Forord

Denne oppgaven er skrevet som diplomoppgave i fordypningsfaget TDT4900 Informasjonssystemer, 5. års trinn (10. semester) ved Norges teknisk-naturvitenskaplige universitet (NTNU).

Vi vil benytte anledningen til å takke veileder Camilla AC Tepfers, for gode råd, svar på spørsmål og veiledning underveis, og Ingunn Viken for god korrekturlesning og gramatikkhjelp.

Litteratur og kilder

Den teknologiske utviklingen på feltet e-handel går veldig raskt, og vår beste kilde for informasjon om denne utviklingen har vært internett. Tidsskrifter og aviser gir en god pekepinn på hvordan utviklingen går, og er derfor et godt utgangspunkt for videre forskning. Mye av teknologiene har vært utviklet over flere år, og er derfor godt dokumentert i bøker og artikler.

Trondheim 15.06.2005

Eystein Bye Stein Lagim

Innhold

Figurer

Tabeller

Innledning

Mobilhandel har idag flere svakheter, men det mest hemmende for utbredelsen er at det er for tidkrevende å utføre en handel. Dette gjør at få brukere benytter seg av tilbudet og bedrifter vil da ikke bruke penger på å markedsføre seg på m-handelsløsninger. Vår hypotese er at ved å hjelpe brukerne til å raskere komme igang med selve kjøpet og dermed forkorte kjøpsprosessen vil m-handel kunne bli mer utbredt. Ved å gi mobiltelefonen mulighet til å kommunisere direkte med reklame, brosjyrer og plakater så forkortes kjøpsprosessen for brukerne.

For å få til dette må reklame, brosjyrer og plakater også kunne lagre sin informasjon digitalt. Den optimale løsningen for lagring av data hadde vært på en silikonbrikke. Dette hadde sikret at vi hadde rikelig med lagringskapasitet og gjenbrukbarhet. Den mest vanlige løsningen av denne type i dagliglivet er smartkort. Ulempen er at de vanlige smartkortlesere har behov for metallisk kontakt for å kunne lese innholdet. En kontaktløs overføring hadde vært mye mer praktisk. Dersom silikonbrikken skulle kunne sende sitt innhold trådløst til leseren trenger den også strøm, og det ville være svært upraktisk om brikkene kunne gå tom for strøm. Løsningen er at leseren sender et signal til silikonbrikken som aktiverer den, energien som brikken behøver blir altså levert trådløst av leseren. Slike systemer kalles RFID, og blir stadig mer anvendt. Slike RFID-brikker kan være veldig små (helt med til 0.1mm tykke). Dette gjør de meget godt egent for integrering i reklame, plakater, brosjyrer og mobiltelefoner.

Oppgaven beskriver hvordan RFID-teknologi i varer og reklame kan forenkle kjøpsprosessen, og gjøre m-handel mer brukervennlig og tilgjengelig for alle.

Leseguide

Oppgavens hovedtema er e-handel, og oppgaven starter derfor med å ta for seg de forskjellige former for handel; fra byttehandel til m-handel. For at bruken av mobilhandel skal vokse, er det viktig at det utvikles en elektronisk lommebok. En personlig profil vil være viktig for å øke bruken av den elektroniske lommeboken. Mobiltelefonteknologi er svært avgjørende for utviklingen av en elektronisk lommebok, og oppgaven behandler derfor temaene mobiltelefon, dens operativsystem og SIM-kort.

Dagens mobilhandel har en del svakheter som gjør at bruken ikke er så utbredt som ønsket. Oppgaven foreslår et sett av forbedringspunkter for å øke bruken og brukervennligheten til mobilhandel. og oppgaven utreder for at RFID kan være løsningen. RFID er et auto-ID system, med mange likhetstrekk med dagens strekkoder, men har også et mye større potensial. Oppgaven belyser bruksområdene til RFID ved å utrede de tekniske spesifikasjonene til RFID, og ved å beskrive dagens bruksområder av RFID. Noen av de RFID-løsninger som kan forbedre mobilhandel blir spesifisert og modellert, og de krav som stilles til infrastrukturen for å realisere disse løsningene blir beskrevet.

Strukturen av kapittlene er:

