Anvendelsesområder og sikkerhetsløsninger for RFID-teknologi i helsesektoren

av

Christian Frederik Skinnes
Walter Sørvik

Hovedoppgave til mastergraden i informasjons- og kommunikasjonsteknologi

Høgskolen i Agder
Fakultet for teknologi
Grimstad, mai 2004

Sammendrag

Radio Frequency Identification (RFID) er en teknologi som inneholder mange muligheter, spesielt i sammenheng med annen mobil kommunikasjonsteknologi. Ved Sørlandet Sykehus HF i Arendal ønskes en økt identitetssikring og kvalitetskontroll på prøver som blir analysert ved laboratoriet. Det har derfor vært ønskelig å se på hvordan RFID-teknologien kan benyttes i sammenheng med rutiner for prøvetaking, og hvilke begrensninger og muligheter som ligger i lagring av sensitiv informasjon i RFID-brikker.

På bakgrunn av observasjoner, intervjuer og oppfølgingsmøter med nøkkelpersoner ved sykehuset har det vært mulig å se hvordan RFID kan benyttes på en best mulig måte i forbindelse med prøvetaking. Metoden Contextual Design er godt egnet til å lage en god systemløsning for laboratoriet. Gjennom en enkel demonstrator visualiseres prinsippet for merking av pasienter og prøver med RFID-brikker, og hvordan en digital identitet kan knyttes til prøver. Demonstratoren dannet et grunnlag for en brukerevaluering fra de ansatte ved laboratoriet.

Gjennom en brukerundersøkelse kom det frem at de ansatte ved laboratoriet er positive til en slik type teknologi, og mener den vil gi en økt kvalitetssikring under prøvetaking. Det er også stor enighet om at noe bør gjøres med dagens rutiner. TAM (Technology Acceptance Model) sier at *oppfattet nytteverdi* og *oppfattet enkelhet ved bruk* virker inn på holdninger til systemet, og til slutt bruk av systemet. Med støtte i denne modellen kan vi anta at et system for merking av prøver og pasienter, basert på RFID vil kunne bli tatt godt imot av de ansatte ved laboratoriet. Det forutsettes at komponenter og brukergrensesnitt er godt tilpasset målgruppen.

Informasjon som behandles i forbindelse med prøver og prøveresultater er å betrakte som sensitiv dersom den kan knyttes opp mot en bestemt person. Hvis en RFID-brikke skal brukes som informasjonsbærer av sensitive data, stilles det strenge krav til overføring og autentisering. Det finnes kun noen få typer brikker på markedet i dag som har innebygd funksjonalitet for god nok kryptering og autentisering. For å redusere kompleksitet på både overføring og brikke, kan en god løsning være å overføre et identifikasjonsnummer til brikken, for så å hente de sensitive dataene ut fra en database ved hjelp av en PDA og trådløst nett. Kun informasjon som kan være nyttig for effektiv logistikk trenger å bli lagret i brikken.

Resultater og tilbakemeldinger under arbeidet med oppgaven peker på at det ligger et stort potensial for å utvide et slikt identifikasjonssystem til også å gjelde legekontorer ute i distriktene som sender prøver inn til sykehuset for analyse. Dette forutsetter selvfølgelig at sykehuset innfører systemet først, og at legekontorene er koblet opp mot laboratoriesystemet som blir benyttet ved sykehuset.

Forord

Denne rapporten er skrevet som en avsluttende del av masterutdanningen innen informasjons- og kommunikasjonsteknologi (IKT) ved Høgskolen i Agder, avdeling for teknologi i Grimstad. Arbeidet har pågått fra januar til mai 2004 og teller 30 studiepoeng.

Gjennom oppgaven har vi hatt et godt samarbeid med laboratorieavdelingen ved Sørlandet Sykehus i Arendal. Vi vil derfor få lov å takke alle som har hjulpet oss. En spesiell takk går til Beth Dahl-Paulsen og Karin Bergland ved laboratorieavdelingen. I tillegg vil vi takke vår veileder Førstelektor Rune Fensli ved HiA for råd og hjelp underveis.

Grimstad, 1. juni 2004

Christian Frederik Skinnes

Walter Sørvik

Innholdsfortegnelse

Figurliste

Tabelliste

1. Innledning

1.1. Oppgavedefinisjon

RFID-teknologien inneholder mange muligheter for lagring av informasjon om objekter, og kan blant annet benyttes for effektiv logistikk. Det er ønskelig å vurdere hvorledes denne teknologien kan anvendes innenfor helsevesenet for å oppnå en øket kvalitetssikring og mulig effektivisering.

En skal forsøke å finne mulig anvendelse av RFID-teknologien sett i sammenheng med muligheter for mobilitet ved hjelp av trådløs kommunikasjon. For å visualisere teknologiens muligheter, er det ønskelig å lage en enkel demonstrator som gjennom en brukerevaluering kan danne grunnlag for en fremtidig teknologiløsning.

I forhold til lagring av sensitiv informasjon stilles det strenge krav til teknologien og anvendelsen av den. Det er ønskelig å analysere hvilke begrensninger som eksisterer i forhold til lagring av sensitiv informasjon, med sikte på å finne frem til egnede anvendelsesområder og hvor det kan implementeres aktuelle sikkerhetstiltak. En skal se nærmere på de sikkerhetsmessige krav som stilles, og finne frem til egnede løsninger for sikker autentisering og integritet i meldingsutveksling. Ut i fra dette skal en foreslå aktuell teknologi/programvare som kan benyttes for bruk av håndholdte terminaler og sikker meldingsutveksling, og hvor RFID-brikker kan benyttes som informasjonsbærer.

1.2. Bakgrunn for oppgaven

Opprinnelig var oppgaven tenkt som en del av et større forskningsprosjekt som ble planlagt sammen med Telenor FoU, Tell IT Solutions, Applica og Høgskolen i Agder. Dette prosjektet ble det imidlertid ingenting av. Derfor ble vår oppgave gjennomført gjennom et godt samarbeid mellom Høgskolen i Agder og Sørlandets Sykehus HF i Arendal.

Høsten 2003 ble det gjennomført et prosjekt i forbindelse med faget IKT 4200 Koordineringsteknologi ved HIA, som gikk på det samme tema i samarbeid med Sørlandets Sykehus. Vi vil i vår oppgave gå en del dypere inn i problemstillingen og se på mer helhetlige løsninger hvor vi også tar opp problemstillinger rundt sikkerhet.

Sykehuset bruker i dag et relativt gammelt system for merking og identitetskontroll av pasienter og blodprøver ved sykehuset. Dette systemet er i dag basert på strekkoder og skjemaer som leses maskinelt. I tillegg benytter sykehuset et forholdsvis nytt datasystem for elektroniske pasientjournaler som kalles DIPS. Ved laboratoriet brukes et datasystem som kalles Uni-Lab som er betraktelig eldre enn DIPS. Dette systemet tar seg av merking av prøver og behandling av prøveresultater. I DIPS er det mulig å hente all informasjon om en pasient. Det er også mulig å rekvirere prøver elektronisk. Kommunikasjonen mellom DIPS og Uni-Lab skjer ved hjelp av en såkalt *Lab-pumpe* som hele tiden oppdaterer og sender over informasjon.

Dagens rutiner er slik at flere trinn i prøvetakingsprosessen blir gjort manuelt. Ved alle manuelle rutiner er det muligheter for at menneskelige feil kan oppstå. Dette er noe de ansatte er klar over, men de fleste feil er ikke lett å oppdage. De ønsker derfor en økt kvalitetssikring. Merkingen av prøveglassene er basert på strekkoder, og vi ønsker å se på hvordan ny teknologi kan brukes til økning av kvalitetssikring og eventuell effektivisering av arbeidsflyten ved prøvetaking. Den trådløse teknologien som kalles Radio Frequency Identification (RFID) er en teknologi som kan være egnet til å

identifisere og merke pasienter og prøver ved et sykehus. Ved å se på denne teknologiens funksjonalitet og muligheter opp mot hvilke behov sykehuset har, kan vi forsøke å se om RFID kan bidra til å redusere risikoen for feil, samt bidra til effektivisering ved sykehuset.

I oppgaven har vi valgt ulike metodeteorier som grunnlag for får vår forskningsstudie. Vi har ved hjelp av disse teoriene forsøkt å kartlegge, på en best mulig måte hvordan vi kan tilpasse teknologien slik brukeren ønsker det. I tillegg til dette har vi forsøkt å få frem muligheter som ligger i teknologien og hvilket potensial dette eventuelt kan ha i sykehussammenheng.

1.3. Begrensninger

Hovedmålet med oppgaven er å belyse de mulighetene vi mener RFID-teknologien har innen for helsesektoren. Siden helsesektoren er stor har vi gjort visse begrensninger når det gjelder hvilke områder vi vil se på. Vi har i begrenset oss til å se på prøvetaking ved sykehuset og fokusert på rutiner og prosesser som skjer i forbindelse med prøvetaking av inneliggende pasienter ved Sørlandets Sykehus HF i Arendal. Det finnes høye krav til sikkerhet når det gjelder behandling av sensitive personopplysninger. Vi har derfor sett på sikkerheten som må implementeres når det gjelder RFID-teknologien og utveksling av sensitiv informasjon over trådløst nett. I oppgaven har vi valgt å fokusere på kommunikasjonen mellom håndholdt enhet og RFID-brikken. For å kunne billedgjøre mulighetene som ligger i teknologien og sette den i sammenheng med rutinene ved sykehuset, har vi valgt å lage en enkel demonstrator. Denne har bare til hensikt å vise prinsippet og gjennom en demonstrasjon ved sykehuset gi oss tilbakemeldinger fra de ansatte. Derfor har vi ikke lagt vekt på sikkerhet i demonstratoren, men heller tatt for oss sikkerhet teoretisk i rapporten.

2. RFID teknologi og anvendelsesområder

2.1. Historikk rundt RFID teknologien

Strekkoder som også blir omtalt som barkoder, revolusjonerte i sin tid måten å identifisere varer på. Teknologien var veldig enkel, strekkodene var enkelt å implementere i varer og i tillegg var systemet ekstremt billig. Men strekkoden har likevel sin begrensning i at den bare har mulighet til å "lagre" en begrenset mengde data og at informasjonen ikke kan endres. Teknologene så da en løsning i å kunne benytte silikonbrikker som lagringsenhet. Kort som er basert på et kontaktfelt, slik som telefonkort eller SIM-kort i mobiltelefoner, er eksepler på denne typen løsninger. Likevel er behovet for fysisk kontakt ofte upraktisk i noen sammenhenger, og teknologene ønsket derfor å finne en løsning der dataoverføringen kunne skje trådløst for å gjøre det mer fleksibelt. Dermed ble kontaktløse identifikasjonssystemer utviklet og som vi i dag kaller for RFID-systemer (Radio Frequency Identification) [6].

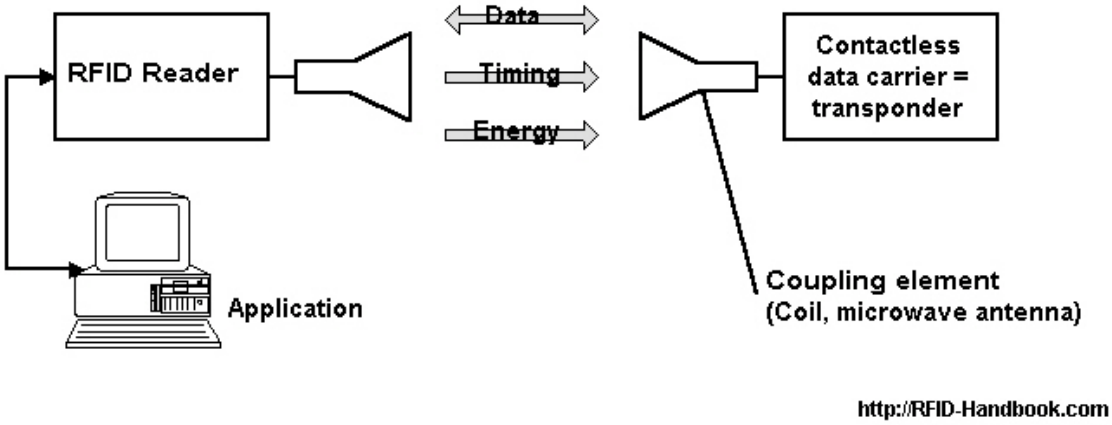
Selv om RFID-teknologien er i vinden i disse dager er denne teknologien på ingen måte noen ny teknologi. Etter at radar ble funnet opp på 1920-tallet begynte man å leke med tanken om å få noe til å svare på radiosignaler automatisk. I 1948 skrev Harry Stockman et paper med tittelen *"Communication by Means of Reflected Power"*, noe som var starten på utviklingen av RFID-teknologien. Men det skulle ta nærmere 30 år før det virkelig ble fart i RFID-teknologien. Først da hadde man funnet opp transistorer, integrerte kretser og mikroprosessorer. På 1960- og 1970-tallet ble det eksperimentert mye, men det var først på 1980-tallet at RFID-teknologien virkelig skjøt fart. Da ble det tatt i bruk RFID-brikker i forbindelse med bomstasjoner, adgangskontroll, heiskort i alpinbakker, og sporing av dyr. Det var mest i Europa at teknologien ble tatt i bruk, men på 1990-tallet ble det mer utbredt også i USA [4]. I dag kan en se at RFID-teknologien blir tatt i bruk i stadig flere sammenhenger**.**

I dag har det blitt satt en del standarder RFID-systemer, og RFID-teknologien er spådd en god fremtid i mange medier. I kombinasjon med annen trådløs teknologi kan nye muligheter åpnes for RFID-teknologien, og den kan brukes i nye sammenhenger.

2.2. Ulike typer RFID systemer

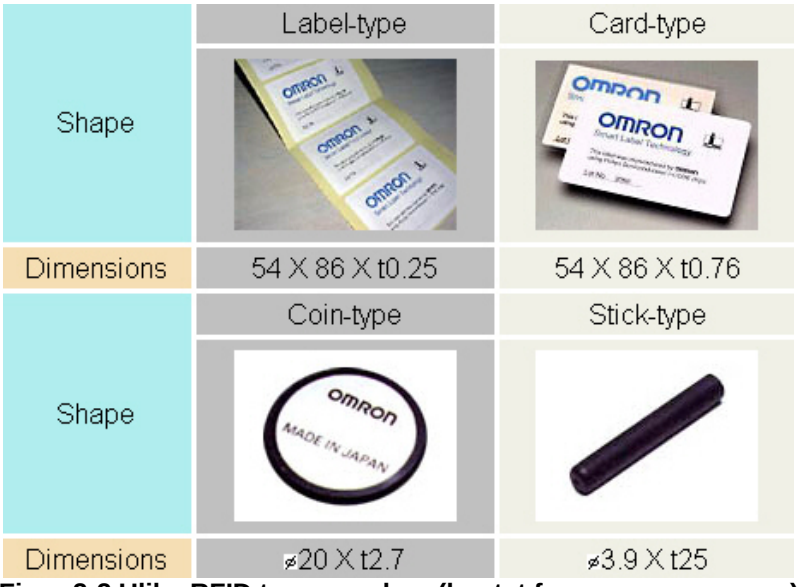
RFID-systemer finnes i mange ulike typer og fasonger. For å få en bedre oversikt over de ulike systemene som eksisterer, tar vi for oss de ulike utformingene og bruksområdene som finnes i dette avsnittet. Dette for å finne ut hvilke komponenter som er best egnet i vårt tilfelle. Kapittel 1 og 2 i *RFID Handbook* [6] er brukt som kilde.

Det finnes forskjellige typer frekvenser og rekkevidder på de ulike systemene, noe vi skal komme tilbake til senere. Felles for alle systemer er at det er en leser i den ene enden av systemet, og en transponder i den andre enden. Dette er hovedkomponentene som finnes i et RFID-system, se Figur 2-1. Transponderen er trådløs og har enten en liten strømkilde, eller mottar nok energi fra leseren til at den kan sende svar uten å ha en egen strømkilde. Hvor mye data som kan lagres i transponderen varierer mellom de ulike komponentene.



Figur 2-1 Hovedkomponenter i et RFID system [6]

Konstruksjon og utforming av transponderen er vanligvis tilpasset bruksområdet systemet er tenkt å benyttes i. Transponderen kan fåes innkapslet i plastikk eller glass, utformet som små skiver eller plater. Transpondere innkapslet i glass blir ofte operert inn under huden på dyr slik at man kan identifisere dem. Det finnes også noe større plastbrikker som inneholder transpondere. Bomringer bruker brikker av denne typen. Også transpondere som er bygget inn i bilnøkler har denne utformingen. Størrelsen på brikkene kan variere avhengig av hvor avanserte de er, eller hvilke krav som trengs til innkapsling. Noen transpondere er spesiallaget for adgangskontroll og er utformet som nøkkelringer eller integrert i klokker. Et format som en mye brukt er såkalte kontaktløse Smartkort. Disse har samme form som et minibankkort og inneholder en transponder. Et format som kan være aktuelt å bruke innen helsesektoren, er såkalte *smart labels*. Dette er transpondere som er lagt på en tynn plastikkfolie som ikke er tykkere enn 0,1 millimeter. De er ofte laminert på et papirstykke og kan festes på ulike steder.
Figur 2-2 viser fire forskjellige typer transpondere levert av Omron.

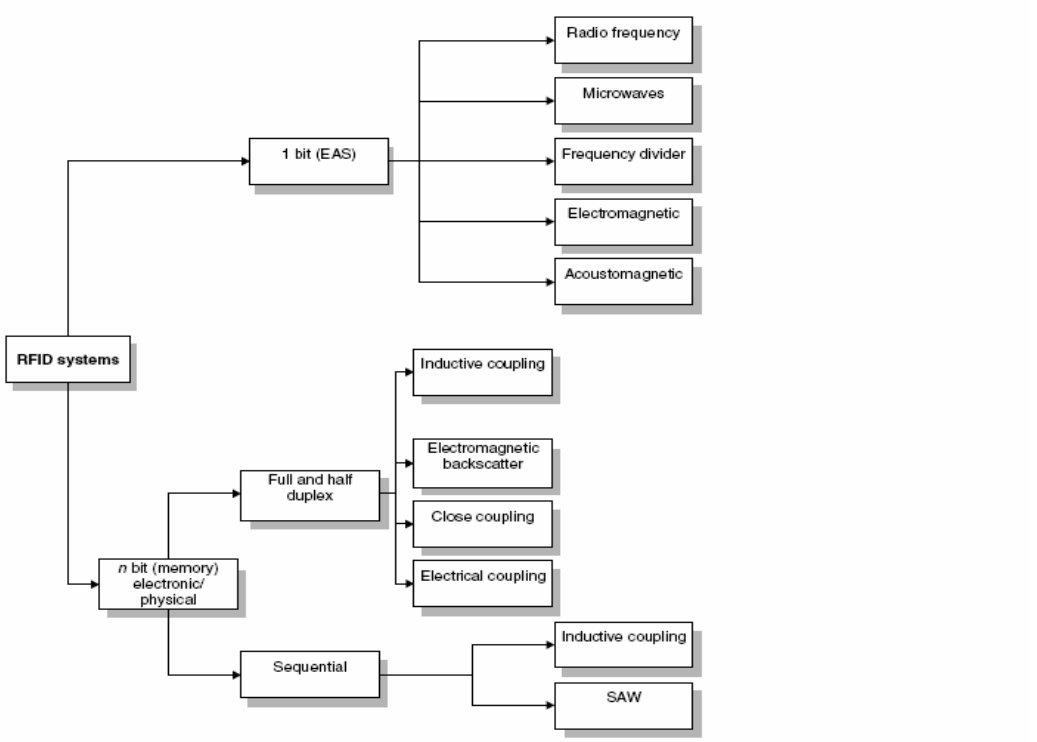


Figur 2-2 Ulike RFID transpondere (hentet fra www.omron.com)

2.3. Virkemåten til RFID

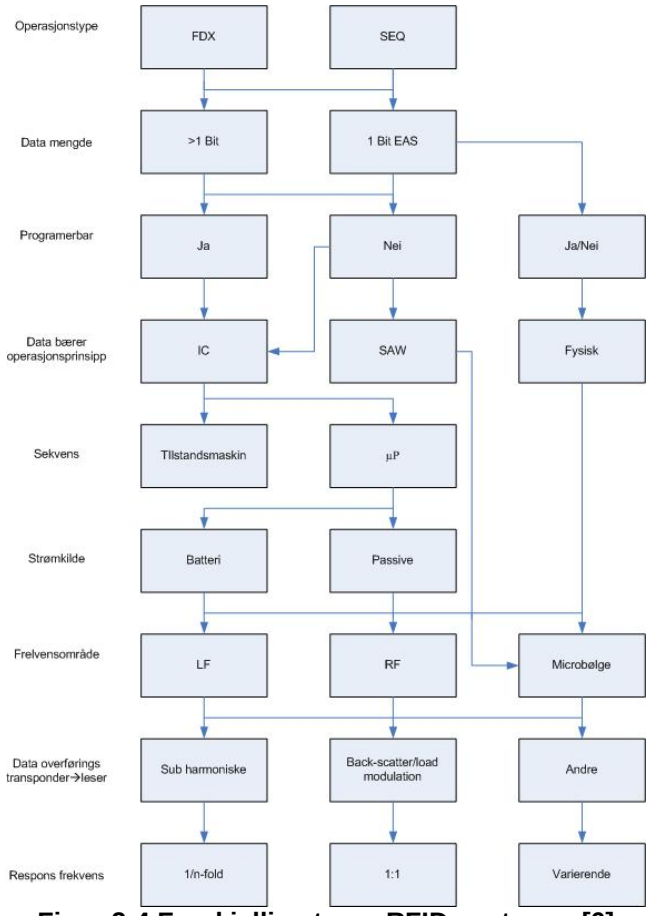
For å få finne frem til en god løsning for vårt system har vi valgt å gi en grundere oversikt over virkemåte og egenskaper til de ulike systemene som finnes. Som kilde i hele kapittel 2.3 har vi brukt *RFID handbook* [6].

RFID-systemer eksiterer i som nevnt i utallige formater, og produsert på mange ulike måter. Figur 2-3 viser en oversikt over de forskjellige operasjonsmåtene innen RFID-systemer.



Figur 2-3 Skjema over de forskjellige opperasjonsprinsippene i RFID systemer [6].

RFID-systemene kan grovt deles opp i to hovedgrupper etter hvorvidt de har lagringskapasitet eller ikke. 1-bits systemer er enkle, men har likevel ulike operasjonsprinsipper, som vi har valgt å ikke komme nærmere inn på i første omgang. Av RFID-systemene som har lagringskapasitet, er det to grunnleggende prinsipper som finnes. Disse er full dupleks (FDX) / halv dupleks (HDX) eller sekvensielle systemer (SEQ). Som en kan se ut av Figur 2-3, opererer også både FDX-/HDX- og SEQ-systemene med ulike prinsipper. Dette gjør at RFID-systemene har flere ulike egenskaper og kan derfor implementeres i mange ulike sammenhenger. Vi skal ta for oss dette nærmere senere i kapittelet. Egenskapene til de forskjellige typene kan også beskrives ved hjelp av oversikten i Figur 2-4.



Figur 2-4 Forskjellige typer RFID-systemer [6]

Ut fra Figur 2-4 over kan en se at det både innenfor FDX- og SEQ-systemene, eksisterer forskjellige kombinasjoner av egenskaper som de ulike RFID-systemene har.

2.3.1. Ulike RFID-systemer

Full dupleks- og halv dupleks-systemer

Kommunikasjonsprosedyrene til FDX-, HDX- og SEQ-systemene betegner hvordan transponderen kommuniserer med RFID-leseren. I motsetning til 1-bits transpondere benytter FDX og HDX transpondere en elektronisk mikrobrikke som databærer. Denne kan bære data opptil flere kilobits. For å kunne lese eller skrive data til databæreren, må det være mulig å overføre data mellom leseren og transponderen. Sendereffekten fra leseren er mye sterkere enn fra transponderen og det er derfor innført bestemte kommunikasjonsprosedyrer.

Kommunikasjonsprosedyren i HDX-systemet, sender og mottar informasjon annen hver gang mellom leser og transponder. HDX-transponderne opererer med en frekvens som ligger under 30 MHz. HDX-systemene er ikke like utbredt som FDX-systemene, og benyttes mest i transpondere som brukes til dyremerking.

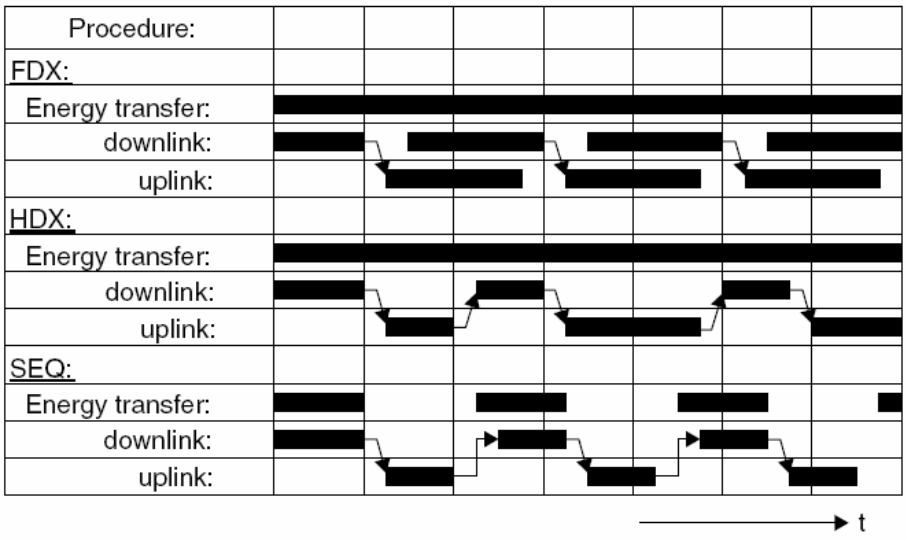
Kommunikasjonsprosedyren i FDX-systemet fungerer slik at dataoverføringen fra transponderen til leseren skjer samtidig som dataoverføringen fra leseren til transponderen. Frekvensområdet som blir benyttet i FDX-systemene ligger under 30 MHz. Dette er i dag den mest utbredte kommunikasjonsformen blant RFID-systemer, og er også det systemet som blir brukt i *smart label* transpondere.

Sekvensielle systemer

I SEQ-systemer blir utelukkende frekvenser under 135 kHz brukt. På tilsvarende måte som i HDX- og FDX-systemer, benytter SEQ-systemer seg av den induktive spenningen som blir generert i transponderspolen. Denne spenningen blir generert ved hjelp av det vekslende magnetiske feltet leseren genererer, og brukes til strømforsyning for mikrobrikken i transponderen. For å kunne få en så effektiv dataoverføring som mulig, må frekvensen til transponderen og leseren være helt lik. Transponderen har derfor i tillegg en *on-chip trimming* kondensator for å sikre at frekvensen blir korrekt. I tillegg har ikke sekvensielle systemer en kontinuerlig energioverføring, i motsetning til HDX og FDX systemer.

