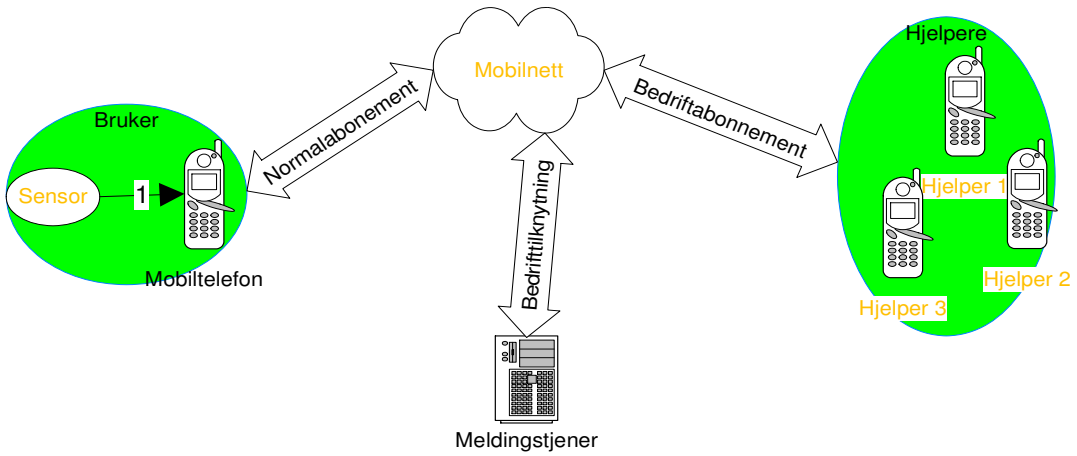
Ved offentlig bruk bør en meldingstjener benyttes for å ajourføre alarmer og knytte disse til tilgjengelige offentlige hjelpere. Meldingstjeneren bør inneholde database med minimum følgende informasjon:

- Tidsskjema med hvem som er primærhjelper for hvilken bruker.
- Eventuelt supplert med "flåtestyring" via posisjonsbestemmelse.
- Logg for innkommende alarmer, inneholdende varslinger til hjelpere.
- Funksjoner for sikring og kryptering av loggen j.fr. seksjon 2.3.2 om konfidensialitet.
- Funksjoner for generering og oppfølging av MMS alarmmeldinger til hjelpere.
- Rutiner for behandling og loggføring av hjelpernes journalføring etter hjelp.

Helsepersonellovens krav om journalføring på person må møtes. Dette kan gjøres ved at meldingene sorteres i egne logiske mapper.

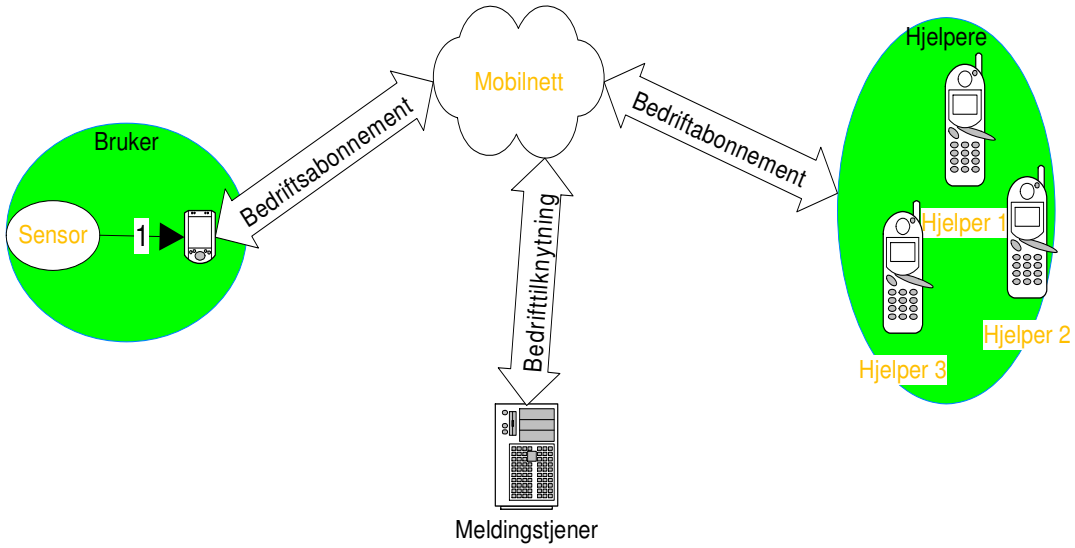
5.2 Tilgjengelige tjenester

I det foreslåtte systemet er det muligheter for tre typer abonnement; brukerens meldingstjenerens og hjelpernes abonnement. Brukere kan ha forskjellig behov. Noen brukere vil foretrekke å ha en "vanlig" mobiltelefon og bruke den som dette, men med alarmen som tillegg. Andre vil foretrekke en dedikert alarmenhet. Utsagn fra brukerpanel viser også at det neppe finnes en løsning som er optimal for alle brukere. Bruksmåten angir typen av abonnement for brukeren. Ønsker brukeren en dedikert alarmenhet uten telefonmuligheter vil et bedriftsabonnement teknisk sett være å foretrekke. Hjelpeorganisasjonen må da stå som eier av abonnementet. Brukere som ønsker å benytte mobiltelefonen som vanlig mobiltelefon vil velge alarmen som en tjeneste. I dette tilfellet er det ikke noe i veien for at brukeren fortsetter sitt private abonnement etter å ha fått installert brukerapplikasjonen og opplæring i denne.
På den private hjelperen side er det heller ikke nødvendig eller formålstjenelig med noe ekstra abonnement. Vanlig mobilabonnement som støtter videotelefoni holder.
På den offentlige hjelperens side er det også visse valgfriheter, men trolig vil de fleste organisasjoner foretrekke å utstyre sine hjelpere med en tjenestetelefon. Det er da naturlig at det benyttes et bedriftsabonnement til disse. I alle tilfelle må kommunikasjonen med hjelpere, som i lovens forstand inneholder helseopplysninger, beskyttes av VPN.



Figur 35 Nødvendige abonnement ved offentlig bruk

Meldingstjeneren må for å møte kravene til datasikkerhet kobles til SMSC med en VPN tunnel. Det er her nødvendig både med et abonnement for SDSL linjen og for tilgangen til SMSC gjennom VPN.
Figur 35 viser tilfellet ved offentlig bruk der brukeren ønsker å benytte mobiltelefonen til vanlige teletjenester. Et alternativ er vist i Figur 36 hvor brukerens mobiltelefon er låst til kun alarm- funksjonene.



Figur 36 Variant hvor brukeren har dedikert alarm

5.3 Valg av mobiltelefon

5.3.1 Aktuelle operativsystem

I dag finne stort sett fire operativsystem til mobiltelefoner. ZDNET Networks artikkel ”A guide to handheld operating systems” [32] gir en oversikt over disse. Her faller Palm ut fordi den ikke ser ut til å utvikles videre, utviklingsselskapet er kjøpt opp og den siste versjonen av operativsystemet ble aldri brukt, selv ikke av palm selv. Windows Mobile Ver.6 er det siste som har kommet på markedet fra Microsoft.[73]. God integrasjon med andre Microsoft produkter og multimedia, støtter Iptelefoni over Wi-Fi men ikke sømløs overgang mellom Wi-Fi og UMTS. Blackberry støtter ikke videotelefoni, men har meget god støtte for email. Symbian støtter videotelefoni og sømløs overgang mellom Iptelefoni over Wi-Fi og UMTS. Samt kan kjøre Blackberry sitt epostsystem. Det er verdt å merke seg at disse funksjonene må implementeres også hos mobilnettoperatøren. I senere ZDNET Networks artikkel ” Access launches mobile Linux push”[69] og ” Palm touts stability of Linux-based Treos” [70] anonserer at palm utvikles videre med linux som kjerne og skal lanseres i full skala i løpet av 2007. Også norske Trolltech har linux utviklingsmiljø klart for mobiltelefoner i løpet av andre kvartal 2007. Det betyr at det enda er litt tid igjen før Linux er aktuell på telefoner i butikkhyllene.
Man sitter altså igjen med to aktuelle operativsystem: Windows Mobile og Symbian. Resultatene fra funksjonsbeskrivelsen gir ingen krav som favoriserer mellom operativsystemene. Derfor står valget mellom hvilke programmeringsmiljø man vil velge å benytte. Windows Mobile er knyttet opp mot .NET teknologien [74], mens Symbian har verktøy i C og Java [72].

5.3.2 Valg av personlig nettverkteknologi

Det finnes flere PAN (Personal Area Network) tilgjengelig, og flere teknologier er i modningsfasen. I dette prosjektet velger vi Bt intuitivt ut fra at de aller fleste avanserte mobiltelefoner leveres med denne løsningen.

5.3.3 Kriterier.

Ut fra funksjonsbeskrivelsen skal utstyret møte følgende krav:

Tabell 26 Krav til mobiltelefon

Bruker / System	Krav	Bruker	Hjelper
Brukerkrav	Ha stor skjerm med tydelig display og mye bakgrunnslys	X	X
Brukerkrav	Få, men store taster og tydelige ikoner	X	X
Brukerkrav	Tåle et fall	X	X
Brukerkrav	Skal varsle når systemet ikke fungerer	X	X
Brukerkrav	Kunne brukes som fjernkontroll til elektriske installasjoner i boenheten	X	
Systemkrav	Skal kunne programmeres i Java (Spesifisert i oppgaven)	X	X
Systemkrav	Skal ha Bt mellomkobling	X	
Systemkrav	Skal ikke være av foldetype	X	
Systemkrav	Skal ha videokamera for videosamtaler på front	X	X
Systemkrav	Bør ha innebygd GPS.	X	

Av de listede kravene over er et av brukerkravene og to av systemkravene ikke absolutte. Dette gjelder kravet om å kunne brukes som fjernkontroll til intelligent hus og kravet om GPS samt Java som programmeringsspråk. GPS blir etter hvert standard på avanserte mobiltelefoner, i mellomtiden blir eksterne GPS med Bt mellomkobling stadig mindre og billigere. Pris for ekstern GPS med Bt mellomkobling ligger i skrivende stund i prisleiet under 1000 kr og størrelse som ei (lita) sigarettpakke. Hjelper er krysset av til å forlange stor skjerm med tydelig display og godt bakgrunnslys. Dette har med ergonomi i hverdagen å gjøre, hjelperne vil ha stort display for å kunne se detaljene i bildene fra brukeren tydelig. Store taster er viktig for å unngå å famle i en tidspresset situasjon.

5.4 Beskrivelse av sensor

Konstruksjon av enheten faller utenfor oppgaven, her skal derfor kun nevnes kritterier til enheten. Det sees bort fra muligheten til å kombinere fallsensoren med GPS – modul. Dette er i så fall opp til eventuell produsent.

5.4.1 Kriterier for sensorenhet

Til sensorenheten finnes det noen krav som er naturlige å stille etter gjennomgang av brukerkrav og systemkrav.

Tabell 27 Nøkkelkriterier for fallsensor.

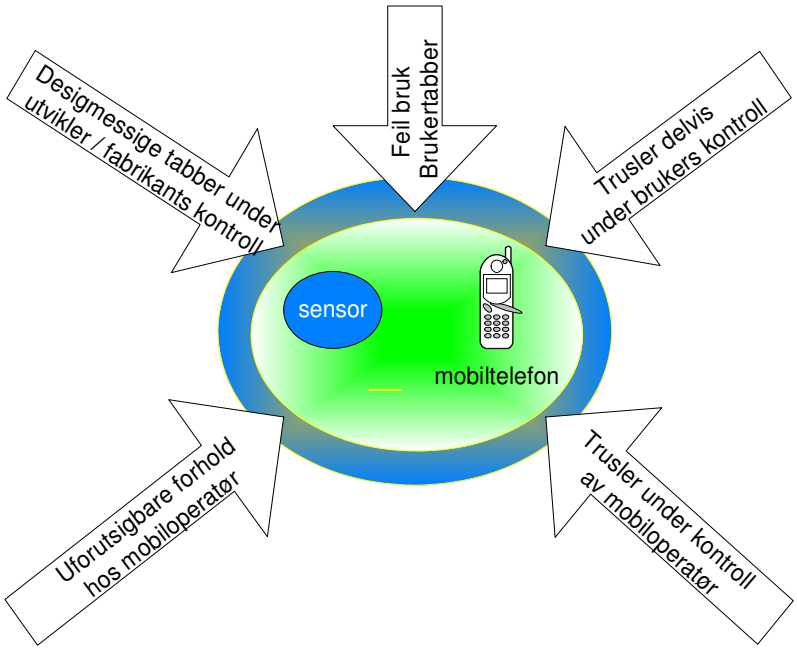
Område	Fasilitet	Verdi	Bruker-krav	System-krav
Mekanisk	Måleområde	0-6 G		X
Mekanisk	Terskel for alarm	3 G [18]		X
Mekanisk	Utførelse av hus	Hygienisk, uten skarpe kanter, vanntett. [31]	X	X
Mekanisk	Fastspenning	Må ha feste for stropper uten skarpe kanter. [31,	X	

		18]		
Mekanisk	Bæres hvor	På bryst, skulder. [18]		X
Mekanisk	Støttålighet	Tilsvarende fall fra 3 meter i betongguly.	X	X
Mekanisk	Vekt	Mindre enn 80 gram.	X	
Elektrisk	Ladningsteknikk	Kontaktløs, via magnetfelt. Ingen kontakter.	X	X
Elektrisk	Batterilevetid	Minst 3 år.		X
Elektrisk	Brukstid pr.lading	Minst 5 døgn.	X	
Elektrisk	Batteriladetid	Mindre enn 3 timer.	X	
Applikasjon	Ladetilstand	Overføres til masterenhet, skala 0-7		X
Bt	Type	Slave forenklet.		X
Bt	Effektklasse	2		X
Bt	Link sikkerhet	Forsterket (Kryptert)		X
Bt	Enhetssikkerhet	”Trusted” min 8 bit PIN kode.		X
Bt	Applikasjonssikkerhet	Kodet nøkkel, ingen klartekst.		X
Bt	Profil	HID Human Interface Device		X

Tabellen over bygger på fakta fra brukerbeskrivelsen, fra tidligere kapitler i rapporten, ”Forskrift av 19. august 1994 om konstruksjon, utforming og produksjon av personlig verneutstyr”[31], Bource et al [18] og Bluetooth SIG [88].

5.5 Trusselvurdering mot mobile alarmer

Med trusler menes situasjoner som kan skade eller sette systemet ut av spill. Første trussel mot systemet oppstår allerede med valget av en håndholdt eller bærbar enhet. Enhetene er eksponert for støtskader. Neste trussel er utbrente batterier i sensor eller mobiltelefon.



Figur 37 Hovedområder som kan true mobile alarmer

Tabell 28 og Tabell 29 viser enhetene og utstyret brukeren besitter listet opp med kjente trusler og skadelige situasjoner. Det er ikke tatt høyde for samtale utenom mobilsentraldomenet. (Dvs. der hvor man benytter ulike kjernenett eller ulike mobiltelefonoperatører.) De følgende tabeller søker å avdekke mulige trusler som kan degradere systemet eller sette det ut av drift. Mange av momentene som nevnes kommer igjen i flere tabeller, men fra ulike innfallsvinkler. Forklaring til typene finnes i Tabell 33. I type er første siffer utstyr, andre siffer er situasjon.

Tabell 28 Ulike trusler mot personlige enheter under utviklers / fabrikants kontroll.

Type	**Risiko**	**Enhet UMTS / GSM**	**Trussel**	**Tiltak**
1.1	Middels	Alarmsensor	Mekanisk støtskade	Robust konstruksjon
1.2	Stor	Alarmsensor	Utbrent batteri som følge av lav batterikapasitet.	Batterialarm Økt batterikapasitet / redusert strømforbruk.
3.2	Stor	Mobiltelefon	Utbrent batteri som følge av lav batterikapasitet.	Batterialarm Økt batterikapasitet / redusert strømforbruk.
1.20	Liten	Alarmsensor	Defekt, ukjent årsak	Robust konstruksjon
2.11	Liten	Bt-forbindelse alarmsensor / mobiltelefon	Brudd pga. radiointerferens	Repeterende signal (til en viss grad innbygd)
3.1	Middels	Mobiltelefon	Mekanisk støtskade	Robust Telefon / Hylster
3.20	Liten	USIMkort / SIMkort	Defekt, ukjent årsak	
5.7	Stor	Mobilforbindelse til Node B / basestasjon, bruker eller hjelpeperson	Skygge i dekningsområde. Eks. kjøpesenter, boligblokk,fjellhall, kino	Stemme-varsling i telefonen om lavt signalnivå.
5.8	Stor	Mobilforbindelse til Node B / basestasjon, bruker eller hjelpeperson.	Utenfor dekningsområde	Stemme-varsling om utenfor UMTS alarmområde.

Tabell 29 Trusler under bruker / hjelpers kontroll

Type	**Risiko**	**Enhet UMTS / GSM**	**Trussel**	**Tiltak**
1.2	Stor	Alarmsensor	Utbrent batteri	Batterialarm / Personlige rutiner
3.4	Stor	Mobiltelefon	Enhet eller applikasjon avslått.	Personlige rutiner
3.2	Stor	Mobiltelefon	Utbrent batteri.	Batterialarm / Personlige rutiner
3.5	Middels	USIMkort / SIMkort	Ugyldig abonnement.	Personlige rutiner
4.4	Stor	Mobiltelefon hjelpepersonell	Enhet eller applikasjon avslått.	Personlige rutiner / duplisering av hjelpe-enheter
4.2	Stor	Mobiltelefon hjelpepersonell	Utbrent batteri.	Personlige rutiner / duplisering av hjelpe-enheter
4.3	Middels	Mobiltelefon hjelpepersonell	Feil eller ikke installert applikasjon.	Personlige rutiner / duplisering av hjelpe-enheter
4.5	Middels	Hjelpepersonell USIMkort / SIMkort	Ugyldig abonnement.	Personlige rutiner / duplisering av hjelpe-enheter
4.20	Liten	Hjelpepersonell USIMkort / SIMkort	Defekt, ukjent årsak.	

Tabell 30 Trusler mot mobilsamband påvirket av bruker / hjelper

Type	Risiko	Enhet UMTS / GSM	Trussel	Tiltak
5.7	Stor	Mobilforbindelse til Node B / basestasjon, bruker eller hjelpeperson	Skygge i dekningsområde. Eks. kjøpesenter, boligblokk, fjellhall, kino	Ta hensyn til varsling i telefonen om lavt signalnivå.
5.8	Stor	Mobilforbindelse til Node B / basestasjon, bruker eller hjelpeperson	Utenfor dekningsområde	Ta hensyn til varsling om utenfor UMTS alarmområde.

Tabell 31 Trusler mot mobiltelefoninettet under kontroll av mobiloperatørene

Type	Risiko	Enhet UMTS / GSM	Trussel	Tiltak
6.10	Stor	Node B / Basestasjon	Avvist samtale, metningskontroll	UMTS: Rel-4, sterkere utbygging.
6.20	Middels	Node B / Basestasjon	Strømstans, uvær, midlertidig ute av drift.	Sterkere nødstrømløsninger. Duplisering av utstyr og linjer. Flere lokasjoner / roaming.
6.21	Liten	Node B / Basestasjon	Strømstans, lynnedslag, med fysisk skade.	Sterkere nødstrømløsninger. Duplisering av utstyr og linjer. Flere lokasjoner / roaming.
6.9	Liten	Node B / Basestasjon	Sabotasje, datainnbrudd.	Logisk og fysisk sikring Flere lokasjoner / roaming
6.0	Liten	Node B / Basestasjon	Ute av drift, uhell	Kvalitetssikring av vedlikeholdsoperasjoner. Flere lokasjoner / roaming
7.20	Middels	Forbindelse Node B / Basestasjon – Radionettverkskontroller / Basestasjonskontroller	Strømstans, uvær, midlertidig ute av drift.	Sterkere nødstrømløsninger. Duplisering av utstyr og linjer. Flere lokasjoner / roaming
7.21	Liten	Forbindelse Node B / Basestasjon – Radionettverkskontroller / Basestasjonskontroller	Linjebrudd, Strømstans, lynnedslag, med fysisk skade	Sterkere nødstrømløsninger. Duplisering av utstyr og linjer. Flere operatører / roaming
7.9	Liten	Forbindelse Node B / Basestasjon – Radionettverkskontroller / Basestasjonskontroller	Linjebrudd, sabotasje	Logisk og fysisk sikring Flere lokasjoner / roaming
7.0	Liten	Forbindelse Node B / Basestasjon – Radionettverkskontroller / Basestasjonskontroller	Ute av drift, uhell	Kvalitetssikring av vedlikeholdsoperasjoner. Flere lokasjoner / roaming
8.10	Stor	Radionettverkskontroller / Basestasjonskontroller	Avvist samtale, metningskontroll	UMTS: Rel-4, sterkere utbygging.
8.20	Middels	Radionettverkskontroller / Basestasjonskontroller	Strømstans, midlertidig ute av drift.	Sterkere nødstrømløsninger. Duplisering av utstyr og linjer. Flere lokasjoner / roaming
8.21	Liten	Radionettverkskontroller / Basestasjonskontroller	Strømstans, lynnedslag, fysisk skade.	Sterkere nødstrømløsninger. Duplisering av utstyr og linjer. Flere lokasjoner / roaming
8.9	Liten	Radionettverkskontroller / Basestasjonskontroller	Sabotasje, datainnbrudd.	Logisk og fysisk sikring / roaming
8.0	Liten	Radionettverkskontroller / Basestasjonskontroller	Ute av drift, uhell	Kvalitetssikring av vedlikeholdsoperasjoner. Flere lokasjoner / roaming

9.10	Liten	Kjernenett	Overbelastning	Sterkere utbygging./ roaming
9.9	Liten	Kjernenett	Sabotasje, datainnbrudd.	Logisk og fysisk sikring / roaming
9.20	Middels	Kjernenett	Linjebrudd, midlertidig	Duplisering av utstyr og linjer. Flere lokasjoner / roaming
9.21	Liten	Kjernenett	Linjebrudd, fysisk skade av uvær	Duplisering av utstyr og linjer. Flere lokasjoner / roaming
9.0	Liten	Kjernenett	Ute av drift, uhell	Kvalitetssikring av vedlikeholdsoperasjoner. Duplisering av utstyr og linjer. Flere lokasjoner / roaming