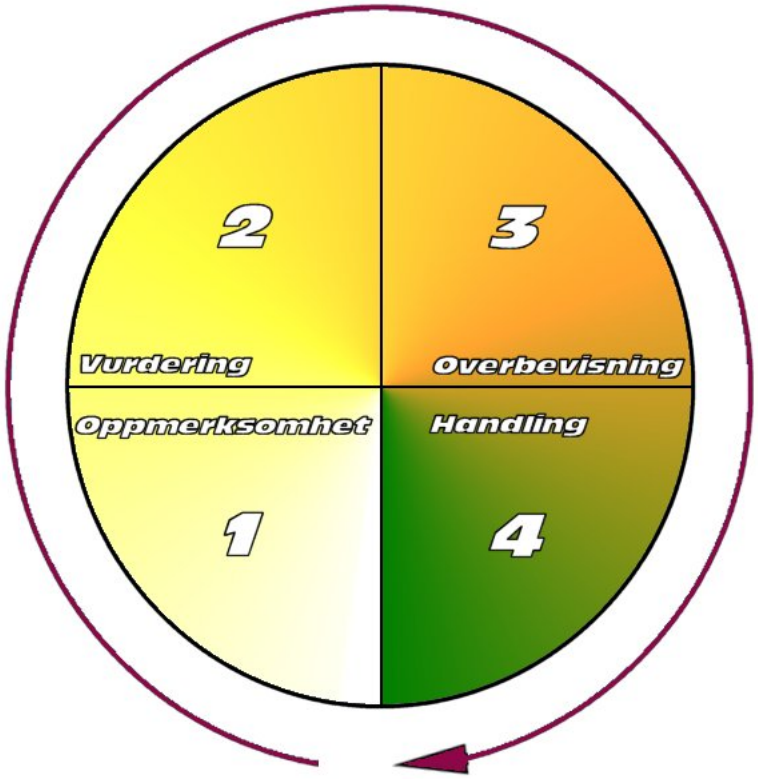
1. Handel
   Her går oppgaven inn på handel, kjøpsprosessen og dagens e-handelsløsninger.
2. Elektronisk lommebok i mobilen
   Oppgaven belyser her komponentene som kreves for en elektronisk lommebok og personlig profil.
3. Mobiltelefoner
   Dette er en introduksjon til mobiltelefonteknologiene. Oppgaven belyser spesiellt teknologiene operativsystem, SIM-kort og mobilnettet.
4. Automatiske ID-systemer
   Her presenteres bruken av auto-ID systemer, og RFID introduseres som et auto-ID system.
5. Virkemåten til RFID
   Teknologien bak RFID og de problemene som er blitt løst med RFID-teknologi.
6. Vår løsning
   Hvordan RFID kan løse problemene til dagen mobilhandel.
7. Systemkrav
   De kravene som stilles til infrastrukturen for å utvikle en komplett elektronisk lommebok som beskrevet i "vår løsning".
8. Avslutning
   Her avsluttes oppgaven med oppsumering og konklusjon.

1 Handel

Kjøpsprosessen er den prosessen som gjennomgås fra kjøperen føler et behov, til handelen er utført. Det er viktig å gi kundene anledning til å orientere seg om produkter, tilbud og priser på en så enkel og oversiktlig måte som mulig, og så tidlig i kjøpsprosessen som mulig.

Kjøpsprosessen består av følgende fire trinn:

1. Oppmerksomhet (kunden gjøres oppmerksom på et behov eller en mulighet)
2. Vurdering (det foretas en vurdering av behovet)
3. Overbevisning (kunden må overbevises, finne trygghet i at løsningen er den riktige)
4. Handling (det faktiske salg/kjøp foretas). Kundeservice har mulighet til å få kunden tilbake til trinn 1.



Figur 1: Kjøpsprosessen

1.1 Betalingsformer

For å kunne akseptere et bytte av tjenester og varer mot penger, må man kunne stole på at disse pengene igjen kan byttes mot andre varer og tjenester. I tidligere tider ble dette løst ved å lage pengene selv av gull, sølv eller andre verdifulle materialer. Dette forsikret at pengene hadde en faktisk verdi. Flere tusen år senere kom det virkelig store gjennombruddet, nemlig seddelen. Seddelen har i seg selv ingen verdi. Den er bare et løfte om at man er god for en viss sum.

Etter hvert fikk vi sjekker og kreditt, som tillater at vi kjøper en vare uten at vi betaler for den med en gang. I stedet har vi en mellommann i transaksjonen som garanterer for pengene. Med debetkort og bankterminaler kan vi nå trekke pengene direkte fra vår bankkonto, slik at betalingen skjer med en gang. Når vi i oppgaven snakker om bankkort og betalingsterminaler er det debetkort som menes, i motsetning til kredittkort hvor betalingen skjer via kreditt. Det finnes også andre betalingsformer, som lojalitetspoeng og mikrotransaksjoner.

Vi kan derfor si at det er flere måter å betale for en vare på, som kan deles inn i to grupper: forskuddsbetaling og betaling på etterskudd. Kontanter og bankterminaler gir oss forskuddsbetaling, og sjekker og kredittkort er betaling på etterskudd. Mikrotransaksjoner og elektronisk handel kan være i begge gruppene.

1.1.1 Betalingsterminaler

I 1972 ble Bankenes BetalingsSentral (BBS) AS etablert, og i 1991 ble BankAxept AS etablert. Fra 1. april 1996 opererte konsernet som én organisasjon, profilert med navnet BBS, og i november 2001 fusjonerte mor- og datterselskapet. Det nye navnet ble Bankenes BetalingsSentral AS [BBS].

Det første bankkortet med magnetstripe ble introdusert i 1972 av Europay. Magnetstripen er sammensatt av små jernpartikler i en slags plastikkfilm. Hver partikkel er i virkeligheten en liten magnet, 20-milliontedeler av en tomme stor, som ligner mye på magnetbåndet i en kassett. Magnetstripen kan lagre data fordi de små magnetene kan magnetiseres enten som nord eller sør.