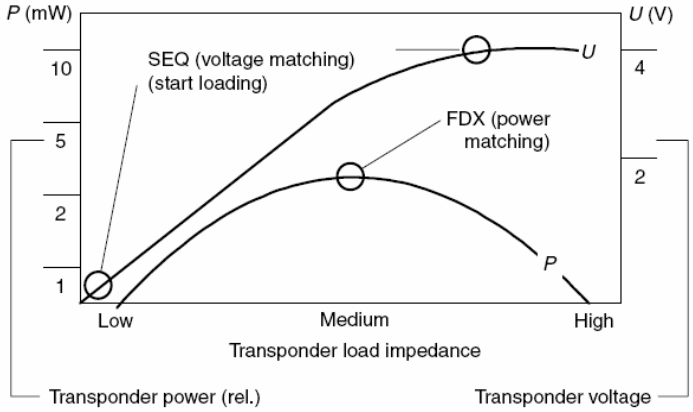
Sammenligning av full /halv dupleks og sekvensielle systemer

I FDX/HDX skjer energioverføringen kontinuerlig og er uavhengig av datastrømmen, se Figur 2-5. Dataoverføring fra leseren til transponderen er betegnet som downlink, mens data fra leseren til transponderen er betegnet som uplink. Innenfor de forskjellige kommunikasjonsformene eksiterer det både passive og aktive transpondere.



Figur 2-5 Energi- og datautveksling i FDX-, HDX- og SEQ-systemer over tid. [6]

En videre sammenligning viser at kommunikasjonsprosedyren i SEQ-systemer innebærer at leseren blir slått av i korte intervaller, i motsetning til FDX- / HDX-systemer. Intervallene der leseren er av, blir registrert av transponderen og blir brukt til å sende data fra transponderen til leseren. Ulempen med den sekvensielle prosedyren er effekttapet til transponderen i løpet av den tiden leseren ikke sender. Dette må bli jevnet ut ved at transponderen innehar en tilleggsenergikilde som for eksempel kan være en kondensator for de passive transponderne eller et batteri for de aktive transponderne. Figur 2-6 illustrerer en sammenligning av transponderens effekt og spenning i FDX- / HDX-systemer og SEQ-systemer.



Figur 2-6 Transponderens effekt og spenning i ulike systemer [6]

I FDX-systemer er effektoverføringen fra leseren til transponderen kontinuerlig og data overføres i begge retningene samtidig. Mikrobrikken i transponderen kan derfor være i operasjonsmodus kontinuerlig. Det er ønskelig å få en så optimalisert energioverføring som mulig. Dette oppnås ved *power matching.* Av Figur 2-6 kan en se at *power matching* inntreffer i FDX-systemene når impedansen på transponderen er middels og effekten er på ca. 2 mW. Ut fra Figur 2-6 kan vi se at maksimal spenning i FDX-systemer er halvparten av hva den er i SEQ-systemer. Den eneste muligheten for å øke spenningen som er til rådighet, er å øke inngangsimpedansen på mikrobrikken. Dette tilsvarer det samme som å redusere effektforbruket. Derfor er det alltid et kompromiss mellom effektforbruk og spenningsforbruk i FDX systemer.

SEQ-systemer fungerer på en annen måte. I oppladningsprosessen er mikrobrikken enten i *stand-by* modus eller i *power-saving* modus, noe som betyr at mikrobrikken har tilnærmet null effektforbruk. Figur 2-6 viser at oppladningskondensatoren i SEQ-systemer er fullstendig utladet når oppladningsprosessen starter, og vil derfor representere en lav motstand for spenningskilden. På dette stadiet vil hele strømforbruket gå til å lade opp kondensatoren. Når kondensatoren begynner å bli fulladet, vil ladestrømmen eksponentielt gå mot null og senderen i leseren blir slått av. Energien som blir lagret i kondensatoren blir bruk til å sende svarmelding til leseren fra transponderen.

Fordelene med SEQ-systemer, er at hele spenningskilden er tilgjengelig for å kunne drifte mikrobrikken. Derfor kan spenningen være dobbelt så høy sammenlignet med FDX- / HDX-systemer. Energien i SEQ-systemer er bestemt av kapasiteten til oppladingskondensatoren og oppladingsperioden, men teoretisk kan begge verdiene bestemmes ut fra det som er nødvendig. Til tross for SEQ-systemer sine fordeler vil ikke FDX- / HDX-systemer være avhengige av ekstra energikilde.

ISO Standarder

Det er også innenfor RFID-teknologien utarbeidet flere standarder. International Organization for Standardization har blant annet utarbeidet ISO-15693 standarden, som flere av produsentene av transpondere forholder seg til. ISO-15693 standarden er delt inn i tre hovedområder [36]**.** ISO-15693-1 (Beskriver den fysiske karakteristikken), ISO-15693-2 (Radiofrekvens effekt og signalgrensenittet), ISO-15693.3 (Anti-kollisjon og overføringsprotokoller). Hver delstandard angir spesifikke retningslinjer for funksjonalitet i RFID-systemer.

Frekvenser

Et annet viktig moment som karakteriserer RFID-systemene, er de forskjellige frekvensene de ulike RFID-systemene opererer med. Ved å benytte ulike frekvensområder oppnår enn at RFID-systemene kan ha ulike egenskaper. Det er i hovedsak tre basiske båndområder som blir brukt.

- LF (Low frequency, 30-300kHz),
- HF (High frequency) / RF radio frequency (3-30 MHz)
- UHF(Ultra high frequency. 300MHz-3GHz) / mikrobølge (>3GHz).

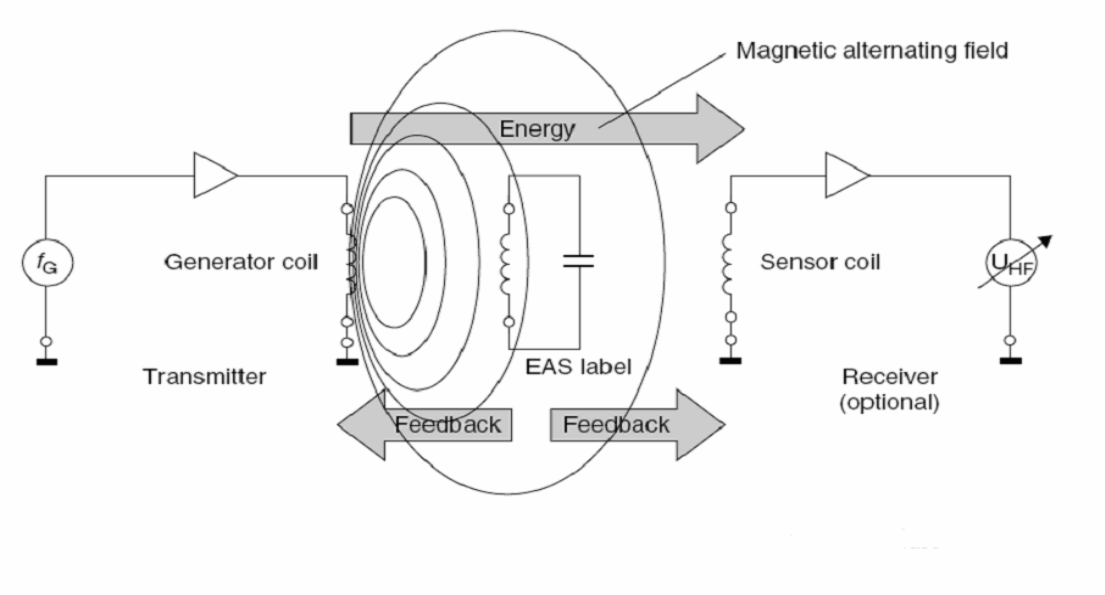
De ulike frekvensområdene har stor forskjell i lese- og skriveavstand mellom RFID-leser og transponder. RFID-systemer som opererer med en kort rekkevidde som typisk er opptil 1 cm, benytter seg av frekvensområder opptil 30 MHz. Slike systemer blir ofte brukt i tilfeller der en ikke trenger lang leseavstand. Dette kan for eksempel være såkalte *close coupling smart cards*. Dersom det er behov for en lengre leseavstand kan det benyttes HF RFID-systemer, med for eksempel 13,56 MHz som bærefrekvens. Såkalte *smart labels* benytter vanligvis denne frekvensen.

I RFID-systemer som opererer med en lengre transmisjonsavstand enn 1 m, benytter seg av frekvenser i UHF- og mikrobølgeområdet. Disse systemene er også kjent som backscatter-systemer. I avstander på opptil 3 m kan en benytte passive backscatter transpondere, men ved lengre avtander må transponderne ha en egen energikilde i form av et batteri.

2.3.2. RFID-transpondere

1-Bits transpondere

1-bits transpondere har en enkel utforming. Som navnet tilsier, består datamengden bare av 1-bit og har ingen tilhørende elektronisk lagringsenhet. Dette er likevel tilstrekkelig til å gi RFID-leseren muligheten til å registrere om en transponder er innen rekkevidde eller ikke. På grunn av den enkle oppbygningen, kan transponderen gjøres spesielt liten. Dette er egenskaper som gjør den spesielt egnet til å benyttes i blant annet tyverisikring av varer i butikker, ofte omtalt som EAS (Electronic Article Surveillance). Det vil være plassert en sender og mottaker på hver side av utgangen på butikken, og hver vare har en RFID-transponder. Skulle en vare med en RFID-transponder komme mellom sender og mottaker, vil dette bli registrert slik Figur 2-7 viser.



Figur 2-7 Operasjonsprinsipp av EAS radiofrekvenssystemet [6]

Når RFID-transponderen kommer innenfor det magnetiske feltet laget av generatoren i RFID-senderen, vil energien fra feltet bli indusert i resonanskretsen i transponderen (Faradays lov). Hvis frekvensen i det alternerende feltet korresponderer med resonansfrekvensen i transponderen, vil dette føre til en *sympathetic oscillation.* Dette betyr at det skapes en interferens mellom signalene, og det oppstår en forsterkning av det opprinnelige signalet. Dette fordi signalet både har lik fase og frekvens. Effekten av dette resulterer i en liten svekkelse i styrken av det magnetiske feltet, og det vil oppstå et spenningsfall i RFID-sensoren. Dette viser at en transponder er i området, og tyverialarmen vil bli utløst. For at ikke tyverialarmen skal bli utløst hver gang en vare med en RFID-transponder kommer forbi, må RFID-transponderen bli deaktivert slik at den ikke påvirker det magnetiske feltet. Dette gjøres ved RFID-transponderen blir ført over et sterkt magnetisk felt, slik at kondensatoren i transponderen blir ødelagt. Transponderen vil ikke lenger være i stand til å påvike det magnetiske feltet. Siden 1-bits-transpondere har en enkel arkitektur vil de være lite egnet til merking av pasienter og prøver.

Datakapasitet

I skrivbare transpondere kan leseren sende data til transponderen og for eksempel gi den en identitet som brukeren bestemmer i tillegg til det unike serienummeret. Det er tre ulike prosedyrer som blir brukt for å lagre data på transponderen:

- Ved induktiv koblede RFID-systemer er EEPROM (Electrically Erasable Programmable Read-Only Memory) dominerende som minnetype. Ulempen med denne typen minne, er at den bruker forholdsvis mye effekt i skriveprosessen. I tillegg er også overskriving av data begrenset noe begrenset (100 000 til 1 000 000 ganger). EEPROM minneteknologi er mest utbredt blant transpondere av typen *smart lables*.
- FRAM (Ferromagnetiv Random Access Memory) er en minnetype som den i senere tid har blitt brukt i enkelte tilfeller. Effekten den bruker ved lesemodus er ca 100 ganger lavere enn ved systemer som benytter seg av EEPROM. I skrivemodus er den ca 1000 ganger lavere. Utviklingen av FRAM-teknologien har fortsatt ikke slått helt igjennom. FRAM minneteknologi er derfor ikke så utbredt og er bare i liten grad brukt i noen få systemer.
- Systemer som benytter seg av frekvenser i mikrobølgelaget (> 3 GHz), bruker SRAM(Static Random Access Memory) minneteknologi for å lagre data. Dette gjør det

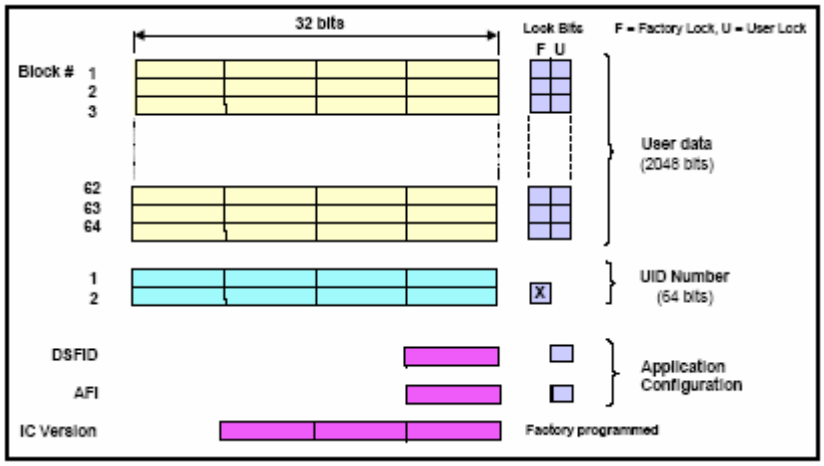
lettere å gjennomføre raske skriveprosesser. I disse systemene kreves det en ekstern strømkilde for å kunne lagre data over lengre tid. Det betyr at transpondere trenger en egen energikilde i form av et batteri, og kan dermed brukes i RFID-systemer som har lenger rekkevidde.

I programmerbare systemer må skrive- og lesetilgangen til minnet bli styrt av databærerens interne logikk. I eldre systemer kan dette være fra en til flere tilstandsmaskiner. Ulempen med tilstandsmaskiner er at de ikke lar seg omprogrammere. Dette fordi det vil være nødvendig å endre kretsen i silikonbrikken. Bruken av mikrobrikker i transponderne gjør produksjonen mer fleksibel, siden samme type mikrobrikke kan brennes med ulike egenskaper. Derfor benyttes mikrobrikker i større og større grad.

Minnearkitekturen

Minnet til de skrivbare transponderne kan som nevnt variere fra en byte til flere kilobytes (mikrobølgetranspondere med SRAM-minneteknlogi kan lagre opptil 64Kbytes). Minnet til transponderen er delt inn i blokker. Disse blokkene er delt inn i en forhåndsdefinert størrelse av bytes som både kan bli lest og skrevet som en enkelt enhet. For å kunne endre innholdet i en minneblokk i transponderen, må først hele blokken bli lest av RFID-leseren før den modifiseres og sendes tilbake til transponderen. Størrelsen på minneblokkene kan i slike system varierer avhengig av størrelsen på minnet.

Som et eksempel vil vi ta frem Tag-It sin HF-I innleggstransponder [39]. Figur 2-8 viser hvordan minnet i denne typen brikker er organisert. Blokk nummer 2 har en 32 bits ROM kode som inneholder produsentkode (7 bit), versjonsnummer (9 bit), blokkstørrelse (3 bit), antall minneblokker som er tilgjengelig for brukeren (8 bit) og 3 bit som er reservert. Denne blokken er imidlertid låst av produsenten (F). Det er to nivåer av blokklåsingsmekanismer som blir støttet. Individuell blokklåsing av brukeren (U) eller individuell blokklåsing av produsenten (F) i produksjonsprosessen. Blokklåsingen er irreversibel og beskytter dataene fra å kunne bli endret.

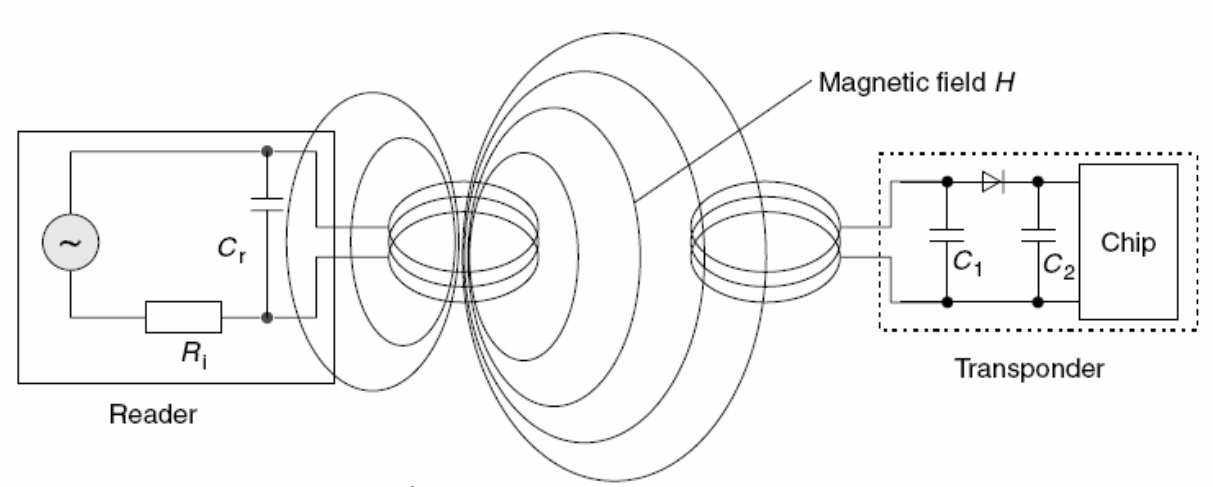


Figur 2-8 Organiseringen av minnet i en Tag-It HF-I transponder [39].

Passive transpondere

Betegnelsen *passive transponder*e betyr at transponderen er avhengig av en ekstern energikilde. Den nødvendige energien induseres når RFID-senderen kommer i nærheten av transponderen. Ved hjelp av denne energien kan transponderen sende informasjon tilbake til RFID-leseren. Vi skal nå se litt nærmere hvordan denne typen transpondere er bygd opp.

En indusert koblet transponder i FDX- / HDX-systemer kombinerer en datalagringsenhet som vanligvis er en enkel mikrobrikke, og en overflatevikling som fungerer som antenne. Disse opererer nesten alltid som passive komponenter. Dette betyr at all energien mikrobrikken trenger for å fungere må den få tildelt fra leseren. Leserens antennevikling må derfor generere et sterkt høyfrekvensaktig elektromagnetisk felt. Frekvensen som blir brukt (135 kHz: 2500 m, 13.6 MHz: 22.1m) utgjør en mye større avstand mellom bølgene enn avstanden mellom leserens antenne og transponderen. Det varierende magnetiske feltet kan derfor bli betraktet som svakt i forhold til avstanden mellom transponderen og antennen. Figur 2-9 viser hvordan det magnetiske feltet påvirker transponderen.



Figur 2-9 Transponder som får energi fra det magnetiske feltet generert av leseren [6].

Spenningen blir generert i transponderens antennespole ved hjelp av induktansen i det magnetiske feltet. Denne spenningen blir likerettet ved hjelp av en diode og er nok til å drive mikrobrikken i transponderen. En kondensator *Cr* er satt i parallell med spolen i leseren. Induktansen i kondensatoren blir valgt i forhold til induktansen i spolen for å kunne forme en parallell resonanskrets. Denne danner en høy strøm i spolen slik at nødvendig styrke i det magnetiske feltet blir generert for å kunne drifte transponderen. Parallellkoblingen av de to kondensatorene i transponderen fungerer som en inngangstransformator. Den praktiske effektoverføringen mellom leseren og transponderen er proporsjonal med frekvensen *f*, antall viklinger *n*, arealet til transponderens spole *A* og vinkelen og avstanden mellom de to spolene. Når frekvensen *f* øker og dermed også induktansen i transponderens spole, vil antall viklinger *n* minke. Transpondere som benytter seg av en bærefrekvens på 13.56 MHz, vil derfor trenge færre viklinger og kan dermed gjøres mindre, enn transpondere som benytter seg av lavere bærefrekvens.

Tag-It HF-I innleggstranspondere fra Texas Instrument er en type passive transpondere som kan være godt egnet til merking av prøver og pasienter. Vi har derfor sett nærmere på denne typen transpondere [39].

HF-I inneleggingstranspondere tilhører gruppen av passive transpondere som følger ISO standarden 15693. Fordelen med disse transponderne, er at de trenger liten effekt og benytter FDX systemet. Den opererer med en bærefrekvens på 13.56 MHz. Både i ned- og opplinken er pakkerammene synkronisert og har innebygd CRC (Cyclic Redundancy Check) sikkerhetsalgoritme for sikrere overføring av data [35]. Transponderen har tilgjengelig 2 kbits brukerminne. Hver Tag-It HF-I transponder har en unik adresse som er 32 bits lang og som blir programmert i produksjonsprosessen. Det er mulig å benytte seg av denne adressen eller en såkalt *non-addressed* mode kan brukes. Dette vil si at brukeren har anledning til å gi transponderen sitt eget identitetsnummer. Transponderne har også innebygd en mekanisme for å redusere kollisjoner når flere transpondere er innenfor lese- og skriveavstand (*Simultaneous IDentification–SID*). Dette gjør det mulig for leseren å kunne kommunisere med flere transpondere samtidig. SID-mekanismen gjør det mulig for leseren å administrere et stort antall transpondere ved hjelp av de ulike adressene i en liten tidsperiode. Dette er avhengig av at transponderne er innen rekkevidde.

Aktive Transpondere

Ved avstander over 1 m mellom transponderen og RFID-leseren, er aktive transpondere mye brukt. Aktive transponder kjennetegnes ved at de må ha et batteri som en tilleggsenergikilde. Operasjonsfrekvensen som blir brukt er i UHF-båndet (868 MHz) eller i mikrobølgebåndet (2.5 GHz). Den korte bølgelengden gjør at antennen kan konstrueres mye mindre og mer effektiv enn det som er mulig ved frekvenser under 30 MHz. Behovet for et batteri i transponderen vil likevel føre til at denne typen transpondere ikke vil være aktuell ved merking av prøver og pasienter. Dette fordi transponderen høyst sannsynlig vil være dyrere enn passive transpondere og i tillegg vil transponderen bli mye større på grunn av batteriet.

3. Trådløs sikkerhet

3.1. Datatilsynets krav ved behandling av sensitive data

Ved bruk av datasystemer som behandler sensitive data er det viktig å sørge for tilfredsstillende sikkerhet, slik at lovene og forskriftene følges. De aktuelle lover og forskrifter finnes på lovdatas nettsider [10], [11], [12], [13], [19]. Det er i dag datatilsynet sin oppgave å regulere dette lovverket i henhold til vedtatte lover. Datatilsynet sier i dag at trådløse nett i utgangspunktet er usikrede nett [16]. Dette innebærer at det må integreres autentiseringskontroll og kryptering i datasystemene som skal benyttes. Ved behandling av sensitive personopplysninger anbefaler datatilsynet at det bør minst benyttes krypteringsnøkkel som tilsvarer DES 128 (112 bits effektiv nøkkel) [17]. Det er viktig å merke seg at datatilsynet ikke har ansvar for sikkerhetsgodkjenning. En må likevel søke om konsesjon og sende melding til datatilsynet med dokumentasjon om at sikkerhetstiltak er iverksatt [19], dersom det skal behandles sensitive data.

Datatilsynets definisjon på informasjonssikkerhet er delt inn i tre hovedpunkter [10]:

Konfidensialitet: Det skal integreres kontrollrutiner slik at informasjon ikke er tilgjengelig uten autorisasjon.

Integritet: Bare personer med nødvendig autorisasjon skal kunne endre eller slette informasjon.

Tilgjengelighet: Det skal legges til rette for at nødvendig informasjon skal være tilgjengelig for medarbeidere slik at oppgavene de blir satt til kan utføres.

I følge datatilsynet skal tilgangen til nødvendig informasjon og tjenester, bestemmes ut fra tjenestelige behov [16]. Det er derfor utarbeidet krav til den systemtekniske sikkerheten. Datatilsynet har satt krav til hvordan tilgangen skal kontrolleres i informasjonssystemer hvor personopplysninger blir behandlet. Dette innebærer at det må opprettes ulike soner med forskjellig grad av tilgangskontroll. Nedenfor er et utdrag fra datatilsynets retningslinjer som omhandler dette [16].

Tilgang til sone hvor sensitive personopplysninger behandles

I sonen hvor det behandles sensitive personopplysninger eller informasjon om sikring av slike opplysninger, skal det etableres egne rutiner slik at en kan gjennomføre kontroll av tilgangen til sonen. Disse rutinene omfatter [16]:

- *retningslinjer for etablering og revurdering av soneinndeling*
- *retningslinjer for å opprette soner med angivelse av teknisk sikkerhetsløsning, eksempelvis ruter.*
- *retningslinjer for ekstern tilgang med krav om at den del av informasjonssystemet som benyttes for ekstern tilgang, etableres i egen sone.*
- *retningslinjer for å registrere forsøk på uautorisert tilgang beskrivelse av ansvar og myndighet*

Tilgang til sensitive personopplysninger

Datatilsynet sier også at tilgangen til data og program som benyttes til behandling av sensitive personopplysninger, eller informasjon om sikring av slike opplysninger, skal kontrolleres. Dette innebærer at kontrollrutinene må omfatte [16]:

- *retningslinjer for tildeling og tilbaketrekking av autorisasjon for tilgang med krav om entydig kobling mellom brukeridentitet og fysisk bruker*
- *retningslinjer for periodisk revurdering av den enkelte medarbeiders behov for tilgang*
- *retningslinjer for identifisering og autentisering av medarbeidere*
- *retningslinjer for automatisk avstengning av utstyr som ikke er i bruk*
- *retningslinjer for registrering av utstyr benyttet for tilgang og forsøk på uautorisert tilgang*
- *beskrivelse av ansvar og myndighet*

Dataoverføring

I tillegg skal all dataoverføring som omhandler personopplysinger kontrolleres. Dette innebærer at en må innføre ulike rutiner for intern og ekstern sone [16].