Tabell 32 Uforutsigbare situasjoner hos mobiloperatørene

Type	**Risiko**	**Enhet UMTS / GSM**	**Trussel**	**Tiltak**
5.11	Middels	Mobilforbindelse til Node B / basestasjon, bruker eller hjelpeperson	Brudd pga. tilfeldig radiointerferens.	
0.12	Liten	System	Gjennomkobling til feil abonnent Ukjent årsak	Systemkontroll
0.13	Middels	System	Manglende gjennom - kobling ukjent årsak	System- kontroll

Tabell 33 Kodeforklaring til tabellene 15 – 19

S1	**Enhet**		**S2**	**Situasjon**	**Opprinnelse**
1	Alarmsensor		0	Uhell	Menneskeskapt
2	Bt-forbindelse / sensor mobiltelefon		1	Mekanisk støtskade	Menneskeskapt
3	Mobiltelefon bruker		2	Utbrent batteri	Menneskeskapt
4	Mobiltelefon hjelper		3	Feil eller manglende applikasjon	Menneskeskapt
5	Forbindelse Mobilapparat -Node B / basestasjon		4	Enhet eller applikasjon avslått	Menneskeskapt
6	Node B / Basestasjon -		5	Ugyldig abonnement	Menneskeskapt
7	Forbindelse Node B / Basestasjon – Radionettverkskontroller / Basestasjonskontroller		6		
8	Radionettverkskontroller / Basestasjonskontroller		7	Radioskygge	
9	Kjernenett		8	Utenfor dekningsområde	
			9	Ondsinnet skade	Menneskeskapt
			10	Overbelastning	Tilfeldig feilsituasjon
			11	Tilfeldig radiointerferens	Tilfeldig feilsituasjon
			12	Feil gjennomkobling	Tilfeldig feilsituasjon
			13	Manglende gjennomkobling	Tilfeldig feilsituasjon
			20	Tilfeldig midlertidig linjebrudd	Uvær
			21	Fysisk skadd linje	Uvær

Som tabellene viser er mange av truslene utenfor brukerens kontroll. Kun punktene med startsiffer 1 - 5 er påvirket av bruker eller hjelpepersonell. De andre punktene er enten avhengige av andre personer, vær eller utstyrsdefekter. Hva som kan gjøres for å minimere truslene avhenger av hva truslene består i og i hvilket område. Forhold rundt abonnement, batteriladning og funksjon av håndapparater inklusive sensorer kan sikres med rutiner. Tilfeldige feil i utstyr er vanskelig å unngå, og kun erfaring kan vise hvor utstyret

svikter. Det er verd å merke seg at radioskygger må vurderes som et problem. Dette fordi UTRA med sin relativt høye radiofrekvens har vanskeligere for å nå inn i bygninger enn de andre mobilradioteknologiene som benytter lavere radiofrekvenser. Dette kan bevirke at MMS via GPRS og samtaler (og SMS) via GSM kan utføres, men ikke videotelefonisamtaler via UMTS [86].
Ekstremt uvær kan ingen gardere seg mot. Strømbrudd kan til en viss grad dekkes opp av nødstrømløsninger i mobilnettet. Sabotasje og direkte ondsinnede angrep på utstyr er forhold kjent fra utlandet vi til nå har vært forskånet for her i landet. Allikevel vil mobiloperatørene måtte ta hensyn til dette under framtidige installasjoner og vanskeliggjøre slike angrep. Datainnbrudd må møtes med tiltak for å vanskeliggjøre dette. Dette problemområdet er inngående belyst i master oppgaven til Ivar Brådland og Per Øyvind Hodøl [87]. Problemstillingene i rapporten er meget aktuelle fordi mobiltelefoni, datakommunikasjon og fasttelefoni kongruerer mot IP overførings -teknologi [46 s7]. Som mottiltak er flere steder nevnt flere operatører/ roaming. I konsesjons-vilkårene for mobiloperatørene finnes bestemmelser som forlanger at operatørene skal samarbeide om installasjoner [53]. Hjemlet i ”forskrift om offentlig telenett og offentlig teletjeneste § 4-7” [97]. Dette kan slå bena under poenget med flere operatører/ roaming, siden disse ofte vil benytte samme fysiske utstyr og/ eller infrastruktur i samme område.

5.5.1 Trussel mot eget utstyr og menneskelige faktorer

Radiosendere forbruker elektrisk energi, både til styringselektronikken og som utstrålt energi. Større utstrålt energi betyr enten større batterier eller kortere brukstid. Selv med det minste effektuttaket vil batterier utlades over tid. Dette betyr at batteriene må skiftes eller lades med jevne mellomrom. Dette igjen indikerer i vårt tilfelle at fallsensorenheten må kommunisere batteristatus til mobiltelefonapplikasjonen og gi en påminnelse om ladning.
Det er menneskelig å glemme. Særlig når man kommer opp i alder. Dette betyr at applikasjonen i sensorer og mobiltelefonen må varsle med lydsignal når det ikke kan oppnås kontakt via Bt. Hvis sensoren er satt opp til å gi alarm bør også alarmsentralen varslets om at systemet er ute av funksjon. Gode personlige innøvde rutiner vil allikevel være den beste garantien for at systemet fungerer etter hensikten.
Utstyr brukt til alarmformål bør være robust og tåle å falle i gulvet. Derfor bør sensorer bygges med tanke på dette. Mobiltelefonene bør utstyres med slagbeskyttelse. Dette kan gjøres med plastetuier som tillater betjening gjennom vinduer, men som dekker hjørner og kanter. Plastetuier må konstrueres slik at de fordeler og demper slag mot enheten de skal beskytte. Materialvalget må velges med hensyn på elektromagnetisk gjennomgang for ikke å forringe funksjonen til håndapparatet.

5.6 Forbedringer

5.6.1 Betraktninger rundt QoS til alarmformål i offentlig mobilnett

Forbedring av QoS i det offentlige nettet begrenser seg til innføring av prioriterte abonnement i GPRS / EDGE, og innføring av Rel-4 i UMTS. Videre viser Tabell 31 at det er rom for forbedringer ved bygge ut parallelle nett og ved å forbedre infrastrukturen til mobilnettene. Dette spørsmålet er delvis behandlet av Ivar Brådland og Per Øyvind Hodøl i “Sikkerhet og sårbarhet i IP basert infrastruktur”[87].

5.6.2 MSMC / MMSC

Det er muligheter både for å ha sin egen SMSC / MMSC og å leie en slik. Dette har til konsekvens at meldingene blir håndtert i en server som ikke blir overbelastet med ikke alarm-meldinger under trafikktopper. (Husk at SMS ikke har leveringsgaranti når det gjelder tid.)

5.6.3 Betraktninger rundt QoS i Bt implementasjoner

I Bt vil man kunne påvirke kommunikasjonssikkerheten positivt med å legge inn gjentatte forsøk på alarmbefordring dersom kvittering uteblir etter fornuftig tid. Dersom en uteblitt kvittering skyldes tilfeldig interferens vil nytt forsøk kunne lykkes. Denne funksjonen ligger delvis innbakt i Bt på lavere funksjons nivå. Dette forhindrer ikke at gjentatte forsøk etter time-out kan gi suksess. Adaptive frekvenshopp er også en funksjon som bør benyttes (må spesifiseres under programmeringen).

5.6.4 Garderinger mot menneskelige faktorer

Mennesker er forskjellige, og menneskers forhold til rutiner varierer. Bruk av sikkerhets og verneutstyr er vanesak og bygger på rutiner og tillit til utstyret. Det er derfor viktig å trene på dagelige rutiner og bruk ved introduksjon av systemet ovenfor brukeren, samt presisere systemets begrensninger. Ved offentlig bruk bør det avholdes periodiske øvelser for å trene brukeren og teste at utstyret fungerer etter hensikten.

5.6.5 Meldingstjeneren

Systemets akilleshæl er meldingsstjeneren. Denne bør dupliseres, både som meldingssentral og linjene fram til denne. Plasseringen av sentralen er fri og kan være i institusjonen, i en driftet serverpark eller etter avtale hos mobiloperatøren. Ved duplisering vil jeg foreslå at duplikatet plasseres i et annet lokale enn hovedtjeneren. Det er et krav i personopplysningsloven [1] § 2-12 at nødvendige data for normal bruk skal kopieres. § 2-11 setter forøvrig krav om at alle lagringsmedia som inneholder konfidensielle data skal merkes. OBS også sikkerhetskopier! Overføring av pasientdata krever VPN til terminaler utenfor institusjonen og dette anbefales også internt i institusjonen for å skille konfidensiell trafikk fra øvrig trafikk..

6 Resultater

6.1 Funksjonsbeskrivelse

I prosjektperioden ble det avholdt samling for å gi ideer til og å lage en funksjons- beskrivelse av produkter som kunne utnytte mobilkommunikasjon. Møteinnkalling finnes i vedlegg 0 og møtereferat i vedlegg 0. Funksjonsbeskrivelsen ble konkretisert med en rekke ideer som siden gikk over til kravgenerering til ideene. Av de to aktivitetene var kravgenereringen fra mitt ståsted den mest vellykkede.

6.1.1 Om brukerpanelet

Brukerpanelet bestod av 2 sykepleiere med bakgrunn fra lukkede demensavdelinger. 1 av disse også fra hjemmesykepleie. 1 av deltakerne er høgskolelektor med demens og geriatri som fagområde. En av gruppedeltakerne er prosjektkoordinatoren for grensebroen i Norge, teknolog med bakgrunn i telekommunikasjon. Ut over dett er gruppen komplettert med 2 studenter 1 fra elektronikk og 1 fra elkraftmiljøet. Gruppen fungerte meget godt på samlingen. Aldersspredningen var positiv i den forstand at de yngre hadde annet forhold til teknologi. Blandingen teknologer / pleiepersonell fungerte også meget godt ved at de utfylte hverandre. Navn på deltakerne framgår av vedlegg 0.

6.1.2 De konkrete forslagene

Først de normative utsagnene:

- Klart tydelig og konkret språk.
- Det verste er falsk trygghet, det beste er reell trygghet.
- Utvidelse av trygghetssonen, til å omfatte mer enn leiligheten.

I mange tilfelle er det vanskelig å skille mellom krav og ideer. I det følgende er derfor tidspunktet for når ideen/ kravet ble samlet inn gitt som styring på dette.
I prosessen ble det i alt stilt 56 ideer / forslag fra de enkle til hele konsepter. Etter en bearbeiding og samling sitter man igjen med disse ideene alle unntatt 1 applikasjonsavhengige, ingen med direkte tilknytning til alarm:

- Stemmestyrt kontroll av mobiltelefonen (Ring <navn>).
- Stedsangivelse og klokkeslett på mobiltelefonen. (Hjemme, Nær<navn>) egen tast.
- Forenklet tastatur. Berøringsskjerm med bilde av pårørende for oppringing.
- Enkelt språk.
- Betjening av kamera i boenhet via mobiltelefon. (Systemavhengig)

Disse ble møtt av i alt 29 krav, disse utmerket seg:

Systemavhengige:

- Lett montering av utstyr, ingen kabeltrekking.
- Utstyret må fungere ved strømbrudd.
- Utstyret må tåle å falle i gulvet.

- Taster må kunne betjenes av stive skjelvende fingre, Skjerm må være stor og tydelig for personer med nedsatt syn
- Stor skjerm, store taster. TV brukt som mobilskjerm. (For å få nok størrelse.)

Og de applikasjonsavhengige:

- Ved alarm: Stedsangivelse på bilde eller skjerm for å identifisere bruker, sted. Også som SMS
- Flere alternative gjennomkoblingsveier. Eg. Ikke avhengig av UMTS for alarm.
- Eventuell posisjonering bør fungere innendørs, kan delvis erstatte kamera.
- Brukeren, pleier eller pårørende må kunne slå av utstyret. (Implisitt lovkrav)
- Klokkeslett, dato og Natt / Dag på skjermen.
- Enkle ikoner på taster.
- Varsling når utstyret ikke er operativt.

Panelet påpekte at det ikke var ett hjelpemiddel som er riktig for alle, men at hjelpemiddeler må velges individuelt. Videre ble det pekt på to viktige områder: Aktivitet og ensomhet. Aktivitet fordi dette hindrer sykdom og demensutvikling. Ensomhet fordi dette gjør pasienter utrygge og sørger for (psykiske) belastninger. Videre påpekte panelet at alt språk må være direkte, konkret og klart.
Språket i forbindelse med fallalarm ble gjenstand for meget konkret diskusjon. Et forslag om at brukeren kunne trykke en knapp for å avverge alarm ble avvist med begrunnelse i at dette ikke er intuitivt nok. I stedet skal det komme en beskjed over høytaleren ”Du falt, jeg ringer etter hjelp” Denne beskjeden gjentas helt til gjennomkobling skjer.
Panelet var også meget klare på at alarmhåndtering ved ulykker ikke er en sak for pårørende, men at dette er en del av det offentlige helsearbeidet. De var også meget klare på at alarmmotaket må ha en backup i både antall og kontinuitet.

6.2 Forslag til implementering av demonstrator

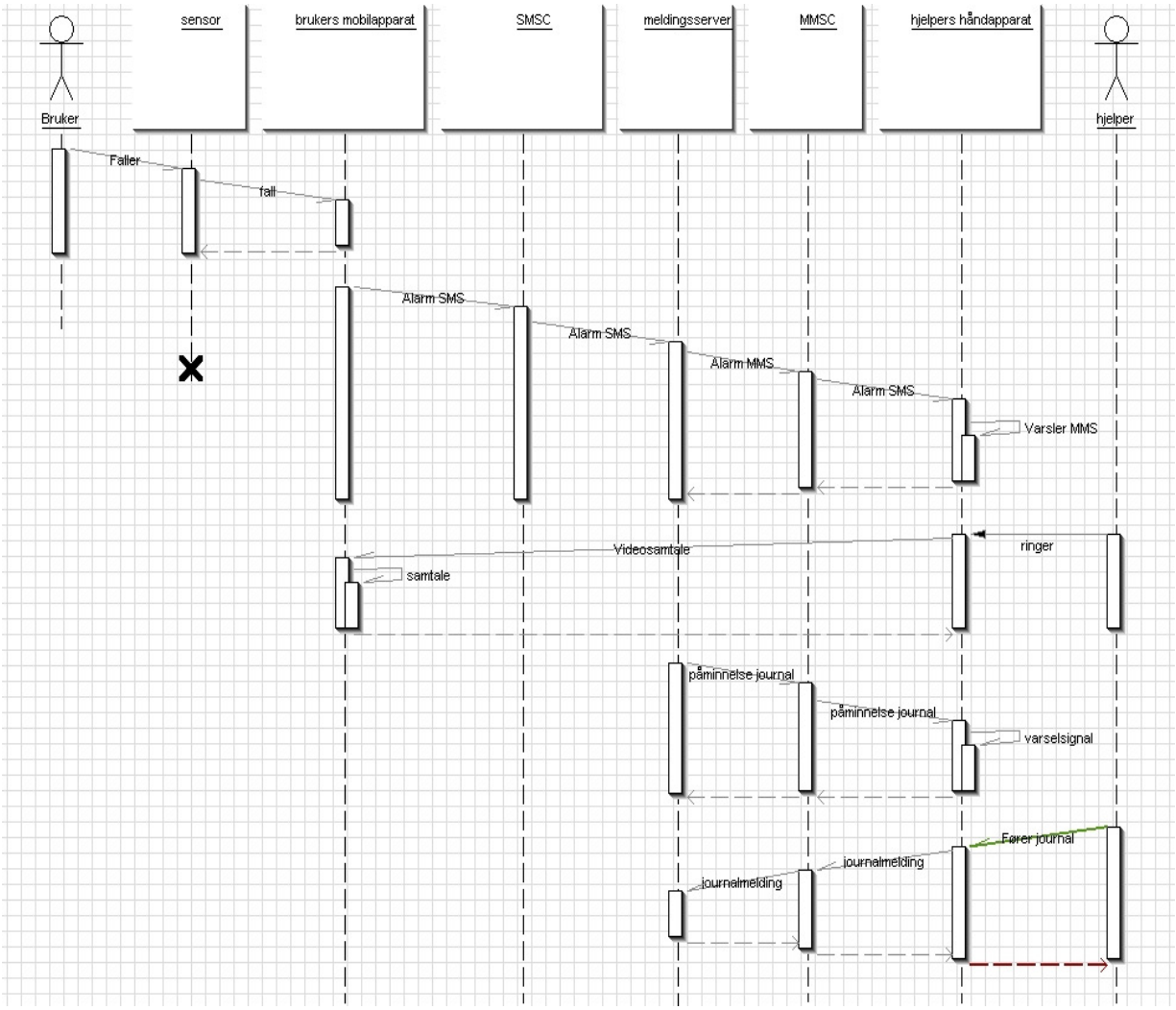
6.2.1 Foreslått systemarkitektur

Jeg foreslår systemarkitektur som bygger på prinsippene i kapittel 5. Blåtann realiseres med SSP for en enkel implementering og med sikkerhetsmodus 2 med autentisering for å hindre sensorenheten i å bli kapret av andre mobiltelefoner som tilfeldigvis skal starte opp i nærheten. Den beskrevne løsningen for privat bruk følges slavisk med en deteksjon av fallet, for så å sende en SMS til hjelper. Deretter skal mobilapparatet detektere om det har UMTS forbindelse eller GSM. Har mobilapparatet UMTS forbindelse ringes videosamtale. Hvis ikke er man henvist til tale. Svarer ikke den oppringte hjelperen innen kort tid sendes en SMS til neste hjelper på lista, samtidig som denne ringes opp. Partene er deretter henvist til å handle på egne vegne. Se Figur 33.
For offentlige bruk er forholdet noe mer komplisert. Jeg foreslår her strengt å følge retningslinjene fra 5.1 med SMS fra brukerens mobilapparat til alarmsentral via VPN mellom SMSC og hjelpeapparatets meldingssentral. Selve arkitekturen er vist i Figur 34.

Sekvensdiagrammet under utdyper hendelseskjeden for et alarmtilfelle hvor videokommunikasjon er tilgjengelig og første hjelper svarer på MMS henvendelsen. Kommentarer til og videre utdyping av diagrammet er:

- Hjelperen må fysisk slå av meldingstone for MMS alarm. (applikasjonsavhengig)
- Avslag av kvitteringstone sørger for oppkobling mot brukeren. (applikasjonsavhengig)
- Meldingsstjeneren registrerer at hjelperen har tatt kontakt med brukeren gjennom MMS kvitteringsmeldingen fra hjelperen.
- Som respons på kvitteringen sender meldingsserveren ny MMS med påminnelse om journalføring.
- Hjelperens svar på denne MMS'en er kladd for journalføringen.

Helsepersonelloven setter klare regler om at journaler skal føres på person. Implementeringen av dette ligger utenfor denne oppgaven jfr. 2.3.1. Se allikevel 5.1.7 for en rettesnor.



Figur 38 Hendelseskjede ved alarm med offentlig hjelp

6.2.2 Mobiltelefonvalg

I jungelen av mobiltelefoner finnes flere telefoner og PDA som kan egne seg for oppgaven. Som brukertelefon vil jeg allikevel velge Nokia N95 ut fra funksjonsbeskrivelse og kriterier fra avsnitt 5.1 om valg av mobiltelefon. Dette grunngis med:

- Telefonen kan programmeres i Java.
- Telefonen har stor skjerm, og få taster med skuffen inntrukket.
- Telefonen har kamera på forsiden.
- Telefonen støtter UPnP for styring av tekniske installasjoner.
- Telefonen har innebygget GPS.
- Telefonen har Bt.
- Taster på front kan reprogrammeres.

Telefonen har noen motargumenter:

- Telefonen er enda ikke markedsført for fullt. (Lansert i Sarpsborg uke 16 2007.)
- Telefonen er ikke bygd robust, og må utstyres med støtabsorberende hylster.
- Telefonen krever et AP i Wi-Fi nettet for å fungere med UPnP.
- Telefonens skjerm og taster er små i forhold til PDA.

PDA'er kan også brukes til dette formålet. Disse er pr. i dag stort sett utstyrt med Windows Mobile, programmerbarheten i Java er derfor et åpent spørsmål. En PDA ville gitt større skjerm og muligheter for touch screen som kan være nyttig selv om vekt og størrelse trekker ned. Brukerpanelet poengterte at utstyret måtte velges etter brukerens forutsetninger, og at ett sett utstyr neppe vil være optimalt.

Hjelpernes mobiltelefoner omfattes av samme problematikk, men her er viktigheten av stor skjerm i følge brukerpanelet enda større. Brukerpanelet har ikke fått Nokia N95 demonstrert.

6.2.3 Valgt abonnement og sikkerhetsnivå i mobilnettet

Til grunn for valg av abonnementtilknytting legges følgende:

- Brukerens mobilapparat skal brukes også til vanlig mobilbruk.
- Alarmtjenesten skal være knyttet til en institusjon.
- Meldingene mellom meldingstjener og hjelpere er medisinsk informasjon og forlanger full beskyttelse.