Det er vanligvis tre spor på magnetstripen. Magnetstripekort bruker vanligvis bare spor 1 og 2. Spor 3 er et lese/skrive spor (som inkluderer en kryptert PIN[1], landskode, valuta type og maksimumsgrense), men dette sporet er ikke standardisert hos bankene.

Magnetkort har en stor svakhet, nemlig at de er mulige å kopiere. For å forbedre dette må magnetstripen byttes ut med en mikrochip. Kort som bruker slike mikrochip kalles smartkort, og fordelen er blant annet at de ikke kan kopieres.

Det første smartkort ble tatt i bruk i Frankrike i 1982. De ble først tatt i bruk i Norge som bankkort i 1987. Usikkerhet omkring teknologien førte til at de nye kortene ikke slo igjennom. Norske banker har enda ikke byttet ut magnetstripekortene, men prosessen er i gang [HowStuffWorks Creditcard].

[1] Personal Indetification number

1.1.2 Kreditt

Vanligst i Norge er bankkort med VISA. Dette er debetkort som trekkes direkte fra bankkontoen din, og som har en VISA-del du kan benytte for eksempel på reise i utlandet. VISA kort har også et kortnummer som er trykket på fremsiden av kortet. Dette kortnummeret kan benyttes til å betale for varer og tjenester over Internett. Brukeren må da oppgi kortnummeret og persondata. Denne form for betaling har noen åpenbare svakheter. Dersom noen stjeler et kort kan de i mange tilfeller betale for sine tjenester med det stjålne kortet. Ved bestilling av varer er det litt vanskeligere, siden leveringsadressen kan avsløre tyven.

1.1.3 Lojalitetspoeng

I dag tilbyr enkelte butikker og bedrifter bonuspoeng eller lojalitetspoeng til kunder som ofte kjøper varer eller benytter seg av tilbudte tjenester. Disse lojalitetspoengene kan brukes videre i samme butikk eller bedrift. Et steg videre vil være å kunne få et felles poengsystem for alle butikker og bedrifter. Dette vil gi brukeren en bedre oversikt over sine lojalitetspoeng.

1.1.4 Mikrotransaksjoner

Mikrotransaksjoner er små enhetsbeløp som for eksempel kjøp av en artikkel på nett eller en musikkfil. Disse små transaksjonene kan behandles på samme måte som telefonregning; man samler opp bruken, og får en regning for eksempel i slutten av hver måned. Ved å samle opp disse til èn regning, slipper man kontobelastninger for hver mikrotransaksjon. Dette gir bedre oversikt på bankkontoen og færre gebyrer.

1.2 Elektronisk handel

Nærings- og handelsdepartementet sier i grunnlagsdokumentet "Rammebetingelser for elektronisk handel" fra november 1998 at e-handel kan i korte trekk defineres slik:

> *"Med elektronisk handel menes alle former for kommersielle transaksjoner og forretningsvirksomhet over åpne elektroniske nett, dvs. all avtaleslutning via nett. Disse transaksjonene kan være knyttet til bestilling og levering av fysiske varer og tjenester, men kan også omfatte overføring av digitaliserte varer og tilgang til tjenester."* [Statens forvaltningstjeneste 1998]

Ut fra dette og den videre beskrivelsen fra Nærings- og handelsdepartementet. Kan vi dele elektronisk handel opp i 4 grader / nivåer:

1. Tilstedeværelse på nettet
2. Bestilling av varer og tjenester på Internett

3. Betaling på Internett

4. Mottak av varer og tjenester på Internett

1.2.1 M-handel

> *Mobilhandel er et supplement til e-handelen hvor informasjonsinnhenting og kjøp foregår via mobiltelefon* [Davidsen & Tepfers 2002].

Det vil med andre ord si at m-handel[2] er elektronisk handel basert på mobil adgang til Internett. M-handel strekker seg fra kjøp av logoer og ringetoner, til bestilling av blomster og betaling av parkeringsavgifter.

Det er pr. i dag registrert 4.376.000 mobilabonnement i Norge. Dette tilsvarer at 96% av befolkningen har mobiltelefon [Post- og teletilsynet 2004]. Markedet for lokasjonsavhengige tilbud er store for mobilhandel. Brukeren har vanligvis med seg telefonen, og tjenesteleverandørene kan tilby varer og / eller tjenester på steder som for vanlig elektronisk handel er umulig [Hansson 2003].

I Norge er det i dag flere store aktører på markedet. Telenor og DnB NOR samarbeider om SmartPay. Andre aktører på markedet er blant annet HandCash og Payex.

SmartPay

SmartPay er et prosjektsamarbeid mellom DnB NOR og Telenor. Prosjektet er innen mobilhandel og sikre betalingsløsninger for mobiltelefon.

Figur 2: MobilHandel sin logo

Telenor Mobil tilbyr sine brukere en tjeneste som heter MobilHandel. Denne tjenesten gjør det mulig å betale for enkelte varer og tjenester med mobiltelefonen. Betalingsløsningen i MobilHandel er SmartPay. Tjenesten ble introdusert i slutten av 2001 [TNMH1].