Intern dataoverføring

Datatilsynet sier at det skal være rutiner for kontroll med overføring av sensitiver personopplysninger og informasjon om sikring av slike i virksomhetens informasjonssystem. Rutinene skal minst omfatte [16]:

- *retningslinjer for å sikre at data ikke endres eller slettes under overføring, eksempelvis ved bruk av integritetskontroll.*
- *retningslinjer for fysisk sikring av overføringsmedium*
- *retningslinjer for registrering av dataoverføring*
- *beskrivelse av ansvar og myndighet*

Sikkerhetskrav

Videre har også datatilsynet gitt en anbefaling om minstekrav til sikkerhet når det gjelder behandling av sensitiv pasientinformasjon. I sin referansemodell gir de retningslinjer for de mest nødvendige sikkerhetsnivåene som må integreres ved behandling av denne typen informasjon [14]. I veiledningen i informasjonssikkerhet for kommuner og fylker [15], har datatilsynet utarbeidet en anbefaling til løsning for systemteknisk sikkerhet, inkludert implementasjon av sikkerhetsbarrierer. Dette innebærer at det må benyttes soner som et grunnleggende prinsipp i sikkerhetsarkitekturen, som vist i Figur 3-1.

Figur 3-1 Sikkerhetsarkitektur med soner [15]

Under vises et utdrag av kravene datatilsynet har utarbeidet for en løsning med nettverksforbindelse [14]:

- Sikkerhetsløsningen må ha tilfredsstillende metode for å skille mellom brukerens rettigheter til henholdsvis intern og sikret sone
- Det må skilles mellom brukerens / brukergruppers rettigheter til filsystemet / nettverksressursene ved hjelp av identitet / passord.
- Brukerne i sikret sone må tildeles til alternative brukerprofiler, hvis tilgang til ekstern nettverk skal gis til disse brukerne.

Dette innebærer at det kun gis tilgang til informasjon i sikret sone eller tilgang til intern sone, samt tilgang til tjenester og informasjon i eksterne nettverk. Dersom det skal lagres sensitiv informasjon på PDA, vil denne måtte være innenfor sikker sone.

3.2. Datasikkerhet i WLAN systemer

For å kunne overføre sensitive data slik som personopplysninger over et trådløst nett (WLAN), kreves det sikkerhetstiltak, som er nevnt i kapittel 3.1. Det vil derfor være nødvendig å beskytte dataene som blir overført, adgangen til håndholdte terminaler og adgangen til nettverket ved hjelp av aksesskontroll og kryptering.

I denne forbindelse er det gitt ut et paper for hvordan dette kan gjennomføres på en tilfredsstillende måte, og som ivaretar sikkerheten i henhold til datatilsynets krav. I *Security Aspects of Wireless Medical Computer Networks* skrevet av Fensli og Thorstensen [18], er det gjort ulike betraktninger og kommet til en konklusjon rundt datasikkerhet i WLAN-systemer.

Når vi tar for oss sikkerhet kan vi dele opp det trådløse nettverket i tre hoveddeler som bør beskyttes:

- Håndholdte enheter
- Aksesspunkter
- WLAN aksess

Tabell 3-1 viser en oversikt over ulike sikkerhetstiltak som kan gjøres i forholt til å beskytte en håndholdt enhet hvor sensitive data skal behandles.

Tabell 3-1 Beskyttelse av den håndholdte enheten [18]

Sikkerhetsnivå	Tiltak	Beskrivelse
H-G	Beskytter informasjonen som er lagret i den håndholdte enheten.	Kryptere all informasjon som er lagret på den håndholdte enheten ved hjelp av et krypteringsprogram.
H-F	Sikker brukerautentisering	Autentiserer brukeren ved hjelp av en digital ID og smartkort eller liknende.
H-E	Kryptert kommunikasjon	Krypterer kommunikasjonen mellom den håndholdte enheten og brannmuren med en VPN-tunnel med minst DES128 bit nøkkellengde.
H-D	Unngå å lagre sensitiv informasjon på den håndholdte enheten.	Bruker en såkalt *tynnklient* på den håndholdte slik at den kun fungerer som en terminal, og ingen data blir lagret lokalt.
H-C	Beskytte den håndholdte enheten mot angrep utenfra.	Bruker en brannmur på den håndholdte for å hindre at utenforstående får tilgang.
H-B	Beskytte den håndholdte enheten mot virus.	Bruker et antivirusprogram som oppdateres automatisk.
H-A	Tillat kun tilkobling til forhåndsdefinerte aksesspunkt.	Ikke tillat trådløse Ad-hoc tilkoblinger eller tilkobling til ukjente WLAN aksesspunkt.

Etter å ha sett hvordan de håndholdte terminalene kan beskyttets tar vi for oss ulike sikkerhetstiltak som kan gjøres i forhold til selve aksesspunktene, se Tabell 3-2.

Tabell 3-2 Beskyttelse av aksesspunktene [18]

Sikkerhetsnivå	Tiltak	Beskrivelse
A-G	Sikker pålogging av bruker	Bruk digital ID og smartkort eller liknende for å få sikker autentisering av brukeren ved pålogging.
A-F	Autentisering av aksesspunkt	Bruk digital ID til å verifisere aksesspunktet og autentisere brukeren.
A-E	Beskytte tilgang fra aksesspunktene.	Definerer aksesspunktene innenfor atskilte grupper. Bruker brannmur for å beskytte mot det sikre LAN nettverket i sikret sone.
A-D	Beskyttelse av brukers pålogging og autentisering	Bruke en påloggingsserver som RADIUS eller KERBEROS og kryptere brukerpassord for å begrense lovlig tilgang til aksesspunktet.
A-C	Bruk kraftig WEP algoritme	Benytt 128 bits WEP algoritme.
A-B	Beskytt de godkjente brukeradressene.	Beskytt tilgangen til de registrerte MAC-adressene og bruk permanente IP adresse. Ikke bruk DHCP.
A-A	Skjul aksesspunktene.	Bruk unik SSID på alle aksesspunktene og skjul SSID for brukeren. Ikke bruk webbasert konfigurasjon av AP og aktiver pålogging. Monter antenner slik at det vil være vanskelig å få tilgang fra utsiden av bygningen.

I Tabell 3-3 ser vi på hvordan tilgangen til det trådløse nettverket kan beskyttes.

Tabell 3-3 Beskyttelse av WLAN tilgang [18]

Sikkerhetsnivå	Tiltak	Beskrivelse
W-E	Bruk *honeypots*	Bruk såkalte *honeypots* for å lure en inntrenger inn i en felle.
W-D	Bruk IDS beskyttelse	Bruk Intrution Detection System (IDS) for å hindre en inntrenger i å få tilgang til informasjon fra nettverket.
W-C	Rollebasert aksesskontroll	Bruk digital ID og løsninger for rollebasert aksesskontroll for å kunne sikre lovlig tilgang til sensitiv informasjon.
W-B	Beskyttelse av tilgang til informasjon	Bruk brannmur mellom aksesspunktene og det sensitive nettverket for å hindre direkte tilgang til beskyttede servere med sensitiv informasjon.
W-A	Beskyttelse av nettverkstilgang	Begrens tilgangen til det interne nettet ved hjelp av en ruter, hvor aksesspunktene er koplet gjennom et separat virtuelt nettverk.

Ut fra de retningslinjer og krav som datatilsynet stiller vil det være nødvendig å sikre det trådløse nettverket med en kombinasjon av sikkerhetstiltakene nevnt ovenfor. Dette innebærer at den håndholdte enheten må sikres med tiltakene nevnt fra H-A til H-E. Tilsvarende må sikkerhetstiltakene fra A-A til A-E innføres for aksesspunktene og til slutt så må tilgangen til WLAN sikres med sikkerhetstiltakene fra W-A til W-B. Ved å innføre disse tiltakene, tilfredstilles datatilsynets krav om behandling av sensitive data og det vil være mulig å behandle sensitiv pasientinformasjon via PDA'en [18].

3.3. Datasikkerhet i RFID-systemer

3.3.1. Sikkerhetstrusler

Utviklingen i RFID-teknologien har gjort det mulig å benytte teknologien innen flere områder. Eksempler på dette er nøkkelautentisering i biler, sporing av klesplagg, pakkesporing og bruk av ID-kort. Dette har ført til at RFID-teknologien i mange tilfeller kan true personvernet [25]. Mye av grunnen til dette, er at RFID-systemer fungerer på en annen måte enn andre identifikasjonssystemer. Dette fordi radiokommunikasjonen verken er kontaktbasert, eller må ha fri sikt til leseren. Det vil igjen gjøre det vanskeligere å kontrollere hvem som skal kunne få tilgang til informasjonen som ligger på brikken, i motsetning til for eksempel magnetstripen på et bankkort, der fysisk kontakt er nødvendig for å få tilsvarende informasjon. Det vil likevel være en begrensning i å kunne lese informasjonen på transponderne, siden leseavstanden ofte er noe begrenset.

Behovene for å innføre sikkerhetstiltak, kommer an på sammenhengen som systemet brukes i og hvilke data som overføres. Dersom et RFID-system skal behandle sensitive opplysninger, som for eksempel er knyttet til pasienter ved et sykehus, vil det være ekstra viktig å ivareta sikkerheten slik at ikke uvedkommende kan få tilgang til informasjonen.

RFID-systemer som trenger høy sikkerhet bør ha et forsvar mot følgende angrep [6]:

- Uautorisert lesing av lagringsenheten i brikken og mulighet for å kopiere eller endre dataene.
- Plassering av en fremmed brikke innenfor rekkevidden til en leser for å kunne motta informasjon som denne sender ut.
- Avlytte radiokommunikasjonen for så å modifisere og videresende signalene.

Det er flere mekanismer innenfor RFID-teknologien som kan bidra til å at sikkerheten og personvernet blir ivaretatt på en tilfredsstilende måte. For å få en mer grunnlegende forståelse i hvordan de ulike sikkerhetsmekanismene fungerer, har vi i kapittel 3.3.2 – 3.3.6 tatt for oss de ulike sikkerhetsmekanismene i RFID. RFID handbook [6] er brukt som kilde i 3.3.2 og 3.3.3.

3.3.2. Toveis autentisering

Ved å autentisere toveis, vil både transponderen og leseren blir autentisert. Både transponder og leser må ha en forhåndsdefinert hemmelig nøkkel *K*. Figur 3-2 viser hvordan toveis autentisering foregår.

Figur 3-2 Toveis autentisering [6]

Det som skjer når en leser skal lese en transponder, er at leseren sender en GET_CHALLENGE melding. Transponderen svarer med å sende et tilfeldig generert tall R_A. Leseren vil deretter generere et tilfeldig tall R_B og sender både R_A, R_B, sin egen ID_A og en del kontrolldata tilbake til transponderen. Alle disse dataene blir kryptert med en felles nøkkel *K* og krypteringsmetode e_K. Deretter samles dataene i en blokk som kalles for *Token 1* før dataene oversendes til transponderen. *Token 1* blir dekryptert av transponderen med nøkkelen *K*, og tallet R_A blir sjekket om den er den samme som transponderen sendte. Hvis dette stemmer, betyr dette at leseren bruker riktig nøkkel og leseren er autentisert.

$$Token\ 1 = e_K(R_B || R_A || ID_A || \text{Text 1})$$

For å autentisere transponderen blir det laget et nytt nummer R_{A2} og en ny blokk *Token 2* blir satt sammen og kryptert med *K*. *Token 2* inneholder R_{A2}, R_B og kontrolldata. Når leseren mottar *Token 2* blir blokken dekryptert og R_B blir sjekket om den stemmer med det nummeret som leseren sendte i *Token 1*. Stemmer dette er også transponderen autentisert.

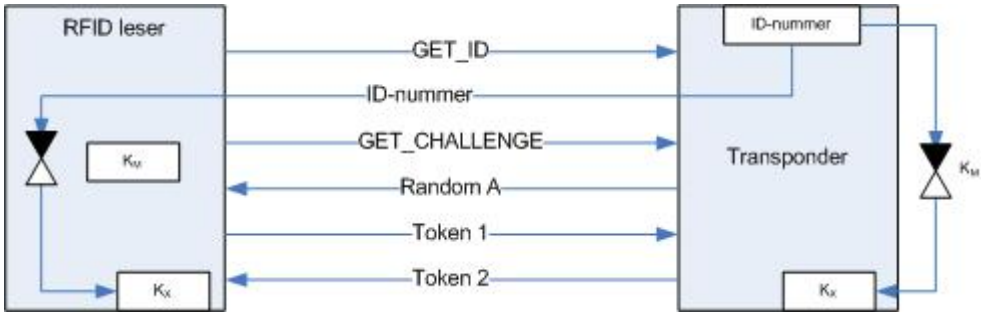
$$Token\ 2 = e_K(R_{A2} || R_B || \text{Text 2})$$

Nå er begge enhetene autentisert, siden man er sikker på at de har den riktige nøkkelen *K*.

3.3.3. Toveis autentisering med genererte nøkler

Den metoden som er nevnt over fungerer slik at alle transpondere og lesere har samme nøkkel. I RFID-systemer hvor det er mange transpondere som er spredt over et større område, kan det være vanskelig å forsikre seg om at ingen kopierer nøkkelen. En løsning på dette problemet kan være å utstyre hver transponder med ulike nøkler. Denne nøkkelen blir beregnet på bakgrunn av serienummeret til transponderen og en hovednøkkel K_M ved hjelp av en kryptografisk algoritme.

Selve autentiseringen starter med at leseren ber om ID fra transponderen. Leseren mottar transponderens ID, og lager en unik nøkkel K_X på bakgrunn av hovednøkkelen og ID-nummer. Deretter gjøres samme prosedyre som ble beskrevet i 3.3.2. Forskjellen blir da K_X brukes til å kryptere dataene istedenfor K som var en felles nøkkel, se Figur 3-3. På den måten reduseres faren for at uvedkommende kan få tilgang til alle transponderne ved at det blir laget en ny krypteringsnøkkel for hver transponder.



Figur 3-3 Autentisering med genererte nøkler [6]

3.3.4. Andre autentiseringsmetoder

Tilsvarende som i andre trådløse kommunikasjonssystemer, har det også innenfor RFID-teknologien blitt utviklet ulike autentiseringsmetoder. Fra *RFID Systems and Security and Privacy Implications* [26], har vi hentet informasjon om hvordan hash-funksjoner kan benyttes som autentiseringsmetode.

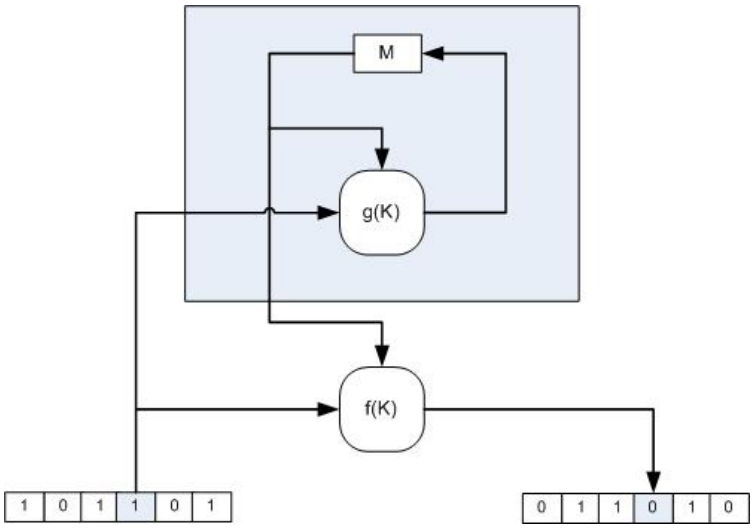
Hash-funksjoner kan brukes til å gi lesere tilgang til data som er lagret på brikker. En maskinvareoptimalisert kryptografisk hash-funksjon i brikkene kan i mange sammenhenger både være tilstrekkelig og krever ofte mindre ressurser enn for eksempel symmetrisk kryptering. I denne metoden vil brikkene avsette en egen del av minnet til en "meta-ID" og opererer i to tilstander; enten lukket eller åpen tilstand. I åpen tilstand vil alt som ligger i minnet og all funksjonalitet være tilgjengelig for alle som er innenfor leseavstand. For å få transponderen over i lukket tilstand må det lages en hash-verdi ved hjelp av en tilfeldig generert nøkkel. Denne sendes over til transponderen som en låsekommando. Transponderen vil lagre denne verdien i minnet der meta-ID er lokalisert og går over i lukket tilstand. Transponderen vil nå være lukket for alle RFID-lesere som ikke har den aktuelle meta-ID verdien, og det vil ikke være mulig å få ut noe informasjon. For å låse opp transponderen må en sende over den originale nøkkelverdien til transponderen. Transponderen vil hash-transformere denne verdien, for så å sammenligne den med verdien som er lagret og låst i meta-ID minnet. Hvis verdiene stemmer overens, vil transponderen gå over i åpen tilstand. Enhver transponder vil alltid svare på alle forespørsler som blir sendt ut fra en leser for å avsløre at den er i området, men transponderne låser seg opp kun for autoriserte lesere. Skulle dataoverføringen mellom transponderen bli brutt eller bli forstyrret av støy, vil transponderen automatisk gå tilbake til lukket tilstand.

For å forhindre forsøk på trådløs sabotering eller at uautoriserte saboterer autorisert kommunikasjon, kan det implementeres rutiner som øker sikkerheten når kritiske funksjoner gjennomføres. Dette kan f. eks være at det må være fysisk kontakt mellom transponderen og leseren når disse funksjonene gjennomføres. På den måten opprettets en sikker kommunikasjonskanal når en skal administrere viktige funksjoner som nøkkeladministrasjon og leserautentisering. Dette vil i mange sammenhenger være tilstrekkelig for å sikre dataene.
MAC (Medium Access Control)-funksjonalitet på transponderne vil gjøre det mulig for transponderne å autentisere seg selv. I dette ligger det at transponderen selv kan sørge for å kontrollere om leseren er autorisert og utveksling av autentiseringsnøkkelen unngåes [41]. På den annen side kan funksjonen også føre til at prisen på transponderne øker. En manglende kryptering av autentiseringskoden, kan føre til en økt fare for "man-in-the-middle" angrep siden det kan utføres en spørring mot transponderen av meta-ID. Deretter kan dette sendes til en legitimert leser for så å låse opp transponderen med leserens svarnøkkel.

3.3.5. Krypteringsprinsipp av dataoverføringen

Vi har nå sett på hvordan man kan begrense hvem som får tilgang til å lese av eller lese inn data til en transponder. Selv om man bruker autentisering finnes det fremdeles ingen garantier for at kommunikasjonen mellom leser og transponder blir avlyttet. I resten av dette avsnittet er RFID handbook [6] brukt som referanse. Ved å innføre kryptering av dataoverføringen er det liten sjanse for at noen uautoriserte kan hente ut informasjon ved å avlytte overføringen. Dataene blir kryptert med en hemmelig algoritme og nøkkel *K* og kalles da *cipher data*. Hos mottakeren dekrypteres dataene med *K'*. Dersom *K* og *K'* er like eller har koblinger mellom hverandre (*K = K'*), kalles denne prosedyren for *symmetrisk nøkkelprosedyre*. Det er denne typen som brukes i forbindelse med RFID. Dersom hver karakter blir kryptert hver for seg før overføringen, kalles dette *sequential ciphering* (*stream ciphering*). Hvis karakterene blir delt inn i grupper, eller blokker, kalles dette for *block ciphering*. Siden *block ciphers* ofte krever mye kalkulering, er denne typen kryptering lite brukt i sammenheng med RFID-systemer.

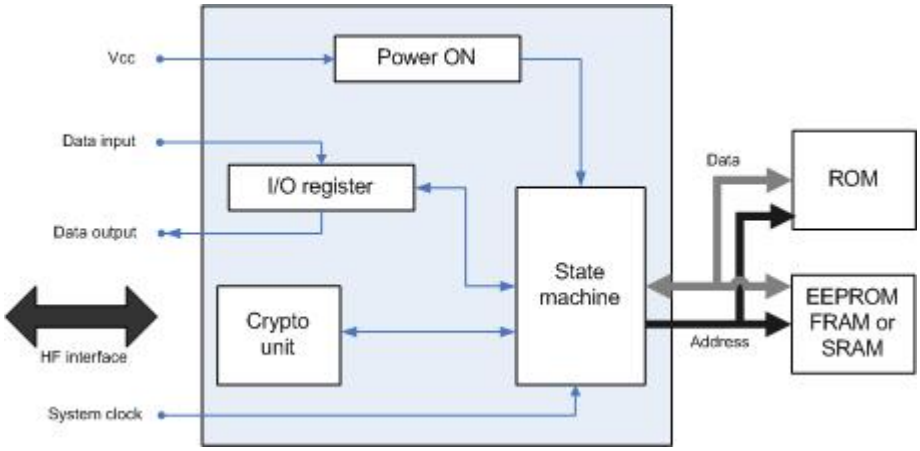
Stream ciphers er altså kryptoalgoritmer som krypterer hver enkelt karakter. Det brukes en tilfeldig generert nøkkel *K* som er minst like lang som den meldingen som skal overføres. Denne nøkkelen XOR'es med meldingen. Problemet med denne metoden å kryptere på er at nøkkelen nå distribueres over til mottakeren, noe som er upraktisk og vanskelig å få til i RFID-systemer. Det er derfor laget en prosedyre som kalles *psaudorandom sequence*. Her blir nøklene generert av en såkalt *psaudorandom generator*, se Figur 3-4.



Figur 3-4 Nøkkelgenerering ved hjelp av psaudorandom generator [6]

Generatoren består av interntilstanden *M* og tilstandstransformasjonsfunksjonen *g(K)*. *M* blir endret av *g(K)* etter hvert krypteringssteg. Sikkerhetsnivået på systemet kommer an på antall tilstander *M* kan ha, samt kompleksiteten til *g(K)*.

For å kunne kryptere og autentisere må det være innebygd en enhet som tar seg av dette i brikken. En *crypto unit* tar seg av kryptering av det som overføres, autentisering av leser og nøkkeladministrering.



Figur 3-5 Oversikt over hvordan adresserings- og sikkerhetslogikken fungerer [6].

3.3.6. Datakrypteringsstandarden DES/3DES

DES krypteringsalgoritme har vært benyttet i lang tid som krypteringsalgoritme ved sikring av data. I RFID-sammenheng har krypteringsfunksjoner ikke vært særlig utbredt, men etter hvert som behovet har meldt seg har produsentene også innen for RFID-teknologien utviklet mikrobrikker med denne funksjonaliteten. Vi ønsker derfor å vite hvor sterk denne krypteringsalgoritmen er. Avsnittet nedenfor har vi hentet fra Data Encryption Standard (DES) [27].

Data Encryption Standard (DES) er en algoritme beregnet for å kryptere og dekryptere data i blokker på 64 bits ved hjelp av en 64 bits nøkkel. Den samme nøkkelen brukes til både å kryptere og dekryptere data, men ved dekryptering er planen for å adressere

nøkkelen gjort baklengs i forhold til krypteringen. Av blokken og nøkkelen på 64 bits, er det bare 56 bits som blir randomgenerert og blir brukt til effektiv kryptering. De øvrige 8 bit blir ikke brukt av algoritmen, men blir brukt til feilsjekking.

3DES er en kombinasjon av DES krypterings- og dekrypteringsoperasjoner. I 3DES skjer krypteringen ved at en 64-bits blokk I blir transformert inn i en 64-bits blokk O.

E=encyption, D=decryption

$$O=E_{K3}(D_{K2}(E_{K1}(I)))$$

Blokkskjematisk ser krypteringsprosessen slik ut:

$$\mathbf{I} \rightarrow \boxed{DES\ E_{K1}} \rightarrow \boxed{DES\ D_{K2}} \rightarrow \boxed{DES\ E_{K3}} \rightarrow \mathbf{O}$$

Dekrypteringen i 3DES skjer ved at en transformerer en 64-bits blokk I inn i en 64-bits blokk O.

$$O=D_{K1}(E_{K2}(D_{K3}(I)))$$

Blokkskjematisk ser dekrypteringsprosessen slik ut:

$$\mathbf{I} \rightarrow \boxed{DES\ D_{K3}} \rightarrow \boxed{DES\ E_{K2}} \rightarrow \boxed{DES\ D_{K1}} \rightarrow \mathbf{O}$$

Standard spesifikasjon for nøklene (K1, K2, K3) er at de kan ha en av følgende egenskaper:

1. Nøklene K1, K2, K3 er uavhengige av hverandre
2. K1 og K2 er uavhengige nøkler mens K3=K1
3. K1=K2=K3

Hver enkelt nøkkel er på 56 bit som i DES, men ved å bruke forkjellige nøkler for K1, K2 og K3 kan 168 bits nøkkelkryptering oppnåes. Med 3DES oppnåes sterkere kryptering enn DES kryptering. Det finnes i dag brikker på markedet som støtter 3DES. Et eksempel på dette er Mifare DESFire fra Philips [28]. Denne brikken har innebygd flere sikkerhetsmekanismer som blant annet innebærer DES/3DES kryptering. Vi kan nevne noen av egenskapene til Philips Mifare DESFire:

- Et unikt 7 bits serienummer som blir implementert i hver brikke.
- Gjensidig autentisering med leseren i tre omganger.
- DES/3DES kryptering av dataene som blir overført.
- Dataautentisering med 4 byte MAC.

Denne brikken har altså mange gode sikkerhetsegenskaper som burde kunne tilfredsstille de fleste krav til sikker overføring. I henhold til datatilsynets krav som vi omtalte i kapittel 3.3.1, tilfredstiler den både med tanke på autentisering og kryptering. Det vil derfor være mulig å lagre sensitive data på mikrobrikken. Dette er imidlertid en avansert brikke som trolig vil ligge høyere i pris enn andre typer brikker.

4. Metode

Med bakgrunn i et *paper* utgitt av Blechner et al. har vi valgt Contextual Design som metode i vår oppgave. Dette paperet beskriver bruk av *Contextual Design* som metode for å undersøke informasjonssystemer i en problembasert læringssituasjon for medisinstudenter. De konkluderer sitt arbeid med at denne metoden kan være nyttig innenfor andre områder som fokuserer på brukermedvirkning for design av softwaresystemer. Eksempler på dette er design av ny portal for helseinformasjon, laboratoriesystemer og medisinske journalsystemer. Ut fra dette ser C*ontextual design* ut til å være en egnet metodikk for å involvere bioingeniørene ved laboratoriet på sykehuset i utviklingen av en ny systemløsning som vi ønsker å gjøre i dette prosjektet.

Videre ønsker vi også å se nærmere på holdningene blant bioingeniørene knyttet til innføring av en eventuelt ny teknologi. Her har vi benyttet Technology Acceptance Modell (TAM) som nettopp tar for seg disse spørsmålene. Denne modellen er derfor naturlig å knytte opp mot en vurdering av resultatene i etterkant.

4.1. Contextual Design

I følgende avsnitt har vi tatt for nærmere Contextual Design modellen [40].

Contextual Design starter med å kartlegge hvordan systemet fungerer. Det er en metode for å finne ut hva brukerne trenger, og hvordan et system kan designes. Arbeidsprosessen gjenspeiler brukerens arbeidsmetoder, og på den måten få en forståelse av hvordan datasystemer kan utvikles for å forbedre brukernes arbeidsprosess. Metoden fokuserer på brukerens arbeidsmetoder er grunnlaget for designet i stedet for at utviklerne antar hva brukerne ønsker. *Contextual Design* er delt opp i flere deler. Hver del har et delmål og beskrivelser hvilke problemer den løser.