Brukerens abonnement er et helt alminnelig UMTS abonnement som brukeren velgere fritt. Det samme gjelder de private hjelperne. For institusjoner som vil benytte dedikerte alarmtelefoner vil en bedriftsavtale eller bedriftsabonnement falle rimeligere.
Det for å imøtekomme størst mulig datasikkerhet velges en VPN forbindelse til bruk mellom hjelpernes mobiltelefoner og mobiloperatørens kjernenett.
Også til tilknytningen av meldingstjeneren velges VPN mellom mobiloperatørens kjernenett og tjeneren.
Siden vi ikke skal benytte generell datakommunikasjon står vi igjen med følgende abonnementstilbud jfr. Tabell 22 og Tabell 23 (Merk at priser og abonnementstyper er i stadig utvikling hos alle mobiloperatørene.):

Tabell 34 Aktuelle abonnementstilbud fra Telenor Mobil

Privat / Bedrift	Abonnement	Område i system	Betingelser / Bruk	Pris for	Etablering	Mnd avg.	enh
Bedrift / Data	SMS Access Med MMS Og Nordic Connect	Tjener	Max 22000 SMS / mnd sendt fra server og 700 MMS sendt fra server til Telenorkunder [97].	Etablering Månedlig	9500,-	6500,-	
Mobil-abonnement	Bedrift Netto	Hjelpere	Fri intern mobil telefoni. Priser pr. telefon	Etablering Månedspris Pr SMS Pr MMS Pr Start tale Samtale pr. min	150,-	59,-	 0,59 1,59 0,59 0,59
Mobil-abonnement Privat eller Bedrift	GSM Alarm	Dedikerte alarmer	Passer for dedikerte alarmenheter.	Etablering Månedspris Pr SMS Pr MMS Pr Start tale Samtale pr. min	100,-	16,-	 0,59 1,59 0,49 4,50

Tabell 35 Aktuelle abonnementstilbud fra NetCom as

Privat / Bedrift	Abonnement	Område i system	Betingelser / Bruk	Pris for	Etablering	Mnd avg.	enh
Bedrift	M2M VPN	Tjener	MMS kan sendes til alle abonnenter uansett operatør.	Etablering Månedspris Fast IP pr SIM [106]	10000,-	2000.- 29,-	
Bedrift	Busines Talk Basic	Hjelpere	Ikke subsidierte telefoner. Fri taletelefoni innen bedriften.	Etablering Månedspris SMS MMS Start tale Tale pr. min	161,30	59,-	 0,59 1,59 0,48 0,59
For Private tilknytning til bedrifter som har bedriftsavtaler	Family Business	Brukere		Etablering Månedspris SMS MMS Start tale Tale pr. min	161,30	55,65	 0,56 1,59 0,48 1,36

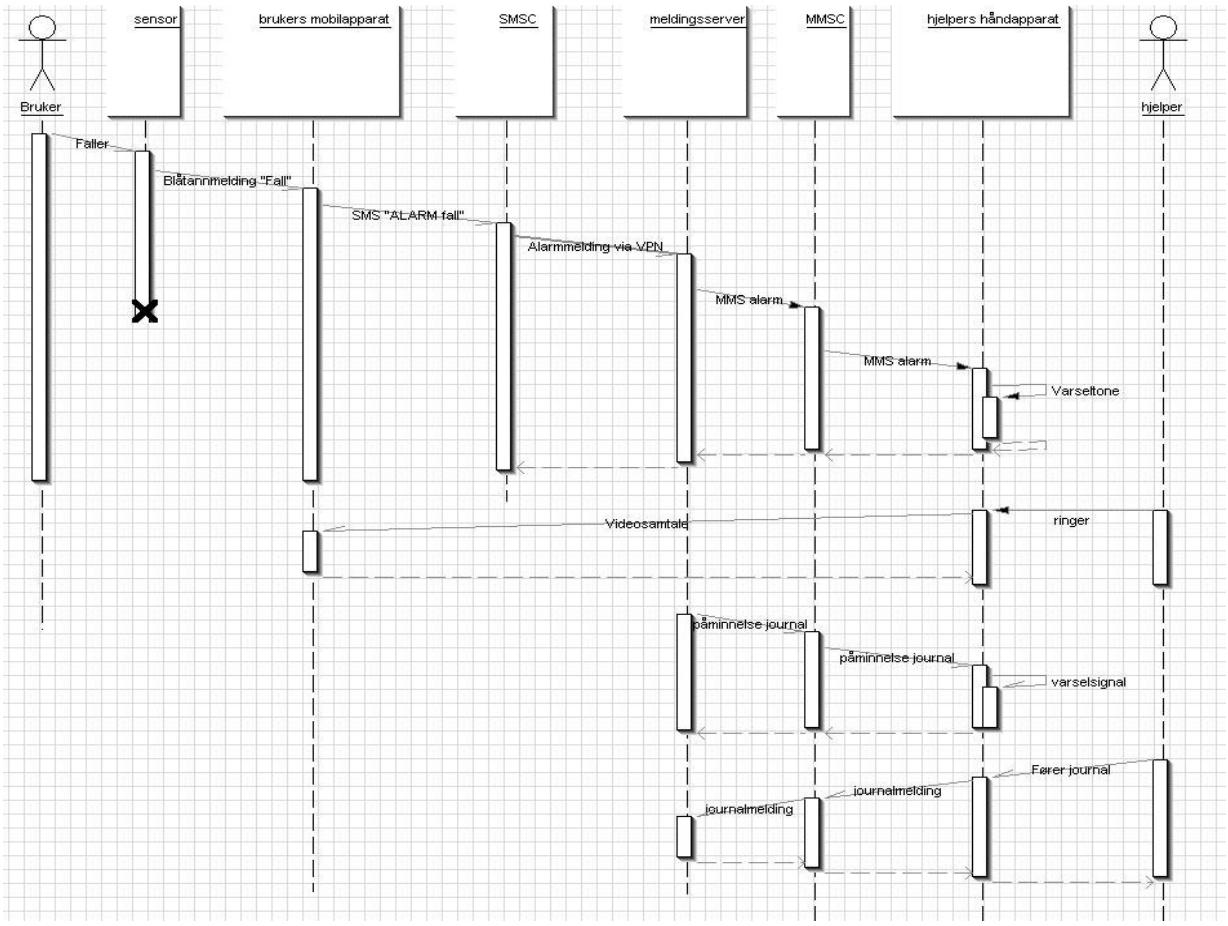
Valget faller derfor på NetCom as sin M2M VPN og Business talk Basis av følgende grunner:

- Fleksibilitet med abonnementstilknytning.
- Lavere fast løpende utgifter så lenge antall hjelpere er under 155 stk. (Kr 2000 + Kr. 29 pr. hjelper pr. mnd i forhold til fastpris kr 6500,-.)
- Enkel administrasjon.

Det understrekes at mobilabonnement -vilkår og -priser er ”ferskvare” og må vurderes ved behov.

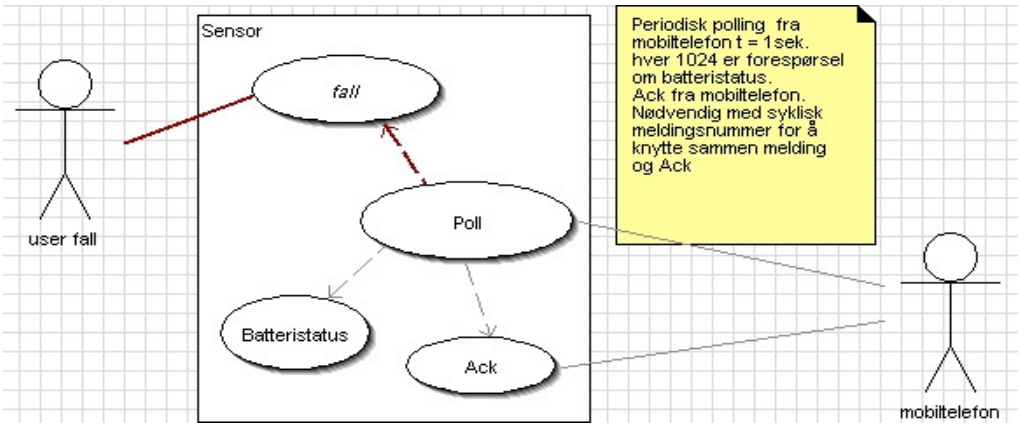
6.2.4 Programmodellering

Under er vist sekvensdiagram for løsningen skissert i 5.1.4 Årsaks- kjeden starter med at bruker faller, sensoren oppdager fallet og sender en Bt-melding til brukerens mobiltelefon. Brukerens mobiltelefon lager en SMS melding som den sender til meldingstjeneren via SMSC. Meldingstjeneren finner rett hjelper og sender MMS til denne via MMSC. Hjelperen ringer brukeren. Hjelperen vil motta en påminnelse fra meldingstjeneren om journalføring. Hjelperen kan da sende journalmelding fra sitt mobilapparat.



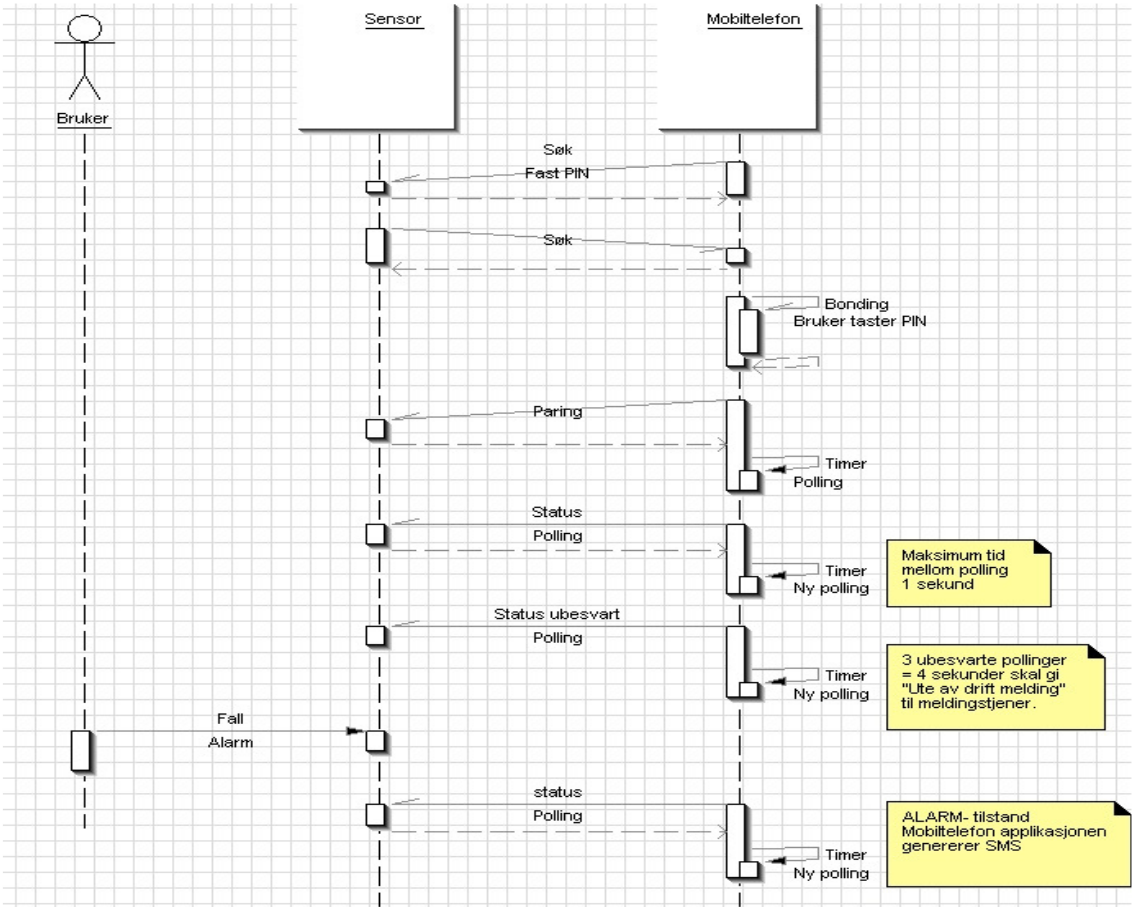
Figur 39 Sekvensdiagram ved generell offentlig bruk

Dette hoveddiagrammet kan brytes ned i flere underdiagrammer. Under er Use-Case - og sekvens - diagrammet for sensoren, for brukerens mobiltelefonapplikasjon, for meldingstjeneren og hjelperens mobilapplikasjon.

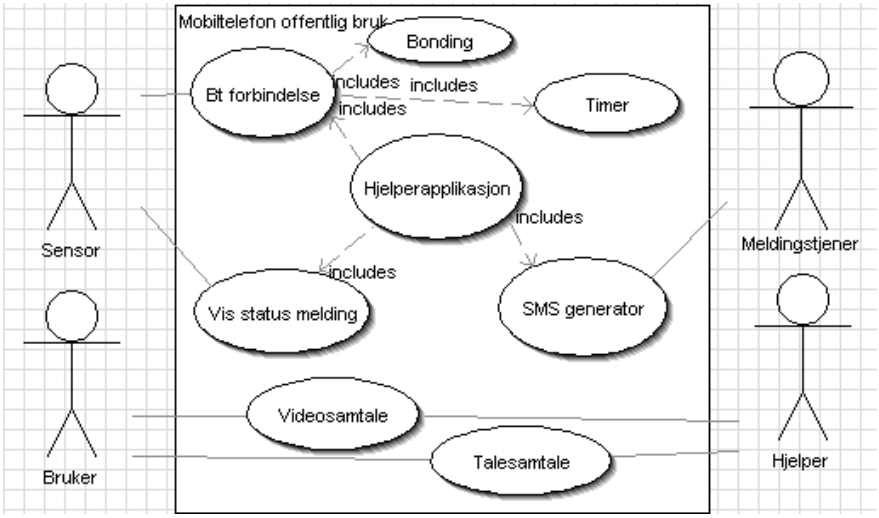


Figur 40 Sensorens Use-Case diagram

Sensorens hovedoppgave er å formidle hendelser i miljøet videre til mobiltelefonen via Bt. Sensoren må også kunne formidle sin batteristatus slik at brukeren kan planlegge ladning av sensoren. Dette skjer ved at mobiltelefonen periodisk ber om dette via pollmeldingen. Sensoren tar aldri initiativ til kommunikasjon med mobiltelefonen, men blir forespurt om status fra mobiltelefonen hvert sekund. Sensoren får bekreftelse på eventuell alarm og batteristatus fra mobiltelefonen slik at eventuelt midlertidig brudd i forbindelsen ikke har annen innvirkning enn forsinkelse.

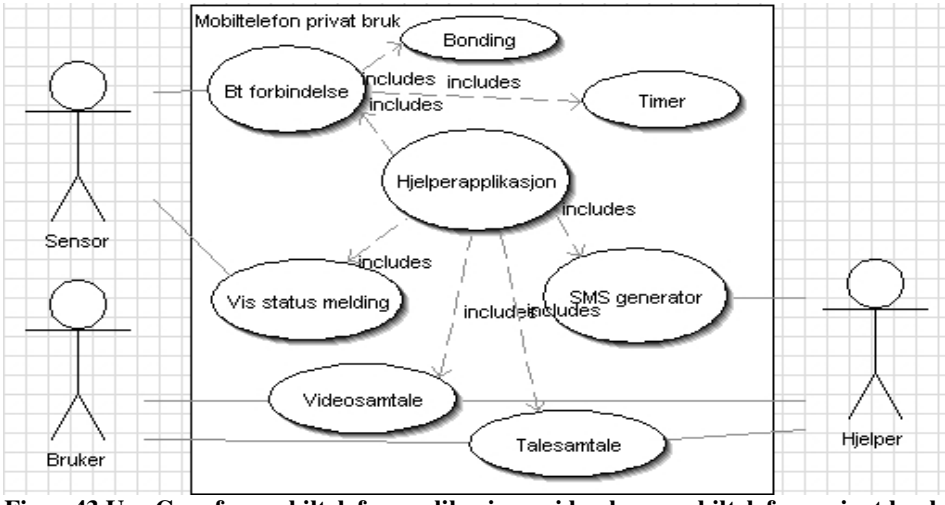


Figur 41 Sekvensdiagram for sensor, fall som eksempel

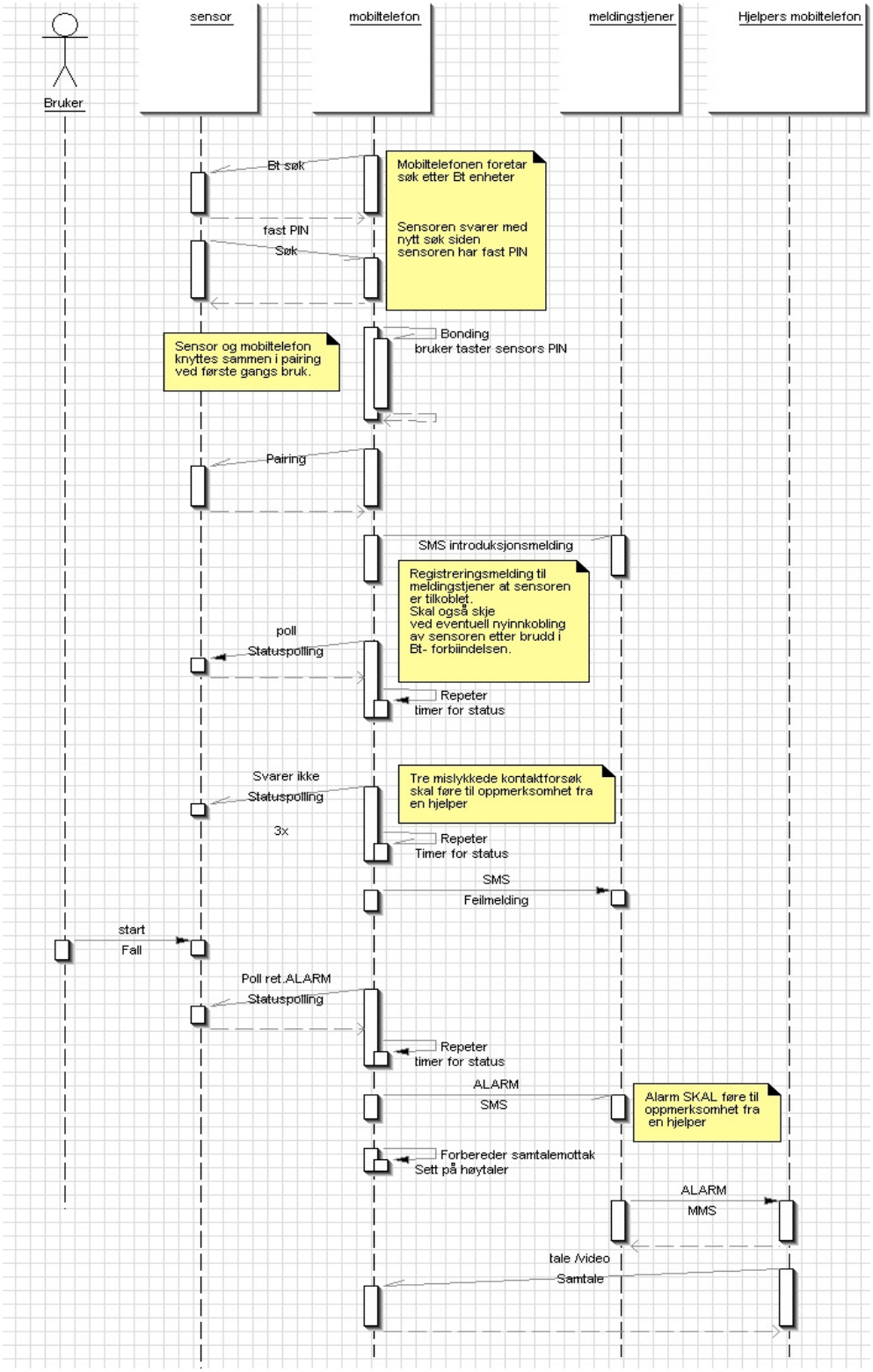


Figur 42 Use-Case for mobiltelefonapplikasjonen i brukers mobiltelefon, offentlig bruk

Mobiltelefonapplikasjonen har ansvar for å opprette og opprettholde Bt forbindelsen med sensoren. Vise status på mobiltelefonens skjerm og generere og sende SMS status og alarmmeldinger. Figur 44 viser sekvensdiagrammet for denne applikasjonen. Verdt å merke seg er at sensoren er en Bt slave og ikke initierer noen forbindelse mellom mobiltelefon og sensor etter at paring har funnet sted. En spesiell situasjon oppstår når mobiltelefonen mister forbindelsen med sensoren. Hvis forbindelsen ikke reetableres innen 4 sekunder bør det sendes en statusmelding til meldingsserver om at systemet er ute av drift. Det finnes tre meldinger som er aktuelle å vise på mobilapparatets display. Batteristatus, påminnelsesmelding hvis forbindelsen til sensoren uteblir og varsel om at brukeren beveger seg i område uten eller med dårlig dekning, de to siste også med lydmelding.
Ved alarm kan det sammen med aktiveringen av høytaleren utløses en talemelding til brukeren om at "Hjelp blir kontaktet" gjentatt inntil telefonigjennomkobling skjer. Hvis ikke talemelding gis bør det gis et lydsignal. Brukeren skal ikke kunne stanse en alarmmelding på grunnlag av fall. Dette grunngis med at personer utsatt for et fall med såpass stor energi som utløser fallsensoren bør i alle tilfelle undersøkes av lege.