SmartPay garanterer brukerne en sikker elektronisk handel. Dette betyr at sensitive kundeopplysninger ikke blir sendt ut på telenettet. ZebSign AS har

[2] Mobilhandel

utviklet løsningen for de elektroniske identifikasjonene. Den elektroniske identifikasjonen ligger lagret på brukerens SIM-kort[3], og det er kun denne ID-en som blir sendt over nettet.

Betalingsløsninger

Betalingsløsningene SmartPay tilbyr er flere. Varer kan betales ved trekk fra vanlig bankkonto, kredittkort eller fra en småpengekonto. Denne småpengekontoen heter SmartCash. SmartCash er en konto som kan sammenlignes med kontantkort for mobiltelefon. Denne kontoen må fylles opp av brukeren for å kunne brukes. Overføring til kontoen skjer som en vanlig banktransaksjon.

Oppstart

Det er en forutsetning at brukeren er kunde av Telenor. For å kunne benytte seg av de tre forskjellige betalingsmåtene må man også være kunde hos DnB NOR. Er man ikke kunde hos DnB NOR, kan man likevel benytte seg av SmartCash løsningen. I tillegg må en kunde inngå en egen avtale med ZebSign. Denne avtalen gjelder bruk av den elektroniske ID-en og et sertifikat ZebSign tilbyr. Denne ID-en kan også brukes i andre sammenhenger. Over 700.000 brukere er i dag tilknyttet SmartPay [Bentzen Ernes 2004].

Andre aktører

Den største konkurrenten til SmartPay er Payex. Payex har til nå fokusert mest på netthandel, men beveger seg nå også mer over på mobilmarkedet. HandCash er en annen aktør som forsøker å komme inn på markedet.

Payex

Dette er en løsning hvor brukeren registrerer en konto. Brukeren kan via nettbank, mobiltelefon, kredittkort, giro eller bank sette inn penger på kontoen.

Kjøperen vil også her på vanlig måte bruke handlekurvene på nettstedet. Men er det aktuelle firmaet registrert hos Payex, vil kjøperen bli koblet direkte mot deres betalingsserver etter å ha valgt denne betalingsformen. Der blir kjøperen bedt om å oppgi brukernavn og passord før vedkommende godkjenner at beløpet trekkes fra kontoen. All bruk er gebyrfri [eSolutions]. Over 375.000 nordmenn har nå etablert en Payex konto for betaling over nett. [Bentzen Ernes 2005]

Figur 3: Payex sin logo

[3]Subscriber Identity Module

HandCash

En annen aktør som forsøker å komme inn på markedet er HandCash. Dette er et kontantkort, som uten personlig registrering, vil gi deg muligheten til å handle i nettbutikker.

Figur 4: HandCash sin logo

> *"Vi tror dette vil være med og bidra til at internetthandel virkelig tar av"*, sier gründer i HandCash, Petter Nemeth.

I startfasen vil det kun være mulig å bestille kortet via Internett, men det vil i løpet av kort tid bli å finne i kiosker og dagligvareforretninger på samme måte som kontantkort til mobiltelefoner. Foreløpig vil det bare være mulig å kjøpe kort med 300kr, men lansering av 100kr og 1000kr planlegges.

Kjøperen vil fremdeles på vanlig måte bruke handlekurvene på nettstedet. Men er det aktuelle firmaet registrert hos HandCash, vil kjøperen bli koblet direkte mot deres betalingsserver etter å ha valgt denne betalingsformen. Der blir kjøperen bedt om å oppgi kortkoden før vedkommende godkjenner at beløpet trekkes fra kortet. [HandCash]

2 Elektronisk lommebok i mobiltelefonen

Elektroniske lommebøker inneholder en samling av informasjon om hvem du er, akkurat slik man finner i en vanlig lommebok i dag. Her ligger legitimasjonskort, førerkort, debetkort, kredittkort, kontanter og medlemskap i organisasjoner, grupper og klubber.

En elektronisk lommebok integrert i en mobiltelefon og kan inneholde personlig betalingsinformasjon som navn, leveringsadresse, kundenummer, personnummer, kredittkortnummer og elektroniske penger. Denne elektroniske lommeboken er personlig eid av den som den er registrert på, slik at ingen har rettigheter til den uten samtykke fra eieren og bruken av den er beskyttet med en PIN kode.

For at en elektronisk lommebok som er integrert i en mobiltelefon skal kunne bli et brukervennlig, sikkert og utbredt produkt, må kjøpsmønsteret ikke gjennomgå store endringer eller gjøres mer komplisert. Trådløs betaling vil være den mest nødvendige integrasjonen i en mobiltelefon for å kunne møte kundenes ønsker om mindre kompleksitet. Dette er en teknikk som flere store firma nå vurderer å satse på. Det japanske firma DoCoMo sa i en pressemelding 27. april 2005 at de hadde planer om å utvikle en mobiltelefonbasert kreditkortløsning basert på trådløsteknologi [Hara2005].

2.1 Komponenter som eksisterer i dag

Det eksisterer i dag teknologi og infrastrukturer for noen av delene som må integreres inn i en elektronisk lommebok. Her er en kort oversikt over noen av de funksjonene som allerede er i bruk i dag.