Oppdelingen er som følger:

- ***Contextual inquiry***

Contextual inquiry avdekker hvordan brukerne egentlig er og hvordan jobben de gjør utføres over lengre tid. Dette kan gjøres ved å gjennomføre feltintervju med brukeren, mens personen arbeider for å avdekke hva som er betydningsfullt i arbeidet. På den måten er det mulig å oppklare detaljene og motivasjonen i brukerens arbeid. De som skal utvikle systemet ser lettere hva brukeren trenger og kan benytte brukerens data som grunnlag for avgjørelser. Med *Contextual inquiry* er det lettere å kunne tolke innsamlede data, og systemutviklerne blir mer samkjørte.

- ***Work modelling***

Work modelling forutsetter at de som skal utvikle systemet må kunne kommunisere med et felles språk for å øke forståelsen innen gruppen av utviklere. *Work modelling* har til hensikt å vise strukturen i arbeidet ved at det samles inn data fra sammenhengende intervjuer. Ved hjelp av Work Modelling er det mulig å få en oversikt over arbeidet til hver enkelt ved hjelp av forskjellige modeller. Fem modeller viser forskjellige perspektiver på hvordan jobben blir gjort.

The flow model: Gjenspeiler kommunikasjon og koordinasjon
Cultural model: Gjenspeiler kultur og arbeidsmetoder
Sequence model: Viser detaljert fremgangsmåte for å oppnå en oppgave.
Physical model: Viser hvordan utstyr brukes som hjelpemiddel i arbeidet.
Artifact modell: Viser hvordan kunst kan bidra.

- **Consolidation**

Consolidation samler dataene fra intervjuene sammen og bidrar til å få en helhetlig oversikt. To typer diagrammer kan brukes:

1. *The affinity diagram*: Samler all innformasjon og innslag fra alle brukerne hierarkiisk for å se kjernen i problemene.
2. *Consolidated model*: Samler de ulike arbeidsmodellene for å få en felles strategi og organisere individuelle forskjeller.

Consolidation gir en bedre oversikt over antall brukere og gjør det lettere å identifisere behovene til brukeren. Det viser underliggende struktur av arbeidet til brukerne uten at arbeidets variasjon blir borte. Kvalitativ datainnsamling kan gjøres raskt og oversiktlig. Innsamlingen kan også bli brukt på nytt i fremtidige prosjekter.

- ***Work Redesign***

Work Redesign samler data til å kunne diskutere hvordan arbeidet kan forbedres i de nye arbeidsmetodene, ved bruk av teknologien. Den fokuserer på hvordan teknologien hjelper til med å få jobben gjort og sørger for at systemet, forretningsallianser og tjenester passer til brukerens arbeidsutførelse. I tillegg samler og summerer *Work Redesign* alle ideene fra hele arbeidsgruppen.

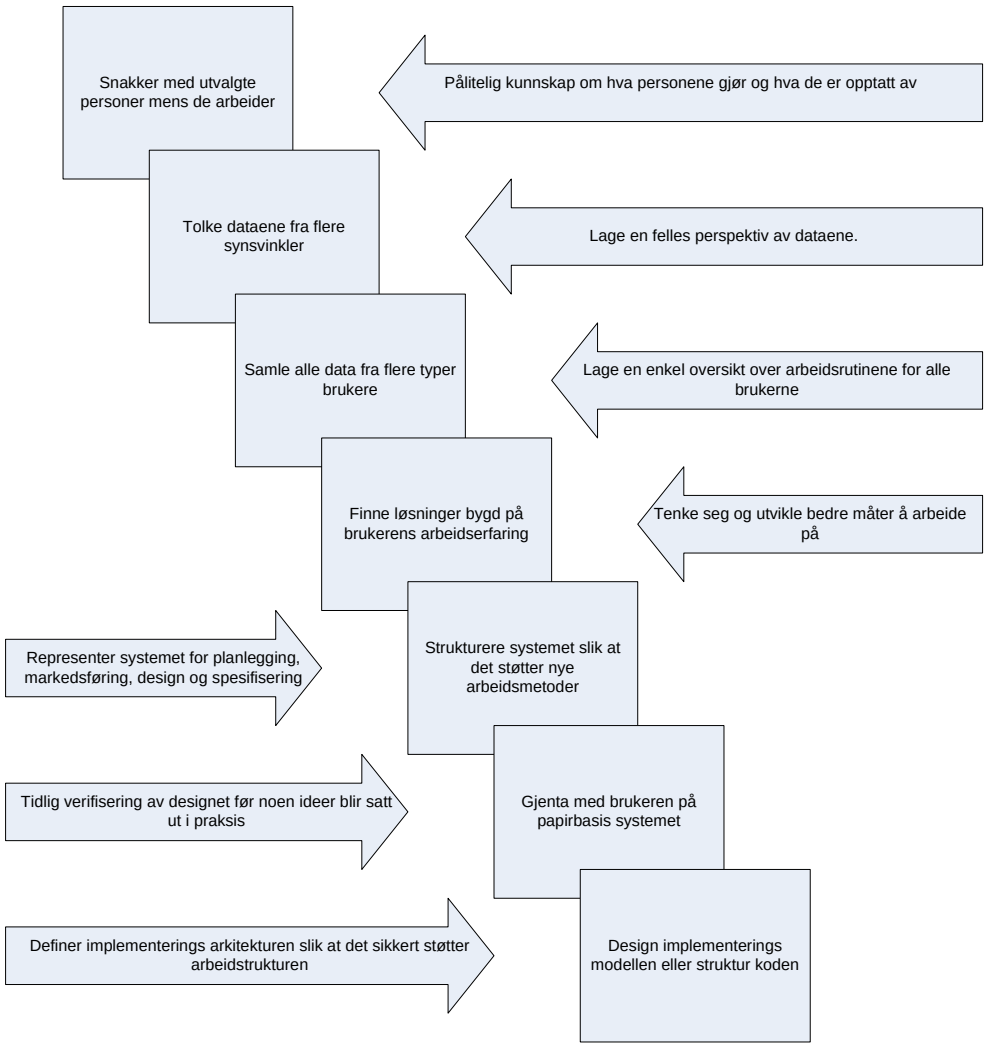
- ***User Environment***

User Environment viser grunnlaget for det nye systemet. *User Environment* viser hver enkelt del av systemet og hvordan det inngår og støtter brukerens arbeid, hvordan funksjonene er tilgjengelig i hver del, og hvordan brukeren veksler mellom de forskjellige delene av arbeidet. Ved hjelp av *User Environment* kan sammenhengen i systemet opprettholdes fra brukerens synsvinkel. Den hjelper utviklerne til å fokusere på hva systemet gjør og ikke så mye på brukergrensesnittet eller implementasjon. Den tillater planlegging og holder utviklerne fokusert på hele systemet og ikke bare hver sin del.

- ***Make up and test with customers***

Make up and test with customers er prosessen der prototypen testes ut sammen med brukeren. Her får utvikleren mulighet til å se om målsettingen er nådd. I denne prosessen er det også mulig å se forbedringspotensialet i den videre utviklingen til et ferdig kommersielt produkt.

Figur 4-1 viser hva de forskjellige delene i Contextual Design innebærer i praksis i kronologisk rekkefølge.



Figur 4-1 Contextual Design [40]

4.2. Technology Acceptance Modell (TAM)

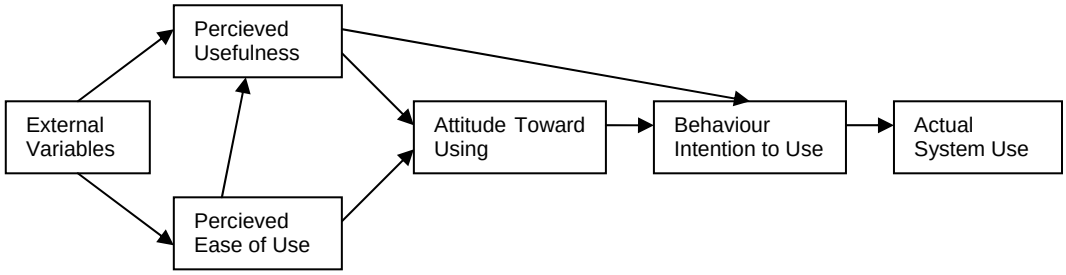
TAM (Technology Acceptance Model) er en modell som er mye omtalt og fått mye oppmerksomhet i forbindelse med innføring av ny teknologi. Modellen er laget av Fred D. Davis og er en adapsjon av Fishbein og Ajzen's *TRA-modell (Theory of Reasoned Action)* som tar for seg ulik atferd, og hva som ligger bak forskjellige typer atferd. TAM går nærmere inn på atferd og holdninger spesielt knyttet til innføring av ny informasjonsteknologi [1].

Skal et nytt system innføres er man avhengig av at det blir godt mottatt av de som skal bruke det. Brukerne må ha lyst til å bruke det og i følge Davis henger dette mye sammen med hvordan brukeren oppfatter systemet. Davis sin modell trekker frem to ulike faktorer. Det er *oppfattet nytteverdi (percieved usefulness)* og *oppfattet enkelhet ved bruk (percieved ease of use)* [2].

Oppfattet nytteverdi *(perceived usefulness)* defineres som *"the degree to which a person believes that using a particular system would enhance his or her job performance."* I dag blir man gjennom provisjoner og høyere lønninger drevet til å yte mer. Det er derfor sterkt ønskelig fra brukerens side at en ny teknologi kan bidra til å oppnå nettopp dette [2].

Oppfattet enkelhet ved bruk (perceived ease of use) blir definert som *"the degree to which a person believes that using a particular system would be free of effort."* Brukeren vil normalt foretrekke et system som er enkelt å bruke. Oppfattet enkelhet sier noe om hvor lett brukeren oppfatter at programmet kan brukes [2].

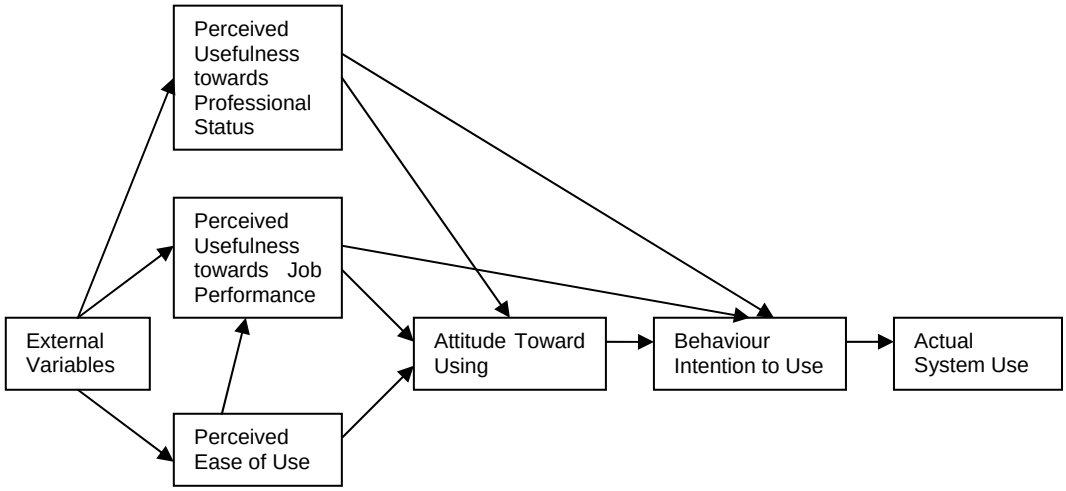
Modellen kan settes opp som vist i Figur 4-2.



Figur 4-2 Technology Acceptance Model (TAM) [1]

Oppfattet nytteverdi og oppfattet enkelhet ved bruk vil ut fra Davis' model innvirke på holdning til bruk av systemet, som igjen vil virke inn på hvordan systemet blir brukt. Ved innføring av et nytt system vil det derfor være essensielt å sette brukeren i sentrum. Utviklingen bør gjerne skje i samarbeid med bruker og det vil være viktig å jobbe med holdningene til brukerne. Det kan være lurt å få brukerne til å forstå at det å innføre et nytt system vil være en fordel for alle.

Melissa J. Succi og Zhiping D. Walter skrev i 1999 en artikkel som tok for seg innføring og adopsjon av IT blant fagfolk i helsesektoren [1]. De tok for seg TAM og foreslo en utvidet versjon som også tar for seg hva slags type fagfolk som blir berørt ved innføring av ny informasjonsteknologi, se Figur 4-3.



Figur 4-3 Modell hvor yrkesstatus er tatt i betraktning [1].

Succi og Walter så spesielt på fagfolk i helsesektoren slik som leger og annet høyt kvalifisert personell. De kom frem til at leger og doktorer lett kunne føle at IT undergravde deres posisjon og ekspertise. Det blir påpekt at høyt kvalifisert helsepersonell kan være mer på vakt enn andre for at ny teknologi kan gjøre andre mindre avhengige av den jobben de utfører. Grunnen kan være at denne yrkesgruppen er meget dominerende i sitt yrke og har de siste årene opplevd store endringer i yrket grunnet bl.a. omlegging i helsepolitikken [1]**.** Siden dette studiet er rettet spesielt mot helsesektoren kan det være sentralt for oss når vi skal se på mulighetene for å implementere ny teknologi.

5. Beskrivelse av sykehusets arbeidsflyt

Vi har tidligere beskrevet metoden *Contextual Design*, og har valgt å støtte oss til den under gjennomføring av oppgaven. I startfasen gjennomførte vi derfor et besøk ved sykehuset for å se på dagens rutiner og hvordan ting blir gjort. Intervjuer med noen nøkkelpersoner og observasjon under vårt besøk har gitt oss et godt utgangspunkt for å se hvilke behov en ny teknologi skal dekke. Diverse notater fra besøket ligger vedlagt i [v1], [v2] og [v3].

5.1. Case

På bakgrunn av vårt besøk ved Sørlandets Sykehus i Arendal, har vi forsøkt å lage en case hvor vi beskriver et tenkt scenario. Ved å følge en pasient gjennom behandlingsprosessen, kan vi se hvordan noen av dagens rutiner fungerer. Scenarioet som blir beskrevet er fiktivt og har ikke skjedd i virkeligheten. Vi ser for oss følgende scenario:

Sykehuset får inn melding fra AMK om at en eldre mann er funnet bevisstløs i Arendal sentrum. Ingen ID er funnet på mannen.

Ved mottak på sykehuset blir pasienten registrert i DIPS med et såkalt *K-nummer*. Dette er et midlertidig nummer som brukes ved registrering dersom pasientens identitet ikke er kjent ved innleggelse. Nummeret er like langt som et fødselsnummer og blir byttet ut med korrekt fødselsnummer og navn så snart dette blir kjent. Et armbånd med K-nummer blir festet på pasienten og sengen. Etter ankomst på sykehuset er fortsatt pasienten bevisstløs. Legen mener det bør taes en blodprøve av pasienten for å kunne stille en diagnose. Blodprøve blir rekvirert som en *straks-prøve* via DIPS, og en bioingeniør blir tilkalt for å ta blodprøven og analysere denne ved bio-laboratoriet.

Prøven blir tappet på riktig type glass og merket med klistrelapper som er skrevet ut fra Uni-Lab. Glassene blir signert av bioingeniøren og fraktet tilbake til laboratoriet for analyse. Det blir samtidig målt blodsukkernivå ute hos pasienten. Resultater fra blodsukkernivået blir notert og overført til Uni-Lab og DIPS etter at bioingeniøren returnerer til laboratoriet. Pasienten får surstoff og kommer etter en stund til seg selv. Han klarer etter hvert å gjøre rede for seg slik at riktig personalia blir funnet og pårørende varslet. Riktig personalia blir lagt inn i DIPS, og K-nummeret blir erstattet med korrekt personnummer. Pasienten klager stadig over at han føler seg svimmel og uvel. Legen ved mottakelsen mener pasienten bør legges inn til observasjon og pasienten overflyttes til en sengepost. Overflyttingen blir registrert i DIPS. Ved overgang fra K-nummer til pasientens riktige identitet, blir rekvisisjonene overført til den nye identiteten. Dersom det er prøver inne til analyse i det K-nummer blir erstattet, kan det oppstå problemer med å knytte prøveresultatene til riktig pasient når disse foreligger. Det er derfor viktig med en dialog mellom avdelingen og laboratoriet i denne perioden.

Etter overflyttingen av pasienten blir resultatene av prøvene klare og blir frigitt fra Uni-Lab til DIPS. Resultatene kan legen på sengeposten lese ut fra DIPS og stille en diagnose på pasienten. Det anbefales at pasienten medisineres med en bestemt medisin og blir liggende på sykehuset i noen dager for overvåkning og ytterligere prøvetaking. Det bestilles en ny blodprøve, en såkalt *rutine-prøve* som skal taes neste dag.

Neste dag klokken 08:00 skriver bioingeniørene ut prøvetakingslister og klistrelapper til prøveglassene. De ulike pasientene er sortert etter avdeling de ligger på. Prøvene som skal taes blir fordelt mellom flere bioingeniører og listene blir delt opp. Bioingeniøren tar

med seg riktig type glass og utstyr, og begynner på runden for å ta prøver. Når bioingeniøren kommer frem til vår pasient, blir pasienten spurt om navn og fødselsnummer. I tillegg blir armbånd sjekket for å kontrollere at identiteten er korrekt. Blodprøven blir tatt og bioingeniøren må finne riktig klistrelapp og feste denne på prøveglasset. Det blir også målt blodsukker med et apparat som bioingeniøren har med seg. Resultatene blir notert ned på en liste, og bioingeniøren returnerer tilbake til laboratoriet etter å ha fullført prøvetakingsrunden. Resultatene fra målingen av blodsukkeret kan lagres i apparatet ved hjelp av strekkoder på en liste. Dette er imidlertid noe som ikke alltid blir brukt.

På laboratoriet blir prøvene satt til sentrifugering og sortert etter prioritering og type. Her blir også resultatene fra blodsukkermålingene lagt inn i Uni-Lab. Blodprøvene blir fordelt på de ulike laboratoriene etter hvilke analyser som skal gjøres. Prøven fra vår pasient blir sendt inn på laboratoriet der de måler hemoglobininnhold i blodet. Analysemaskinen her har toveis kommunikasjon mot Uni-Lab og skanner barkoden på prøveglasset automatisk. Analysen blir gjort i maskinen, og resultatene blir lagret i Uni-Lab. Til slutt blir resultatene sett over av bioingeniøren og frigitt slik at de overføres til DIPS.

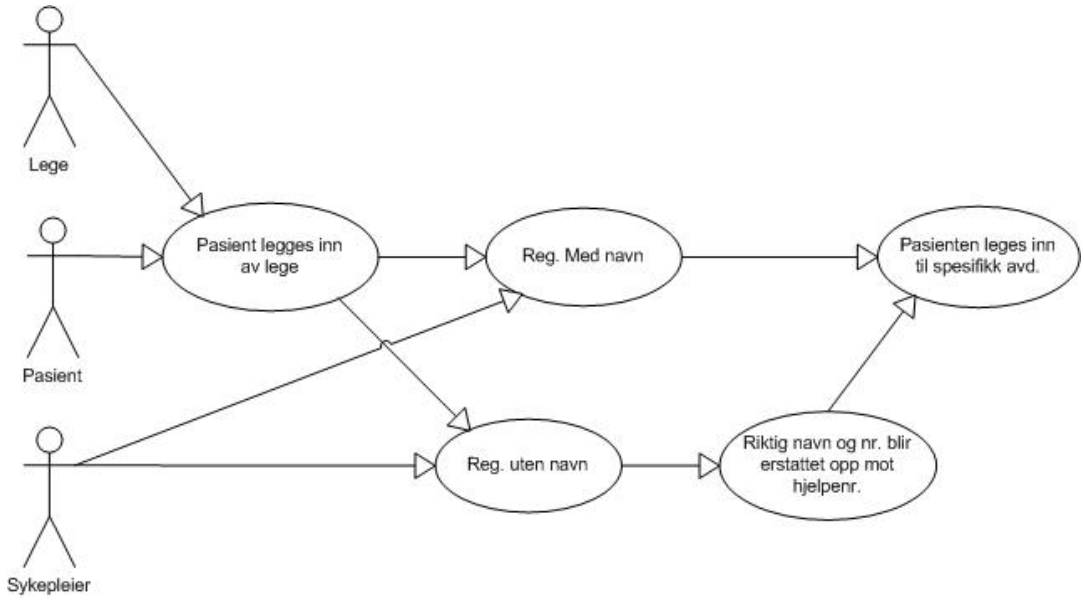
Etter at prøvene er analysert kan legen se resultatene på sin egen PC i DIPS. Dette gjøres i dag på en fastmontert PC. Ut fra disse resultatene kan legen velge ut riktige medisiner og dosering slik at pasienten får riktig behandling og til slutt skrives ut.

5.2. Evaluering av dagens arbeidsflyt

Dagens arbeidsflyt ved sykehuset virker innarbeidet, og kan for mange sees på som den beste løsningen. På den annen side kan det virke som de ansatte er åpne for nye løsninger og måter å gjøre ting på. Vi ønsker å se på hvordan en teknologi som RFID kan brukes til å eventuelt forbedre og øke kvalitetssikringen ved dagens rutiner. Derfor er det viktig å studere dagens rutiner og peke ut enkelte punkter hvor ny teknologi kan bidra med noe.

5.2.1. Rutine ved innleggelse

Ved innleggelse på sykehuset blir pasienten som oftest registrert med sin riktige identitet som består av navn og personnummer. I de tilfellene hvor dette ikke er kjent, slik som i tilfellet beskrevet over, brukes et midlertidig K-nummer. Dette vises i use-case diagrammet i Figur 5-1.



Figur 5-1 Use-case diagram over innleggelse av pasient

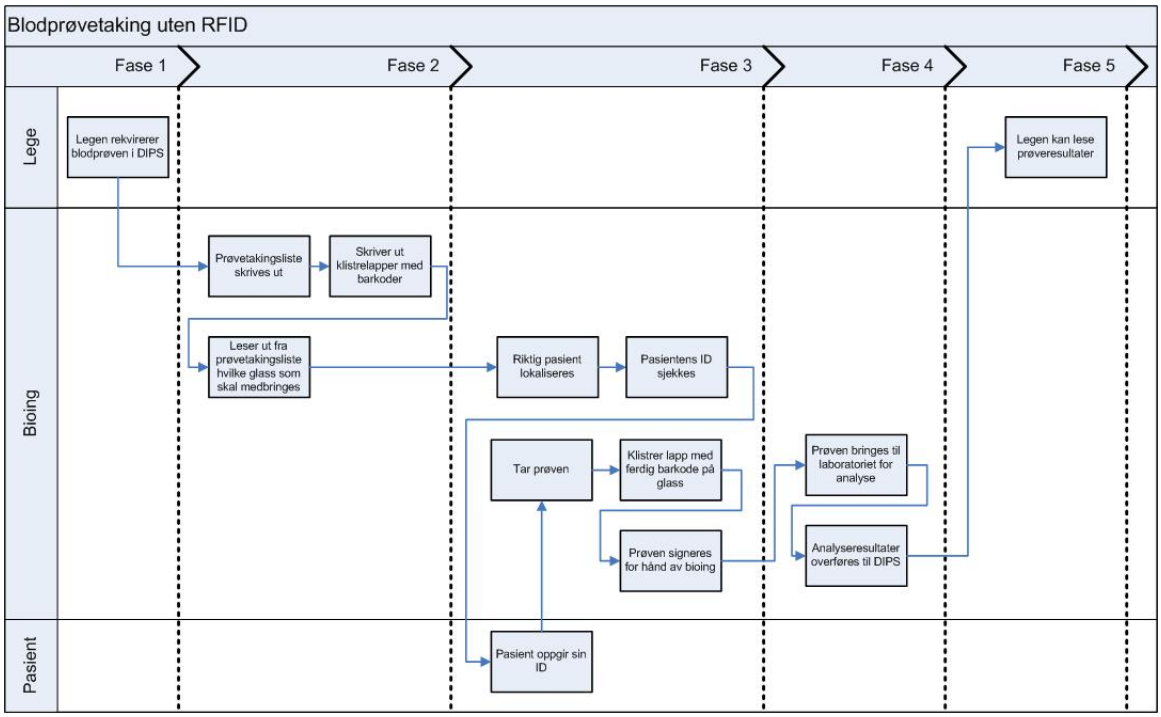
Som det kom frem under gjennomgang av vår case tidligere, kan det oppstå problemer dersom prøver er til analyse ved laboratoriet mens pasientens identitet endres fra K-nummer til korrekt navn og personnummer. Når legen lager en ny rekvisisjon i DIPS får denne et eget DIPS nummer. Når K-nummeret blir erstattet med pasientens riktige personnummer, blir rekvisisjonen flyttet over til denne identiteten. Problemet oppstår trolig på grunn av at dette DIPS nummeret henger sammen med pasientens identitet. Når prøveresultatene er klare fra laboratoriet og skal overføres tilbake fra Uni-Lab til DIPS, finnes ikke lenger den pasientidentiteten som ble registrert på prøven. Dette fordi pasienten har byttet fra K-nummer til personnummer i DIPS.

5.2.2. Rutine ved prøvetaking

Det er flere ulike typer prøver som blir analysert ved bio-laboratoriet. I tillegg til de prøvene som blir tatt av inneliggende pasienter, blir noen prøver tilsendt fra legekontorer i distriktet og noen blir tatt av polikliniske pasienter som er innom sykehuset på dagtid. Det er mange manuelle rutiner i forbindelse med disse prøvene, men vi har valgt å konsentrere oss om de prøvene som blir tatt av inneliggende pasienter.

Prøver som skal taes av inneliggende pasienter ved sykehuset, blir normalt rekvirert via DIPS. Legen kan legge inn en rekvisisjon elektronisk fra sin PC. Rekvisisjonen blir merket med prioritering og automatisk overført til Uni-Lab. Før bioingeniørene skal ut til avdelingene og ta prøver, blir en prøvetakingsliste skrevet ut fra Uni-Lab. Denne viser hvor de ulike pasientene ligger og hvilke typer prøver som skal taes. I tillegg skrives det ut ferdige etiketter som skal klistres på prøveglassene. Disse etikettene inneholder et lab-nummer, fødselsnummer, navn, rekvirerende lege og hvilken maskin prøven skal behandles på, samt en barkode. Bioingeniøren går ut til pasienten for å ta prøven. For å verifisere at det er riktig pasient blir pasientens identitet sjekket ved å spørre om navn og personnummer, samt å sjekke armbåndet til pasienten. Etter at prøven er tatt må bioingeniøren finne den riktige klistrelappen og klistre denne på prøveglasset. Det å klistre riktig lapp på riktig glass er en meget viktig prosedyre. Følgene av feilmerking kan være kritisk for pasienten, siden det kan føre til feilbehandling. Til slutt signerer bioingeniøren glasset med penn. Etter at glasset er merket vil muligheten for at feil kan oppstå være relativt liten. Glassene sentrifugeres og fordeles på de ulike laboratoriene. Det eneste stedet hvor det kan oppstå problemer under analysefasen er når analyseresultatene blir

oversendt til DIPS og pasienten har byttet identitet fra K-nummer til korrekt ID, slik som vi har beskrevet tidligere. Figur 5-2 viser et skjema over arbeidsflyten under prøvetaking slik den er i dag. Den gir et helhetlig bilde av hele arbeidsprosessen under en prøvetaking, og er delt opp i ulike faser for lettere å kunne skille de ulike prosessene fra hverandre.