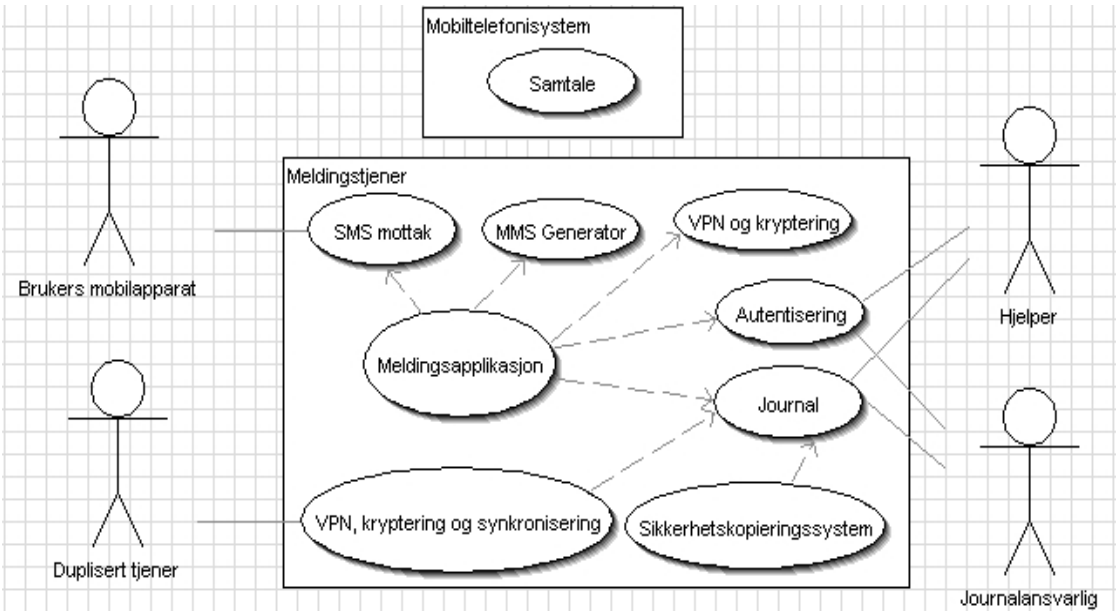


Figur 43 Use-Case for mobiltelefonapplikasjonen i brukers mobiltelefon, privat bruk



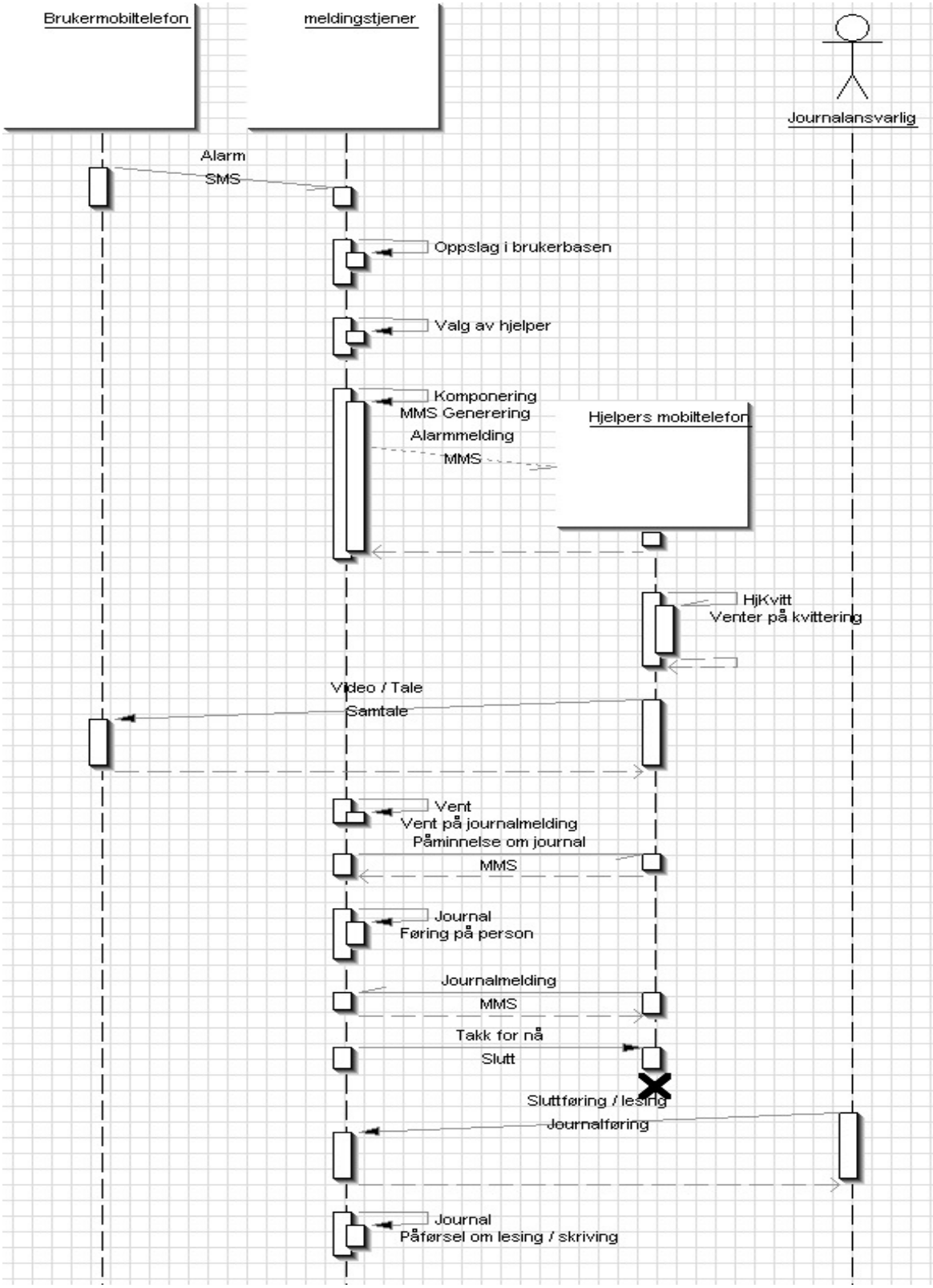
Figur 44 Sekvensdiagram for brukerens applikasjon i mobiltelefonen, offentlig bruk

Merk; dersom det benyttes egen SMSC må telefonnummeret settes til denne av applikasjonen før hver alarm SMS sendes.

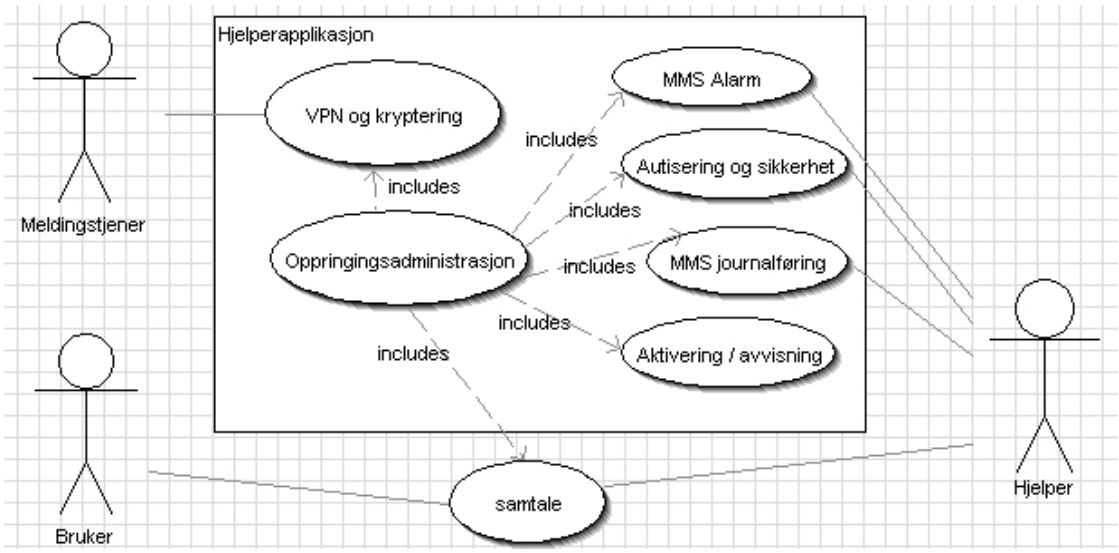


Figur 45 Meldingstjenerens oppgaver vist med Use-Case diagram

Meldingstjeneren er ansvarlig for å motta SMS meldinger, tolke disse og generere MMS alarmmeldinger til hjelper, journalføre disse og journalføre meldinger fra hjelperen i etterkant. Journal må også kunne leses og tilføyes i ettertid av journalansvarlig.
Meldingstjeneren må også inneholde funksjoner for autentisering av hjelper og journalansvarlige samt funksjoner for sikkerhets- kopiering av alle data. Dessuten må meldingstjeneren programvaremessig støtte duplisering for å øke sikkerheten. Jeg foreslår at duplisering utføres ved å plassere en meldingstjener på ulike fysiske lokasjoner i geografi og nett. Under vises sekvensdiagrammet for meldingstjeneren for vanlig drift med alarmtilfelle, journalvedlikehold er også tatt med. Autentisering og kryptering vises ikke, men forutsettes.
Årsakskjeden starter med SMS melding fra bruker. Denne tolkes og registreres og applikasjonen velger en hjelper. Deretter skjer en generering av MMS til hjelperen, med utfyllende opplysninger om brukeren. Applikasjonen noterer alarmtilfellet som aktivt og vil sende en påminnelse om journalføring til den valgte hjelperen etter en forutbestemt tid. Etter mottak av journalmelding legges denne inn i vedkommende brukers journal og alarmtilfellet noteres som avsluttet. Et spesielt tilfelle oppstår når hjelperen ikke er i stand til å besvare MMS meldingen. Enten ved at hjelperen avviser alarmmeldingen og meldingstjeneren mottar en avvisnings - MMS eller at hjelperen forholder seg passiv. Applikasjonen må da sende en ny MMS til neste aktuelle hjelper dersom ikke hjelperen svarer innen rimelig tid. Se Figur 33 hvor situasjonen er skissert for privat bruk.
Journalvedlikehold og lesing av journal utføres av journalansvarlige etter behov. Alle visninger og vedlikehold av journalen loggføres i journalen med hvem som er pålogget på vedkommende terminal.

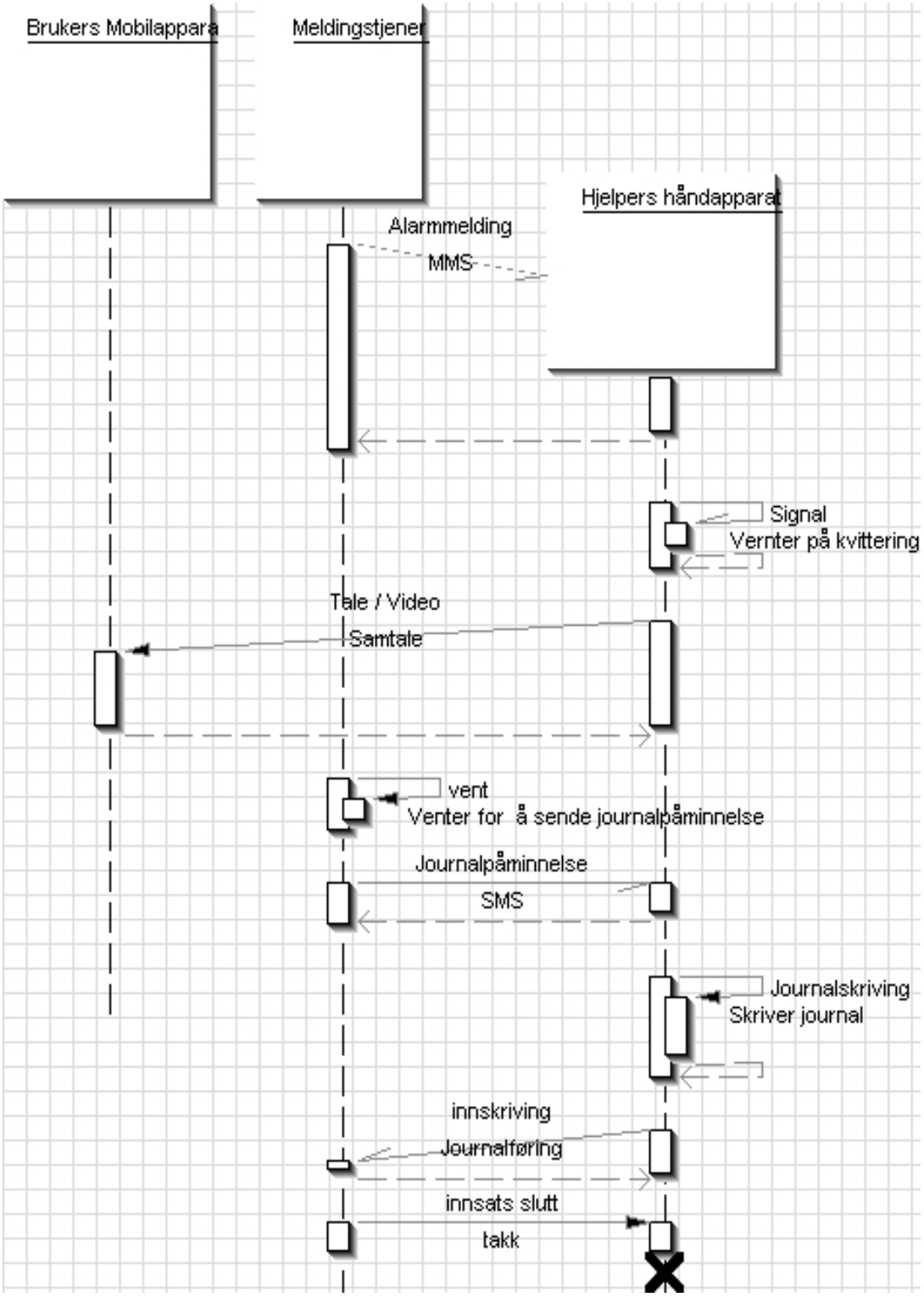


Figur 46 Sekvensdiagram meldingstjener



Figur 47 Funksjoner i Hjelpers mobilapparat

Hjelpers mobilapparat må inneholder applikasjoner for å motta alarm- meldinger og kunne bekrefte mottak eller avvising av alarmmeldingen. Videre må applikasjonen sørge for datasikkerheten til MMS meldingene. Applikasjonen må også tolke alarmmeldingen og klargjøre telefonen for oppringing til brukeren. Videre skal applikasjonen minne om og åpne for MMS melding tilbake til meldingstjener når hjelperen skal avlegge rapport. Ingen andre tilfelle enn alarm skal åpne for muligheter til tilføyelser i journal. Applikasjonen skal også sørge for at display slukkes når ikke hjelper taster på telefonen (eks. 10 sek forsinkelse etter hvert tastetrykk) og forlange ny pinkode dersom telefonen er innaktiv i 1 minutt. Det skal aldri lagres journaldata i mobilenheten.
Figur 48 viser et sekvensdiagram for hjelperapplikasjonen det er ikke vist VPN, kryptering og autentisering, men dette forutsettes. Diagrammet tar utgangspunkt i mottak av en alarmmelding og hvordan denne behandles.
Årsakskjeden starter med mottak av MMS melding som tolkes som alarmmelding, apparatet skal da varsle med vedvarende tone (se under) inntil hjelperen trykker en bestemt tast. Meldingen skal da vises på skjermen. Hjelperen kan da enten avvise alarmen og meldingstjeneren må gå videre til neste hjelper, eller hjelperen kan akseptere alarmen, Applikasjonen vil da sette opp en samtale med hjelperen, fortrinnsvis som videosamtale. Ved samtalens slutt aktiveres MMS editoren med utfylte data fra alarm - MMS meldingen som en oppfordring til å lage og sende rapport – MMS. Det kan forventes at det sendes MMS påminnelse om alarmføring fra meldingstjeneren dersom journalmeldingen uteblir i en forutbestemt tid. Dersom hjelperen forholder seg passiv til MMS alarmmeldingen vil en timer i meldingstjeneren sende alarm – MMS til neste aktuelle hjelper når timeren utløper. Hjelperens apparat vil slå av den kontinuerlige tonen og erstatte denne etter eks. 5 minutter med en ikke kontinuerlig påminnelsestone. Displayet på mobiltelefonen skal aldri passivt vise alarminformasjon eller journaldata.



Figur 48 Applikasjon i hjelpers mobilapparat

6.3 Responstider og risikovurdering

6.3.1 Responstider

Ved alarmer som angår liv og helse er tidsaspektet fra alarmering til innsats kritisk. I det foreslåtte systemet vil vi ha følgende omtrentlige tidsforsinkelser ved offentlig bruk:

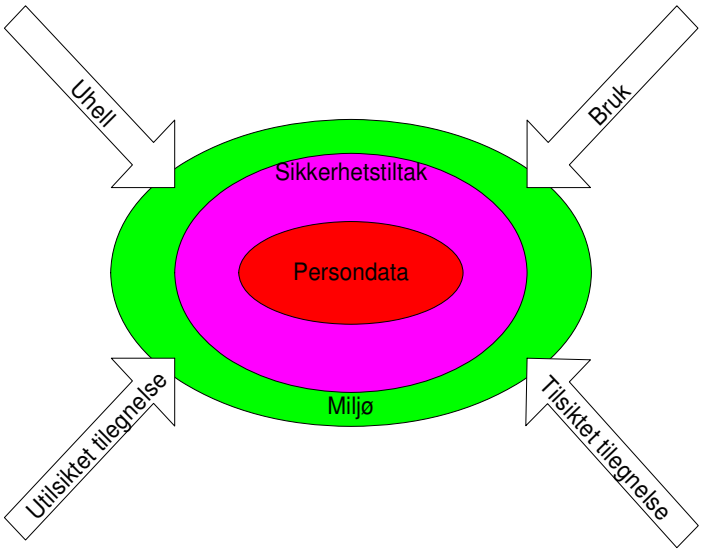
Tabell 36 Anslag over tider for meldinger

Hendelse	Sted i alarmkjede	Proses-tid	Varighet 1.hjelper	Varighet 2.hjelper	Tid	Kommentar
fall	Bruker				0 sek	
Bt melding mottatt	Sensor – mobiltelefon	2 sek			2 sek	Maks beregnet fra Tabell 7 ”normal scan” + programtid.
SMS generert	Prosesstid mobiltelefon til bruker	3 sek			5 sek	Antatt som rimelig verdi
SMS mottatt	Bruker – meldingstjener SMS	8 sek			13 sek.	Typisk tid i normalsituasjon
MMS sendt 1.hjelper	Meldingstjener 1 sek	1 sek			14 sek.	Antatt programtid
MMS mottatt 1.hjelper	Meldingstjener – 1.hjelper MMS	28 sek			39 sek	Typisk tid i normalsituasjon
Mobiltelefon tolker melding	Prosesstid i mobiltelefon til 1.hjelper	3 sek			42 sek	Antatt som rimelig verdi
Reaksjonstid 1.hjelper	Hjelper		3 sek		45 sek	Anerkjent som minimumstid
Oppkobling videosamtale	Mobilnett	20 sek.			1 min 5 sek	Typisk tid i normalsituasjon
Samtale bruker – 1.hjelper	Bruker – 1.hjelper	Etter 1 min 5 sek.				Anslagsvis
Eller: første hjelper nøler	1.hjelper		30 sek.		1 min 15 sek	1. Hjelper opptatt med annet.
Tilbakemelding om at 1.hjelper er opptatt. Motatt i meldingstjener	1.hjelper - meldingstjener	28 sek. Målt			1 min 43 sek	
MMS sendt 2.hjelper	Meldingstjener	1 sek			1 min 44 sek	Antatt som rimelig verdi
MMS mottatt 2.hjelper	2.hjelpers mobiltelefon	28 sek Målt		.	2 min 12 sek	
Reaksjonstid 2.hjelper	2.hjelper			3 sek.	2 min 13 sek	
Oppkobling videosamtale	2.hjelper - bruker	20 sek.			2 min 33 sek	
Bruker i samtale med 2.hjelper	Bruker – 2.hjelper	Etter 2 min 33 sekunder				Anslagsvis

Tidene som er angitt som typiske tider i normalsituasjon er gjennomsnittstider ut fra i et fåtall målinger . Disse data er derfor kun ment i illustrasjonsøyemed. Det er ikke foretatt noen målinger i "travel time" og belastningsgraden på nettet er ikke kjent. Målingene ble foretatt mellom mobiltelefoner 070516 kl 11.[10] – 11.[30]og kl 13.[15] -13.[40]. Målingene ble utført ved å benytte to mobiltelefoner. Tiden ble så målt fra "send" ble trykket til ankomstsignal hørtes i høyttaler (altså ikke den tiden det tok å lese meldingen) Responstiden til meldingstjener er antatt. Tidene viser at responstiden vil føles lang. Særlig hvis man legger til grunn at hjelperen har annet i hendene slik at melding må bli sendt 2. hjelper. Dette viser at mottak av disse alarmmeldingene må være prioritert i forhold til annen aktivitet.
Ved privat bruk vil responsen være langt raskere da brukeren selv ringer til hjelperen.. Tiden vil da være nede i området 25 sekunder før det er etablert kontakt.

6.3.2 Risikovurdering

Som grunn for risikovurdering er lagt Datatilsynets "Risikovurdering av informasjonssystem med utgangspunkt i personopplysningsloven"[15,121] og "Sikkerhetsbestemmelsene i personopplysningsloven med kommentarer" [15] Etter personopplysningslovens §2-4 skal det utføres risikovurdering for virksomheten. § 2-5 setter krav om sikkerhetsrevisjon jevnlig. Begge tiltakene skal dokumenteres og oppbevares jfr. § 2-16. Formålet med risikovurderingen er å avdekke situasjoner "*…der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet, er nødvendig med sikkerhetstiltak*" [2]. Når jeg velger å benytte dette skjemaet, på tross av at også Helsepersonelloven og Helseregisterloven har klare bestemmelser om sikkerhet, er dette med bakgrunn i at lovtekstene er harmonisert. I vårt tilfelle er verdiene vi skal verne om brukernes pasientdata og journal. Denne risikovurderingen vil derfor ta utgangspunkt i hvor disse befinner seg og hvilket sikkerhetsteknisk miljø de er omgitt av.



Figur 49 Sikkerhetsaspekter

Figuren over viser en modell av hvordan datasikkerhet kan tolkes ut fra [120] med data omsluttet av sikkerhetstiltak omsluttet av miljø og utsatt for trussel i forbindelse med bruk, uhell, utilsiktet tilegnelse og kriminell aktivitet (Tilsiktet tilegnelse.). Det er da et behov for å kartlegge hver av disse truslene og møte disse med sikkerhetstiltak.

I denne rapporten skiller vi mellom privat og offentlig bruk. Ved privat bruk faller alle krav om sikring vekk. Det lagres heller ingen sensitive opplysninger ut over selve alarmmeldingen. Her ansees instruksjon om at disse slettes som tilstrekkelig. Resten av dette kapittelet vil derfor dreie seg om offentlig bruk.

Kartlegging av personopplysninger

Ved en gjennomgang av datasikkerheten i en organisasjon er det nødvendig å vite hvilke data som finnes hvor og hvilke sikkerhetsnivå de krever. Første trinn i en slik gjennomgang er en kartlegging av hvilke data som faktisk finnes.

Tabell 37 Kartlegging av personopplysninger, omarbeidet etter [121]

Type	Hjemmel	Pliktig	Sensitive Personopplysninger?	Taushetsplikt ?	Omfang	Konfidensialitet §2-11	Integritet §2-13	Tilgjengelighet §2-12
Telefonliste (Brukere)	Personopplysningsloven		nei	nei	Brukere	3	3	2
Pasientjournal	Helsepersonelloven personopplysningsloven	Meldeplikt	ja	Ja	Brukere med mottatt hjelp	5	5	2
Alarmmeldinger	Helsepersonelloven personopplysningsloven	Meldeplikt	ja	Ja	Brukere under hjelp	3	5	2
Journalmeldinger	Helsepersonelloven	Meldeplikt	Ja	Ja	Brukere under hjelp	5	5	2

Skala 5 Høyest, 0 Ingen

Kommentarer til Tabell 37: Telefonliste inneholder i seg selv ingen sensitive opplysninger, men selve listen avslører et klientforhold og er dermed sensitiv. Listen må også være oppdatert og dataintegriteten må være høy (beskyttes mot uautoriserte forandringer). Tilgjengeligheten behøver ikke være god for andre enn meldingstjenerprogrammet og journaldelen i dette.
Pasientjournal er lovpålagt gjennom helsepersonelloven og skal føres på person. Denne inneholder sensitive opplysninger og skal vernes. Kun autorisert personell skal ha adgang og all lesing av journalen skal føres inn i journalen.