Elektronisk Identifikasjon

En elektronisk lommebok i form av et smartkort, vil ha påtrykt bilde og signaturtrekk som dagens debetkort. Dette vil ikke være mulig å få til på en mobiltelefon og man blir nødt til å bruke et digitalt sertifikat. Et digitalt sertifikat er enkelt sagt legitimasjon i elektronisk form. Digitalte sertifikater benyttes særlig over åpne nett, som internett, for å bevise at man er den man gir seg ut for å være. Digitale sertifikater benyttes også for å kontrollere at en digital signatur er en gyldig og ekte signatur, og ikke en forfalsket digital signatur. Den mest brukte standarden for digitale sertifikater heter X.509 [Lie 2003]. BankID og ZebSign er de største norske aktørene innen PKI [4]. ZebSign leverer blant annet løsninger for SmartPay, mens BankID er bankenes egen standard.

Elektroniske kontanter

Penger som er lagret på smartkort eller andre digitale lagringsmedia blir betraktet som elektroniske kontanter. Elektroniske kontanter har de samme egenskapene som kontanter, de tillater anonym og gebyrfri betaling.

[4] Public Key Infrastructure. Se vedlegg 2 for mer informasjon

eCash er et selskap som har utviklet en løsning for elektroniske kontanter [eCash], som lisensieres bort slik at de kan kjøpes flere steder. Teknologien er basert på kryptering[5] (offentlig-nøkkel), slik at kjøpere kan sende penger via e-post uten frykt for tyveri eller forfalsking.

2.2 Under utvikling/mulige forbedringer

En elektronisk lommebok vil også være nødt til å inneholde flere funksjoner og være anvendbar i forskjellige systemer/infrastrukturer. Under listes mulige fremtidige funksjoner for en elektronisk lommebok.

Lojalitetspoeng
Lojalitetspoeng lagres på mobiltelefonen og vil gi kunden en rask oversikt over hvor mange poeng som er samlet inn. Disse lojalitetspoengene kan lastes opp fra mobiltelefonen og opp til en database for sikker lagring ved evt. tap av mobiltelefonen.

Mikrotransaksjoner
En bruker vil alltid kunne undersøke hvor stor mikrotransaksjonsregningen er da hver handel registreres på mobiltelefonen. Brukeren kan også for eksempel sette en øvre grense for tillatt beløp å bruke på slike kjøp.

Kvitteringshåndtering
For hver transaksjon som utføres i dag følger det med en kvittering. Disse kvitteringene kan lagres digitalt i den elektroniske lommeboken. Dette tillater brukeren enkelt å sette opp regnskap, reiseregninger og lignende ved enten bruke mobiltelefonen eller overføre kvitteringene til en PC og bruke et sterkt verktøy som er tilgjenglig.

Personlige agenter
Den elektroniske lommeboken kan ta imot reklame og bruke tidligere handlingsmønster til å informere om gode tilbud, eller gjennomføre egne periodiske innkjøp på egen hånd.

Informasjonsinnhenting
En trådløs elektronisk lommebok på en mobiltelefon kan lese av informasjon fra systemer som støtter lommeboken og utnytter dens funksjoner. Dette kan være alt fra å lese av en URL[6] og gå direkte til en hjemmeside på WAP[7] uten at brukeren må skrive inn adressen, eller man kan hente ned informasjon om en kinoforestilling fra en plakat og starte en applikasjon for å bestille billetter. Har man to mobiltelefoner med samme system kan man overføre kontanter, visittkort og lignede mellom de elektroniske lommebøkene.

[5] Se vedlegg 2 for mer informasjon om kryptering
[6] Unified Resource Locater
[7] Wireless Application Protocol

2.3 Personlige profiler

Personlige profiler inneholder noen konstante data om brukeren [Davidsen & Tepfers 2002]. Den kan også inneholde en del som endrer seg med bruksmønsteret til eieren. Dette kan være alt fra matvaner til nyhetsinteresser. Denne personlige profilen kan være lagret hos en offentlig godkjent TTP[8] og kan inneholde store mengder informasjon som brukeren endrer og legger til etter ønske. En lokal profil vil ligge på den elektroniske lommeboken i mobiltelefonen og inneholde bare den nødvendige informasjonen for å kunne utføre alle dens funksjoner. Personlige agenter kan også benytte seg av profilen for å finne gode tilbud for brukerne.

Hver gang kunden besøker et nytt nettsted kan kunden sende med den personlige profilen. Dette gir mulighet for å få et personalisert og relevant tilbud. I denne profilen kan kunden selv velge hvor mye informasjon som skal deles med nettstedet, og den gir mulighet for å bli oppdatert på bakgrunn av tidligere handlinger på nettstedet. Informasjonen som sendes vil gi butikkene mulighet til å gi brukerne personaliserte løsninger samtidig som å ivareta sikkerhet og valgmulighetene til kunden. En personlig profil kan brukes av en personlig agent, som følger og lærer av brukerens handlinger. Etterhvert vil agenten kunne muligens ta over kommunikasjonen med nettstedet basert på tidligere handlinger [Davidsen & Tepfers 2002].