Figur 5-2 Flytskjemabeskrivelse av blodprøvetaking uten RFID

6. Koordinering mot sykehuset

For å underbygge metoden Contextual Design, har vi i forkant av utviklingen av demonstratoren kvalitetssikret vår oppfatning av de arbeidsprosessene som vi har gjennomgått. På den måten sikrer vi at de valgene vi tar videre i utviklingen er i henhold til de forventningene og krav bioingeniørene har til systemet. Ved hjelp av den informasjonen vi har samlet inn ved sykehuset har vi laget et arbeidsflytskjema som beskriver arbeidsprosessene slik vi har oppfattet dem. Ved å konsultere bioingeniørene med dette, får vi bekreftet/avkreftet hvorvidt vår oppfattning er riktig. I tillegg la vi frem et utkast til ny løsning med ny arbeidsflyt og funksjonalitet. I følge modellen for Contextual Design (User Enviornment), vil det å innlemme bioingeniørene i prosessen som danner grunnlaget for det nye systemet, hjelpe oss til å fokusere på hva systemet gjør og ikke så mye på brukergrensesnitt og implementasjon. Ved å få tilbakemelding på hvordan bioingeniørene ser for seg det nye systemet, blir det lettere for oss som utviklere og tilpasse systemet på en best mulig måte. I tillegg har også bioingeniørene mulighet til sette fingeren på det de mener er viktig, og komme med nye ideer og innspill.

6.1. Resultat av første oppfølgingsmøte

Det var flere punkter som kom frem under det konsulterende møtet vi hadde med sykehuset. Nedenfor er de viktigste momentene som kom opp under møtet presentert.

6.1.1. Oppdeling av prøvetakingslista

Dersom en skal bruke en PDA til å laste ned en digital prøvetakingsliste før prøverunden, vil det være et behov for å kunne dele opp denne lista slik at de ulike prøvene kan fordeles blant flere bioingeniører. Dette mener vi å kunne løse ved å lage programvaren til den håndholdte enheten på en slik måte at bioingeniørene kan se hvilke prøver som andre tar. De kan ut fra dette velge de prøvene de selv ønsker å ta. Det vil dermed være mulig å dele opp prøvetakingslista blant flere bioingeniører. I tillegg vil det i følge bioingeniørene være behov for at det angis prioriteringsstatus på prøvene og samtidig kunne se hvilke prøver som er blitt behandlet. Bakgrunnen for dette er at det kan være opptil 15 bioingeniører som jobber samtidig med prøvetaking. Dette er noe vi mener kan løses ved å legge inn et statusfelt for prøven. Dette feltet skal vise om prøven er valgt av en prøvetaker, om den er til analyse eller om den ikke er gjort noe med i det hele tatt.

6.1.2. Behov for visuell identifisering av prøveglassene

Med identifisering av prøveglassene ved hjelp av RFID, mener bioingeniørene at det fortsatt vil være behov for en visuell identifisering av prøveglassene. I deres arbeidssituasjon er de avhengige av å kunne lese på glasset hva det inneholder og hvilke analyser som skal taes av prøven uten å måtte lese av en RFID-brikke. Ved andre og større laboratorier er flere av arbeidsprosedyrene automatisert, og vi ser for oss derfor at dette behovet ikke er tilsvarende ved alle laboratorier. Vi har likevel ikke mulighet til å utrede dette noe nærmere og vil derfor forholde oss til det utstyret som finnes og de arbeidsprosedyrene som gjennomføres ved laboratoriet ved sykehuset i Arendal. Vi ser for oss at merking av prøveglassene skjer tilsvarende som i dag med klistring av etiketter på glassene. Merkelappene som blir brukt i dag identifiserer glassene ved hjelp av barkoder i tillegg til visuell informasjon. De merkelappene vi ser for oss skal benyttes i det nye systemet inneholder en ”tom” RFID-brikke, i tilegg til nødvendig visuell informasjon. Denne brikken erstatter dagens barkode. Resultatet blir at den visuelle identifiseringen og identiteten som ligger i RFID-brikken er uavhengige av hverandre. Dette fører til at det blir lettere å kvalitetssikre arbeidsprosedyrene, noe vi kommer nærmere inn på i neste punkt.

6.1.3. Kvalitetssikring av identifisering

Når bioingeniøren er ved pasienten, er det viktig å verifisere at en står ovenfor den riktige pasienten. Deretter er det viktig å få knyttet identiteten på glasset opp mot pasientens identitet, og til slutt verifisere hvem som har tatt prøven. RFID-brikker på prøveglassene gjør at bioingeniøren gir prøven en identitet, først etter at prøven er tatt. Dette bør kunne minimalisere faren for at glasset blir merket med feil identitet. Rutinen av den visuelle merkingen av glasset vil derimot ha tilsvarende risiko for feil som i dag. Dersom det skulle bli klistret feil lapp på et glass vil ikke identiteten på brikken og det som står skrevet på lappen stemme over ens, og det må vurderes om prøven skal taes på nytt. Tilbakemeldingen vi fikk fra sykehuset var at dette er en stor forbedring i forhold til dagens situasjon, hvor det ikke er mulig å oppdage slike feil. Slik det fungerer i dag er det et stort forbedringspotensial når det gjelder signering av prøver, siden dette skjer ved at bioingeniøren signerer prøveglassene for hånd. Med dagens prosedyrer hender det at signering blir glemt. Ved innføring av en ny, digital metode for signering av prøver bør dette kunne øke kvalitetssikringen. Spesielt ved å legge inn en ”sperre” i programvaren som gjør at det ikke er mulig å gå videre uten å signere prøven. Bioingeniørene mente også at dette ville være en god løsning.

6.1.4. Integrering mot legekontorene

Det kom frem under møtet at dagens datasystem på laboratoriet vil gjennomgå en oppgradering i den kommende tiden, men det er enda uklart hva dette innebærer. Mulig kan oppgraderingen føre til at det blir enklere å implementere et RFID-system. Det ble også nevnt at det ville være ideelt å integrere legekontorene i distriktene i det samme datasystemet som benyttes ved laboratoriet. Dersom legekontorene kunne merke de prøvene som blir sendt inn til sykehuset med en RFID-basert merking, ville dette kunne forenkle arbeidsprosessen betraktelig. Med et felles datasystem og tilsvarende håndholdte enheter ute hos legekontorene har ledelsen ved laboratoriet stor tro på at det kan effektivisere arbeidet ved mottak av prøver fra legekontorene siden dette i dag er en tidkrevende og tungvinn prosess. Dette er imidlertid ikke noe vi har fokusert på i vår oppgave, siden vi har begrenset oss til prøver som blir tatt ved sykehuset.

7. Innføring av ny identifikasjonsteknologi

I denne delen tar vi for oss hvordan den nye RFID-teknologien kan innføres i forbindelse med pasientidentifisering og prøvetaking. Vi foreslår hvordan et slikt system er tenkt å fungere, samt hvilke komponenter som trengs. I tillegg vil vi peke på krav til det utstyret som skal benyttes og komme med forslag til konkrete komponenter.

7.1. Helhetlig løsning

Vi vil først se på hvilke komponenter som er nødvendig for å kunne innføre et slikt system på et sykehus.

- Pasienten får et armbånd som inneholder en RFID-brikke hvor informasjon om pasientens identitet kan lagres.
- Til merking av prøveglassene brukes klistrelappene med små RFID-brikker som festes på prøveglassene. Her vil det i tillegg være visuell informasjon om prøvens innhold.
- Bioingeniører og leger bærer ID-kort som inneholder RFID-brikke med informasjon om den ansattes identitet.
- En håndholdt PDA med en RFID-leser som kan lese fra og skrive til brikker. Denne enheten må også ha mulighet til å kommunisere via trådløst nett (WLAN) slik at den kan utveksle informasjon fra databaser som DIPS, Uni-Lab eller andre.
- En skriver som kan skrive visuell informasjon på klistrelapper RFID-brikker.
- Analysemaskinene må ha påmonterte RFID-lesere. Disse vil ha samme funksjon som strekkodeleserne virker i dag.
- Et godt utbygd trådløst nett ved sykehuset.

Ved innleggelse blir alle pasienter utstyrt med et armbånd som inneholder en RFID-brikke. I denne brikken vil det være mulig å lagre et identitetsnummer som refererer til pasientens personlige data. På armbåndet skal det stå navn og personnummer på samme måte som i dag, slik at dette vil være leselig. Ved hjelp av dette armbåndet er det lettere å identifisere pasienter uansett om de sover, er i narkose eller er vanskelige å kommunisere med.

Før bioingeniøren går ut til pasienten, blir en liste over de prøver som skal taes valgt ut og lastet inn på en *håndholdt PDA* via trådløst nett. Ute hos pasienten brukes den håndholdte enheten til å identifisere pasienten ved hjelp av en integrert RFID-leser. Man vil da være sikker på at det er riktig pasient som det blir tatt prøve av. Etter at pasientens armbånd er skannet vil en del informasjon om pasienten komme opp på PDA'en.

I forbindelse med prøvetaking ser vi for oss en løsning hvor klistrelapper med RFID-brikker er festet på glassene. Siden bioingeniørene ønsker å ha visuell merking på prøveglasset, mener vi at den beste løsningen er en kombinert lapp med visuell informasjon og en RFID-brikke. Det finnes også prøveglass med RFID-brikker støpt inn i glasset, men disse er foreløpig kun på utviklingsstadiet. Etter at prøven er tatt blir det skrevet en identitet til brikken på glasset. Dette gjør at det vil være to uavhengige identiteter på glasset.

Etter at prøven er tatt, bruker bioingeniøren sitt eget ID-kort til å signere prøven elektronisk, noe som vil gjøre det lettere å spore opp hvem som har tatt prøven dersom det skulle være behov for det.

På analysemaskinene festes det små RFID-lesere med liten rekkevidde som leser brikken på glasset i det de går inn til analyse på samme måte som det gjøres med barkoder i dag.

7.2. Case

For å se hvordan de ulike prosedyrene kan gjennomføres ved bruk av ny teknologi kan vi bruke samme scenarioet som i kapittel 5.1.

Sykehuset får inn melding fra AMK om at en eldre mann er funnet bevisstløs i Arendal sentrum. Ingen ID er funnet på mannen.

Når pasienten ankommer sykehuset blir han registrert med et *K-nummer* i stedet for personnummer, siden identiteten til mannen er ukjent. Pasienten vil også få et armbånd med RFID-brikke hvor det lagres et eget *RFID-nummer*. Etter ankomst ønsker legen at en blodprøve skal bil tatt av pasienten og det blir rekvirert en *straks-prøve* via DIPS. Ved hjelp av den håndholdte enheten velger bioingeniøren den aktuelle pasienten og skriver ut merkelapper som skal festes på prøveglassene. Disse lappene har synlig informasjon om prøven og pasienten, som i dette tilfellet er et K-nummer. I tillegg er det festet en ”tom” RFID-brikke på lappen som det skal lagres informasjon på etter at prøven er tatt.

Bioingeniøren går ut til pasienten og skanner pasientens armbånd. Pasientens personopplysninger, som foreløpig kun er et K-nummer kommer opp på den håndholdte enheten. Prøven taes og riktig merkelapp blir festet på prøveglasset. Deretter blir det ved hjelp av den håndholdte enheten, lagret informasjon i RFID-brikken. Pasientens identitet blir her knyttet sammen med prøvens RFID-nummer. Til slutt skanner bioingeniøren sitt eget ID-kort for å signere prøven digitalt. Dato og tidspunkt blir også automatisk lagret, og prøvetakingen avsluttes. All informasjon blir lagret fortløpende i en database via trådløst nettverk (WLAN). Blodprøven blir fraktet inn til laboratoriet for sentrifugering og analyse. Samtidig får pasienten oksygen og kommer etter hvert til seg selv. Riktig personalia blir etter hvert funnet og pårørende blir varslet. K-nummeret i DIPS blir byttet ut med riktig personnummer og riktig personalia blir fylt inn. Pasienten får et nytt armbånd med samme RFID-nummer, men med oppdaterte personopplysninger skrevet på. På laboratoriet vil analysemaskinene ha RFID-lesere som leser RFID-brikkene på prøveglassene når de går igjennom maskinen. Resultatene blir kikket over av bioingeniøren, og frigitt til DIPS. Analyseresultatene blir knyttet opp mot identiteten på pasientens RFID-nummer og ikke K-nummer eller personnummer som kan skape problemer. Etter at pasientens tilstand har stabilisert seg blir han overflyttet til en sengepost for å ligge på sykehuset over natten. Informasjon om hvilken avdeling og hvilket rom pasienten befinner seg på blir oppdatert i DIPS. Det blir samtidig rekvirert en *rutine-prøve*.

Klokken 08:00 neste morgen gjør bioingeniøren seg klar til morgenrunden. Den håndholdte enheten viser hvilke pasienter som det skal taes prøver av, og bioingeniøren kan velge ut de pasientene han eller hun ønsker å ta. Før bioingeniøren går ut til pasienten, skrives det ut klistrelapper til prøveglassene med ”tomme” RFID-brikker. Her vil det også være mulig å få opp hvor mange glass av hver type som bioingeniøren må ha med seg ut på prøvetakingsrunden. Når bioingeniøren ankommer vår pasient, blir pasientens armbånd skannet for å bekrefte pasientens identitet. All informasjon om pasienten kommer opp på den håndholdte enheten, inkludert hvilke typer prøver som skal taes. Prøvene blir tatt og merket med riktig klistrelapp. Ved hjelp av den håndholdte enheten skrives informasjon til brikken på glasset, som knyttes sammen med pasientens identitet i databasen. Til slutt signerer bioingeniøren prøven med sin egen brikke og prøven får en digital signatur. I tillegg blir dato og tidspunkt for når prøven er tatt lagret automatisk. Først når prøven er signert kan bioingeniøren gå videre til neste pasient.

Når bioingeniøren returnerer til laboratoriet, blir prøvene satt til sentrifugering og sendt inn til analysemaskinen. I det prøven går inn i analysemaskinen blir prøvens RFID-brikke skannet og analyseresultatene automatisk knyttet opp mot identiteten i brikken. Analyseresultatene blir overført til Uni-Lab før de blir kontrollert og frigitt til DIPS av bioingeniøren.

Ute hos pasienten bruker legen en håndholdt enhet hvor det er mulig å få opp pasientens journal med prøveresultater. Det vil være mulig å "bla frem" til riktig pasientjournal ved å skanne pasientens armbånd. Vår pasient får riktig medisinering og kan etter en stund skrives ut fra sykehuset.

7.3. Evaluering av ny arbeidsflyt

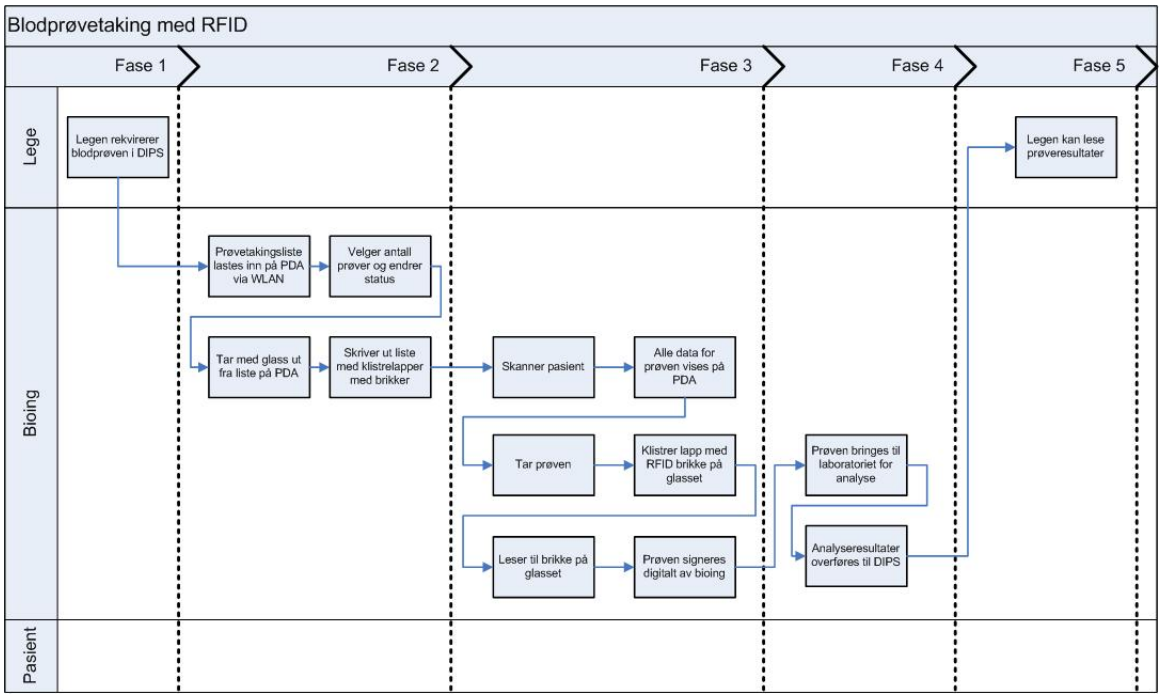
I scenarioet over ble det beskrevet hvordan den nye teknologien er tenkt å taes i bruk. Vi vil nå se på hvordan dagens rutiner må endres.

7.3.1. Rutine ved innleggelse

Dagens rutiner for innleggelse ble omtalt i avsnitt 5.2.1. Ved innføring av en ny identifiseringsmetode på pasientene, må rutinene i forbindelse med innleggelse endres noe. Pasientens armbånd må inneholde en RFID-brikke med en unik identitet, i tillegg til leselig navn og personnummer. Ved ukjent identitet på pasienten kan prøver som blir tatt av pasienten knyttes opp mot identiteten som er lagret i RFID-brikken, i stedet for K-nummer. Når pasientens identitet blir funnet, vil brikkens identitetsnummer forbli uendret. De problemene som kan oppstå ved prøvetaking av pasienter uten kjent identitet, kan dermed elimineres. Dette fordi identiteten til RFID-brikken vil være uavhengig av pasientens navn og personnummer.

7.3.2. Rutine ved prøvetaking

Scenarioet som er beskrevet over viser hvordan vi ser for oss at merking av prøveglass og identifisering av pasienter skal foregå. Figur 7-1 beskriver bioingeniørens arbeidsflyt ytterligere. Der vises de ulike arbeidsprosessene under prøvetaking og analyse.



Figur 7-1 Arbeidsflyt ved prøvetaking med bruk av RFID

Fase 1 vil være slik den er i dag. Legen rekvirerer prøver elektronisk i pasientsystemet DIPS. I Fase 2 bruker bioingeniøren sin håndholdte PDA til å laste ned en prøvetakingsliste via trådløst nettverk (WLAN). Bioingeniøren velger de pasientene han eller hun ønsker å ta prøver av, og status på disse prøvene endres slik at ingen andre kan velge de samme prøvene. Siden dette gjøres via trådløst nettverk er man ikke avhengig av å gjøre disse valgene fra laboratoriet. Før prøvetaker går ut til pasienten må det skrives ut klistrelapper med tomme RFID-brikker på. I tillegg må prøvetakeren ta med seg nok prøveglass til alle prøvene som skal taes. En liste over hvor mange glass av hver type kan vises på skjermen etter at prøvene er valgt.

Fase 3 viser det som skjer ute hos pasienten. For å verifisere identiteten til pasienten skannes pasientens armbånd ved hjelp av skanneren i den håndholdte enheten. Det vil fortsatt være viktig å opprettholde pasientkontakten ved å spørre om pasientens identitet, hvis mulig. Prøven taes av pasienten og prøveglassene merkes med riktige klistrelapper. For å avslutte prøvetakingen skrives en identitet til RFID-brikken på glasset. Dermed har man to uavhengige identiteter på glasset. Det er også mulig å skrive annen informasjon om prøven til brikken. Dersom det blir klistret feil lapp på et glass vil dette kunne oppdages ved at identiteten som er skrevet på lappen og identiteten på brikken ikke er den samme. Man må da vurdere om prøven skal taes på nytt. Det er i dag ikke lett å oppdage slike typer feilmerking. Prøvens identitet og pasientens identitet blir knyttet sammen i en database i tillegg til annen informasjon om prøven. For å avslutte prøven må prøvetakeren signere glasset elektronisk med sitt eget ID-kort. Dermed blir bioingeniørens identitet, dato og tidspunkt lagret i databasen. Dagens system er basert på at prøveglassene signeres for hånd, noe som av og til glemmes. Ved å legge inn en sperre i programvaren kan man sikre at prøven blir signert og det vil være lettere å spore opp hvem som har tatt den aktuelle prøven dersom det skulle være uklarheter rundt prøvetakingen.

I Fase 4 på arbeidsflytdiagrammet blir prøven sentrifugert og analysert inne på laboratoriet. Disse prosedyrene vil i stor grad foregå på samme måte som i dag. Den eneste forskjellen vil være at analysemaskinene må ha RFID-lesere påmontert der det i dag sitter strekkodelesere. Etter at prøvene er analysert blir analyseresultatene kontrollert og frigitt til DIPS, hvor legen kan lese disse.

Med de rutinene som brukes i dag finnes det ingen måter å oppdage om det skulle bli klistret feil lapp på et glass. Ved å skrive en identitet til glasset etter at prøven er tatt vil kvalitetssikringen kunne økes, og faren for feil reduseres. Det vil også være lettere å oppdage dersom en feil har oppstått. En ytterligere faktor som kan bidra til økt kvalitetssikring er identifisering av pasienter ved hjelp av pasientens brikke. Dersom det ikke er mulig å kommunisere med pasienten, må man med dagens system lese teksten som står skrevet på pasientens armbånd.

7.4. Krav til ny teknologiløsning

For at en teknologiløsning skal kunne være aktuell å benytte, må systemet innfri brukerens krav til brukervennlighet. For å oppnå dette må komponentene som brukes være godt egnet til formålet. De må i tillegg tilfredsstille krav fra Datatilsynet og Post- og teletilsynet. Vi har derfor sett på noen krav som bør stilles til utstyret som skal brukes.

7.4.1. Transponder

Transponderne som blir festet på håndleddet på pasienten, bør ha en leseavstand som ikke er lengre en 1 m. Dette for at det ikke skal være mulig å skanne feil armbånd. Når det

gjelder avstanden mellom transponderen på prøveglasset og leseren kan avstanden være kortere. Transponderen bør også ha autentiseringsegenskaper.

De viktigste kravene som transponderen bør tilfredsstille er:

- Leseavstanden mellom transponderen på pasienten og leseren bør ikke være for stor (0.1m – 1.0 m)
- Transponderen må kunne festes lett på armbåndet til pasienten og i tillegg kunne kombineres med en visuell merking
- Transponderen som skal festes på prøveglasset skal kunne lett klistres på glasset, og ha en visuell merking.
- Transponderen må ha mulighet til å kunne lagre data
- Den må tilfredsstille kravene fra Datatilsynet og Post- og teletilsynet.

7.4.2. Håndholdt enhet

Den håndholdte enheten skal kunne laste ned prøvelistene fra eksisterende datasystem ved sykehuset. Dette innebærer at den må ha trådløs kommunikasjon mot datasystemet ved hjelp av WLAN. Den skal ha en brukervennlig skjerm med tilfredsstilende størrelse, og den skal i tillegg kunne kommunisere med RFID-transpondere.

De viktigste kravene som stilles til den håndholdte enheten er:

- Brukervennlig
- Tilfredsstillende skjermstørrelse
- Tilpasset til å benyttes på et sykehus
- Innebyde kommunikasjonsmuligheter for RFID og WLAN, eller mulighet for tilkobling av slikt utstyr.
- Tilfredsstille krav til Datatilsynet og Post- og teletilsynet.

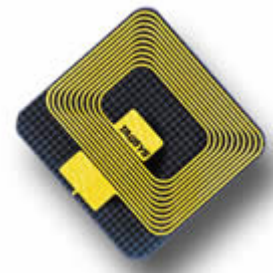
7.5. Forslag til komponenter

Ut fra de krav vårt utstyr må tilfredsstille, mener vi at såkalte *smart labels* er en godt valg. Den typen som er best egnet, er full dupleks HF-transpondere med autentiseringsegenskaper. Funksjonaliteten til disse er forklart i kapittel 2 og 3. Disse brikkene har en bærefrekvens på 13,56 MHz. I forskriften om tillatt bruk av frekvenser, stiller Post og Teletilsynet krav til utstyr som har innebygd radiosendere og mottakere [7]. I følge § 19 om induktive frekvenser, er frekvensbåndet 13,553 – 13,567 kHz tillatt brukt. Maksimal tillatt feltstyrke er 42 dB μA/m ved 10 meters avstand [7]. Utover dette er det sykehusene selv som avgjør hvilket utstyr som skal tillates brukt.

For å gi et innblikk i hvilke komponenter som finnes på markedet i dag, har vi satt opp ulike forslag til utstyr. Vi har også forsøkt å velge ut de komponentene som er best tilpasset våre krav. Utgangspunktet for de ulke forslagene er de ulike produsentenes og leverandørenes hjemmesider. Vi har med andre ord ikke testet ut de ulike komponentene i praksis, og baserer derfor valget på det vi kunne lese ut av de ulike spesifikasjonene.

7.5.1. Transpondere

Alternativ 1:
Tagsys Ario RFID-transpondere har vært på markedet siden 1995, se Figur 7-2. Transponderne er spesialdesignet for å tåle røft bruk og er i dag benyttet i mange sammenhenger i industrien verden over. Frekvensen som benyttes er 13,56 MHz. De kan lett integreres i utstyr og spesifikasjonen tilfresstiller de fleste kravene vi har satt, men leseavstanden på 15-20 cm er noe kort i forhold til det vi ønsker oss. Vi har heller ikke fått konstatert hvorvidt den kan benyttes sammen med en skriver som lager klistrelapper, eller om den har krypteringsegenskaper.