Identifisering av uønskede hendelser

Når kunnskap om forefinnende data er funnet kan man gå videre å lete etter situasjoner som kan være en fare for disse. Man kan da lete etter situasjoner som fører til hendelser som angitt i Tabell 38. Det er da lettest å følge en datastrøm gjennom systemet og se på omgivelsene i hver enkelt fase av strømmen.

Tabell 38 Uønskede hendelser med sensitive data, omarbeidet etter [121]

	Hendelse	Kategori
1.0 1.1 1.2	Utlevering	 Permanent Kan tilbakeføres
2.0 2.1 2.2	Utilgjengelighet	 Permanent Midlertidig
3.0 3.1 3.2 3.3 3.4	Endring	 Permanent, ikke sporbar Sporbar, kan rettes Sporbar og permanent. Kan rettes

I vårt system har vi følgende bruk av systemet.

- Alarm fra bruker til meldingstjener, SMS.
- Melding til hjelper MMS.
- Videosamtale, ev talesamtale.
- Journalføring fra hjelper MMS.
- Uttak av journaler fra meldingstjener.
- Vedlikehold av systemet.

Datatilsynet gjennom [121] benytter en skala for konsekvens og sannsynlighet som også egner seg til vårt formål.

Tabell 39 Oversikt over konsekvensklasser, omarbeidet etter [121]

Klasse	Konsekvens	Beskrivelse
K= 4	Katastrofal	Hendelsen kan føre til tap av liv eller vedvarende helsetap, eller kan medføre betydelig og uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.
K= 3	Stor	Hendelsen kan føre til tap av helse, eller kan medføre uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse og integritet.
K = 2	Moderat	Hendelsen kan medføre betydelig økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatte som krenkende, eller som andre kan gjøre nytte av).
K = 1	Liten	Hendelsen kan medføre økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som følsomme).

Tabell 40 Sannsynlighetsklasser ut fra betraktninger, omarbeidet etter [121]

Klasse	Sannsynlighet	Hyppighet	Letthet	Motivering
S = 4	Svært høy	Flere ganger i året	Sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale resurser. Det er ikke nødvendig med kjennskap til tiltakene.	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.
S = 3	Høy	Årlig	Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten. Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene – det er ikke nødvendig med kjennskap til tiltakene. Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke rutiner som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normale resurser.	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettelig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.
S = 2	Moderat	1 - 10 år pr gang	Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungere etter hensikten. Tiltakene kan likevel omgås/brytes av egne medarbeidere med små til normale ressurser, som i tillegg har normal kjennskap til tiltakene. Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse.	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.
S = 1	Lav	10 - 50 år pr gang	Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå/bryte tiltakene.	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.

Her sammenlignes tre forskjellige metoder for å fastsette sannsynlighet; ut fra hyppighet, letthet og motivering. Hyppighet er metoden der data er kjent, og man har erfaringsgrunnlag i form av feildata, gjerne etter årelang drift. Letthet og motivering må sees i sammenheng og benyttes samtidig innen en organisasjon. Det er også hva jeg benytter i de følgende tabellene. Legg merke til de strenge kravene som settes til ”lav sannsynlighet”, dette er et nivå som er vanskelig å oppnå i praksis.

6.3.3 Sikkerhetsnivå

Systemet behandler sensitive persondata. Disse data skal vernes mot uautorisert innsyn og forandring. Jfr. helsepersonelloven og personopplysningsloven er det straffbart å bryte taushetsplikt i form av å røpe slike data. Imidlertid kan man ikke sikre seg totalt mot uønskede hendelser uten store økonomiske utlegg. Det er derfor nødvendig å sette en terskelverdi for hvor man skal sette inn tiltak for å bedre sikkerheten. I vårt tilfelle må vi sette terskelverdien for hver enkelt hendelse siden noen av hendelsene ikke er påvirkbare, mens andre er lette å påvirke.

6.3.4 Hendelser

Rundt SMS meldinger

La oss se på alarmkjeden fra bruker til meldingstjener, her genereres en SMS som skal befordres til meldingstjeneren,

Tabell 41 Sikkerhetsforhold rundt SMS meldingen

Kategori	Hvor	Hendelse	Hva	Hvorfor	Hvordan	Sannsynlighet	Konsekvens	Risiko	Aksept risiko
1.1.1	Brukeren	Utlevering, permanent	Klientforhold	Alminnelig bruk	Alminnelig bruk	4	1	4	5
1.2.0	Brukeren	Utilgjengelig	Alarmsystem	Se under kap.5.5	Alminnelig bruk	3	4	12	12
1.3.4	Brukeren	Endring, kan rettes	Programvare	Feil bruk av mobiltelefon	”Utvidet ” bruk	2	4	8	12
2.1.0	Brukeren / BTS	Utlevering	Alarmmelding / Klientforhold	Tilsiktet tilegnelse	Modifisert utstyr	2	1	2	4
3.1.0	SMSC	Utlevering	Alarmmelding / Klientforhold	Feil eller dårlige sikkerhetsrutiner hos operatør.	Misbruk av tillitsforhold	2	1	2	4
3.3.1	SMSC	Endring Permanent, ikke sporbar	Alarmmelding	Feil eller dårlige sikkerhetsrutiner hos operatør.	Misbruk av tillitsforhold	1	4	4	4
4.2.2	Meldings-tjener	Utilgjengelig, avgrenset tid	Tjener	Strømbrudd / ingen duplisering	Sikringsbrudd	3	4	12	8
4.2.2	Meldings-tjener	Utilgjengelig, avgrenset tid	Tjener	Strømbrudd i elektrisitetsforsyning	Eks. lynnedslag	3	4	12	8
4.2.1	Meldings-tjener	Utilgjengelig, permanent	Tjener	Ingen duplisering	Hardvarefeil	3	4	12	4
4.2.2	Meldings-tjener	Utilgjengelig, avgrenset tid	Tjener	Ingen duplisering	Softvarefeil	2	4	8	4
4.1.1	Meldings-tjener	Utlevering, permanent	Klientforhold	Utilstrekkelig sikring	Datainnbrudd	2	3	6	8
4.1.1	Terminal til meldings-tjener	Utlevering, permanent	Klientforhold, alarmlogg.	Utilstrekkelig sikring	Uhell	3	3	9	8

Man ser klart at kategori 4.2.2 indikerer sikring av strømforsyning og duplisering av utstyret. Samtidig går det fram at mobilleddet er kjedens svake punkt. Jeg anser at diskresjonsbrudd i form av enkeltavsløringer av klientforhold til familie og venner i form av pkt.1.1.1 er umulig å gardere seg mot og heller ikke særlig skadelig. Hvis dette derimot blir en regel vil dette ikke være forenlig med anerkjente normer for diskresjon, jfr. Diskusjonen rundt utvendige nøkkelskap [122]. Verre er at applikasjonen i brukerens mobiltelefon kan settes ut av spill og at feil kan oppstå i mobilnettet som hindrer alarmmeldingen. Disse forholdene er imidlertid vanskelig å gardere seg ytterligere mot.

Hendelser rundt MMS alarmmeldinger

På veien videre skal meldingstjeneren journalføre meldingen, generere ny MMS melding og sende den til hjelperen. På denne veien skal vi først gjennom en sikret VPN tunnel fram til MMSC og deretter gjennom en ny tunnel til hjelperens mobilapparat.

Tabell 42 Sikkerhetsforhold for Alarm MMS

	Hvor	Hendelse	Hva	Hvorfor	Hvordan	Sannsynlighet	Konsekvens	Risiko	Aksept. Risiko
4.1.0	Meldings - tjener / MMSC	Utlevering	Alarmmelding	Feil eller utilstrekkelige sikkerhetsrutiner hos operatør.	Misbruk av tillitsforhold	2	1	2	4
5.1.0	MMSC / Hjelper	Utlevering	Alarmmelding	Manglende VPN	Feil hos operatør	2	3	6	6
6.1.2	Hjelper	Utlevering, midlertidig	Klientforhold, Alarmmelding	Uautorisert tilgang til hjelpers mobilapparat	Mobilapparat ligger framme	3	2	6	5
6.1.2	Hjelper	Utlevering, midlertidig	Klientforhold, Journal	Uautorisert tilgang til hjelpers mobilapparat	Mobilapparat stjålet	3	3	9	8
6.2.2	Hjelper	Utilgjengelig, midlertidig	Mobiltelefon	Manglende alternativer, duplisering	Se under kap.5.5	4	4	16	10

Her utmerker manglende tilstedeværelse av hjelper seg, dette er også tatt hensyn til i systemet med nestet oppringing til hjelperne. Også hjelpernes arbeidsrutiner berøres med at mobilapparat kan ligge framme og tilgjengelig for uautorisert personell. Mobilapparatet kan også bli stjålet og utgjør da en sikkerhetsrisiko inntil VPN tunnelen blir koblet ned.

Hendelser rundt meldingstjener

Uautorisert personell kan også tilegne seg adgang til meldingstjeneren på forskjellige måter:

Tabell 43 Sikkerhetsforhold rundt meldingstjener

	Hvor	Hendelse	Hva	Hvorfor	Hvordan	Sannsynlighet	Konsekvens	Risiko	Aksept. Risiko
4.1.1	Meldings - tjener	Utlevering, permanent	Journaler	Brudd på sikringstiltak	Datainnbrudd	2	3	6	8

				rundt meldingstjeneren					
4.1.1	Meldings - tjener	Utlevering, permanent	Journaler	Brudd på sikringstiltak terminal	Åpne lokaler	4	3	12	8
4.1.1	Meldings - tjener	Utlevering, permanent	Journaler	Dårlig sikring av autorisert identitet	Stjålet identitet	3	3	9	8
4.3.0	Meldings - tjener	Endring	Journaler	Dårlig sikring av Autorisert identitet	Stjålet identitet	3	4	12	8
4.3.0	Meldings - tjener	Endring	Journaler	Manglende data virusbeskyttelse	Datavirus endrer, sletter eller gjør data utilgjengelige	2	4	12	8
4.1.0	Meldings - tjener	Utlevering	Journaler	Ikke slettet ved avhending	Ved å anvende brukt utstyr	2	3	6	4
4.1.0	Verksted	Utlevering	Journaler, klientforhold	Utilstrekkelig ansvarssikring ved service	Ved service, datahjelp.	2	3	6	4

Her utmerker datavirus, avhending, service, åpne lokaler og stjålet identitet seg som høyrisiko. De to siste er anvender – variable i den forstand at anvenderens vaner kan være en sikkerhetsrisiko. Dette motiverer for holdningsskapning angående dataatferd. Åpne lokaler taler for seg selv. Kun den autoriserte operatøren skal oppholde seg i samme lokale som meldingstjener- terminalen. Terminalen skal heller ikke plasseres slik at den er synlig fra vindu eller dør.

Hendelser rundt journalføring fra hjelper

Hjelperen skal kunne skrive en kort journalmelding fra sin mobiltelefon. Dette fordrer sikkerhet av samme art som ved journaltjener- terminalen.

Tabell 44 Sikkerhetsforhold rundt hjelpers journalføring

	Hvor	Hendelse	Hva	Hvorfor	hvordan	Sannsynlighet	Konsekvens	Risiko	Aksept. Risiko
6.1.2	Hjelper	Utlevering, midlertidig	Klientforhold, Alarmmelding	Uautorisert tilgang til hjelpers mobilapparat	Mobilapparat ligger framme	3	2	6	5
6.1.2	Hjelper	Utlevering, midlertidig	Klientforhold, Journal	Uautorisert tilgang til hjelpers mobilapparat	Mobilapparat stjålet	3	3	9	8
6.3.2	Hjelper	Endring, sporbar og kan rettes	Klientforhold eller journal	Uautorisert tilgang til hjelpers mobilapparat	Hjelper under tvang (ran)	2	4	8	8
5.2.2	MMSC	Utilgjengelig, midlertidig	GPRS nett	Utenfor dekning	Se under kap.5.5	4	1	4	8
4.2.2	Meldings – tjener	Utilgjengelig, midlertidig	Meldingstjener	VPN forbindelse nede	Se under kap. 5.5	2	2	4	5

Her ser vi at uautorisert tilgang til mobilapparat kan være et problem, med en ny innfallsvinkel, at hjelperen kan være satt under tvang med voldelige midler. Dette kan motiveres med at hjelperen er ute i feltarbeid og er uten kollegial beskyttelse.

7 Diskusjon

7.1 Funksjonsbeskrivelse kontra beskrevet modell

Funksjonsbeskrivelsen skisserer ønsker som skal avveies mot tekniske muligheter.
Følgende tabell viser hvilke krav som er blitt innfridd og hvilke som ikke er innfridd.

Tabell 45 Status for krav fra funksjonsbeskrivelsen

Krav fra funksjonsbeskrivelse	Status i foreslått demonstrator	Status i prinsipper/ kommentarer
Lett montering av utstyr, ingen kabeltrekking	Innfridd	Innfridd
Eksterne kamera	Ikke mulig og utenfor oppgave	Utenfor oppgave og ikke mulig
Utstyret må fungere ved strømbrudd	Batterioperert, Skal minst vare 3 døgn fra siste opplading.	Batterioperert, Sensor skal minst vare 5 døgn fra siste oppladning. Mobiltelefon er modellavhengig.
Utstyret må tåle å falle i gulvet	Forsøkt innfridd	Beskrevet.
Taster må kunne betjenes av stive skjelvende fingre	Forsøkt innfridd via reprogrammering. Begrenset av mobiltilbud	Beskrevet
Stor skjerm	Begrenset av mobiltilbud	Beskrevet
TV brukt som mobilskjerm	Ikke innfridd, begrenset i oppgavebegrensning	Foreslått videre arbeid
Stedsangivelse i alarm	Ikke innfridd, begrenset i oppgavebegrensning	Foreslått videre arbeid
Flere alternative gjennomkoblingsveier ikke bare UMTS som signalvei	Innfridd	Innfridd
Stedsangivelse innendørs	Ikke løst	Ikke løst
Klokkeslett, dato og dag natt indikasjon på skjerm	Ikke beskrevet	Beskrevet
Enkle ikoner på taster	Begrenset av mobiltilbud	Beskrevet
Varsling når utstyret ikke er operativt	Foreslått	Foreslått

Som det framgår av tabellen er mange av kravene innfridd, mens de fleste bare er beskrevet i prinsipper. Kravene til en demonstrator er satt for å kunne få en fungerende prototyp ut av prosjektet. Operasjonelle sikkerhetskrav har derfor blitt vektlagt framfor "kjekt å ha" funksjoner. Når det gjelder sanntids-video-overføring så er dette definert utenfor oppgaven og heller ikke anbefalt av Nokia implementert i Java™, men i Symbian C++.

7.2 Risiko i modell

Alle ønsker et absolutt sikkert system. Ingen systemer kan være absolutt sikre, vi kan bare anstrenge oss for å få dem så sikre som mulig. Så også med vårt system. Risikovurderingen i forrige kapittel viste klart at det er mye å hente på å sikre systemet, ikke minst på bruk og betjening. Dette er forsøkt gjort med å foreslå automatikk der det er risiko for menneskelige feiltrinn, et eksempel er i hjelperapplikasjonen hvor brukeren telefonnummer slås på grunnlag av alarmmelding. Ved privat bruk behøver ikke hjelperne gjøre annet enn å ta telefonen. De største risikoene i systemet er radiotilgjengeligheten (dekningen) i mobilnettet og sikkerheten til brukerdata i journalsystem. Radiodekningen til mobilnettet er forsøkt ivaretatt med å benytte

GSM meldinger (SMS) i stedet for dedikert UMTS kommunikasjon. Sikkerheten rundt journaltjeneren er behandlet i 5.6.5 , 6.3.2 og 6.3.4 I scenarioet i avsnitt 2.2 nevnes at gjennomkobling av videosamtale skal skje i 99,5 % av anropene. Dette er svært urealistisk. Vi må være fornøyd om 99,5 % av de utløste alarmene blir registrert i meldingstjeneren. Hvis så 50 % av disse tilfellene lar seg gjennomføre som videosamtaler vil vi ha god 3G dekning. Vi må altså justere forventningene våre til at 99,5 % får en gjennomkoblet samtale, tale eller video. Allikevel er dette mye bedre enn uten alarmsystem. Vi har gjennom prosjektet redusert og utkrystallisert funksjonene til å bli prioritert i denne rekkefølgen.

1. Alarmregistrering. Alarmen når fram til meldingstjeneren.
2 Oppkobling mot hjelper. Alarmen når fram til hjelperen.
3 Hjelper får kontakt med bruker, med tale. Hjelperen får lyd- kontakt med brukeren.
4 Hjelper får kontakt med bruker, med videosamtale. Hjelperen ser brukeren på video.

Dette har gått på bekostning av den opprinnelige ideen fra Grensebroen Arena med en videobasert alarmtelefon. Til gjengjeld er selve alarmen blitt prioritert og videobildet befordret der dette er mulig.

7.3 Andre muligheter for alarmkjeder

7.3.1 Responstider

I avsnitt 6.3.1 responstider blir det pekt på at det går lang tid før en offentlig hjelper når å opprette telefonikontakt med brukeren. Det kan derfor tenkes en annen alarmkjede hvor brukerens applikasjon via meldinger får oppgitt direkte hvilke alarmnummer som er aktuelle i prioritert rekkefølge slik at applikasjonen kan ringe disse direkte. Dette åpner også muligheter for å benytte tjenesten gruppeanrop. Denne løsningen er ikke blitt nærmere belyst ut fra betraktningen at den ikke sikrer journalføring. Imidlertid er det hjelpepersonellets ansvar å føre journal, ikke systemets! En implementering av et slikt system vil antagelig falle lettere. De antatte tidene for meldinger som er oppgitt i Tabell 36 er gitt under normale driftforhold. Meldinger som sendes under forhold med stor trafikk vil være vesentlig tregere (timer) For å unngå dette og stabilisere systemet under stor meldingstrafikk kan det være en ide å benytte seg av en egen SMSC / MMSC, med direkte tilknytning til det sikrede VPN nettverket.

7.3.2 Hjemmesykepleiebasert hjelp kontra alarmsentral

Det skal nevnes at brukerpanelet ved en anledning diskuterte bruk av stasjonær PC kontra mobiltelefon for hjelpepersonellet. Dette er ønskelig ut fra hurtighet i respons på alarmer, dette fordrer imidlertid to operatører (vakter) for kontinuerlig å holde denne bemannet. Det ble derfor sett på som urealistisk slik de kjente sin arbeidssituasjon i kommunehelsetjenesten. Imidlertid er det slik at en vaktsentral godt kan være både interkommunal og regional med den alarmfrekvensen dette medfører. Panelets tanker dreide seg nok mer om at det var brukerens egne hjemmesykepleiere som skulle stå for bistanden og da vil det foreslåtte systemet med mobiltelefoner være mer fleksibelt. Dette åpner også for muligheten til å benytte en ”mild” form for posisjonsbestemmelse av hjelperne via lokaliseringstjeneste og benytte nærmeste hjelper dersom utrykning av hjelpere er ønskelig.

7.4 Tilrådninger

7.4.1 Meldingstjeneren

Meldingstjeneren må dupliseres for å gi god nok driftstabilitet. Også terminaler til meldingstjeneren er et svakt punkt som må sikres. Her gjelder at kun autorisert personell skal ha tilgang og at dette skal skje i enerom, uten mulighet for innsyn på skjerm eller tastatur fra vindu eller dører. Videre skal meldingstjeneren sikres med antivirusprogramvare og brannmur. Passord skal skiftes med jevne intervaller og det skal benyttes passordpolicy som krever kvalitativt gode passord. Det skal være flere journalansvarlige ved hver institusjon for å sikre tilgangen til journalen. Selve tjeneren bør dupliseres i to lokaler. Det skal rutinemessig tas kopi av driftsdata og lagres i safe. Husk at disse skal merkes "konfidensielt" og avhendes på en trygg måte. Videre skal servicepersonell avgi taushets erklæring samt at alle lagringsmedia fra brukt maskinvare destrueres på en sikker måte ved avhending. Det er krav om oppbevaring av journal i ti år etter siste innføring.

7.4.2 Hjelpers mobilapparat

Det må finnes en rutine for å koble ned VPN tunnel til et mobilapparat fra meldingstjenerens terminal slik at stjålne mobiltelefoner kan kobles raskt fra det sikrede nettverket. Det må også utarbeides administrative rutiner slik at alltid flere hjelpere kan anropes. Visning av meldinger på hjelpers mobiltelefon må kun foregå i kort tidsrom etter tasteberøring og nytt passord (ev. pinkode) bør benyttes for å aktivere ny visning eller betjening av apparatet. Videre kan det avtales et alarmsignal som viser at hjelperen er under tvang. Videre må all klientinformasjon i MMS meldinger slettes når meldingsinnsatsen er over. Det foreslås at hjelperen ikke gis tilgang til andre journaler enn den alarmen gjelder for og avstenges fra journalsystemet når det ikke foreligger aktive alarmer (Aktive alarmer er alarmer hvor det ikke er ført journalmelding.). Videre foreslås at det ikke sendes nye alarmer fra meldingstjeneren til hjelperen før denne har ført journal for forrige – melding. (Kun en aktiv alarmmelding av gangen.)

7.4.3 Generell sikkerhetspolicy, anbefaling

Det anbefales sterkt at det utarbeides kursmateriell for hjelpere og journalansvarlige i datasikkerhet. Materiellet bør fokusere på daglige gjøremål og omgang med datautstyr inneholdende sensitive opplysninger samt passordmekanismer, valg og bruk av passord. Fagerli og Fyhn avdekket i [6] at sykepleieres kunnskap rundt datasikkerhet var generelt dårlig selv om unntak forekom. Det er grunn til å minne om personopplysningslovens §2-8 som pålegger medarbeidere som er autorisert å ha nødvendig kunnskap om informasjonssystemet for å kunne bruke dette som forutsatt. Samme bestemmelse pålegger registrering av autorisert bruk. (loggføring)
Ved service på utstyr bør "Norm for informasjonssikkerhet i helsesektoren" [14] benyttes som kontraktgrunnlag.