Standard

OPS[9] er foreslått som en standard for personlige profiler, men ingen avgjørelse er avtalt på dette tidspunkt. OPS har en todelt funksjon: Tillate websider å personalisere sine sider mot hver enkelt individuell bruker, og tillate brukeren å ha full kontroll over hvilken informasjon han/hun vil dele med nettsiden. OPS var foreslått som plattform for P3P[10] av W3C[11] I 1997.

For at en personlig profil skal kunne være levedyktig og kunne anvendes på alle nettsteder må den være universell. Det finnes mange krav til universelle profiler, her er noen av dem:

- Den personlige profilen må kunne gi kunden automatisk identifisering
- Kunden må ha tilgang til å oppdatere profilen og bestemme hvilken informasjon de ulike butikkene skal få ta del i
- Så mange bedrifter som mulig må støtte universelle profiler
- Det bør ikke finnes noen sentral institusjon som kan lese alle profildata

Det finnes tilbud på profiler på nettet i dag, og to av dem er: Microsoft Passport og AOL Magic Carpet [Davidsen & Tepfers 2002].

[8] Tiltrodd Tredje Part, se vedlegg 2 for mer informasjon
[9] Open Profiling Standard
[10] Privacy Preferences Project
[11] World Wide Web Consortium

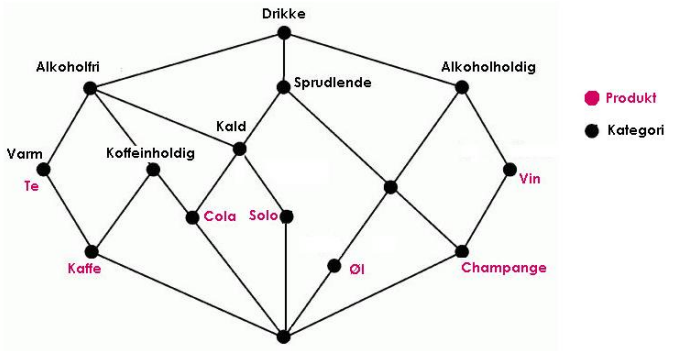
En personlig profil bør inneholde følgene:

- En unik ID for profilen.
- En unik ID for hver nettside som er besøkt. Brukes til å kontrollere hvor mye av profilen en nettside skal få se.
- Demografiske data (Land, postnr., alder, kjønn).
- Kontaktinformasjon (Navn, adresse, postnr., telefonnummer, e-post o.l.)
- En eller flere seksjoner for e-handel informasjon, som kredittkortnummer.
- Detaljerte personlige preferanser (Hobbyer, favorittaktiviteter, favorittfilmer, favorittblader osv)
  [Whatis2005]

Varekategorisering

For at den personlige profilen skal kunne filtrere ut tilbud som ikke er aktuelle for brukeren må vareinformasjonen være representert på en standarisert måte. Det må være mulig for agenten å finne ut nøyaktig hvilket produkt det reklameres for. For å lese dette problemet har W3C utviklet en standard med navnet Resource Description Framework [Brickley og Guha 2004], et språk for å gjøre informasjon ikke bare maskinleselig, men også maskinforståelig. For å kunne integrere denne semantikken i en tekst trenger man en ontologi. En ontologi er et system innenfor et bestemt fagområde som inneholder termer, spesifikasjon av disse termene og hvordan de er beslektet. Ontologier gir muligheten til å skape en unedelig mengde av forskjellige semantiske relasjoner. Ontologier er også en del av utviklingen av semantisk web dvs. det som liger i ønsket om å utvikle web'en til å bli et vertøy som gir muligheter for mer direkte kommunikasjon.

Under er en enkel illustrasjon av en liten ontologi. Vi ser for eksempel av figuren at produktet Solo tillhører kategoriene: kald, sprudlende, alkoholfri og drikke.



Figur 5: Eksempel på en enkel ontologi

3 Mobiltelefoner

En mobiltelefon er en bærbar kombinert radiosender og -mottaker. Ofte kalles den bare mobil. Mobiltelefoner har eksistert siden midten av åttitallet, men det er ikke før rundt 1995 at de begynte å få en overkommelig pris og størrelse for de fleste [SSB2000].

Mobiltelefoner sender signaler til nærliggende basestasjoner som er tilknyttet telefonnettet ved hjelp av en optisk fiberkabel eller en radio som bruker mikrobølger. Når mobiltelefonapparatet forlater en basestasjons dekningsområde overfører telefonsentralens datamaskin telefonen til neste basestasjon. Mobiltelefonene brukte opprinnelig FM[12], men for tiden benyttes forskjellige digitale modulasjoner. Standarden for mobiltelefoni i Europa er GSM[13], mens USA og andre deler av verden benytter CDMA2000[14] samt andre standarder. Disse standardene er som oftest kompatible, slik at man kan benytte europeiske apparater i Amerika, og motsatt. Den første norske og nordiske standarden ble kalt NMT[15].