Figur 7-2 TAGSYS ARIO™ RFID Tags [29]

Alternativ 2:
Produsenten Maxell har kommet langt i utviklingen av 13.56 MHz RFID transpondere. De har klart å utvikle transpondere som både har stor lagringskapasitet (opptil 4Kb), og som ikke er større enn 2.5 mm i diameter x 2. 5 mm tykk, se Figur 7-3. Grunnen til at de har klart å lage de så små, er at de har bygget antennen inn i mikrobrikken. Dette resulterer også i at leseavstanden ikke blir lengre enn 1 – 3 mm, noe som er for kort. Til tross for leseavstanden, mener Maxell at transponderen egner seg godt til bruk i prøveglass ved at den støpes inn i bunnen [20]. Kostnadsrammen på denne transponderen ligger noe over andre typer, men Maxell mener at prisen kommer til å ligge under $1 [9]. Transponderen har autentiseringsegenskaper, men støtter ikke kryptering.

Figur 7-3 RFID-brikke fra Maxell [30]

Alternativ 3:
I-CODE transponderne fra Philips [31] bruker 13,56 MHz som bærefrekvens, og er mulig å få integrert i armbåndet vi nevner senere. De kan også integreres i merkelapper som skal festes på prøveglassene. Transponderne har innebygde autentiseringsegenskaper, men støtter ikke kryptering av data. Dersom vi skal se bort fra kryptering mellom leser og transponder, vil denne brikken være meget godt egnet til vårt formål.

Vi har også sett på en annen transponder fra Philips som kalles Mifare DESFire. Denne støtter både kryptering og autentiserting [28]. Denne komponenten blir vanligvis levert innebygd i kontaktløse smartkort. Det er imidlertid ikke verifisert hvorvidt denne komponenten kan leveres som en label.

7.5.2. Printer

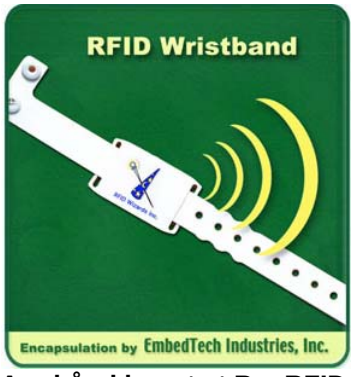
RFID-printeren R 402 fra Zebra er godt tilpasset til de øvrige komponentene, se Figur 7-4. RFID-printeren kan både lese og skrive til transponderen, og samtidig skrive visuell informasjon enten det gjelder armbånd eller merkelapper på prøveglassene. Vi mener derfor denne er et godt egnet til å skrive ut armbånd og klistrelapper til prøveglass.

Figur 7-4 R 402 Printer fra Zebra Technologies [33]

7.5.3. Armbånd

Alternativ 1:

Leverandøren BuyRFID.COM selger RFID-armbånd beregnet for ulike formål [38]. Armbåndet er laget i hardplast, bruker 13,56 MHZ og innfrir våre krav til leseavstand, kommunikasjonsmuligheter og lagringskapasitet. Transponderen støtter ikke kryptering og er kan ikke benyttes sammen med en RFID-printer fra Zebra.



Figur 7-5 Armbånd levert at BuyRFID.COM [38]

Alternativ 2:

PDC Smart Compuband fra PDC er det armbåndet som er best tilpasset vårt formål, se Figur 7-6. Det er tilpasset til å fungere med en RFID-printer fra Zebra [32] og kan leveres med Philips I-CODE transpondere. Ved hjelp av RFID-printeren, kan de skrives ut både med visuell informasjon og informasjon som lagres på RFID-brikken. Utformingen er ikke helt ulik de armbåndene som blir brukt ved sykehuset i dag, og er robust nok til å benyttes i et sykehusmiljø.

Figur 7-6 PDC Smart CompuBand [32]

7.5.4. Håndholdt enhet

Recon 400 som leveres av Handheld Scandinavia AB, mener vi er et godt valg av håndholdt enhet, se Figur 7-7. Den innfrir både når det gjelder brukervennlighet, tåler vann så den kan rengjøres og ikke minst er solid nok til å tåle røft bruk. Per i dag leveres ikke denne modellen med innebygd WLAN. Dette er noe vi mener er en forutsetning for at modellen skal være aktuell. Vi har derfor vært i kontakt med leverandøren og fått bekreftet at dette er noe som vil bli integrert i de kommende modellene i løpet av året. Når det gjelder programvaren, leveres den enten med operativsystemet Microsoft CE.NET 4.1 eller PocketPC2003. Den har ikke innebygd RFID-leser. Dette må derfor kobles til via en CF-port. Under viser vi et utvalg RFID-lesere som kan passe.

Figur 7-7 Recon 400 håndholdt PDA

7.5.5. RFID-leser

Det vanligste grensesnittet for små RFID-lesere er i dag Compact Flash (CF), og vi har sett på to typer CF-lesere.

Alternativ 1:
CF-lerseren fra Omron er tilpasset til å fungere på håndholdte enheter med Compact Flash grensesnitt, se Figur 7-8. Den opererer i 13.56Mhz båndet og støtter de vanligste transponderne. Leseavstanden er fra 3-5cm, noe som er for kort.

Figur 7-8 RFID CF-leser fra Omron [34]

Alternativ 2:
Alternativet fra Syscan er det beste alternativet vi kunne finne med CF grensesnitt (se Figur 7-9). Denne RFID-leseren kan også lett integreres i en håndholdt enhet. Den støtter de fleste transpondere og en leseavstand som er mellom 5 og 10cm. Leseavstanden er noe kort i forhold til det vi hadde ønsket oss. Vi ser for oss at leseavstanden ideelt sett bure være mellom 50 – 100 cm. Ting tyder på at dette er noe produsentene ønsker å gjøre noe med [24].

Figur 7-9 RFID CF-leser fra Syscan [24]

8. Sikkerhet ved behandling av sensitive data

8.1. Håndholdt enhet

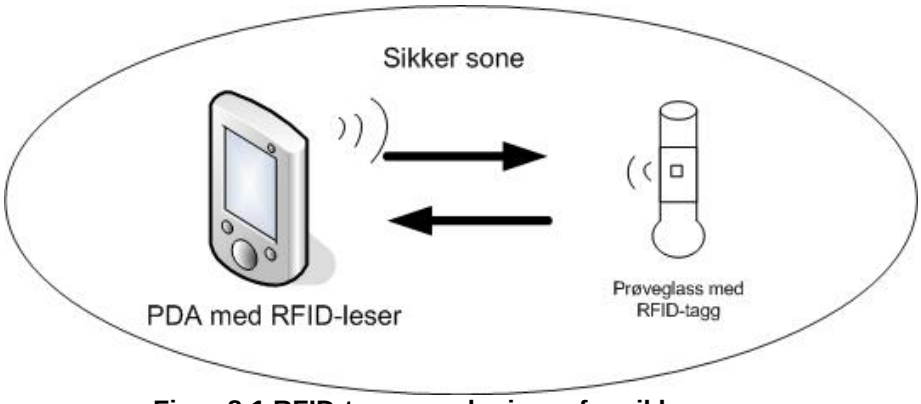
Som vi har nevnt tidligere, kan bruk av tynnklienter være et tiltak for å sikre sensitive data ved bruk av en håndholdt enhet. Da vil den håndholdte enheten kun fungere som en terminal og ingen informasjon blir lagret lokalt. I vårt tilfelle kan bruk av tynnklient by på problemer, siden vi ønsker å hente ut noe av informasjonen som ligger i sikker sone og skrive den til RFID-brikken. Når informasjon skal skrives til brikken, må dette gjøres via kommunikasjonsporten på den håndholdte enheten. Det vil si at informasjonen må mellomlagres lokalt før det sendes ut. I kapittel 3.2 har vi beskrevet ulike tiltak som må gjøres i trådløse nett for å opprettholde en tilfredsstillende sikkerhet ved behandling av sensitive data. Dersom vi ikke benytter oss av tynnklient på den håndholdte enheten, vil dette si at vi ikke kan oppfylle nivå H-D i Tabell 3-3. Dersom vi øker sikkerhetsnivået til å også gjelde nivå H-F som omfatter innføring av sikker brukerautentisering, mener vi likevel at kravene til sikkerhet for den håndholdte enheten kan opprettholdes. Sikker autentisering oppnår vi ved at brukeren benytter en form for digitalt sertifikat for å få aksess til den håndholdte enheten. Dette kan være et ID-kort som er basert på RFID-teknologi. I tillegg bør brukeren benytte seg av et passord for å kunne logge seg inn på den håndholdte enheten. Når det gjelder beskyttelse av aksesspunktene og WLAN-aksess, bør det ikke være nødvendig å endre på sikkerhetstiltakene i forhold til det som er nevnt i kapittel 3.2.

8.2. RFID-brikken

Vi ønsker å se nærmere på hvilke muligheter det er for lagring av sensitive data i selve RFID-brikken i forhold til de sikkerhetstiltak som må gjennomføres. I henhold til datatilsynets krav må det innføres tiltak i forhold til autentisering og kryptering av overføring. Disse har vi omtalt i kapittel 3.1. I vårt tilfelle er det snakk om pasientinformasjon som skal beskyttes. Det er snakk om navn, personnummer eller annen informasjon som lett kan knyttes til en bestemt person. Dersom opplysningene ikke inneholder slik informasjon, vil ikke informasjonen være sensitiv. Vi vil derfor se på to ulike alternativer for lagring av data i RFID-brikken. I det ene alternativet lagres navn eller personnummer på brikken sammen med annen data. I det andre alternativet lagrer vi et eget ID-nummer i brikken som knytter informasjonen til en bestemt pasient i en database.

8.2.1. Lagring av sensitiv informasjon i RFID-brikken

Dersom sensitive data skal overføres til RFID-brikken, må denne overføringen tilfredsstille datatilsynets krav som er minst 128 bits DES kryptering. Dette innebærer at transponderen må være på innsiden av en sikker sone, slik som vist i Figur 8-1.

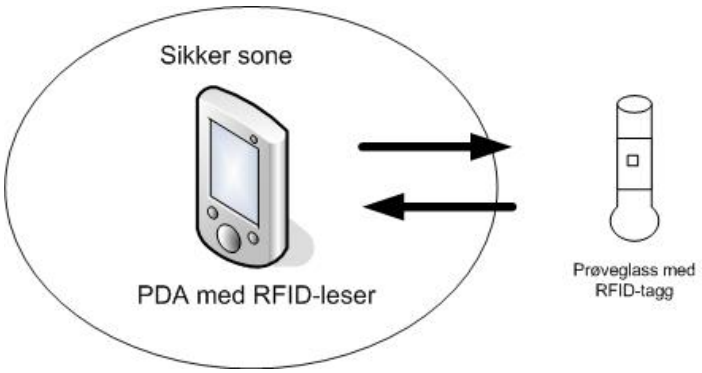


Figur 8-1 RFID-transponder innenfor sikker sone

Transponderen og den håndholdte enheten må derfor ha innebygde sikkerhetsmekanismer som sikrer autentisering og kryptering i henhold til de krav som stilles. Ved å bruke for eksempel 3DES kryptering med ulike nøkler oppnåes en kryptering på 168 bits, noe som bør være tilfredsstillende.

8.2.2. Bruk av RFID-nummer i transponderen

Ved å bruke et unikt RFID-nummer til å knytte pasientdata opp mot pasienten, bør det ikke være nødvendig med samme type sikkerhetstiltak som nevnt tidligere. Dette nummeret blir overført til transponderen når pasienten får sitt armbånd eller når bioingeniøren har tatt de ønskede prøvene. Data som navn og personnummer blir lagret i databasen, og det unike RFID-nummeret vil knytte prøven til pasienten i databasen. Et RFID-nummer vil ikke være å betegne som sensitiv informasjon så lenge det ikke er mulig å knytte dette opp mot en bestemt pasient. Uansett vil det være mulig å bruke brikken til lagring av prøvedata som for eksempel hva prøven inneholder, hvilke analyser som skal taes av prøven og hvilken analysemaskin prøven skal settes i. Siden informasjonen som er lagret på glasset ikke kan knyttes opp mot en bestemt pasient, trenger kommunikasjonen mellom PDA og transponder ikke være på innsiden av en sikker sone, slik som vist på Figur 8-2.



Figur 8-2 RFID-transponderen utenfor sikker sone

RFID-nummeret vil være prøvens identitet på linje med dagens lab-nummer. I det prøven blir rekvirert av en lege knyttes et RFID-nummer til rekvisisjonen, som senere blir skrevet til glasset. Hvor mye informasjon som lagres på brikken i tillegg til RFID-nummeret kommer an på hva som er ønskelig å kunne lese ut av glasset uten å være knyttet opp mot en database.

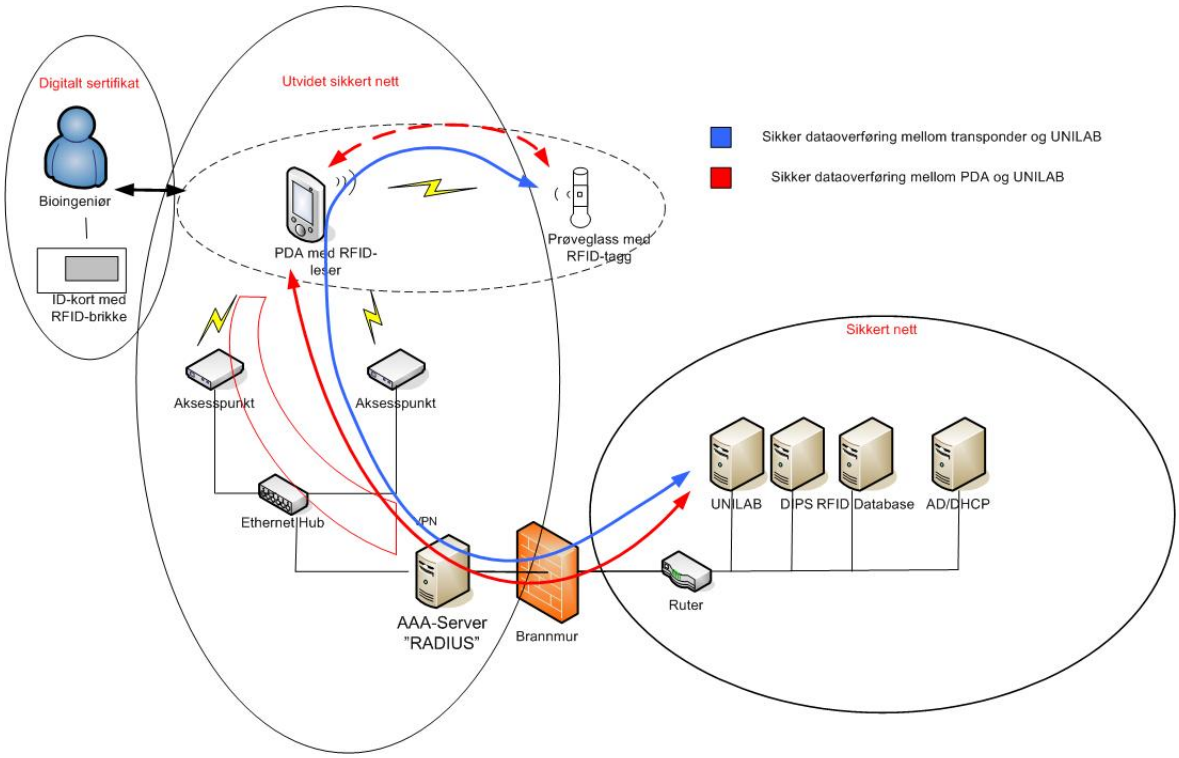
8.3. Drøfting av løsninger

Vi har nå sett på to ulike måter å lagre informasjon i RFID-brikkene på. I tillegg har vi sett på løsninger på sikkerhet ved behandling av sensitive data på en håndholdt enhet. Vi ønsker å konsentrere oss om kommunikasjonen mot RFID-brikken, siden dette er det sentrale i vår oppgave.

Ved å lagre sensitiv informasjon på transponderne kreves en utvidelse av sikkerhetssonen til også å gjelde kommunikasjonen mellom den håndholdte enheten og transponderne. Dette innebærer at det de nødvendige sikkerhetsmekanismene også må være implementert i RFID-leseren og RFID-transponderen. Philips har transpondere som tilbyr god nok kryptering. Fordelen med å lagre sensitiv informasjon i transponderen, er at datastrømmen mellom de ulike enhetene kan reduseres. Autorisert personell vil da kunne ha tilgang til ønsket informasjon direkte fra pasienten eller fra prøven uten at den håndholdte enheten alltid måtte være i kontakt med databasen. Dette kan forenkle infrastrukturen på nettverket, men krever samtidig mer avanserte brikker og lesere. Man er også avhengig av å ha god lagringskapasitet i brikkene.

Ved å unnlate å lagre sensitive data i selve brikken vil det ikke være behov for et høyt sikkerhetsnivå mellom transponderen og den håndholdte enheten. Det vil ikke være nødvendig å velge transpondere som har innebygde krypteringsmekanismer, noe som kan bidra til en lavere pris på brikkene ved innkjøp. Dette kan være en viktig faktor, siden det er snakk om et stort antall brikker. Det vil også være flere produsenter å velge mellom, siden det finnes få transpondere med krypteringsmekanismer. Dersom det ikke lagres personopplysninger i brikken, er det nødvendig å være i kontakt med en server for å kunne hente alle opplysninger om prøven. Et godt utbygd WLAN ved sykehuset er derfor en forutsetning. Dersom det lagres informasjon i brikken om hvilke analyser som skal taes av prøven, kan det enkelt kontrolleres om prøven er satt i riktig analysemaskin uten å kjøre en spørring mot databasen. Slik informasjon kan også benyttes for å få en mer effektiv logistikk.

Figur 8-3 viser en skisse over sikkerhetsarkitekturen for et trådløst nett med en håndholdt enhet. Her er sikkerhetstiltakene som er nødvendig i et trådløst nett som behandler sensitive data forsøkt skissert opp.



Figur 8-3 Helhetlig nettverkskonfigurasjon[18]

Den blå linjen viser at sensitiv informasjon blir overført fra Uni-Lab og helt ut til RFID-brikken. Kommunikasjonen mellom leser og brikke må i dette tilfellet være kryptert.

Den røde linjen viser metoden hvor sensitive data ikke blir skrevet til brikken. Her blir de sensitive dataene kun utvekslet mellom PDA og Uni-Lab. Den stiplede linjen viser at kun anonymiserte data blir skrevet til brikken. Det vil i dette tilfellet ikke være nødvendig med kryptering, men det bør være autentisering mellom leser og brikke.

9. Demonstrator

For å vise hvordan et system som bruker RFID-teknologi til merking av pasienter og blodprøver kan fungere, har vi valgt å utvikle en enkel demonstrator som inneholder de hovedfunksjonene et slikt system trenger. Systemet er tenkt kjørt på en håndholdt PDA, men siden det viste seg vanskelig å få lånt en PDA som var egnet til vårt bruk, blir demonstratoren utviklet og kjørt på en bærbar PC. Grunnlaget for prototypen er en applikasjon som ble utviklet av en gruppe i forbindelse med et prosjekt ved HIA i faget IKT 4200 høsten 2003 [5]. Dette var et prosjekt som omhandlet samme problemstilling og de hadde bygget inn noen funksjoner. Vi vil videreutvikle denne applikasjonen til en prototyp som er spesialtilpasset sykehusets rutiner og arbeidsflyt for bedre å visualisere den nye teknologiens muligheter. I dette kapittelet vil vi beskrive hvordan oppbygning og funksjonalitet i demonstratoren bør være.

9.1. Komponenter

- Syscan RFID-leser (13,56 MHz) med CF-II grensesnitt. Adapter fra CF-2 til PC-Card.
- Tag-it RFID-brikker produsert av Texas Instrument. 13,56 MHz og 2 kbits lagringskapasitet.

Figur 9-1 RFID-leser med to brikker

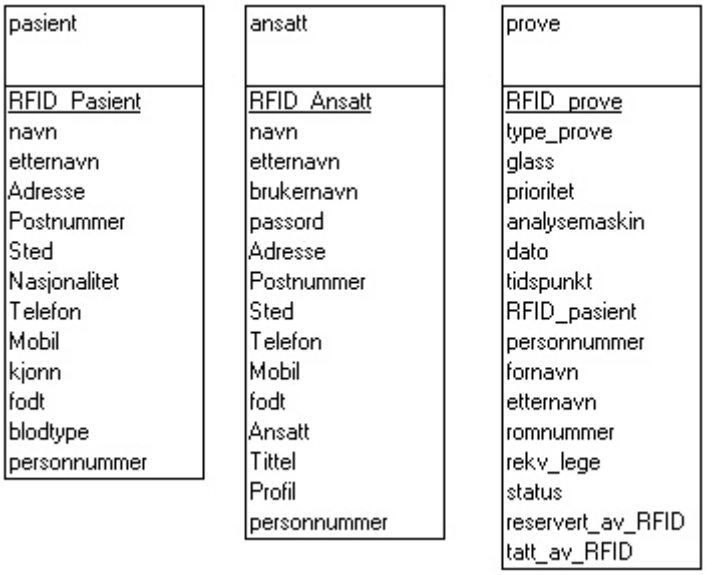
Utstyret som benyttes i demonstratoren opererer på frekvensen 13,56 MHz. Utstyret ble kjøpt inn av skolen i forbindelse med et annet prosjekt, så leseravstanden er noe mindre enn det som er ønskelig for oss. Leseravstanden på dette utstyret er kun noen få cm, så det er nødvendig å holde brikkene ganske nær leseren for å kunne lese og skrive til dem. Brikkene er også nokså store. Leseren bruker grensesnittet CF-II, og for å få denne til å passe i en bærbar PC benytter vi en adapter fra CF-II kort til PCMCIA. For å kommunisere med de ulike komponentene brukes følgende programvare:

- MySQL database
- MySQL ODBC 3.51 driver for aksessering av MySQL
- Visual Basic 6.0
- PCMCIA driver for Syscan RFID-leser (CF-reader module)

9.2. Demonstratorens oppbygging

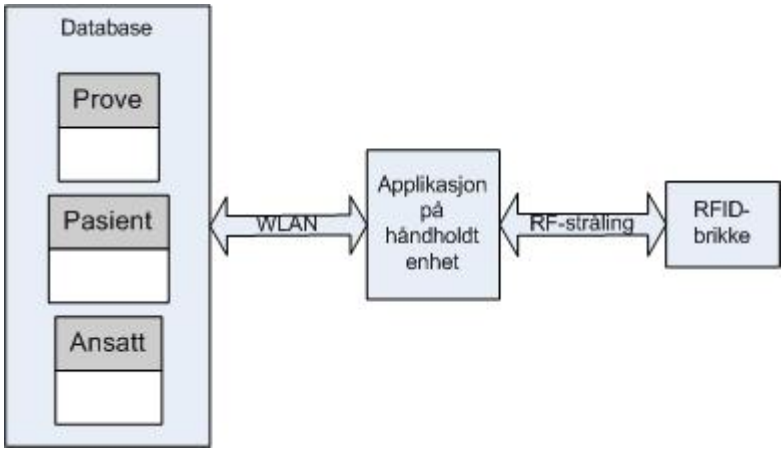
Demonstatoren er bygget opp av en Visual Basic Applikasjon og en SQL-database. SQL-databasen inneholder pasientinformasjon, informasjon om prøver og informasjon om ansatte. De ulike attributtene i databasen vises i Figur 9-2. Tabellen *prove* er manuelt generert for å simulere det laboratoriesystemet som sykehuset benytter i dag. Vi forutsetter at de dataene som ligger i denne tabellen kan hentes ut fra for eksempel Uni-Lab. De attributtene som har å gjøre med selve prøvetakingen skal fylles ut etter at

prøvene er tatt. Tabellen *pasient* skal benyttes til oppslag av pasientinformasjon, mens *ansatt* skal brukes til signering av prøver og innlogging.



Figur 9-2 Databasearkitektur for demonstratoren

Koblingen mellom MySQL og Visual Basic skal gjøres ved hjelp av en ODBC-driver. Det er ikke tatt høyde for sikker overføring av data i demonstratoren.



Figur 9-3 Skisse av systemet

Figur 9-3 viser en enkel oversikt over hvordan applikasjonen skal fungere. Hver gang applikasjonen spør om informasjon skal dette bli hentet fra SQL-serveren via trådløst nettverk. Etter at prøven er tatt skal et RFID-nummer bli skrevet til brikken på prøveglasset slik at dette får en unik identitet som dataene kan knyttes opp mot i databasen. Kommunikasjonen mot RFID-brikkene skjer med radiofrekvent stråling på 13,56 MHz.

9.3. Demonstratorens hovedfunksjoner

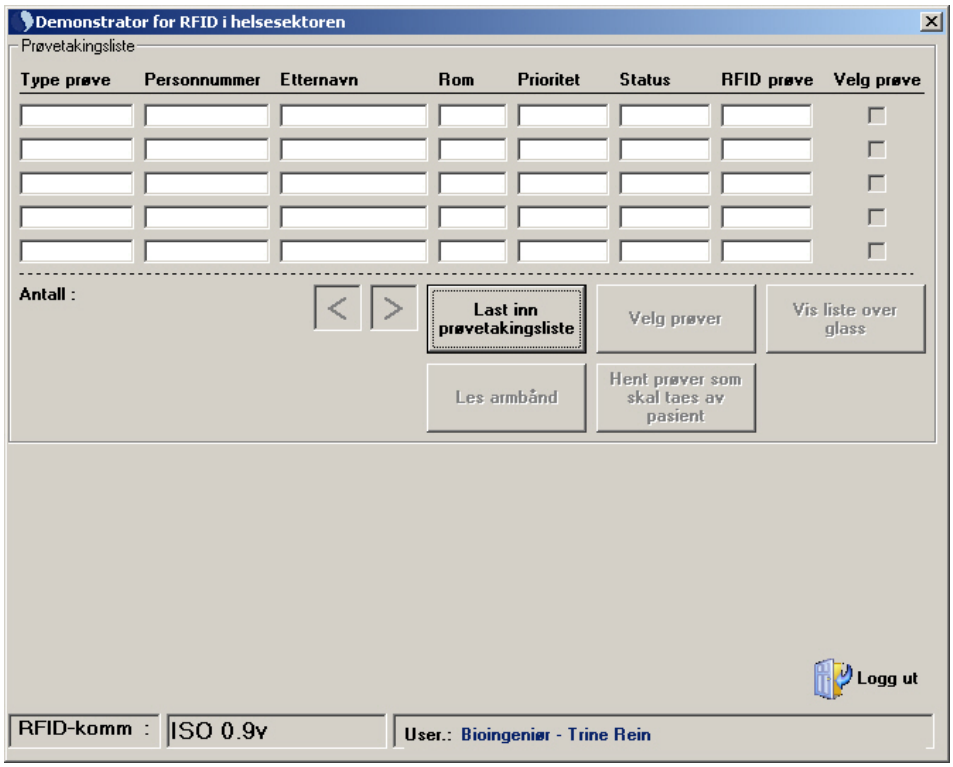
Funksjonene i demonstratoren er tenkt laget slik at den i størst mulig grad skal samsvare med prosedyrene bioingeniørene gjør i forbindelse med prøvetaking. Vi har konsentrert oss om fase 2 og 3 som ble presentert i arbeidsflytdiagrammet i Figur 7-1. De ulike funksjonene er som følger:

- Innlogging
- Nedlasting av prøveliste
- Valg av prøver
- Oversikt over glass
- Skanning av pasient
- Skriving til glass
- Signering / avslutting av prøve

Innloggingsfunksjonen på demonstratoren er tenkt todelt. Det vil være mulig å logge inn med brukernavn og passord, eller innlogging med en RFID-brikke. Brikken inneholder et nummer som samsvarer med nummeret i tabellen *ansatte* i databasen. Ved pålogging blir det sjekket om nummeret stemmer, og brukeren blir logget inn. En slik form for pålogging vil være praktisk når programmet skal kjøres på en PDA. Av sikkerhetsmessige grunner er det sannsynlig at det bør brukes en brikke som har gode egenskaper for autentisering, og gjerne et passord i tillegg. Siden vi ikke har tatt hensyn til sikkerhetskravene i denne demonstratoren, visualiserer vi denne funksjonen med en vanlig RFID-brikke uten autentisering.