7.4.4 Evaluering

Ved igangsettelse av alarmsystemer av denne art bør systemene evalueres og feil rettes. Ses@m [7] i Tromsø lærte at bruken av systemene ikke alltid var slik den var beregnet fra start, men at brukerne fant nye anvendelser for systemet. En endring i systemet fanget også inn den opprinnelige tenkte bruken. Dette systemet er mye større enn vårt enkle alarmsystem, men mange av problemstillingene blir allikevel like. Vårt system bør derfor evalueres etter en tids bruk og revideres. Videre bør ideer og synspunkter fra slike evalueringer tilbakekobles til et miljø som kan ta vare på også de mer perifere ideene og utvikle disse. Et slikt miljø er nettopp hva Grensebroen Arena ønsker å være.

7.5 Ideer og videre arbeid

7.5.1 Nye ideer som bør vurderes

Gjennom arbeidet med prosjektet har det til tider kommet fram nye ideer og framlegg som ikke har blitt behandlet i rapporten, de fleste fordi de faller utenfor rammen av oppgaven, eller at teknologien ikke er moden i øyeblikket.
En ide er å ha en Bt-enhet fast montert i egen boenhet slik at mobiltelefonen kan gi tale påminnelse når den mister forbindelsen til denne enheten. Påminnelsen kan være av typen ” Har du husket å låse døra?”, eller ”Har du kledd deg for været i dag?” Enheten vil også kunne fungere som bekreftelse på at brukeren befinner seg hjemme. Enheten løser delvis problemet med GPS skygge dersom det benyttes stedfesting via GPS i alarmsystemet.
En annen produktidé generert gjennom brukerpanelet er et veldesignet armbånd med høyttaler, kamera, stort og tydelig display for at hjelper skal kunne kommunisere effektivt med brukeren. Det er essensielt at dette utstyret til vanlig viser en tydelig og lettlest klokke, og kanskje gir påminnelse om dagelige rutiner med lydsignal og symboler ved utvalgte klokkeslett. Enheten kan kommunisere med mobiltelefonen via Bt eller en datasentral via Bt eller annet PAN / WAN. Kjernen er at designen er så god at brukeren får lyst til å bære enheten på armen. Det essensielle med stor og tydelig klokke er at dette er noe de fleste lett demente har et forhold til. I Grensebroen Arenas underprosjekt Teldre blir det arbeidet med stedfesting av brukeren innendørs. Dette er ønskelig ut fra et akuttmedisinsk synspunkt for å finne forulykkede brukere.

7.5.2 Gamle gode ideer som bør utvikles.

Grensebroen Arena har en ide om at mobilapparatet kan benyttes som server for et system av flere kamera i brukerens boenhet på en slik måte at hjelperen kan inspisere leiligheten. Dermed vil man forenkle tilsynet med en bruker fra å være en nattpatrulje på et sykehjem til å være en videotelefonoppringing eller en datakommunikasjonssesjon mellom pleier og hjemmeboende bruker. Eventuell utvikling kan da ikke skje i Java™ med dagens bibliotekfunksjoner.
I rapporten er det enkelte steder nevnt stedfesting med GPS. Dette er en ide som bør tas videre med i etterfølgende utredninger rundt alarmsystemet. Siden GPS er et amerikansk (og tidligere militært) styrt system [125, 126] bør også Galileo vurderes til dette. Det foregår arbeid for å harmonisere systemene.

7.5.3 CDMA450

3G telefonisystemet ICE som bygger på CDMA 450 og tilbys som datakommunikasjon er verdt å studere nærmere fordi det benytter det relativt lavfrekvente båndet rundt 450 MHz (relativt til UMTS 1,92 til 2,17 GHz) hvilket vil kunne gi en litt bedre dekning innendørs. Det bør derfor vurderes i hvilken grad retningslinjene og forslagene i denne rapporten kan implementeres i ICE mobiltelefonsystemet.

8 Konklusjon

Det er sannsynlig at alarmsystem via mobilnettet lar seg realisere. Utstyr for personalarm faller i to grener; privat og offentlig bruk. Privat bruk blir å betrakte som private telefonsamtaler og private meldinger.

Lovverket setter betingelser for offentlig bruk av alarmsystem dersom alarmene angår helseforhold og krever en journalførende enhet tilknyttet alarmsystemet. Det settes krav om at journalføringen skal være på person. Det kreves videre tiltak som beskytter følsomme data mot utlevering og endring.

Teknologien setter klare grenser for toveis kommunikasjon av levende bilder (videotelefoni). Det genererende ønske om toveis kommunikasjon med levende bilder direkte tilknyttet alarmmeldingen er derfor forlatt til fordel for en sikrere alarmbefordring.

Til alarmbefordring foreslås å benytte Bluetooth kommunikasjon mellom sensor og brukerens mobilapparat, SMS mellom brukerens mobilapparat og meldingstjener og endelig MMS mellom meldingstjener og hjelpers mobilapparat.

Det er problemer med usikre responstider i mobiloperatørenes SMS og MMS sentraler, slik at det bør vurderes bruk av dedikerte meldingssentraler.

Det anbefales utstrakt bruk av virtuelle private nettverk der journaldata blir befordret. Videre kreves autentisering av hjelper mot journal, men ikke mot alarmmeldinger. Det anbefales ikke å oppbevare journaldata på mobile enheter.

Journalførende enhet (meldingstjener) anbefales duplisert i nett og geografi med automatisk synkronisering mellom tjenerne. Det kreves kryptering og sikkerhetskopisystem tilknyttet journalsystemet. Meldingstjenerens terminaler må beskyttes mot ufrivillig utlevering av journaldata. ”Norm for informasjonssikkerhet i helsesektoren” anbefales fulgt og brukt som kontraktgrunnlag mot tredjepart.

9 Forkortelser og akronymer

Fork	Engelsk	Ev Norsk overs.	Assosieres med
3GPP	3rd Generation Partnership Project		3G, UMTS, GERAN, EDGE
AFH	Adaptive Frequency Hopping	Tilpassende frekvenshopping	Bt
API	Application Programming Interface		programmering
AUC	AUthentication Centre	Autentiseringssenter	GSM / UMTS
BB	BaseBand	Basisbånd	Bt, Radiotelefoni, telefoni
BQTF	Bluetooth Qualified Test Facility	Bt testprogram	Bt
BSC	Base Station Controller	Basestasjonskontroller	GSM
Bt	Bluetooth	Tidligere : Blåtann	PAN, sensor, mobiltelefon
BTS	Base Transreceiver Station	Basestasjon	GSM
BTSM	Base Tranreceiver Station Management	Basestasjonsstyring	GSM
CLDC	Connected Limited Device Configuration		Java, mobiltelefoner
CM	Call Management	Koblingsstyring	Telefoni
CPA	Content Provider Access	Innholdsleverandør tilkobling	(Mobil)telefoni
DHCP	Domain Host Configuration Protocol		IP
DNS	Domain Name System		IP
EDGE	Enhanced Data rates for Global Evolution		GSM, GPRS, GERAN
EIR	Equipment Identity Register	Utstyrsidentifikasjonsregister	GSM, UMTS
ETSI	European Telecommunications Standard Institute		Standarder
FEC	Forward Error Correction		Datapakking
GAP	Generic Access Profile		Bt
GERAN	GSM EDGE Radio Access Network		GSM, EDGE
GFSK	Gaussian Frequency Shift Keying		Modulasjon
GGSN	Gateway GPRS Support Node		GPRS, UMTS
GMM	Global Multimedia Mobility		3G, UMTS
GMSC	Gateway Mobile Switching Centre		GPRS, UMTS
GPRS	General Packet Radio Service		GSM
GPS	Global Possitioning System		Stedfesting
GR	GPRS Register		GPRS, UMTS
GSM	Global System for Mobile communications		2G
HID	Human Interface Device		Bt
HLR	Home Location Register		GSM / UMTS
IP	Internet Protocol		GPRS, EDGE, UMTS
ISDN	Integrated Services Data Network		Telefoni
ISM	Industrial Scientific and Medical band		Radiofrekvensbånd
IWF	InterWorking Functions		GSM, UMTS
J2ME	Java 2 Micro Edition		Programmering, Bt, mobiltelefoner,
JVM	Java Virtal Machine		Programmkjøring
KVM	K Virtual Maskine		Java, mobiltelefoner
L2CAP	Logical Link Control And Adaption Control		Bt
LAPDm	Link Access Procedure for D channel, mobile		GSM
MIDP	Mobile Information Device Profile		Java , mobiltelefoner

MM	Mobile Management		GSM
MMS	Multimedia Message Service		GPRS, EDGE, UMTS
MMSC	MulitiMediaServiceCenter	MMS sentral	MMS, GPRS
MOF	Meta Object Facility		Modellering
MS	Mobile Station	Mobilt apparat	Mobiltelefoni
MSC	Mobile Switching Centre	Mobil svitsj	GSM
MT	Mobile termination		GSM, UMTS
NSS	Network and Switching Subsystem		UMTS
OCL	Object Constrain Language		Modellering
OMC	Operation and Maitenance Centre		UMTS
OMG	Object Management Group		Modellering
OPP	Object Push Profile		Bt
OSI	Open Systems Interconnection basic reference modell		Telekommunikasjon, datakommunikasjon
OSS	Operation SubSystem		UMTS
PAN	Personal Area Network	Personlig nettverk	Bt
PCM	Pulse Code Modulation.		Modulasjon
PDA	Personal Data Assistent	Personlig dataassistent	Datautstyr
PLMN	GSM Public Land Mobile Network		GSM
PSTN	Public Switched Telephone Network	(Fast)Telefoninettet	Telefoni
PTP	Point To Point		Kommunikasjon
PTP-CLNS	PTP ConnectionLess Network Service		Kommunikasjon, GPRS
PTP-CONS	PTP Connection Oriented Network Service		Kommunikasjon, GPRS
QoS	Quality of Service	Tjenestekvalitet	
RSS	Radio SubSystem		UMTS
SDP	Service Discovery Protocol		UMTS
SDSL	Symetrical Digital Subscriber Line		
SDSL	Symetrical Digital Subscriber Line		Datakommunikasjon
SGSN	Serving GPRS Support Node		GPRS, UMTS
SIG	Special Interest Group		Bt
SIM	Subskriber Identity Module	SIM kort	GSM
SMSC	Short Message Service Center		GSM, SMS
SPP	Serial Port Profile		Bt
SPP	Serial Port Profile		Bt
STP	Service Transfer Point		GSM, GPRS, CPA
TCK	Tecknology Compatibility Kit		Programmering, test
TCP	Transmission Control Protocol		Internett
TDD	Time Division Duplex		Radio og Datakomm
TE	Terminal Equipement	Terminalutstyr	
UDP	User Datagram Protocol		Internett
UML	Unified Modelling Language		Programmering, presentasjon
UMTS	Universal Mobile Telecommunication System		3G
USB	Universal Serial Bus		Datakommunikasjon
UTRA	Universal Terrestrial Radio Access		UMTS
UTRAN	Universal Terrestrial Radio Access Network		UMTS
UUID	Universally Unique IDentifier		Bt
VLR	Visitor Location Register		GSM
VM	Virtual Machine		
VPN	Virtual Private Network		Datakommunikasjon
WLAN	Wireless Local Area Network	Radiolokalnett	Datakommunikasjon Wi-Fi
XML	eXtended Markcup Language		Programmering

10 Referanser

[1] Lov om behandling av personopplysninger (personopplysningsloven).
http://www.lovdata.no/all/nl-20000414-031.html
Verifisert 061218

[2] Forskrift om behandling av personopplysninger (personopplysningsforskriften).
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html
Verifisert 061218

[3] Helseregisterloven.
http://www.lovdata.no/all/hl-20010518-024.html
Verifisert 061219

[4] http://www.wi-fi.org/ Beskriver Wi-Fi trådløse nettverk.
Verifisert 061219

[5] http://www.tryggogsikker.no/html/131.html Hjelpemidler for hjemmeboende.
Verifisert 061218

[6] Liv Berit Fagerli og Per Gunnar Fyhn ”intervjuundersøkelse av sykepleiere i hjemmesykepleien
ISBN 82-7825-165-1

http://fulltekst.bibsys.no/hiof/rapport/2005/hefte1-05.pdf

verifisert 061218

[7] Lotherington et al 2006: Telemedisin i pleie og omsorgtjenesten: Et nødvendig redskap for utvikling av primærhelsetjenesten ?
http://www.norut.no/norut_samfunn/publikasjoner/rapporter/telemedisin_i_pleie_og_omsorgstjenesten
verifisert 061219

[8] UML Unified Markup language.
http://www.uml.org
verifisert 061218

[9] JAVA J2ME
http://java.sun.com/javame/index.jsp
verifisert 070323

[10] Statistisk sentralbyrå; hjemmesider om framskrevet befolkning:
http://www.ssb.no/emner/02/03/nos_folkfram/nos_d319/nos_d319.pdf
verifisert 070126

[11] Christopher P.Nemeth: “Human Factors for Design; Making Systems Human-Centred “
CRC Press LLC 2004 ISBN: 0-415-29798-2 Biblioteket HiØ Sarpsborg 331.101.1 Ne

[12] Johansen et al: “Personopplysningsloven Kommentarutgave” Universitetsforlaget 2001 ISBN: 82-518-3702-2

[13] Øyvind Børthus og Tomas Mikael Engh ”Privacy protection in a mobile Biomedical Information Collection Service. HiA Master thesis May 2005

[14] Sosial og helsedirektoratet ”Norm for informasjonssikkerhet i helsesektoren” http://www.shdir.no/samspill/informasjonssikkerhet/norm_for_informasjonssikkerhet_i_helsesektoren_53069 Verifisert 070323

[15] Datatilsynet veiledere i sikkerhet og risikovurdering: http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/SV100_00.pdf http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/tv202_2005_1.pdf http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering_TV-506_02.pdf http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Veileder_tynneklienter.pdf Verifiserte 070323

[16] Datatilsynet: http://datatilsynet.no Verifisert 070323

[17] Prof. Dr.-Ing. Habil. Jochen Schiller http://www.inf.fu-berlin.de/inst/ag-tech/resources/mobkom/material/English/PDF-Handout/C04-Wireless_Telecommunication_Systems.pdf Verifisert 070323

[18] AN OPTIMUM ACCELEROMETER CONFIGURATION AND SIMPLE ALGORITHM FOR ACCURATELY DETECTING FALLS A.K. Bourkeφ, C. Ni Scanaillφ,K.M. Culhaneφ, J.V. O’Brien*, G.M. Lyonsφ φ Biomedical Electronics Laboratory, Department of Electronic and Computer Eng, University of Limerick, Limerick, Ireland. http://delivery.acm.org/10.1145/1170000/1166534/p156-bourke.pdf?key1=1166534&key2=0110959611&coll=&dl=ACM&CFID=15151515&CFTOKEN=6184618 Lest 070517

[19] ISO/IEC 14496-10 Information technology – Coding of audio-visual objects-Part 10: Advanced Video Coding http://webstore.iec.ch/preview/info_isoiec14496-10%7Bed3.0%7Den.pdf Lest 070517

[20] ISO/IEC 14496-10 Wikipedia http://en.wikipedia.org/wiki/H.264 Gir innføring i H264 lest 23032007

[21] H.263 Audio/Video kommunikasjons- protokoll. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc2190.txt Lest 070323

[22] Ericsson AB: White paper: EDGE Introduction of high-speed data in GSM/GPRS networks. http://www.ericsson.com/technology/whitepapers/edge_wp_technical.pdf Lest 070309

[23] Helsenett: http://www.helsenytt.no/artikler/hjemmeulykker.htm Lest 070517

[24] Helsenett: intervju med Reante Pettersen av Eva Fosse: ”Om falltendens hos eldre”
http://www.helsenytt.no/artikler/falltendens_eldre.htm
Lest 070517

[25] Helsenett: Intervju med Jorunn L. Helbostad intervjuet av Eli Gunnvor Grønsdal
”Fall hos Eldre”
http://www.helsenytt.no/artikler/fall_eldre.htm
Lest 070517

[26] ETSI Universal Mobile Telecommunications System (UMTS);
Quality of Service concept and architecture (3GPP TS 23.107 version 4.6.0 Release 4)
Fordrer søk med “TS 23.107 version 4.6.0” på
http://pda.etsi.org/pda/queryform.asp
Lest 070517

[27] Oliver Yu and Shashank Khanvilkar Department Of Electrical and Computer Engineering
University of Illinois at Chicago 851 South Morgan Street, 1020 SEO.
http://mia.ece.uic.edu/~papers/publications/Monet2002.pdf
Lest 070517

[28] 3GPP arbeidsgruppe WG1 Møte i Oulu Finland 22-24.11.99
http://www.3gpp.org/ftp/tsg_cn/WG1_mm-cc-sm/Ad-hoc-CN1-meetings/TSGN1_adhoc_GSM-UMTS-interworking/Report/Oulu9911.rtf
Lest 070517

[29] 3rd Generation Partnership Project (3GPP) initiativ
http://www.3gpp.org
Lest 070517

[30] 3GPP TS 25.401 V Technical Specification Group Radio Access Network;
UTRAN overall description (Release 4) 4.6.0
http://www.3gpp.org/ftp/Specs/archive/21_series/21.101/21101-4d0.zip
Lest 070517

[31] Direktoratet for samfunnssikkerhet og beredskap:
http://oppslagsverket.dsb.no/docweb/page/mainpage.jsp
Lest 070517

[32] ZD net Co UK: A Guide to handheld operating systems
http://www.zdnet.co.uk/misc/print/0,1000000169,39280712-30000029c,00.htm
Lest 070517

[33] General Pacet Radio Service EN 301 344 V6.1.1 forlanger søk etter EN 301 344 V6.1.1 på
http://pda.etsi.org/pda/queryform.asp
verifisert 070517

[34] Arto Holopainen, Nokia Blogg 24. jan. 2007
http://blogs.forum.nokia.com/view_entry.html?id=381
Lest 070517

[35] Personlig telefonsamtale med Inge Fagerbakke NetCom as.

[36] Personlig henvendelse til Telenor helpdesk 0703223.

[37] Personlig telefonsamtale med Sverre Engelschiøn datatilsynet. 070212.

[38] Personlig telefonsamtale med Arild Hammer, Avdelingsdirektør Direktoratet for samfunnssikkerhet og beredskap, Forebygging og elsikkerhet, enhet Elektriske produkter 070329.

[39] Trådløs Pasient http://www.sintef.no/content/page12____13052.aspx
Lest 070329

[40] Jochen Schiller : "Mobile Communication" Second Edition, 2003 Addison-Wesley
ISBN 0 321 12381 6

[41] Telenor Mobil:
http://telenormobil.no/tjenester/3G/merom.do
Lest 070329

[42] NetCom:
http://netcom.no/tjenester/3g/videotelefoni.html
Lest 070329

[43] Norsk Standard NS-ISO 60601-1-1

[44] Direktoratet for samfunnssikkerhet og beredskap; "Forskrift av 20 august 1999 nr 955 om bruk og vedlikehold av elektromedisinsk utstyr" henviser til [43]
http://oppslagsverket.dsb.no/docweb/page/mainpage.jsp;jsessionid=ED8AA23167D99FEE1DE445F31757C086
lest 070330

[45] Norsk telemuseum " Mobiltelefonens historie i Norge"
http://telemuseum.no/mambo/content/view/29/1/
lest 070330

[46] Frode Sørensen: "Moderne IP-nett" IDG Norge Books AS ISBN 82-7772-279-6

[47] Tore Riksaasen: "Telematikknett" Universitetsforlaget AS 1995 ISBN 82-00-41489-2

[48] IEC Web ProForum Tutorials
http://www.iec.org/about/terms.html
Lest 070517

[49] Telenor mobil dekningskart UMTS:
http://telenormobil.no/dekninginnland/index.do
Lest 070517

[50] NetCom dekningskart:
http://dekning.netcom.no/
Lest 070517

[51] 3th Generation Partnership Project TSG GERAN Hjemmeside:
http://www.3gpp.org/TB/GERAN/GERAN.htm
Lest 070410

[52] Telenor mobil MMS tjenesteannonsering:
http://telenormobil.no/tjenester/mms/
Lest 070411

[53] Samferdselsdepartementet ”Konsesjon for å anlegge, inneha og drive et offentlig telenett av type UMTS”
http://www.regjeringen.no/nb/dep/sd/dok/andre/konsesjon/2000/UMTS-konsesjon-Telenor.html?id=424145
Lest 070411

[54] Samferdselsdepartementet ”Konsesjon for å anlegge, inneha og drive et offentlig telenett av type UMTS”
http://www.regjeringen.no/nb/dep/sd/dok/andre/konsesjon/2000/UMTS-konsesjon-NetCom.html?id=424146
Lest 070411

[55] 3th Generation Partnership Project TSG CT (Om MMS)
http://www.3gpp.org/ftp/Specs/html-info/23140.htm
Lest 070411

[56] NORTEL white paper ”HSDPA and beyond” Nortel Networks
http://www.nortel.com/solutions/wireless/collateral/nn_110820.01-28-05.pdf
Lest 070411

[57] 3th Generation Partnership Project ”Long Term Evolution”
http://www.3gpp.org/Highligts/LTE/LTE.htm
Lest 070411

[58] Incontext ”Contextual Design Process”
http://www.incontextdesign.com/cd/methodology.html
Lest 070411

[59] Helsepersonelloven
http://www.lovdata.no/all/hl-19990702-064.html
Lest 070411

[60] Forskrift om pasientjournal
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001221-1385.html
Lest 070411

[61] Forskrift om elektronisk kommunikasjon med og i forvaltningen
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html
Lest 070412

[62] Lov om elektronisk signatur
http://www.lovdata.no/all/hl-20010615-081.html
Lest 070412

[63] Post- og Teletilsynet: ”Norsk veiledning for rapportering av tjenestekvalitet”
http://www.npt.no/iKnowBase/Content/veiledning2.pdf?documentID=50396
Lest 070412

[64] ETSI European Telekommunication Standardisation Institute
http://pda.etsi.org/pda/queryform.asp Søk etter EG 202 057-2 og registrer epost -adresse for fri nedlasting
Lest 070412

[65] Lov om pasientrettigheter (pasientrettighetsloven)
http://www.lovdata.no/all/nl-19990702-063.html
Lest 070412

[66] Bluetooth SIG. Inc. The Official Bluetooth® Technology Info Site
http://www.bluetooth.com/bluetooth/
Lest 070412

[67] Bluetooth SIG. Inc.”Bluetooth Basics”
http://www.bluetooth.com/Bluetooth/Learn/Basics/
Lest 070412

[68] Bluetooth SIG. Inc. ”Spesification documents, Core Spesification v2.0 + EDR
http://www.bluetooth.com/NR/rdonlyres/1F6469BA-6AE7-42B6-B5A1-65148B9DB238/840/Core_v210_EDR.zip
Lest 070511