Mobiltelefoner kan både ringes med og brukes til å sende korte tekstbeskjeder, også kalt SMS[16]. Etter hvert har telefonapparatene blitt mer avanserte og enkelte modeller er utstyrt med digitalkamera. Med MMS[17] kan telefonen brukes til å sende og motta digitale bilder.

3.1 Telenettsystemer

Det mobile telenettet har eksistert i knappe 25 år men har rukket å endre seg mye. Det er også mange endringer som står for tur. Hver stor oppdatering av det mobile telenettet betegnes som en ny generasjon. Vi betegnet det første nettet som 1G, og har nå akkurat innført det vi kaller 3G.

1G (NMT)

Det mobile telenettet NMT ble åpnet i 1981. Dette nettet var et analogt telenett som opererte i frekvensområdet 450MHz. Dette blir av mange kalt første generasjons mobilnett 1G. I 1985 var trafikken så stor på nettet at noe måtte gjøres. I Oslo-området var det et gjennomsnitt på 22.000 samtaler daglig. Televerket hadde i 1983 startet utviklingen av et større nett, NMT-900. NMT-900 ville innebære bortimot tredobling av kapasiteten på nettet. Det nye nettet ble åpnet i slutten av 1986. 30 land innførte etter hvert NMT-450, drøyt ti land fikk også NMT-900. NMT fikk også senere implentert SMS, men dette ble ikke støttet i Norge.

[12] Frekvensmodulasjon
[13] Globalt System for Mobilkommunikasjon
[14] Code-Devition Multiple Access
[15] Nordisk mobiltelefonsystem
[16] Short Message Service
[17] Multimedia Messaging Service

2G (GSM)

ETSI[18] begynte arbeidet med å utvikle GSM i 1982, og opprinnelig sto GSM for Group Special Mobile, senere ble dette endret til det engelske Global System for Mobile Communication. GSM regnes som 2. generasjons mobilsystemer 2G. I 1993 kom oppfølgeren til NMT, det digitale nettet GSM, som opererer i frekvensområdet 900MHz. Dette nettet ble svært populært og på slutten av 90-tallet måtte nettet utbygges med et ekstranett i frekvensområdet 1800MHz. I dag er alle telefoner dualband telefoner, det vil si at de støtter begge GSM nettene. Telefonen bruker mindre strøm når den bruker 900MHz nettet, og velger derfor dette som standard. Skulle dette nettet ha stor trafikk, så bytter telefonen selv til 1800MHz. Dette skjer uten at brukeren merker noe.

GSM brukes i nesten alle europeiske land. USA, Canada og flere land i Asia bruker kompatible standarder. Forskjellige land bruker forskjellige bånd; Norge har 900 MHz og 1800 MHz, mens USA og Canada bruker 1900 MHz. Mobiltelefoner som støtter alle tre frekvenser kalles tri-band-telefoner.

Selv om det er finske (Nokia) og svenske (SonyEricsson) firma som gjør store penger på mobilteknologi er GSM-standarden en norsk oppfinnelse. Standarden ble utviklet av Torleiv Maseng i 1987, da han ledet et prosjekt ved Sintef/Elab som skulle lage Norges forslag til radiodelen til ny europeisk standard for digital mobiltelefon [Gran 2004].

GSM tillater i tillegg til stemmeoverføringstjenester andre tjenester som SMS og WAP. GSM tillater dataoverføring med hastigheter på 9,6 Kbps (inntil 38,4 kbps. med HSCSD[19]).

2.5 G (GPRS)

GPRS[20] er en standard for trådløs mobilkommunikasjon, og etterfølgeren til GSM. Mens GSM har en maksimal dataoverføringshastighet på 38,4 kbps, er maksimal hastighet til GPRS på 171,2 kbps. Dette er imidlertid en teoretisk øvre hastighet. Her i Norge er maksimal hastighet for første generasjon GPRS på 40 kbps. GPRS ble introdusert i Norge i begynnelsen av 2001. GPRS er en pakkesvitsjet teknologi (GSM er linjesvitsjet), som gir en forbindelse som alltid er på, dvs. at man kan motta e-post, surfe på Internett, e.l. uten å måtte koble seg opp først. I stedet for tellerskritt betaler man enten en fast månedsavgift eller for de datamengdene som blir overført. Her i Norge blir det siste betalingsalternativet benyttet. Mobiltelefoner som støtter GPRS kalles gjerne GPRS-terminaler. Brukerne i GPRS-nettet deler på kapasiteten som er tilgjengelig, slik at ytelsen i praksis kan variere i den tiden man er oppkoblet. Dersom all kapasitet på basestasjonen er oppbrukt, vil taletrafikk ha prioritet fremfor data, og dataoverføringshastigheten vil synke. GPRS er en såkalt 2,5G teknologi [Wiley2001].

[18] European Telecommunications Standards Institute
[19] High-speed Circuit-Switched Data
[20] General Packet Radio Service

EDGE

EDGE[21], er en utbygging av GSM, som gir hastigheter opp til 384 Kbps. EDGE standarden er bygget på det eksisterende GSM-nettet, og bruker den samme TDMA[22] strukturen.