Før bioingeniøren går ut til pasienten må listen over de prøver som skal taes, lastes ned på den håndholdte enheten. Videre må hver enkelt bioingeniør velge de prøvene han eller hun ønsker å ta. Som vi har sett tidligere, gjøres dette i dag ved å skrive ut en liste og deretter fordele listen mellom de som skal ta prøver. I vårt system ser vi for oss at det skal være mulig å laste inn hele prøvetakingslisten ved å klikke på en knapp. Den nødvendige informasjonen om prøvene vil bli hentet ut fra SQL-databasen og skrevet ut i et grensesnitt som viser fem og fem prøver av gangen. Det skal være mulig å bla i prøvene med piler som er plassert under. Når en bioingeniør ønsker å velge en prøve, må det krysses av i et felt bak den aktuelle prøven. Når alle de ønskelige prøvene er valgt, tenker vi at brukeren klikker på en ny knapp, og kun de prøvene som er valgt vises på skjermen. Et bilde av hvordan dette vil se ut vises i Figur 9-4.

For at bioingeniøren skal være sikker på å ha med seg nok glass av ulik type, vil vi integrere en funksjon som viser en liste over hvor mange glass av ulik type som behøves på prøvetakingsrunden.



Figur 9-4 Layout for hvordan prøvetalingslisten vil se ut.

Når et pasientarmbånd blir skannet, skal automatisk pasientdata bli hentet ut fra databasen og vist på skjermen. De prøvene som skal taes av pasienten skal komme opp i et eget vindu når bioingeniøren klikker på en knapp for å ta prøver. For å minne prøvetakeren på de ulike rutinene som skal følges, vil vi legge inn ulike meldingsbokser som kommer opp.

Etter at prøven er tatt av pasienten, skal det skrives en identitet til brikken på glasset. Et RFID-nummer vil bli skrevet til glasset, og pasientens RFID-nummer vil bli knyttet til prøven. Etter at identiteten er skrevet til glasset, vil vi legge inn en funksjon som automatisk leser glassets RFID-nummer for å kontrollere at glasset har fått riktig identitet. For å avslutte prøven, skal bioingeniøren signere prøven med sin egen brikke. I denne prosessen skal prøvetaker, dato og tidspunkt for prøvetakingen lagres i databasen, og neste prøve som skal taes dukke opp.

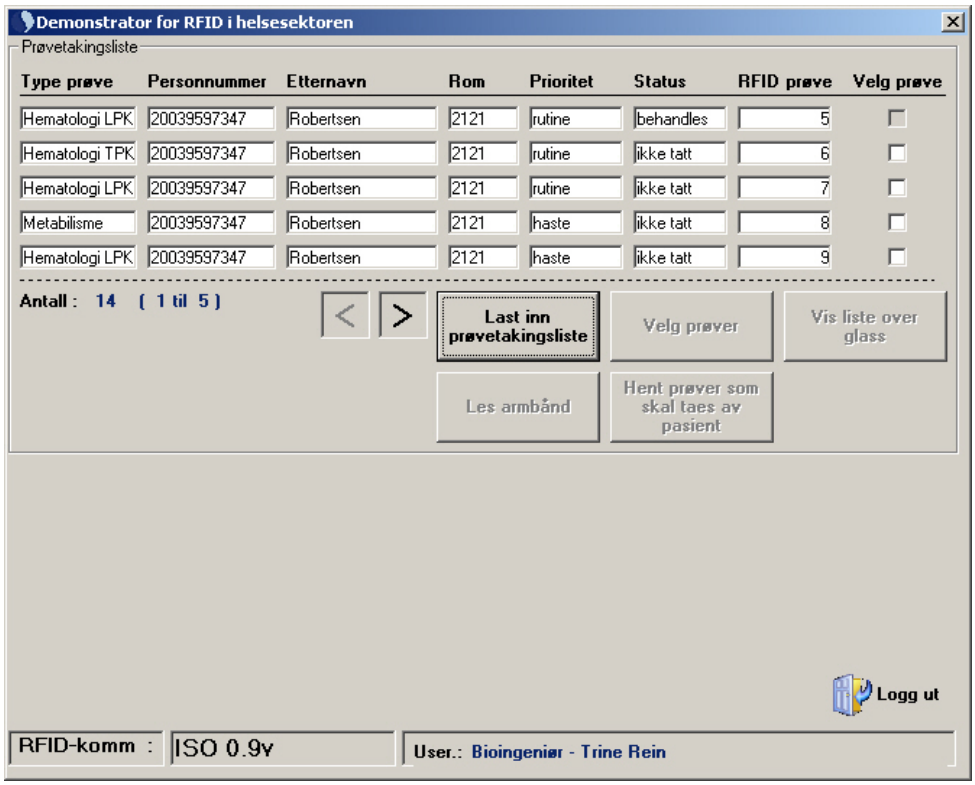
10. Resultater

På bakgrunn av den funksjonaliteten og oppbygningen som er beskrevet i kapittel 9 har vi utviklet en demonstrator. Kildekoden ligger vedlagt [v4]. I dette kapittelet vil vi vise resultater fra demonstratoren. Gjennom en presentasjon for bioingeniørene ved Sørlandets Sykehus i Arendal ble demonstratoren vist, og vi fikk gode tilbakemeldinger. I denne forbindelse gjennomførte vi en spørreundersøkelse som vi også vil vise resultatene av i dette kapittelet.

10.1. Presentasjon av demonstrator

Ved å gå igjennom de ulike funksjonene i demonstratoren, vil vi vise hvordan de fungerte og vise noen skjermbilder av applikasjonen slik den så ut under vår presentasjon.

Innloggingen fungerte slik som den skulle, både med passord / brukernavn og med RFID-brikke. Brikken som ble brukt til pålogging hadde et RFID-nummer som ble sjekket mot tabellen over ansatte. Med en gang dette nummeret ble lest og funnet i databasen, ble brukeren logget inn og en tom prøvetakingsliste vises. For å laste inn prøvetakingslisten, må brukeren klikke på knappen ”Last inn prøvetakingsliste”. De ulike prøvene som er rekvirert blir hentet fra tabellen ”prove” i databasen og presentert slik som vist i Figur 10-1. Det er kun den viktigste informasjonen som er vist i denne listen for å få et mest mulig oversiktlig grensesnitt. Et eget felt viser status på prøven. Dersom noen andre har valgt prøven, og er på vei ut til pasienten for å ta den, vil status være ”behandles”. Som Figur 10-1 viser, vil det ikke være mulig å velge prøven dersom status er satt til ”behandles”.



Figur 10-1 Visning av prøveliste.

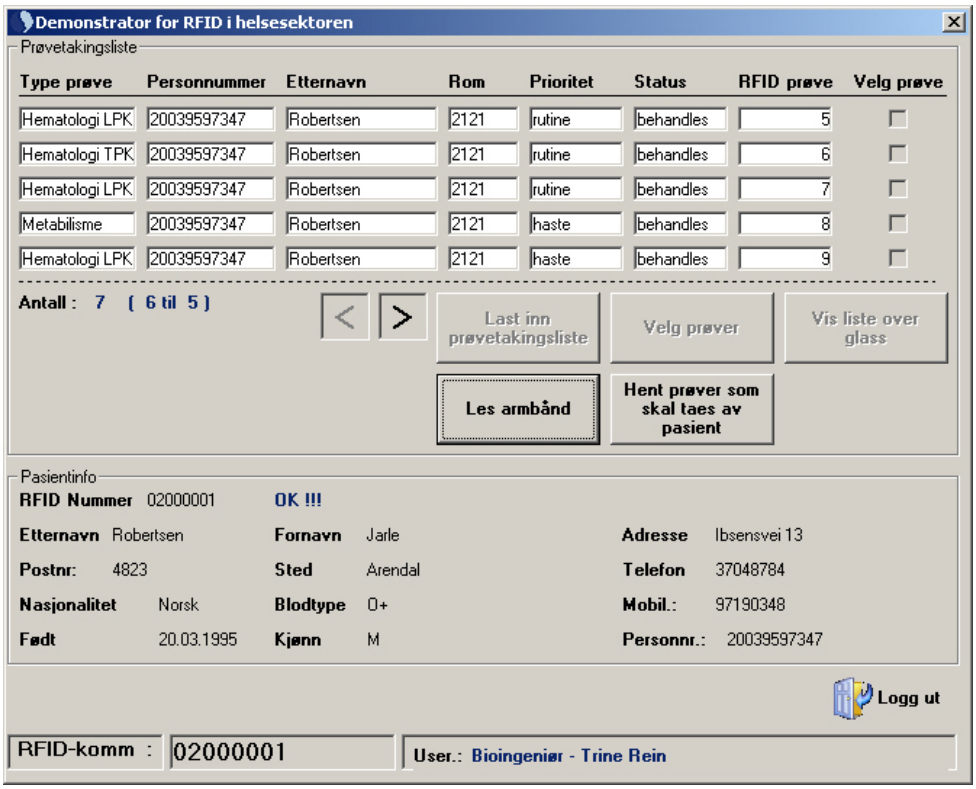
Etter at de prøvene som skal taes er valgt, må brukeren klikke på knappen ”velg prøver” og kun de valgte prøvene vil vises. Knappen ”Vis liste over glass” åpner en oversikt over

ulike glass som trengs for å ta de prøvene som er valgt. Figur 10-2 viser hvordan listen over glass ser ut.

Type glass	Antall glass
enzy1	1
hema1	3
hema2	1
hema3	1
meta2	1

Figur 10-2 Liste over prøveglass

For å gjøre seg klar til å gå ut til pasienten, tar bioingeniøren med seg de glassene som skal brukes og skriver ut klistrelapper med tomme RFID-brikker. Funksjonen for utskrift er ikke bygget inn i vår demonstrator, siden vi ikke har en slik skriver tilgjengelig. Ute hos pasienten blir pasientens armbånd lest. Armbåndet inneholder et RFID-nummer, og applikasjonen sjekker om nummeret stemmer med et nummer i tabellen *pasient* i databasen. Dersom dette stemmer blir opplysninger slik som navn, adresse, personnummer, blodtype, o.s.v. hentet ut fra databasen og vist på skjermen. Figur 10-3 viser hvordan pasientdataene ble vist og at dette fungerte bra.

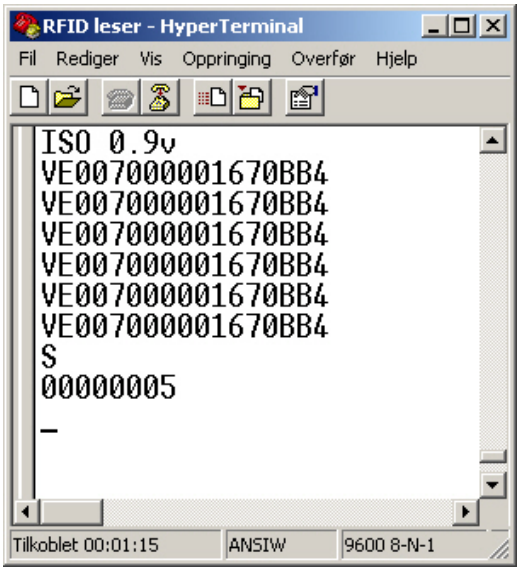


Figur 10-3 Skanning av pasient og visning av pasientdata.

Etter å ha skannet pasienten kan de prøvene som skal taes av den aktuelle pasienten vises ved å klikke på ”Hent prøver som skal taes av pasient”. Et nytt vindu kommer opp som viser prøvene som skal taes. Figur 10-4 viser hvordan dette vinduet så ut. Informasjon om hva slags type prøve som skal taes, hva slags glass som skal brukes, prøvens prioritet o.s.v. vises i dette vinduet. Dersom ingen prøver skal taes av pasienten, kommer det en melding om dette.

Figur 10-4 Visning av prøve som skal taes av en pasient.

Etter at prøven er tatt må bioingeniøren klikke på knappen ”Skriv ID til glass” og holde glasset i nærheten av leseren. Et RFID-nummer som er knyttet til prøven i databasen vil bli skrevet til brikken som sitter på lappen på glasset. For å sjekke at skrivingen var vellykket blir brikken lest, og nummeret blir sjekket opp mot det nummeret som ble skrevet. Dersom dette stemmer vil det komme frem en bekreftelse på dette som sier at skrivingen var vellykket. For å vise at vi har klart å lagre nummeret som er vises under *Prøve RFID* i Figur 10-4, kan vi hente informasjon fra brikken ved å bruke Hyperterminal.



Figur 10-5 Viser at riktig nummer ble skrevet til brikken på glasset.

Nederste linje i terminalvinduet viser at vi klarte å lese nummeret *00000005* ut fra brikken. Dette stemmer med det nummeret vi skrev til brikken med vår applikasjon. Etter at dette nummeret er skrevet til prøven skal prøven signeres med bioingeniørens identitet. I vår applikasjon har vi gjort dette ved å lese identiteten på bioingeniørens RFID-brikke. Ved å holde brikken i nærheten av leseren og klikke på ”Signer prøve”, blir RFID-nummeret lest fra brikken og lagret i databasen. Bioingeniørens identitet blir dermed knyttet opp mot prøven i databasen. I tillegg blir dato og tidspunkt for prøvetakingen lagret. Figur 10-6

viser et utdrag fra databasen hvor prøvetakers RFID-nummer, samt dato og tidspunkt for prøvetakingen er lagret databasen (utringet). Status på prøven er satt til ”utført”, noe som gjør at prøven blir borte fra prøvetakingslisten. Etter signering blir prøven avsluttet, og neste prøve som skal taes kommer opp.

	RFID_prove	type_prove	glass	dato	tidspunkt	RFID_pasient	personnummer	fornavn	etternavn	romnummer	rekv_lege	status	reservert_av_RFID	tatt_av_RFID
1	00000001	Hematologi LPK	hema1		00:00:00	02000003	25027999999	Bjarne	Nilsen	2103	nole	ikke tatt	0	0
2	00000002	Metabolisme HbA1c	meta2		00:00:00	02000003	25027999999	Bjarne	Nilsen	2103	nole	ikke tatt	0	0
3	00000003	Metabolisme HbA1c	meta2		00:00:00	02000003	25027999999	Bjarne	Nilsen	2103	nole	ikke tatt	0	0
4	00000004	Urin stix	Urin1		00:00:00	02000003	25027999999	Bjarne	Nilsen	2103	nole	ikke tatt	0	0
5	00000005	Hematologi LPK	hema1	10.05.2004	19:19:50	02000001	20039597347	Jarle	Robertsen	2121	nole	utført	1000003	1000003
6	00000006	Hematologi TPK	hema2	10.05.2004	19:20:31	02000001	20039597347	Jarle	Robertsen	2121	nole	utført	1000003	1000003
7	00000007	Hematologi LPK	hema1	10.05.2004	19:20:46	02000001	20039597347	Jarle	Robertsen	2121	nole	utført	1000003	1000003
8	00000008	Metabilisme HbA1c	meta2	10.05.2004	19:21:00	02000001	20039597347	Jarle	Robertsen	2121	nole	utført	1000003	1000003
9	00000009	Hematologi LPK	hema1	10.05.2004	19:21:15	02000001	20039597347	Jarle	Robertsen	2121	nole	utført	1000003	1000003
10	00000010	Hematologi TPK	hema2		00:00:00	02000001	20039597347	Jarle	Robertsen	2121	nole	ikke tatt	0	0
11	00000011	Hematologi EVF	hema3	10.05.2004	19:21:30	02000001	20039597347	Jarle	Robertsen	2121	nole	utført	1000003	1000003
12	00000012	Enzymer ASAT	enzy1		00:00:00	02000011	21088123423	Anne Lise	Holm	2104	nole	ikke tatt	0	0
13	00000013	Hormoner Fritt T4	horm1		00:00:00	02000011	21088123423	Anne Lise	Holm	2104	nole	ikke tatt	0	0
14	00000014	Koagulasjon Fibr	koag2		00:00:00	02000011	21088123423	Anne Lise	Holm	2104	nole	ikke tatt	0	0

Figur 10-6 Utdrag fra databasen

10.2. Spørreundersøkelse under demonstrasjon

I forbindelse med vår presentasjon ved sykehuset ønsket vi en tilbakemelding fra bioingeniørene på vårt system, og delte derfor ut spørreskjemaer. Tilbakemeldingene virket positive. Siden flere av bioingeniørene hadde begrenset med tid var det mange som kom og gikk under seansen. Det var derfor ikke alle som fylte ut et spørreskjema. Til slutt satt vi igjen med 8 utfylte skjemaer. Dette er kun et utvalg av de som jobber ved laboratoriet, men vi antar at resultatet kan være en indikator på hvordan oppfatningen på avdelingen er.

10.2.1. Spørreskjemaet

Spørreskjemaet bestod av 12 ulike utsagn som gikk på RFID-teknologi og synspunkter på systemet. Deltakerne skulle si seg enig eller uenig i utsagnene. Utsagnene var som vist i Tabell 10-1.

Tabell 10-1 Utsagn som skulle vurderes i spørreskjema.

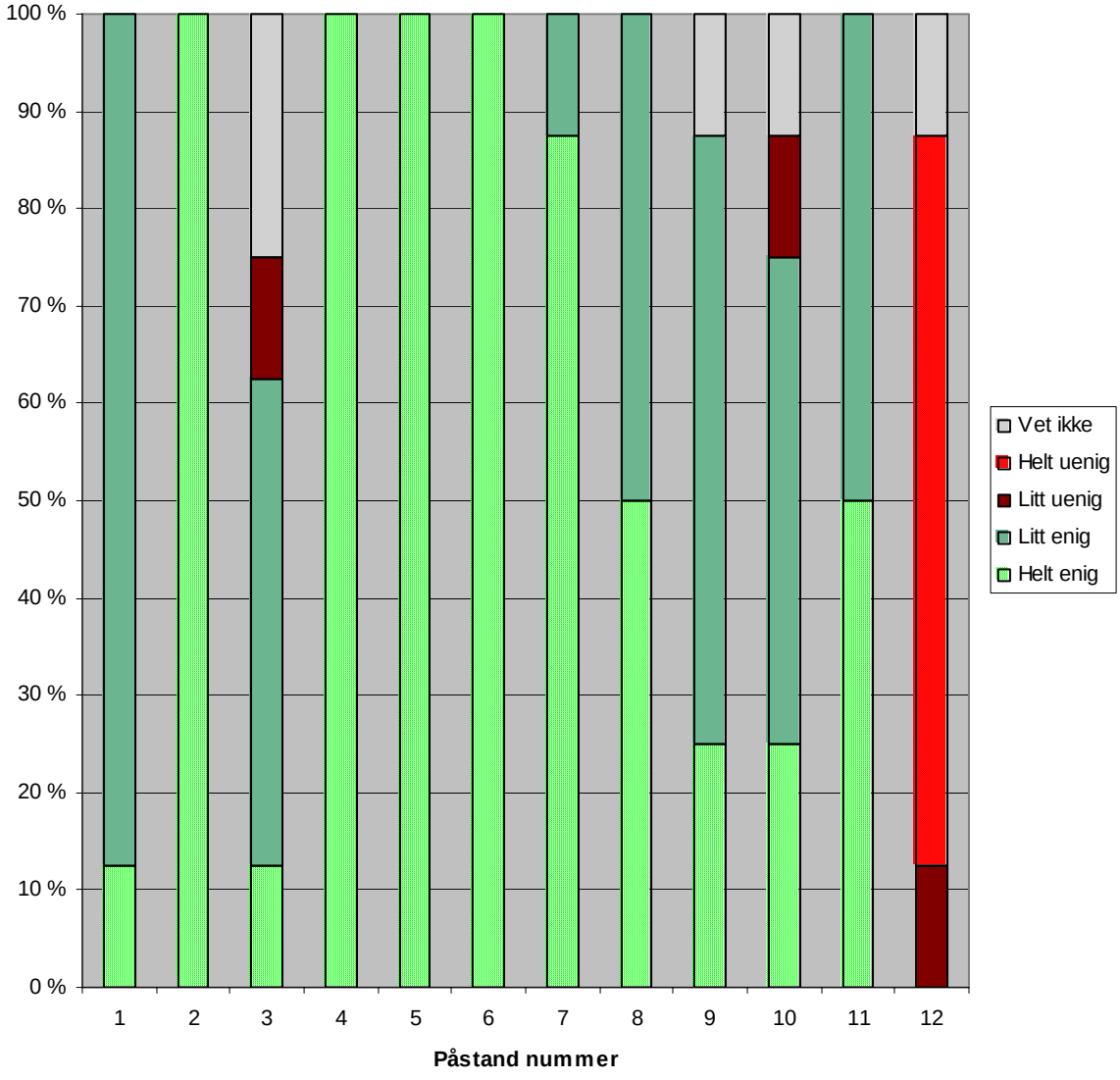
1. Innføring av RFID vil effektivisere arbeidet.
2. Innføring av RFID vil øke kvalitetssikringen.
3. Systemet vil bidra til å forenkle min hverdag.
4. Det er positivt å ta i bruk ny teknologi.
5. Systemet bidrar til å eliminere mange av dagens feilkilder.
6. Det er behov for å endre dagens rutiner.
7. Det er behov for å innføre et slikt system.
8. Systemet vil virke kostnadsbesparende i form av effektivisering og reduserte feil.
9. Systemet er noe som ville blitt tatt godt imot av bioingeniørene.
10. Systemet virker enkelt å bruke.
11. Dette er et system jeg gjerne ønsker å bruke.
12. Dagens rutiner bør opprettholdes og ny teknologi trengs ikke.

Til slutt tok vi med et punkt hvor deltakerne kunne komme med forslag til endringer, samt andre kommentarer. Spørreskjemaet var nokså kort og hadde få spørsmål. Grunnen til dette var at de ansatte ved laboratoriet måtte delta på presentasjonen og svare på

skjemaene innimellom deres gjøremål på laboratoriet. Dersom skjemaet hadde vært mer omfattende kunne vi risikert å få enda færre utfylte skjemaer tilbake.

10.2.2. Resultat fra spørreundersøkelse

Ut fra de resultatene vi fikk på de utfylte spørreskjemaene har vi laget en grafisk fremstilling av hvordan de forskjellige svarprosentene var. Diagrammet viser en prosentfordeling av de svarene som kom inn på de forskjellige utsagnene. De ulike fargene viser i hvilken grad de var enig eller uenig i utsagnene som stod på skjemaet. Diagrammet må sees i sammenheng med Tabell 10-1. Kommentarene som kom frem på det siste punktet i spørreskjemaet, som gikk på forslag til endringer i systemet er ikke tatt med i diagrammet. Dette vil vi kommentere senere.



Figur 10-7 Resultat av spørreundersøkelse

Ut fra Figur 10-7 kan vi se at de aller fleste er enige i at en innføring av en slik type teknologi har noe for seg, siden det generelt var mange positive tilbakemeldinger. På det første spørsmålet som gikk på effektivisering av arbeidet ved laboratoriet hadde de fleste litt tro på at det kunne ha en effektiviseringseffekt. Men det var tydelig litt tvil om dette siden flertallet krysset av på "litt enig". På spørsmål nummer to var samtlige enige i at det

ville bli en bedre kvalitetssikring med bruk av et RFID-system. Hvis vi ser på den tredje søylen viser den at det var litt mer uenighet om hvorvidt et RFID-system kan forenkle bioingeniørenes hverdag. I denne søylen var det også en del som valgte "vet ikke". Påstanden om det er positivt å ta i bruk ny teknologi var samtlige enige i. Søyle nummer fem viser at alle er enige i at systemet kan bidra til å eliminere dagens feilkilder. Utsagn nummer seks gikk på om de ansatte mener det er behov for å endre dagens rutiner. Også denne påstanden var samtlige enige i. I søyle nummer syv er det nokså stor enighet i at det finnes et behov for å innføre et slikt system. Den 8. søylen viser de ansattes synspunkt på om systemet kan være kostnadsbesparende i form av effektivisering og reduserte feil. Halvparten har sagt seg litt enig og halvparten har sagt seg helt enig i at systemet kan virke kostnadsbesparende. I søyle nummer 9 spurte vi om systemet ville blitt tatt godt imot av bioingeniørene. Mange har svart at de er litt enige på dette punktet. Noen har sagt seg helt enig, mens noen har valgt "vet ikke". 10. søyle tar for seg brukervennligheten på systemet. Flertallet er litt enige i at systemet virket enkelt å bruke og en del er helt enige i dette. Det er imidlertid noen som har sagt seg "litt uenig" i at det er enkelt å bruke, mens noen ikke vet. Under punkt 11 ville vi vite om bioingeniørene ønsket å bruke et slikt system. Her valgte alle enten "helt enig" eller "litt enig". Siste påstand var at dagens system burde opprettholdes og det var ikke nødvendig med ny teknologi. Her var de fleste uenige i påstanden og mente altså at noe burde gjøres. Noen valgte imidlertid "vet ikke" her. De utfylte spørreskjemaene ligger vedlagt [v5].