[69] ZDNET Networks.co.uk Beta ”Access launches mobile Linux push” 12. feb. 2007
http://news.zdnet.co.uk/communications/0,1000000085,39285891,00.htm
Lest 070413

[70] ZDNET Networks.co.uk Beta “Palm touts stability of Linux-based Treos” 11. april 2007
http://news.zdnet.co.uk/communications/0,1000000085,39285891,00.htm
Lest 070413

[71] ZDNET Networks.co.uk Beta “Trolltech releases mobile Linux suite”
http://news.zdnet.co.uk/communications/0,1000000085,39284915,00.htm
Lest 070413

[72] Nokia Forum
http://forum.nokia.com/
Lest 070413

[73] Window mobile Microsoft download center
http://www.microsoft.com/downloads/details.aspx?FamilyId=06111A3A-A651-4745-88EF-3D48091A390B&displaylang=en
Lest 070413

[74] Microsoft “A Guide to Windows Mobile Programming for Symbian OS Developers”
http://msdn2.microsoft.com/en-us/library/aa454908.aspx
Lest 070413

[75] Statistisk sentralbyrå Dødsårsaker
http://statbank.ssb.no/statistikkbanken/
Lest 070413

[76] Pressemelding Bloetooth SIG: Bluetooth SIG presents new Specification, and two Implementation Guides
http://bluetooth.com/Bluetooth/Press/SIG/Bluetooth_SIG_presents_new_Specification_and_two_Implementation_Guides.htm
Lest 070414

[77] Bluetooth SIG: Architecture – Core System
http://www.bluetooth.com/Bluetooth/Learn/Works/Core_System_Architecture.htm
Lest 070417

[78] Bluetooth SIG: Architecture – Data transport
http://www.bluetooth.com/Bluetooth/Learn/Works/Data_Transport_Architecture.htm
Lest 070417

[79] Bluetooth SIG: Bluetooth Wireless Technology Profiles
http://www.bluetooth.com/Bluetooth/Learn/Works/Profiles_Overview.htm
Lest 070417

[80] Bluetooth SIG: Bluetooth HID Profile, HID_010_SPC_ PFL/1.0
http://www.bluetooth.com/NR/rdonlyres/0BE438ED-DC1B-41D1-AAC0-1AAA956097A2/980/HID_SPEC_V10.pdf
Lest 070417

[81] Helsetilsynet Lov om rettigheter for og begrensning og kontroll med bruk av tvang m.v. overfor personer med demens – Høring.
http://www.helsetilsynet.no/templates/LetterWithLinks____5158.aspx
Lest 070418

[82] Stortinget: Innst.O.nr.14 (2003-2004)
http://www.stortinget.no/inno/2003/200304-014-002.html
Lest 070418

[83] Nokia: Bluetooth_Technology_Overview_v1_0_en.pdf
http://forum.nokia.com/info/sw.nokia.com/id/98f61174-e3fc-499f-be81-7ce66c0a99aa/Bluetooth_Technology_Overview_v1_0_en.pdf.html
Lest 070418

[84] Bluetooth: Membership Benefits
https://programs.bluetooth.org/membership/benefits.htm
Lest 070419

[85] Datatilsynet: Faste IP addresser
http://www.datatilsynet.no/templates/Page____1625.aspx
Lest 070419

[86] Telenor mobil : Dekning, 3G
http://telenormobil.no/dekning/3G
Lest 070419

[87] Ivar Brådland og Per Øyvind Hodøl "Sikkerhet og sårbarhet i IP basert infrastruktur"
Masteroppgave Høgskolen i Agder 2006 IKT
http://fag.grm.hia.no/ikt590/hovedoppgave/
Lest 070419

[88] Bluetooth SIG: Wireless Security
http://www.bluetooth.com/Bluetooth/learn/Security/
Lest 070419

[89] Post og teletilsynet v/ Jarl Kristen Fjerdingby personlig telefonsamtale 070420

[90] Nordisk Mobiltelefon Norway AS: Kundesenter personlig samtale med Kim Ensrud

[91] The Aerospace Corporation Crosslink: Charles Wang, Dean Sklar, and Diana Johnson "Forward Error Correction Coding"
http://www.aero.org/publications/crosslink/winter2002/04.html
lest070420

[92] "Forskrift om krav til akuttmedisinske tjenester utenfor sykehus."
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20050318-0252.html
Lest 070425

[93] "Forskrift om offentlig telenett og offentlig teletjeneste (offentlignettforskriften)."
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19971205-1259.html
Lest 070426

[94] Telenor partnerportalen
http://www.partnerportalen.no/hXGYBmwJrYYs.4.idium
Lest 070426

[95] Telenor: "SMS Access and SMS Bedrift Expanded Product Sheet"
http://www.partnerportalen.no/filestore/SMSBedriftUtvidetProduktark.pdf
Lest 070426

[96] Personlig samtale med Telenor kundesenter telefon 9000 og NetCom kundesenter telefon 23888000 ,kontakt 070427.

[97] Partnerportalen Telenor "SMS Aksess priser"
http://www.partnerportalen.no/filestore/SMSAksesspris.pdf
lest 040727

[98] Telenor :”CPA Messaging Agreement”
http://cpa.telenor.no/cpa/cpamessaging/CPA%20Messaging.pdf
Lest 070427

[99] Telenor: ”Priser på Mobil Data Aksess”
http://www.telenor.no/bedrift/produkter/mobil/mobil_data_aksess_priser.html
Lest 070427

[100] Partnerportalen Telenor: ”SMS Bedrift og SMS aksess, Requirements”
http://www.partnerportalen.no/filestore/SMSBedriftAksessKravApplikasjon.pdf
Lest 070427

[101] Telenor: ”CPA retningslinjer”
http://cpa.telenor.no/cpa/contentprovider/guidelines/CPARetningslinjer.pdf
Lest 070427

[102] Telenor: produktark ”Mobil data aksess”
http://www.telenor.no/bedrift/produkter/mobil/other/produktark_mda.pdf
Lest 070428

[103] NetCom as: ”M2M VPN”
https://netcom.no/bedrift/telemetri/m2mvpn.html
Lest 070428

[104] NetCom as ”Telemetri”
https://netcom.no/bedrift/telemetri.html
Leste 070428

[105] NetCom as ”Telemetri” priser
https://netcom.no/bedrift/telemetri/priserabo.html
Lest 070428

[106] NetCom as ”Priser NetCom Telemetri tilleggstjenester”
https://netcom.no/bedrift/telemetri/prisertjenester.html
Lest 070428

[107] NetCom as ”M2M Basic”
https://netcom.no/bedrift/telemetri/prisertjenester.html
Lest 070428

[108] NetCom as ”M2M VPN”
https://netcom.no/bedrift/telemetri/m2mvpn.html
Lest 070428

[109] OMG’s Meta Object Facility
http://www.omg.org/mof/
Lest 070430

[110] Unified Modeling Language: Infrastructure
http://www.omg.org/docs/formal/07-02-04.pdf
Lest 070430

[111] Unified Modeling Language: Superstructure
http://www.omg.org/docs/formal/07-02-03.pdf
Lest 070430

[112] Introduction to OMG's Unified Modeling Language™ (UML®)
http://www.omg.org/gettingstarted/what_is_uml.htm
Lest 070430

[113] Omondo: Welcome
http://www.tutorial-omondo.com/
Lest 070430

[114] Bluetooth SIG " Part K:5 Serial Port Profile"
http://www.bluetooth.com/NR/rdonlyres/9C6DB2A4-A7D9-47A6-81B3-5F03981AE9C4/986/SPP_SPEC_V11.pdf
Lest 070510

[115] Bluetooth org: "Bluetooth assigned Numbers"
https://www.bluetooth.org/foundry/assignnumb/document/assigned_numbers
(Krever passord til www.bluetooth .org)
Lest 070510

[116] Motorola Mobile Devices software: "Java ™ APIs for Bluetooth™Wireless Technology (JSR 82)"
Motorola 2.september 2005.
http://192.18.108.235/ECom/EComTicketServlet/BEGIN47E25A85ED021FE6AB3957CDADAA26E9/-2147483648/2120364963/1/741602/741590/2120364963/2ts+/westCoastFSEND/bluetooth-1_1-mrel3-oth-JSpec/bluetooth-1_1-mrel3-oth-JSpec:1/bluetooth-1_1-mrel-spec.pdf
lest 070511

[117] SUN Microsystems "CLCD API 1.0"
http://java.sun.com/j2me/docs/pdf/cldcapi.pdf
Lest 070513

[118] SUN Developer Network "Java ME Mobile Information Device Profile (MIDP); JSR 37, JSR 118"
http://java.sun.com/products/midp/
Lest 070513

[119] Forum Nokia :" Example: Creating a client/server pair using RFCOMM"
http://www.forum.nokia.com/document/Java_ME_Developers_Library/index.html
Lest 070513

[120] Datatilsynet "eCall" Artikkel Sverre Engelsciøn 8. mai 2007
http://www.datatilsynet.no/templates/Page____1833.aspx
Lest 070514

[121] Datatilsynet "Risikovurdering av informasjonssystem med utgangspunkt i personopplysningsloven"
http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering_TV-506_02.pdf
Lest 070514

[122] Datatilsynet: Gunnel Helmers, artikkel publisert 070412 ”Hjelpetrengande må få bestemme sjølv”.
http://www.datatilsynet.no/templates/Page____1791.aspx
Lest 070515

[123] European Space Polity ” Navigation, timing and positioning: The Galileo Programme”
http://ec.europa.eu/enterprise/space/programmes/galileo_en.html
Lest 070521

[124] Nokia forum resources, technologies, audioviedo
http://www.forum.nokia.com/main/resources/technologies/audiovideo/
Lest 070522

[125] US Government: Global Positioning System
http://www.gps.gov/
Lest 070522

[126] National space-based Positioning, Navigation and Timing executive committee.
http://pnt.gov/
Lest 070522

[127] Symbian Software Limited “Signing tips” åpent nettsted
http://nds2.fds-forum.nokia.com/fdp/interface?fid=A1A1UKEDVTET&st=aed9JJe9UWMv5665ffb64979751d42e8864085157de73c76094e1872d608b406ef230db9a2fddcace811687ca5f7935bbf805730e7d608b686ece931c73ee9ca2953eb134ec03e6311ac09b9678db497c0eecb5959356466762e5afaffcfc5f640a8f865babe9fa96b7785473a655072e1e97ce0e63251d4dbecc471240c97efe5e35389bd11b0b66ea0b6271b41e3e3d610c1d43a5aa3ac444bf4c56f9cfd7d194366e178b4f4d76901436bd87e&lid=FN

Tilsvarende for medlemmer av Forum Nokia:
http://forum.nokia.com/info/sw.nokia.com/id/58e85b9e-88b6-4300-a367-16c9c2562db7/Signing_Tips_v2_0_en.pdf.html
Lest 070523

[128] ETSI TS 123 040 Ver 3.10.0 juni 2003 “Digital cellular telecommunication system (Phase 2+); Universal Mobile Telecommunication System (UMTS); Technical realization of Short Message Service (SMS) (3GPP TS 23.040 version 3.10.0 Release 1999)
http://webapp.etsi.org/exchangefolder/ts_123040v031000p.pdf
Lest 070524 Krever registrering.

11 VEDLEGG

Tillempet kontekstuell design med "Focus Group"

Kontekstuell design [58] anvendes ofte til å definere programvares funksjonalitet og GUI. Denne metoden kan virke tung nedbrutt som under, men ser man nøyere på temaene i leddene ser man at metoden kan tillempes til mitt formål: Å definere en funksjonsbeskrivelse til alarmsystemet. Tillempingen presenteres i tabellen under.

Stadium	Kontekstuell design	Tillempning
1	Intervju under arbeid. Målet er på skaffe seg forståelse av arbeidets art og samhandlingen mellom system og mennesker.	Temaspørsmål i plenum "Hva gjør vi om?"
2	Tolkningsmøte, hvor de forskjellige intervjuene fra første stadium presenteres for utviklingsteamet. Mål er å avdekke nødvendige funksjoner og kvantifisere behov. Samt å få en felles forståelse av aktiviteten.	Idegenerering med innledning fra pkt. 1.
3	Kvalitetssikring av funn i samsvar med andre kunders ønsker. Generering av funksjonsnettverksdiagram.	Kravgenerering til systemet. Kan ikke gjøre slik. Det fungerer ikke. Osv. Siling av ideene fra pkt.2 etter kriteriene som kommer fram.
4	Nydesign av funksjonene med henblikk på hva teknologi kan benyttes til i funksjonene og nettverkskoblingen. Fokus på hva teknologi kan gjøre for medarbeiderne. Ikke hva medarbeiderne skal gjøre for teknologien! Mål er å lage en visjon som inneholder mål, suksessfaktorer og metoder.	Uforandret.
5	Design av nytt system med ressursdiagnose. Originalt kalt "User environment design". Omhandler ikke brukermiljø i vanlig forstand. Modeller systemet.	Uforandret.
6	Prototype beskrivelse av brukermiljø. "Papirprototype laging" Utføres med å spille scenarier med Post It lapper over ei tavle! Meget realistisk!	Uforandret.
7	Fysisk implementering!	Uforandret.

En metode for idegenerering og ideverifisering

Ide (og krav) generering foregår med at man har skaffet seg et panel av mennesker. Før selve idegenereringsmøtet sender man ut et preemeeting dokument som forklarer formålet, hva som skal skje på møtet. Man ber deltakerne tenke ut tre ideer i stikkordsform som de skriver ned og tar med på møtet. Møtet foregår på den måten at man sørger for at deltakerne har det bra og sørger for en avslappet stemning. (kaffe, bevertning) Man sørger for å gi en introduksjon til temaet som går ut over hva som er framkommet i preemeetingdokumentet. Man går så over til selve idegenereringen. De medbrakte forslagene anbringes i en bolle midt på et bord som deltakerne plasseres rundt. Deltakerne skriver ned ytterligere ideer og plasserer disse til høyre for seg selv. Deltakerne tar så opp ideen sidemannen på venstre side har skrevet, og skriver ned sine assosierende ideer til denne. Under seansen er det absolutt forbud mot negative tanker og kritikk av noe slag. Resultatet er at man får mange ideer. Både gode og dårlige. Ideene må derfor siles.
Dette kan gjøres med å bruke foregående panel, men nå med en felles presentasjon av kjente problemer og krav, for deretter å spørre etter flere. Gjerne i form av ”kunne være kjekt om”.
Siste sesjon er da å sile ideene i fellesskap mot kravene for så å rangere ideene som blir igjen.
Vedlegg 0 inneholder PM dokumentet og det er utarbeidet en egen power-point presentasjon til panelmøtet.

Forslag til oppgave i kommunikasjonsnett bachelor degree.

Konstruksjon og utvikling av fallsensor.

Konsept:

En enhet til å feste på overkroppen inneholdende fallsensor, GPS og temperaturføler kommuniserer med en mobiltelefon for å varsle om bæreren faller. Fallsensoren sender melding til en mobiltelefon via Bt som setter opp en multimediasamtale til hjelpepersonell. Samtidig sendes en SMS med utstyrets posisjon. Hvis hjelpepersonellet ikke får kontakt med den forulykkede må det sendes personell til stedet for å hjelpe. Siden det er en multimediasamtale som settes opp vil hjelpepersonalet kunne se omgivelsene og allerede da bedømme situasjonen.

Bakgrunn:

Fallulykker er den suverent største skadeårsaken blant eldre personer[1]. Ved å varsle fallulykker automatisk vil den forulykkede kunne komme raske i kontakt med hjelpepersonell.
Automatisk varsling vil innebære varsling dersom den forulykkede ikke selv er i stand til å ta kontakt med alarmenhet.

Motivasjon (tese):

Dersom eldre personer føler seg trygge vil de leve et mer aktivt liv og dermed beholde helsa lengre. En fallalarm vil kunne gjøre at eldre personer tør bevege seg på steder der de ellers ikke vil våge.

Teknikk:

Fallsensoren er et treakse akselerometer som føler av akselerasjonen det utsettes for. Dersom tyngdens akselerasjon minskes eller forsvinner, for så å bli snudd, før den igjen blir normal tyder på at et fall har funnet sted. Ved å inkludere en GPS posisjonering i alarmen vil hjelpepersonell stedfeste ulykken når denne skjer utenfor bygninger. En temperaturføler vil fortelle om enheten faktisk befinner seg på bæreren eller har blitt skjøvet ned av nattbordet.
Det er altså nødvendig med en databearbeiding av rådataene fra fallsensoren i en mikrokontroller, samt videreformidling av posisjonsdata og temperatur.

Vilkår for alarm:
Temperaturen er over 33 ºC og Tyngdens akselerasjon har vært redusert fulgt av snudd akselerasjon (dreid i en vinkel på mer enn 60º) og falt tilbake på normalt nivå der normalt nivå avviker mer enn 60º fra den opprinnelige akselerasjonen.

Oppgaven vil bestå i å finne egnet hardvare, utviklingsmiljø og protokollstack, samt programmering av hardvare. Se www.elfa.se/pdf/73/733/0733898.pdf for eksempel på akselerasjonssensor. Valg av hardware må optimaliseres på: Strømforbruk, kompleksitet (Lav totalkostnad). Eksempel på Btinterface: http://www.bluegiga.com
Mvh Reidar Nordby
Referanser:

[1] http://www.helsenytt.no/artikler/hjemmeulykker.html

[2] http://www.helsenytt.no/artikler/falltendens_eldre.htm

[3] http://www.helsenytt.no/artikler/fall_eldre.htm

Brukerpanelmøter

Idegenerering

Reidar Nordby
Grensebroen / HiØ

Til deltakere i brukerpanel.

Hei, du har blitt sjanghaiet til å være med på å gi ideer, synse og forhåpentligvis prøve ut mobilt utstyr beregnet på å forlenge eldre menneskers boperiode i egen bolig.

Første samling blir holdt i grensebroens lokaler på Høgskolen i Østfold i Sarpsborg den 27. feb kl10.00 (Tuneveien 20, Syd-Vestre del av bygningen mot RV118 og parkeringsplass.)

Aktiviteten er delt i 2 tema :

1 avd. er idegenerering.
2 avd. med ide-siling og spesifisering av funksjonsbeskrivelse.
Samlingen vil vare ca. 4 timer.

Til dette møte vil jeg at du tenker ut 3 løse ideer som går på trådløs kommunikasjon brukt til å lette livssituasjonen for eldre hjemmeboende. Ideene skal kunne beskrives i en setning med maks. 8 ord. Har du flere forslag så tar jeg gjerne imot. Disse ideene skriver du ned på forhånd eller før vi begynner på tirsdag. Disse ideene blir samlet inn og lagt ut på bordet under idegenereringen (husk, ingen underskrift, alt er anonymt), og vil fungere som tankeføde for de andre deltakerne og deg selv. Under denne seansen er alle negative tanker, ytringer og kommentarer forbudt.

Under andre del av møtet velger vi i felleskap ut de ideene som vi synes er best av hele den haugen vi lagde i første del. Nå skal de negative tankene fram og vi skal forsøke å finne fallgruvene ved de forskjellige (gode) ideene. Av de ideene vi finner praktisk gjennomførbare lager vi en brukerspesifikasjon i felleskap (slik og sånn, minst så mye, ikke mer enn, osv).
Ut fra denne spesifikasjonen vil jeg forsøke å lage det dere foreslår. De gode ideene som eventuelt blir til overs overlater vi grensebroen for videre bearbeidelse.

Det er planlagt i alt 3 treff med brukerpanelet. Treff nr 2 blir avholdt i midten av mars. Temaet på dette møte blir å korrigere modeller og konsepter basert på spesifikasjonen fra første møte.

Treff nr. 3 blir i første del av mai. På dette treffet legger jeg fram resultatene fra prosjektet mitt. Også på dette møtet ønsker jeg kommentarer fra dere. (Kunne du ikke gjort slik i stedet? Hvorfor gjorde du ikke slik?)

Vel møtt til et hyggelig møte

_____
Reidar Nordby

Idegenerering Brukerpanelmøte 27 feb. -07

Frammøtte:

Ann Karin Helgesen Høgskolen i Østfold, Helsefag
ann.k.helgesen@hiof.no

Kjersti L. Jørgensen Fredrikstad kommune
klab@fredrikstad.kommune.no

Marit Smittil Fredrikstad Kommune
masm@fredrikstad.kommune.no

Safdar Abbas Høgskolen i Østfold, ingeniørfag E2
saabb@online.no

Tomas Moe Høgskolen i Østfold, ingeniørfag E2
tomasmoe@msn.com

Per-Thomas Huth Høgskolen i Østfold, ingeniørfag prosjektleder grensebroen
per.t.huth@hiof.no

Reidar Nordby Høgskolen i Østfold, ingeniørfag masterkandidat HiA
reidar.nordby@hiof.no

Åpning med Per-Thomas: Velkommen, om Grensebroens bakgrunn, orientering om historie og prosjekter.
Reidar: Introduksjon til oppgaven. Møtets formål, bakgrunn og agenda.