10.2.3. Kommentarer og tilbakemeldinger

Under fremvisningen av demonstratoren ble det kommentert noen momenter som gjaldt brukergrensesnitt og måter ting ble gjort på under valg av prøver og signering av prøver. Det ble påpekt at det ville være enklere å velge hvilke pasienter hver bioingeniør skal ta prøver av, i stedet for hver enkelt prøve. Det vil være naturlig å ta alle prøver som er rekvirert av en pasient samtidig, uavhengig av prioritet og type. Det bør kanskje gjøres enkelte unntak dersom det er snakk om spesielle prøver slik som urinprøver og andre typer prøver hvor det brukes andre prøvetakingsmetoder. Et annet moment som kom frem var at signeringen av prøvene virket noe tungvinn. I vår demonstrator er det lagt opp til at alle prøvene skal signeres en og en. Det ble påpekt at dette ville ta lang tid siden det er snakk om mange prøver. En løsning kan være å signere alle prøvene til slutt. Det bør likevel legges inn en sperre slik at det ikke er mulig å avslutte en prøvetaking hos en pasient uten å ha signert alle prøvene. Responsen fra laboratoriekonsulenten var at en signatur med dato og klokkeslett ville være nyttig informasjon slik at prøvetakeren kan spores opp dersom noe er uklart. Det kan også være mulig å registrere hvor i bygget prøven er tatt dersom det registreres hvilket aksesspunkt som er brukt under prøvetakingen.

Nederst på spørreskjemaet som ble delt ut under seansen var det et eget felt for endringer og andre kommentarer. Her fikk vi inn noen kommentarer som gikk på at systemet burde tilpasses best mulig laboratoriets rutiner og gjerne i samarbeid med de ansatte. Det ble også kommentert at dette er et spennende system som kan bli effektivt etter noen tilpasninger mot laboratoriet.

I forbindelse med demonstrasjonen ved sykehuset var også Agderposten invitert, noe som endte ut i en fin reportasje [v6].

11. Drøfting

11.1. RFID v.s. barkoder

Sykehuset benytter i dag et system som er basert på barkoder. Barkoder er et forholdsvis enkelt system som inneholder et nummer for å identifisere gjenstanden barkoden er festet på. RFID-brikker har den fordelen at det kan lagres større mengder data i brikken. Det vil si at det er mulig å lagre informasjon om den gjenstanden brikken er festet på og bruke selve brikken som informasjonsbærer. I vårt tilfelle kan det være nyttig å lagre informasjon om for eksempel hva slags type blod et prøveglass inneholder og hvilken analysemaskin prøven skal analyseres i. En stor fordel med RFID-brikker er at det er mulig å lese ut data uten å ha fri sikt til brikken. Ved lesing av barkoder er det nødvendig med fri sikt og kort avstand mellom barkodeleser og barkode. En RFID-brikke kan for eksempel leses gjennom klær eller sengetøy, noe som vil være nyttig i sykehussammenheng. Det er også mulig å lese flere brikker samtidig.

11.2. Sammenligning av arbeidsflyt

For å kunne se ulike muligheter for å ta i bruk RFID-teknologi ved sykehuset gjennomførte vi en kartleggingsprosess. I kapittel 5 har vi beskrevet hvordan prosedyrene fungerer i dag, mens vi i kapittel 7 viser et forslag til hvordan den nye teknologien kan innføres. Vi har beskrevet prosedyrene ved å bruke en case for å vise hvordan prosedyrene fungerer til daglig.

Ved å diskutere arbeidsflytdiagrammene opp mot hverandre kan vi se hvilke endringer og forbedringer en eventuell innføring av RFID-merking kan bidra til. Hvis vi ser på skjemaene i Figur 5-2 og Figur 7-1, visualiseres forskjellen på rutinene med og uten RFID-merking av prøver. Under de faste prøvetakingsrundene er det mange prøver som skal taes samtidig. Prøvene blir derfor fordelt på flere bioingeniører. I dag blir det skrevet ut en prøvetakingsliste på papir og fordelt mellom prøvetakerne. Ved å innføre RFID-merking av prøvene kan dette gjøres digitalt ved hjelp av en PDA via trådløst nettverk. Man er derfor ikke avhengig av å være på laboratoriet for å velge prøver. Det eneste man må hente fra laboratoriet er de prøveglassene som trengs og klistrelapper med tomme RFID-brikker. Denne måten å fordele prøvetakingen på kan virke effektiviserende, siden man slipper at alle skal velge prøver og fordele lister fra samme datamaskin. Det at man kan få opp hvor mange glass av hver type som trengs på prøvetakingsrunden, kan også bidra til å hindre at man eventuelt må avbryte runden for å hente flere glass. Ute hos pasienten kan man enklere lese pasientens armbånd enn i dag. Det er ikke nødvendig med fri sikt til brikken for å kunne lese den, noe som gjør at sengetøy eller klær godt kan ligge mellom leser og brikke. Dette er noe som kan virke effektiviserende. En skanning av pasientens armbånd bør også kunne gi en sikrere identifisering av pasienten enn dagens manuelle avlesing av armbåndet. Dette gjelder spesielt pasienter som ikke er ved bevissthet. Det bør likevel være et poeng at pasientkontakten opprettholdes, slik at prøvetakeren fortsatt har en dialog med pasienten og gjerne verifiserer navn og personnummer. I tilfeller hvor pasientens identitet er ukjent, vil en RFID-merking kunne forenkle overgangen fra K-nummer til pasientens personnummer, siden det hele tiden vil være samme RFID-nummeret knyttet til pasienten.

Etter at prøven er tatt av pasienten blir det klistret en lapp på prøveglasset med nødvendig lesbar informasjon, samt en tom RFID-brikke. Merkingen av prøveglasset vil skje på samme måte som i dag, men i tillegg skrives en identitet til en RFID-brikken. Glasset signeres også med bioingeniørens ID-kort, og dato og tidspunkt for prøvetaking blir registrert. Ved å gi glasset en identitet ute hos pasienten vil det ikke være fatalt å

klistre feil merkelapp på et prøveglass, slik det vil være med dagens rutiner. Dette fordi den digitale identiteten er uavhengig av den visuelle merkingen. Dersom en kan forhindre at glass blir feil merket, vil det være mulig å unngå at prøver må taes på nytt, eller i verste fall at pasienter får feil behandling. Mario Plebani og Paolo Carraro har gjort forskning på dette området [3], og de viser at faren for feilbehandling er reell. Det kan her være snakk om økonomiske innsparingsmuligheter. Ved å ha en digitalt signert prøve, vil det være lettere å spore tilbake til prøvetaker dersom det skulle være nødvendig. I følge bioingeniørene selv kan det av og til skje feil under prøvetaking, og disse feilene er ofte vanskelig å oppdage. Merking av prøveglassene med en digital identitet som programmeres ute hos pasienten mener vi kan virke kvalitetssikrende og redusere antall feil. Ved denne typen merking blir de manuelle rutinene redusert, noe som bør kunne bidra til å øke kvalitetssikringen.

11.3. Demonstrator

Ved hjelp av en enkel demonstrator har vi forsøkt å visualisere RFID-teknologiens muligheter overfor de ansatte på laboratoriet ved Sørlandets Sykehus i Arendal. Vi har forsøkt å lage demonstratoren slik at den passer best mulig inn i de rutiner og arbeidsprosesser som de ansatte har i dag. For å få til dette har vi støttet oss til en metode som kalles Contextual Design. Metoden har vi beskrevet i kapittel 4.1. Contextual Design går i hovedsak ut på å ha et tett samarbeid med brukeren gjennom hele utviklingsprosessen, noe vi har hatt under vårt arbeid.

I startfasen jobbet vi med en datainnsamlingsprosess. Contextual Design sier at en skal snakke med utvalgte personer mens de arbeider og gjennom en analyse av resultatene lage en oversikt over arbeidsrutiner. Til slutt skal en lage forslag til endringer som kan gjøres. Gjennom et todagers besøk ved sykehuset samlet vi inn mye nyttig informasjon om arbeidsrutiner, og vi fikk et bedre inntrykk av problemer som kunne dukke opp med dagens system. På bakgrunn av disse resultatene laget vi arbeidsflytskjema for dagens rutiner og et forslag til hvordan en ny arbeidsflyt kan se ut. Gjennom oppfølgingsmøter fikk vi verifisert våre løsninger med våre kontaktpersoner ved sykehuset, og noen mindre justeringer ble gjort. Demonstratoren ble så designet for å passe med vårt utkast til ny arbeidsflyt.

Resultatet var en demonstrator som prinsipielt passer bra med bioingeniørens arbeidsrutiner. I en PDA vil brukergrensesnittet naturlig nok se annerledes ut. I demonstratoren viser vi at det er mulig å skrive data til en RFID-brikke i form av et ID-nummer. Vi viser også hvordan en elektronisk ID på prøveglasset kan kobles sammen med pasientinformasjon ved hjelp av en database. Vi mener hovedfunksjonene som trengs i forbindelse med selve prøvetakingen finnes i demonstratoren, og at den fungerte fint til å visualisere hvordan et slikt system er ment å fungere.

11.4. De ansattes synspunkter

Spørreundersøkelsen vi gjorde under vår presentasjon ved Sørlandets Sykehus i Arendal, kan brukes som en indikator på hvilken oppfattning de ansatte ved laboratoriet har, siden den kun involverte en mindre gruppe av de ansatte. Hvis vi ser på resultatene fra Figur 10-7, kan vi oppsummere med at bioingeniørene ved laboratoriet mener det bør gjøres noe med dagens rutiner, og at de virker positive til å ta i bruk ny teknologi. Det som er nokså oppsiktsvekkende er at alle var enige i at det er behov for å endre dagens rutiner. Det kan tyde på at dagens rutiner kan gjøres bedre og det kan oppstå feil. I kapittel 3.2 så vi på TAM-modellen og holdninger til innføring av ny teknologi. Der nevnte vi Melissa J. Succi og Zhiping D. Walter som har skrevet et paper om innføring av IT blant fagfolk i helsesektoren [1]. Det de kom frem til var at høyt kvalifisert helsepersonell lett kunne være

redde for at deres ekspertise kunne undergraves av den nye teknologien. Ut fra den responsen vi har fått fra bioingeniørene kan det tyde på at bioingeniørene har forstått at teknologien foreslås kun for å kunne kvalitetssikre og gjøre deres prosedyrer lettere og mer effektive i forbindelse med prøvetakingsfasen. Siden bioingeniørene helhetlig sett virker positive til innføring av ny informasjonsteknologi virker det ikke som de er redde for at sin posisjon kan bli undergravd. Bioingeniørens posisjon både under prøvetakingen og spesielt under analysering av prøver vil fortsatt være den samme. Sykehuset ligger i dag langt fremme når det gjelder bruk av ny teknologi som elektroniske pasientjournaler og trådløse nett. Det at ny informasjonsteknologi allerede er en del av de ansattes hverdag kan også være en medvirkende faktor til at de ser positivt på slikt utstyr.

TAM-modellen omtaler *oppfattet nytteverdi* og *oppfattet enkelhet ved bruk* [2]. Ut fra resultatene fra spørreskjemaene kan det virke som bioingeniørene er noe negative når det gjelder *oppfattet enkelhet ved bruk*. Det var under utsagnene som gikk på hvor enkelt systemet var å bruke og om systemet kunne bidra til å forenkle bioingeniørens hverdag, vi fikk mest negativ tilbakemelding. Siden systemet ble demonstrert på en bærbar PC med et noe uegnet utstyr, kan systemet ha sett tungvint ut å bruke. Med egnet utstyr og god opplæring av brukerne vil forhåpentligvis innstillingen til bruk av systemet bedre seg, forutsatt at brukergrensesnittet er brukervennlig og enkelt og bruke. Hvis vi ser på *oppfattet nytteverdi* som blir omtalt i TAM-modellen, er dette et område hvor brukerne virker mer positive. Ut fra TAM-modellen er det *oppfattet nytteverdi* og *oppfattet enkelhet ved bruk*, som sammen virker inn på holdninger til bruk av systemet. Disse faktorene virker også inn på hvor mye systemet vil bli brukt [2]. Det er viktig å få aksept blant brukerne av systemet hvis det skal bli suksess, derfor vil det være avgjørende at systemet må være enkelt å bruke og det kan bidra til å forenkle bioingeniørens hverdag. Ut fra spørreundersøkelsen mener de aller fleste at systemet har stor nytteverdi spesielt i form av kvalitetssikring. Helhetlig sett viste spørreskjemaet at de fleste syntes det var en god løsning og at det hadde noe for seg. Det må imidlertid taes i betraktning at dette var en liten spørreundersøkelse, og kan kun brukes som en indikator.

11.5. Sikkerhet

I kapittel 8 diskuterte vi hvordan sikkerheten kan ivaretaes med tanke på overføring av sensitive data. Når data skal overføres til brikken, diskuterte vi to ulike løsninger. Enten lagring av sensitive data i brikken, eller erstatte de sensitive dataene med et RFID-nummer som knytter prøven opp mot pasienten i en database. Siden informasjonen ikke inneholder sensitive personopplysninger, slipper vi å kryptere den informasjonen som blir overført. Ved bruk av RFID-nummer i stedet for personopplysninger vil kommunikasjonen mot brikken forenkles. En kan i tillegg benytte brikker og lesere som er mindre komplekse og vi mener derfor at det er en bedre løsning. I vår demonstrator viser vi også at dette er en løsning som fungerer. Det er rimelig å anta at brikker som ikke har kryptering er billigere enn brikker med kryptering. Pris vil være et sentralt punkt i denne sammenhengen, siden det dreier seg om et stort antall brikker. For å kunne sikre at ikke uvedkommende skriver til en brikke bør leser og brikke støtte autentisering. Autentisering av brukeren på den håndholdte enheten bør skje ved å bruke en digital signatur i form av et RFID-basert ID-kort og et passord. Det er en forutsetning at man har et godt utbygd og sikkert trådløst nett for kontinuerlig kommunikasjon med databasen ved hjelp av den håndholdte enheten. Sikkerheten i et slikt nett er ikke noe vi har vektlagt i vår oppgave.

11.6. Videre arbeid

Siden vi i vår oppgave har konsentrert oss om merking av pasienter og prøveglass ved sykehuset, kan det finnes flere områder hvor RFID-teknologien kan brukes innen helsesektoren. Ved hjelp av såkalte portaler er det mulig å registrere dersom en RFID-brikke passerer portalen, og på den måten ha oversikt over hvor de ulike brikkene befinner seg. I det prøvene blir sendt inn til analyse på laboratoriet, kan dette være en nyttig egenskap. Det vil også være mulig å finne ut hvilken avdeling pasienter befinner seg på ved å montere portaler ved inngangene til de ulike avdelingene. Denne informasjonen kan det være nyttig for bioingeniøren å vite når det skal taes prøver.

Gjennom vårt arbeid har det også kommet frem at det er mange manuelle rutiner ved mottak av prøver som blir sendt til sykehuset fra legekontorer ute i distriktene. Dette tyder på at det også her kan være muligheter for å øke kvalitetssikringen og effektiviteten. Ved at legekontorene blir knyttet tettere sammen med sykehusets datasystem, kan det være mulig at RFID-teknologien eliminerer en del av de manuelle rutinene ved mottak av prøver.

12. Konklusjon

I oppgaven har vi tatt for oss arbeidsprosessene under prøvetaking ved laboratoriet på Sørlandets Sykehus HF i Arendal. Vi har kartlagt rutinene slik de er i dag, og gjennom en dialog med nøkkelpersoner ved avdelingen kommet frem til løsninger for hvordan RFID-teknologi kan innføres på en god måte. Under kartleggingen av de ulike arbeidsprosessene kom vi frem til at det er rutinen hvor bioingeniøren skal klistre merkelapper på prøveglassene, det er størst fare for at feil kan oppstå. Dersom en lapp blir klistret på feil glass, vil det være vanskelig å oppdage feilen. Derfor mener vi at merking av glasset med RFID-brikker ute hos pasienten, kan bidra til økt kvalitetssikring av prøvens identitet. En slik type merking kan brukes i kombinasjon med en PDA og trådløst nett. Vi mener også at man kan forenkle identifiseringen av pasienter ved hjelp av RFID-armbånd. Dersom antall feil ved prøvetaking kan reduseres, vil innføring av RFID-teknologien virke effektiviserende ved at man kan unngå at prøver må taes på nytt, eller eventuell feilbehandling av pasienter. Et annet effektiviseringsmoment kan være at ulike prosesser under prøvetakingen blir automatisert.

For å kunne visualisere hvordan et RFID-basert system kan fungere, har vi på bakgrunn av vår kartlegging ved laboratoriet, laget en prinsipiell demonstrator. Demonstratoren viser at vi kan bruke RFID-brikken som en informasjonsbærer og identifikator. Den viser også at vi kan bruke en database til å knytte pasientinformasjon opp mot dataene på brikken.

Demonstratoren ble brukt til å visualisere teknologiens muligheter for de ansatte ved laboratoriet. Ut fra tilbakemeldinger vi fikk, kan det tyde på at det er rom for forbedringer av rutinene ved sykehuset. Bioingeniørene er villige til å benytte seg av ny teknologi og er enige i at RFID-teknologien kan bidra til økt kvalitetssikring. Tilbakemeldingene som gikk på hvor enkelt systemet var å bruke, var noe mer usikre. Grunnen til dette mener vi kan ligge i komponenter og brukergrensesnitt som ble brukt i demonstratoren. Vi mener likevel at vi med bakgrunn i TAM kan konkludere med at tilbakemeldingene indikerer at systemet kan bli tatt i bruk.

Datatilsynet stiller strenge krav til behandling av sensitiv informasjon. Kravene innebærer tiltak i forhold til konfidensialitet, integritet og tilgjengelighet. Dersom sensitive data skal overføres til en RFID-brikke, må det være autentiseringsmekanismer mellom leser og brikke. Dataene må også krypteres ved hjelp av en krypteringsnøkkel som tilsvarer DES 128 kryptering (112 bits effektiv nøkkel). Det finnes i dag RFID-systemer som tilfredsstiller disse kravene. Disse systemene er imidlertid forholdsvis komplekse. Vårt forslag er å lagre et ID-nummer i brikken som refererer til sensitive personopplysninger i en database. Siden opplysningene i brikken ikke kan knyttes til en bestemt person, unngår vi at informasjonen er sensitiv. Vi oppnår dermed at sikkerhetstiltakene kun må omfatte brukerautentisering på PDA'en i form at et digitalt ID-kort og et passord. Dataoverføringen i WLAN må imidlertid ha tilfredsstillende kryptering og autentisering. Så lenge informasjon som skal lagres i RFID-brikken ikke kan knyttes opp mot en pasient, vil det ikke være problematisk å lagre den i brikken uten kryptering. Vi anbefaler likevel at det bør benyttes autentiseringskontroll mellom leser og brikke, slik at uautoriserte ikke kan skrive til og lese fra brikken. I tillegg har vi kommet med forslag til komponenter som kan benyttes i et RFID-basert system for merking av pasienter og prøver.

Referanser

[1] Melissa J. Succi and Zhiping D. Walter
Theory of User Acceptance of Information Technologies: An Examination of Health Care Professionals
University of Connecticut
http://www.computer.org/proceedings/hicss/0001/00014/00014013.PDF
(03.04.2004)

[2] Fred D. Davis
Percieved Usefulness, Percieved Ease of Use, and User Acceptance of Information Techology.
University of Michigian
MIS Quaterly, 1989

[3] Mario Plebani and Paolo Carraro
Mistakes in a stat laboratory: types and frequency.
Clin. Chem. 43:8 -97
http://www.clinchem.org/cgi/reprint/43/8/1348.pdf
(19.01.2004)

[4] Dr. Jeremy Landt, TransCore's Chief Scientist an Amtech Technology Founder
Shrouds of Time - The history of RFID
An AIM Publication
AIM, Inc. 2001

[5] Trond H. Johansen, Vermund Lea, Ørnulf Storm
RFID Identifikasjon av pasienter og pasientprøver på Sørlandets Sykehus I Arendal
IKT4200 – 2003 HiA

[6] Klaus Finkenzeller
RFID Handbook – Fundamentals and Applications in Contactless Smart Cards and Identification
Second Edition, Wiley 2003

[7] Forskrift om tillatt bruk av frekvenser
Post og Teletilsynet, 20 des. 2000
http://www.lovdata.no/for/sf/sd/td-20001220-1399-0.html
(27.04.2004)

[8] Retningslinjer om informasjonssikkerhet ved behandling av personopplysninger
Datatilsynet. TR-100:1998
http://www.datatilsynet.no/infosik/retning/TR100_98.pdf
(27.04.2004)

[9] New RFID Tag with More Memory
RFID Journal Inc, 2004
http://www.rfidjournal.com/article/articleview/544/1/73/
(27.04.2004)

[10] Lov om behandling av personopplysninger av 14.04 – 2000 nr 31
http://www.lovdata.no/all/nl-20000414-031.html
(03.05.2004)

[11] Lov om teleregistre og behandling av helseopplysninger av 18.05 -2000 nr 24
http://www.lovdata.no/all/hl-20010518-024.html
(03.05.2004)

[12] Forskrift om pasientjournal av 21.12 – 2000 nr 1385
http://www.lovdata.no/for/sf/hd/xd-20001221-1385.html
(03.05.2004)

[13] Lov om elektronisk signatur av 15.06 – 2001 nr 81
http://www.lovdata.no/all/nl-20010615-081.html
(03.05.2004)

[14] Veiledning ved bruk av tynne klienter for å skille samtidige brukerrettigheter i Interne og sikre soner.
Datatilsynet: TV – 204:1999
http://www.datatilsynet.no/dtweb/attachment/790/TV204_99.pdf
(03.05.2004)

[15] Veiledning i informasjonssikkerhet for kommuner og fylker
Datatilsynet: TV – 202:1999
http://www.datatilsynet.no/dtweb/attachment/783/Kommuneveiledning.pdf
(03.05.2004)

[16] Retningslinjer for informasjon ved behandling av personopplysninger
Datatilsynet: TV – 100:1998
http://www.datatilsynet.no/infosik/retning/TR100_98.pdf
(03.05.2004)

[17] Sterkere kryptering nødvendig
Datatilsynet: 14.09 - 2001
http://www.datatilsynet.no/dtweb/attachment/468/kryptering.html
(03.05.2004)

[18] Rune Fensli, Agder University College, Faculty of Technology, Grimstad, Norway
Heidi Thorstensen, Systemsikkerhet ASA, Arendal, Norway
Security Aspects of Wireless Medical Computer Networks.
A Proposal of Combined Security Measures.
Procedure for Scandinavian Conference in Health Informatics 2003
June 12-13 Arendal, Norway

[19] Lov om helsepersonell av 07.02 – 1999 nr 64
http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-19990702-064.html&dep=alle&titt=lov+om+helsepersonell&
(10.05.04)

[20] RFID Journal
Putting tags on test tubes,
http://www.rfidjournal.com/article/articleview/922/1/1/
(10.05.04)

[21] Precision Dynamics Corporation
http://www.pdcorp.com/rfid/rfid_products.html
(10.05.04)

[22] Søknader og meldinger til datatilsynet
http://www.datatilsynet.no/soknad/soknadmain.html
(10.05.04)

[23] Alain Berthon, Texas Instruments and Michael Guillory, Intermec Technologies
Security in RFID
ISO/IEC JTC1 SC31/WG4/SG1 N050-R3
http://stud.ita.hsr.ch/ss03/ss0304/
University Of Applied Science - Rapperswil - Switzerland /
(10.05.04)

[24] RFID Journal
Get RFID Readers in a Flash (Card), April 22 2003
http://www.rfidjournal.com/article/articleview/393/1/1/
(13.05.2004)

[25] Personvernrapporten, datatilsynet, april 2004
http://www.datatilsynet.no/arkiv/andreforsideoppslag/v2004/pvrapp04.pdf
(13.05.2004)

[26] Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels
RFID Systems and Security and Privacy Implications
Auto-ID Center, Massachusetts Institute of Technology
Cambridge, MA 02139
www.autoidcenter.org
http://theory.lcs.mit.edu/~sweis/ches-rfid.pdf
(14.05.2004)

[27] U.S Department of commerce/National Institute of Standards and Technology
DATA ENCRYPTION STANDARD (DES), 25.10.1999
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
(14.05.2004)

[28] Philips offisielle dokumentside
Mifare DESfire, Contactless Multi-Application IC with DES and 3DES security MF3 IC D 40
http://www.semiconductors.philips.com/acrobat/other/identification/SFS075530.pdf
(18.05.2004)

[29] TagSys RFID Systems
http://www.tagsys.net/eng/rfid/tagsys_produit/rfid_product-33.html
(19.05.04)

[30] Maxell, Mini Mold
http://www.maxell.com/Home/rfid/Products.html
(19.05.04)

[31] Philips offisielle dokumentside
I-CODE
http://www.semiconductors.philips.com/markets/identification/datasheets/index.html#icode
(19.05.04)

[32] Precision Dynamics Corporation
PDC RFID Wristbands
www.pdcorp.com/rfid/rfid_wristbands.html
(19.05.04)

[33] Zebra Technologies
RFID-printers
www.zebra.com/PA/Printers/product_R402.htm
(19.05.04)

[34] Omron RFID Systems
http://oeiweb.omron.com/Products-RFID.shtm#v720
(19.05.2004)

[35] Cyclic Redundancy Check (CRC)
http://www2.rad.com/networks/1994/err_con/crc.htm
(19.05.2004)

[36] TI-RFID
RFID Technology Central
http://www.rfidusa.com/rfid_iso15693doc.html
(19.05.2004)

[37] Michael Blechner MD, Valerie Monaco PhD, Isabella Knox MD and Rebecca S. Crowley MD
Using Contextual Design to Identify Potential Innovations for Problem Based Learning
University of Pittsburgh
http://www.health.pitt.edu/users/rebecca/Publications/Blechner_2003_AMIA.pdf
(19.05.2004)

[38] BuyRFID.COM
http://buyrfid.com/catalog/product_info.php?cPath=21_37&products_id=32
(19.05.2004)

[39] Tag-it HF-I Transponder Inlays, Texas instruments technology, 11-09-21-053
http://www.ti.com/tiris/docs/manuals/refmanuals/hfi_inlays_ref_guide.pdf
(19.05.2004)

[40] Hugh Beyer and Karen Holtzblatt
InContetxt Enterprises, Inc
Contextual design
(19.05.2004)

[41] A. Nasipuri, S. Ye, J. You and R. E. Hiromoto,
A MAC Protocol for Mobile Ad Hoc Networks Using Directional Antennas
Division of Computer Science
University of Texas, San Antonio
http://www.coe.uncc.edu/~anasipur/pubs/s12p2.pdf
(20. 05.2004)

Vedlegg

[v1] Intervju med dataansvarlig ved laboratoriet, Astrid Sines

[v2] Intervju med systemansvarlig for DIPS, Helge Olsen

[v3] Notater fra besøk ved Sørlandet Sykehus HF, Arendal

[v4] Demonstratorens kildekode

[v5] Resultater fra spørreundersøkelse

[v6] Reportasje i Agderposten