Idegenerering: Deltakerne hadde på forhånd formulert noen ideer som de la i potten når seansen startet. Idegenereringen fulgte mønstret med å notere nye ideer på PostIt lapper som ble sendt bordet rundt til å gi inspirasjon til nye ideer.
Resultater av idegenerering: 56 ideer og åpne ideområder med spennvidde over alt fra intelligent hus til måter å oppnå sosial kontakt.
Kravgenerering: Kravgenerering ble utført på samme måte som idegenereringen, etter en introduksjon om emnet for deltakerne. Deltakerne ble bedt om å se bort fra krav fastsatt i lover og normer og ble i stedet bedt om å gi praktiske, bruksmessige krav. Resultat av kravgenereringen: 29 krav spennende fra teknisk krav til sosialetiske ble inngitt.
Ideene og kravene er samlet i tabellene under. Kommentarene er lagt til for å belyse eller spinne videre.

nr	Ide	Kategori	Kommentar
1	Brann og tyverialarm	Intelligent hus	Lovpålagt i institusjoner.
2	Lysstyring, samt komfyr/strykejern, TV	Intelligent hus	Når beboer forlater bolig og natt? Godnattknapp? Demensrelatert?
3	Lys og varmestyring ved utgangen	Intelligent hus	
4	Seriekoblet nattlys som følger beboer rom til rom	Intelligent hus	Bevegelsessensor?
5	Sensor som kontrollerer varme, varmt vann, komfyr, lys og stikk på tid.	Intelligent hus	
6	Sensor for forlate område	Intelligent hus	Demensrelatert
7	Dørklokke med video på TV	Intelligent hus	Er utviklet, krever melding til datatilsynet
8	Komfyrvakt	Intelligent hus	
9	Kommunikasjonsanlegg som aktiveres med enkeltord og stemmevalør.	Intelligent hus / Kommunikasjon	Er utviklet på mobiltelefoner for oppringing.
10	Skjerm på kjøkkenskap som forteller (Avhengig av tidspunkt på dagen) om avtaler, rutiner (koke kaffe, smøre mat, forvente middag)	Enkelt hjelpemiddel	Kommentert som meget aktuelt.
11	Hindre kaffetrakter i å stå på over 1 time.	Enkelt hjelpemiddel	
12	Komplett system for styring (hjelp) til disponering av dagen med (avtaler, måltider, piller, TV, etc.)	Enkelt hjelpemiddel	Se nr.10
13	Et apparat som gjør det enkelt å kontrollere alt.	Intelligent hus	Mobiltelefon?
14	Mulighet til å gjøre beboer oppmerksom på mat/drikke som er tilgjengelig.	Enkelt hjelpemiddel	Talemelding på mobiltelefon Push to Talk gruppe? Vindu i kjøleskapdør?
15	Sensor ved alle utgangsdører som kan brukes til styring av lys og andre ting ved behov.	Intelligent hus	
16	Skjerm på utgangsdør som forteller hvor vidt det er natt eller dag, og om det er kalt ute. Forebygge nattevandring ute.	Enkelt hjelpemiddel mobiltelefonapplikasjon	Plakat ved døra på eller over et (stort) speil. ”Det er kalt ute, Har du kledd på deg”
17	Bruker: Hvordan får jeg ny resept.	Åpent ideområde	Gitt som eksempel på gjentatt spørsmål fra brukere. Slik informasjon bør finnes lettilgjengelig og gjentas for brukerne.
18	Sikre at bruker er hensiktsmessig kledd når vedkommende går ut.	Avansert hjelpemiddel	Se 16. IR kamera?
19	Avbilde bruker når denne går ut + klokkeslett.	Avansert hjelpemiddel	Se 18,17 Lett å få til, meldepliktig til datatilsynet.
20	Hindre at beboer blir gående våt	Sensor med mobilkommunikasjon	Bt?
21	Melde fra hvis en person fremdeles er i sengen på dagtid.	Sensor med mobilkommunikasjon	Bt?
22	Sensor for fall	Sensor med	Bt?

		mobilkommunikasjon	
23	Sensor som reagerer hvis lokket til medisinene åpnes.	Sensor med mobilkommunikasjon	Bt? Alarm dersom mønster brytes?
24	Trenger hjelp til medisinering	Åpent ideområde	Demensrelatert
25	Hvordan sikre at pillene blir tatt riktig	Åpent ideområde	Demensrelatert
26	Økning av hjemmehygge	Åpent ideområde	
27	Hvordan sikre eldre utendørs	Åpent ideområde	
28	Videotelefonsamtale på storskjerm	Videokommunikasjon	
29	Bilder av pårørende Eks. Tast der det står barn (og bilder av barna blir vist)	Videokommunikasjon	Er bla til finn OK?
30	Direkte-tavle video tilstede m. alle barn.	Videokommunikasjon	
31	Webkamera som går direkte til familie / omsorgstjeneste	Videokommunikasjon	
32	Tilstedeværelse ved hjelp av tale/ video ved måltider og laging av mat	Videokommunikasjon	
33	Pårørendemøter på nett.	Videokommunikasjon	Pårørende i vid forstand? Videokonferanse?
34	Elektronisk informasjonssentral (for hjemmet) med åpen telefonlinje (lyd og bilde) til vaktsentral.	Video/data kommunikasjon	Mulig å utføre på mobiltelefon? Ide hentet fra medisinsk oppfølging.
35	Storskjerm med blikk inn i pårørendes leilighet	Videokommunikasjon	
36	Hvordan få kjapp kontakt med pårørende (sosial kontakt)	Åpent ideområde	
37	Hvordan få hjelp til betjening av TV innstilling osv. når hjelperen ikke er til stede.	Åpent ideområde	
38	På mobilen: Stor skjerm, få taster. Ikke for avansert teknologi.	Usability	Tillegge ”utad”?
39	Ikon som viser tid og sted med enkelt tastetrykk	Usability	
40	Forenkling av mobiltastatur (Alle taster er svar eks)	Usability	De fleste mobiltelefontastatur er for små til å betjenes av personer med problemer med (fin)motorikken.
41	Lett å bruke, Ingen bruksanvisning. En teknologi som taler enkelt	Usability	Språk?
42	Presentasjon av navn automatisk	Usability	Under videobilde?
43	Ruteplanlegger fra oppholdssted utendørs. (led meg hjem)	Mobilapplikasjon med GPS	Blir standard i toppmodeller av mobiltelefoner.
44	Karttjeneste med hvor venner og pårørende befinner seg.	Mobilapplikasjon med GPS	Se over. + nettverktjeneste.
45	Hvordan kan en hjemmepleier enklest mulig ha oversikt over pasienten når han / hun ankommer?	Åpent ideområde	Bt? Mulig å integrere inn i mobiltelefonen til pleieren?
46	Samarbeid mellom pårørende og det offentlige.	Åpent ideområde	Alarmhåndtering?

47	Jeg opplever meg alene, hvor avskåret er jeg fra omverden?	Åpent ideområde	Demensrelatert
48	Hvor mange barn har jeg igjen, voksne? Bor de i byen? Hvem hjelper meg?	Åpent ideområde	Demensrelatert
49	Gi kontinuerlig og beroligende informasjon om at hjelp finnes, mat i skapet.	Usability	Demensrelatert
50	Gi den eldre forsikring og oversikt over faktiske forhold	Usability	Demensrelatert
51	Mulighet til å få forsikring om materiell hjelp, men før den eldre (litt rotete) begynner å lure..	Usability	Demensrelatert
52	Bør begynne med dette i god tid før man blir syk.	Normativt	Demensrelatert om tekniske hjelpemidler.
53	Vite hvor personen er til enhver tid	Normativt	Demensrelatert
54	Ved alarm: stemme på mobiltelefon som sier: "Jeg tror du trenger hjelp, trykk en tast hvis jeg ikke skal ringe etter hjelp"	Alarmoverføring Mobilteknologi	Skapte debatt når utsagnet ble konkretisert til fallalarm som endte opp i følgende "Har du falt? Hjelp blir tilkalt. (pause) Hvis du ikke vil ha hjelp trykk rød knapp på mobiltelefonen." Hvor siste to setninger blir gjentatt helt til samtale blir besvart.
55	Omsorgsgiver kan fjernstyre kamera / skjerm	Alarmoverføring / tilsyn	
56	Hva skjer ved strømbrudd i huset?	Åpent ideområde	

Min evaluering av ideene:

Mange av ideene faller utenfor feltet jeg arbeider med (Alarmer overført med mobiltelefon), allikevel er mange av utsagnene og ideene nyttige. Av de mest aktuelle ideene for meg er nr. 9,38,39,40,41,54 og 55. Jeg kommer til å gå nærmere inn på disse i forslaget mitt til et system. De resterende forslagene overlater jeg til andre grupper innen grensebroen. Mange av ideene er aktuelle for klassen til Safdar og Thomas.

Kravene som framkom var disse:

	Krav	**Kategori**	**Kommentar**
1	Sikring av alle elektriske artikler, fjernstyring av belysning i underetasje fra overetasjen og vice versa.	Teknisk	
2	Lett montering av alt utstyr, ingen kabeltrekking.	Teknisk	
3	Ved alarm: Stedsangivelse på SMS og videobilde.	Teknisk	
4	Systemet må kunne fungere ved	Teknisk	

	strømbrudd.		
5	Mobilutstyret må tåle å falle i gulvet.	Teknisk	
6	Systemsikkerhet når deler av systemet svikter. For eksempel nett nede.	Teknisk	Krever flere typer nettilganger
7	Posisjonsangivelse må fungere også i eget hjem.	Teknisk	Ved bruk av IPtelefoni over internett er ikke dette selvfølgelig.
8	Krav til feilmarginer i utstyret	Teknisk	
9	Krav til overstyring av systemet i visse tilfelle. For eksempel av pårørende eller pasient.	Teknisk /etisk	Må kunne slå av systemet. (lovkrav)
10	God ventilasjon siden brukeren tilbringer nesten all tid inne	Teknisk Mobilkommunikasjon	Miljøstyring
11	Backup når pasienten / eldre svikter. Selvstendiggjøring	Hjelpemidler Personlig Data Assistanse.	Demensrelatert
12	Den teknologiske gevinsten (verdien) bør anvendes slik at personalets ressurser bedre kan utnyttes.	Institusjonell / Etisk	
13	En vaktsentral bør kunne etableres i kommunen. (Pleie og omsorgsenhet)	Institusjonell / Etisk	
14	God teknologi må ikke bli en kommunal sovepute	Institusjonell / Etisk	
15	Den eldre må kunne føle seg som et fritt menneske.	Etisk	
16	Ikke erstatte personell, men bedre arbeidssituasjonen. Også forbedre hverdagen for den eldre.	Institusjonell / Etisk	
17	Teknologiske gevinster må ikke erstatte helsepersonell og bemanning.	Institusjonell / Etisk	
18	Teknologien (tilgang og overvåkning) må ikke legge byrder på pårørende.	Pårørende / Etisk	
19	Pårørende vakt ved anrop.	Pårørende / Etisk	Pårørende tar vakt på rundgang?
20	Ikke å forvente at alle pårørende vil eller bør være tilgjengelige på (bilde) nett kommunikasjonen. Må opprettes en vaktsentral til betjening / oppfølging	Pårørende / Institusjonell / Etisk	
21	Alarmsystemet må ha backup på mottakersiden.	Institusjonell / Etisk / Teknisk	
22	Stor skjerm, store taster, fast skjerm hjemme. Forstå ved å se der og da.	Usability	Informasjonssystem og vanlig videotelefoni.
23	Stor og tydelig rulletekst på skjerm (kontinuerlig) samt dagens dato, ukedag, klokke, dag/ natt.	Usability	Informasjonssystem
24	Enkle ikoner	Usability	
25	Teknologien må ikke øke forvirring / skremme.	Usability	
26	Intuitiv bruk	Usability	
27	Stor nok skjerm	Usability / mobiltelefon	
28	Skjermen/ betjeningspanelet (fjernkontrollen) må være lette å bruke/ håndtere for stive, skjelvende hender og lesbar for øyne med nedsatt syn.	Usability	
29	Godt lys på skjermer.	Usability	Lang forsinkelse på lysreduksjon

			etter påslag.

Min evaluering av kravene:
Mange av kravene er høyst relevante. Noen av kravene (som ideene) er gjengangere i litt forskjellig drakt, men de mest aktuelle kravene for meg er nr 2,3,4,5,6,7,9,22,23,24,28 og 29. Disse kravene kommer til å bli innarbeidet i rapporten!

Normative utsagn:
Under diskusjonen kom det fram flere (generelle) normative utsagn:

- Klart, tydelig og konkret språk.
- Utvidelse av trygghetssonen, til å omfatte mer enn leiligheten.
- Det verste er falsk trygghet, det beste er reell trygghet.

Veien videre:
Jeg vil gjerne holde denne gruppen i live videre, vi har avtalt nytt møte 24. april kl. 10.30 hvor temaet blir å verifisere bearbeidelsen av de ideene jeg har blinket ut. Samt å komme med innspill til nye. Resultatet av hele prosjektet skal leveres for bedømming 29. mai og presenteres 13. juni på Høgskolen i Agder, Grimstad.

Reidar Nordby

Brukerpanelmøte 2, Innkalling

Reidar Nordby
Grensebroen / HiØ

Til deltakere i brukerpanel Valaskjold 070417

Ann Karin Helgesen	ann.k.helgesen@hiof.no
Kjersti L. Jørgensen	klab@fredrikstad.kommune.no
Marit Smittil	masm@fredrikstad.kommune.no
Safdar Abbas	saabb@online.no
Tomas Moe	tomasmoe@msn.com
Per-Thomas Huth	per.t.huth@hiof.no

Innkalling til panelmøte 2

Tid; 24. april 2007 kl $10^{\underline{30}}$. Sted: Grensebroens lokaler HiØ Sarpsborg.

Hei igjen, takk for forrige møte.

Siden sist har jeg arbeidet for å få til en beskrivelse av en mobiltelefon med alarm. Mye av arbeidet til nå har gått på selve mobiltelefonnettet og hva man kan forvente. Mye skuffende resultater til nå, fordi det viser seg at mobilnettet ikke garanterer at oppringing med videosamtaler blir gjennomført. Imidlertid så husker dere at systemet hadde to anvendelsesområder. Det ene anvendelsesområdet er en alarm som går mot privatpersoner. Dette er uproblematisk. Det andre er en alarm som går mot institusjoner. Her forlanger Helsepersonellovens § 39 at alt skal journalføres. "Forskrift om pasientjournal" § 9 forlanger at bilder skal oppbevares i journal inntil "informasjon er nedtegnet på forsvarlig måte". Dette blir litt av en nøtt fordi det innebærer at det må inn med en datasentral, og fordi det må en kryptering til i kommunikasjonen mellom mobiltelefon og datasentral.

Temaet for møte 2 er de foreløpige resultater hvor vi ser litt på hva jeg har kommet fram til, og jeg vil gjerne ha kommentarer til dette.

Det blir servert enkel lunsj og møtet forventes å være ferdig ca. kl. $13^{\underline{00}}$.

Vel møtt til et hyggelig møte.

_____
Reidar Nordby

Brukerpanelmøte 24 apr. -07

Referat skrevet 24- 25 apr. 07 rno

Frammøtte:

Ann Karin Helgesen ann.k.helgesen@hiof.no	Høgskolen i Østfold, Helsefag
Kjersti L. Jørgensen kjbjoerk@online.no	Fredrikstad kommune
Tomas Moe tomasmoe@msn.com	Høgskolen i Østfold, ingeniørfag E2
Per-Thomas Huth per.t.huth@hiof.no	Høgskolen i Østfold, ingeniørfag prosjektleder grensebroen
Reidar Nordby reidar.nordby@hiof.no	Høgskolen i Østfold, ingeniørfag masterkandidat HiA

Møtets formål var å presentere oppgaven så langt og å diskutere rundt mottaksordninger for alarmer, dessuten verifisere konseptet rundt mobiltelefon som alarmbefordrer.
Møtet åpnet med at vi inntok smørbrød mens Reidar gjennomgikk status og arbeidet så langt. Status dannet grunnlaget for en løs diskusjon rundt prosjektet.

Den etterfølgende diskusjonen avdekket følgende momenter:
Fallsensor: Hvordan feste den, kan det være et smykke?
Produktidé: Armbånd med tydelig (analog) klokke, høyttaler, mikrofon og kamera.
Panelet uttrykte bekymring for at eldre kan være skeptisk til å ikle seg utstyr de ikke fra før har forhold til. God design er derfor en nøkkelfaktor. Også glemsomhet ble nevnt i denne sammenheng.

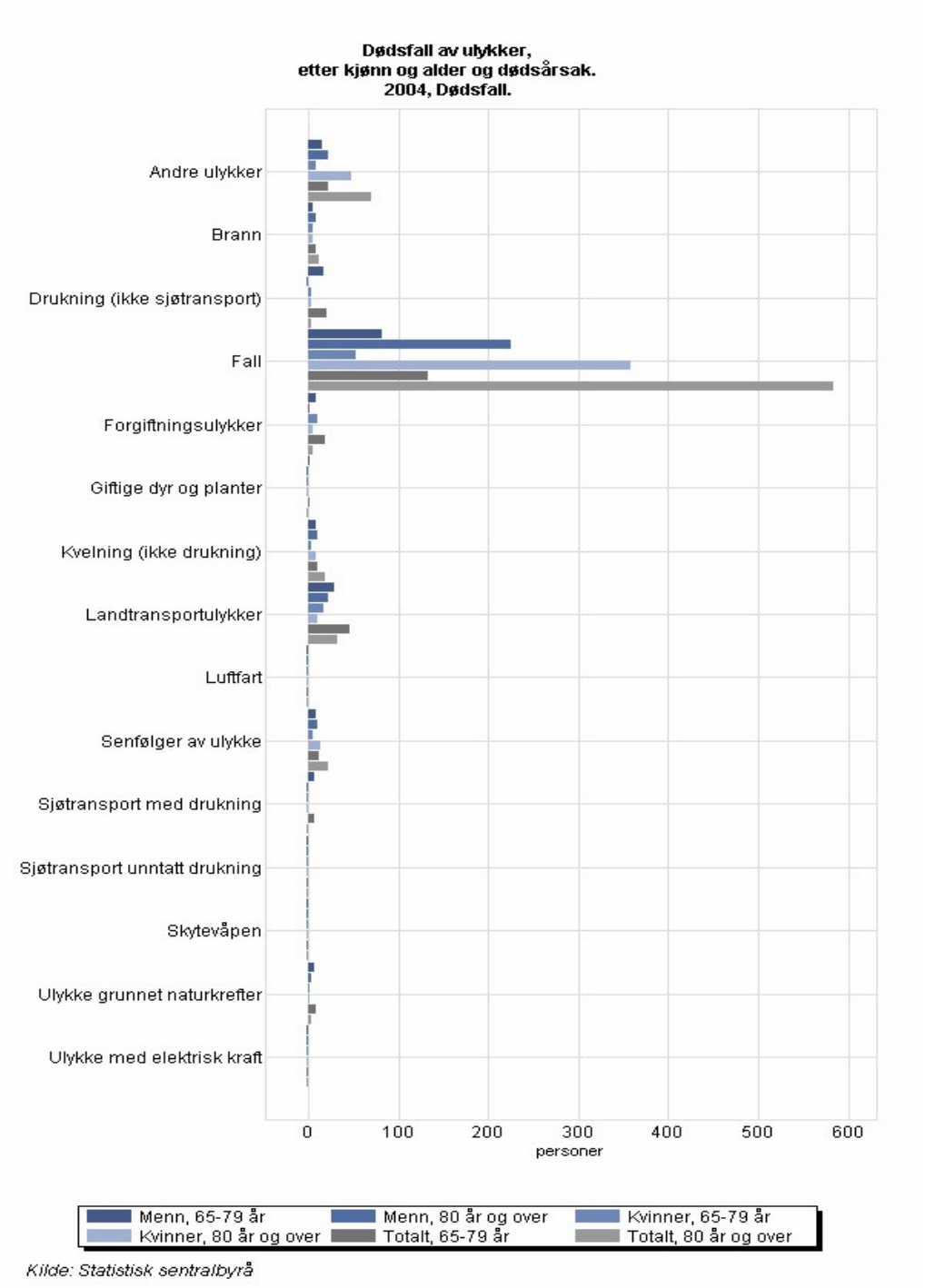
Følgende spørsmål ble stilt panelet:

- Hva bør være en rimelig rutine for journalføring?
- Hvem bør være alarmmottakere?
- Hvilke funksjoner bør finnes i alarmmottak?
- Hvilken type utstyr forventes?

Samsvar mellom journalføring i prosjekt og praksis ble oppfattet som lik.
Panelet påpekte at systemet må sees i helhet for å bli tatt i bruk. Isolert betyr systemet en merutgift dersom det skal integreres i kommunale tilbud. Vaktselskaper og private aktører ble diskutert som alarmmottakere. Av utstyr som ble forventet ble dette påpekt som avhengig av mottakets størrelse. For kommunale mottak vil en mobiltelefon med mulighet for journalføring være tilstrekkelig.

Reidar Nordby

Dødsfall av ulykker.



Grafikk produsert av Statistisk sentralbyrå via [75]

Forespørsel Telenor mobil

Reidar Nordby
Høgskolen i Østfold
Ingeniørfag
1757 Halden

2007-03-26

Telenor kundeservice
PB216 Sentrum
3701 Skien

Hei. Jeg er en ansatt ved høgskolen i Østfold som tar videreutdanning (mastergrad) innen mobilkommunikasjon ved Høgskolen i Agder. Jeg har nå kommet såpass langt at jeg skriver hovedoppgave. Oppgaven min har som ordlyd: "Mobilteknologi til videokommunikasjon ved trygghetsalarmer." Oppgaven som sådan er gitt av Interreg IIIA prosjektet Grensebroen Arena, som har deltakere fra næringsliv, kommuner og akademia i Østfold – Fyrbodal. . Grensebroen Arena har et prosjekt de kaller "Ett år lengre hjemme", som henspeiler på personer som ønsker å forlenge botiden i egen bolig inn i alderdommen. Om Grensebroen se www.grensebroen.com og www.grensebroen.com/arena.html
Prosjektet går ut på å undersøke mulighetene for å benytte videokommunikasjon i forbindelse med mobile alarmer (eg. fallalarmer) for å kommunisere med eldre etter ulykker. Dersom brukeren er ved bevissthet og klarer å snakke i telefonen, kan det gis noen beroligende ord, er brukeren i stand til å betjene telefonen kan hjelperen via videobilder få et overblikk over situasjonen. I denne forbindelsen er det noen punkter som er sentrale og som jeg trenger hjelp til.

- Kjenner Telenor Mobil til at det i dag i noen sammenheng finnes applikasjon for video-kommunikasjon (en vei) over GPRS?
- Tilbyr Telenor Mobil i dag i noen sammenheng (applikasjon) videokommunikasjon (toveis) over EDGE/GPRS?
- Hva er i tilfellet QoS profilen til tjenestene?
- Hva er priser på slike oppsett?
- Deres videotelefonitjeneste over UMTS er kjent, men hva er avvisningsraten, og har Telenor noen planer om å innføre QoS (UMTS Release 4) i nær framtid?

Et av hovedspørsmålene oppgaven reiser er om mobiltelfonnettet er egnet til videoalarmformål. I så tilfelle: Har Telenor mobil muligheter til å utøke sikkerheten i EDGE/GPRS for eksempel ved faste IP-adresser? Jeg setter umåtelig pris på å få høre fra Dem. Skriftlig eller muntlig, gjerne via email.

Med vennlig hilsen

_____

Reidar Nordby
Student / Avdelingsingeniør
Email: reidar.nordby@hiof.no
Mobiltelefon 905 30 571