EDGE ble ikke tilgjengelig før november 2004, samtidig som UMTS. EDGE kan ikke måle seg med hastigheten til UMTS[23], men kan være et bra supplement i de områdene som ikke har UMTS dekning.

3G (UMTS)

UMTS, eller 3G som det også kalles er bredbånd, pakke-svitsjet transmisjon med en hastighet på opp til 2Mbps[24]. Standarden er basert på GSM, og kan derfor bygges ut i store deler av verden. Brukere har da en trådløs bredbåndsforbindelse og kan surfe på Internett mens de er på reisefot. Skulle man komme til et område som ikke har UMTS-dekning, så byttes det automatisk til den teknologien som er tilgjengelig. Dette skjer på samme måte som mobiltelefoner i dag bytter mellom GSM 900 og 1800.

Dagens mobiltelefoner er hovedsaklig linje-svitsjet, hvor forbindelsen avhenger av tilgjengeligheten på linjer. En pakke-svitsjet forbindelse som bruker IP[25], har en forbindelse som er alltid på. Høyere båndbredde på UMTS gir også rom for flere muligheter, som videokonferanser [Wiley2001].

3.2 Overføringsprotokoller

For å kunne benytte mobiltelefonen til å surfe på nett eller å motta tekstmeldinger og bilder er det standardisert en del protokoller. SMS og MMS brukes til å sende informasjon til eller fra en mobiltelefon. WAP er en protokoll som går over GPRS eller UMTS.

SMS

SMS er en tjeneste som er tilgjengelig på de fleste moderne mobiltelefoner. Tjenesten gjør det mulig å sende korte meldinger (også kalt SMS-er eller tekstmeldinger) mellom mobiltelefoner, andre håndholdte enheter, og også fasttelefoner.

En meldings maksimale størrelse er 140 bytes; dette gir enten 160 7-bits tegn, 140 8-bits tegn. Ikke-teknisk informasjon om hvor meldingen skal sendes og annen meta-informasjon kommer i tillegg. De fleste nyere mobiltelefoner tillater imidlertid at lengre meldinger kan sendes ved at mobiltelefonen deler opp meldingen og sender hver del for seg. Mottakerens mobiltelefon setter så sammen denne meldingen igjen, slik at det virker som om det bare er én større melding som er blitt sendt. Det er verdt å merke seg at denne metoden fører til at man belastes for flere sendinger ikke bare én sending [Longueuil2002].

[21] Enhanced Data GSM Environment
[22] Time-division multiple access
[23] Universal Mobile Telecommunications Service
[24] Megabits per sekund
[25] Internet Protocol

MMS

MMS tillater sending og mottak av bilder, lyd og tekst i en og samme melding til mobilen. MMS kan sende meldinger med opp til 100KB.

WAP

WAP er en åpen internasjonal standard for trådløs overføring av data, til f.eks. mobiltelefoner og Internett. WAP ble utviklet av Ericsson, Nokia, Motorola og Phone.com (tidl. Unwired Planet). De første WAP-telefonene ble lansert i november 1999. Språket som blir brukt til WAP er WML[26] [Longueuil2002].

3.3 Dataoverføring

Stadig flere mobiltelefoner støtter også dataoverføringsmetoder som ikke benytter telenettet. IrDA[27] har tidligere vært den vanligste overføringsmetoden, men stadig flere mobiler støtter nå blåtann. Planer om å integrere RFID[28] i mobiltelefoner finnes også.

IrDA

IrDA-standarden kom tidlig på 90-tallet takket være Hewlett-Packard. IrDA hadde i starten støtte for 115.2-Kbit/s overføringshastighet, og med 1m rekkevidde. En 4-Mbit/s versjon ble senere utviklet. Denne ble meget utbredt på bærbare PC-er. En 16-Mbit/s versjon ble også laget. Problemet med IrDA er ikke bare den korte rekkevidden, med også at den trenger LOS[29] [Frenzel 2002].

Blåtann

Blåtann[30] er en radiooverføringsprotokoll som benyttes for å sende og motta data trådløst mellom enheter i et personlig datanett sammensatt av mobiltelefon, datamaskin, og/eller andre enheter som støtter protokollen. Blåtann krever en liten transponder som kan sende og motta i et til nå ubrukt frekvensområde 2.45 GHz (noen små variasjoner finnes fra land til land). Maksimumavstanden er 10m, og datahastigheten er 1Mbps. Blåtann trenger ikke LOS, den kan til og med gå gjennom vegger. Blåtann ble først utviklet av Ericsson, og senere formalisert av SIG[31], som ble presentert den 20. mai 1999. SIG var sammensatt av Sony Ericcsson, IBM, Intel, Nokia og Toshiba.

Navnet er inspirert av kong Harald Blåtann (Harald II (Gormsson) Blåtann) som forente Danmark og Norge og var konge fra 958 til 987 [Ganguli2002].

[26] Wireless Markup Language
[27] Infrared Data Association (infrarød dataoverføring)
[28] Radio Frequency Identificaton
[29] Line-of-sight (fri sikt)
[30] Engelsk: Bluetooth
[31] Bluetooth Special Interest Group

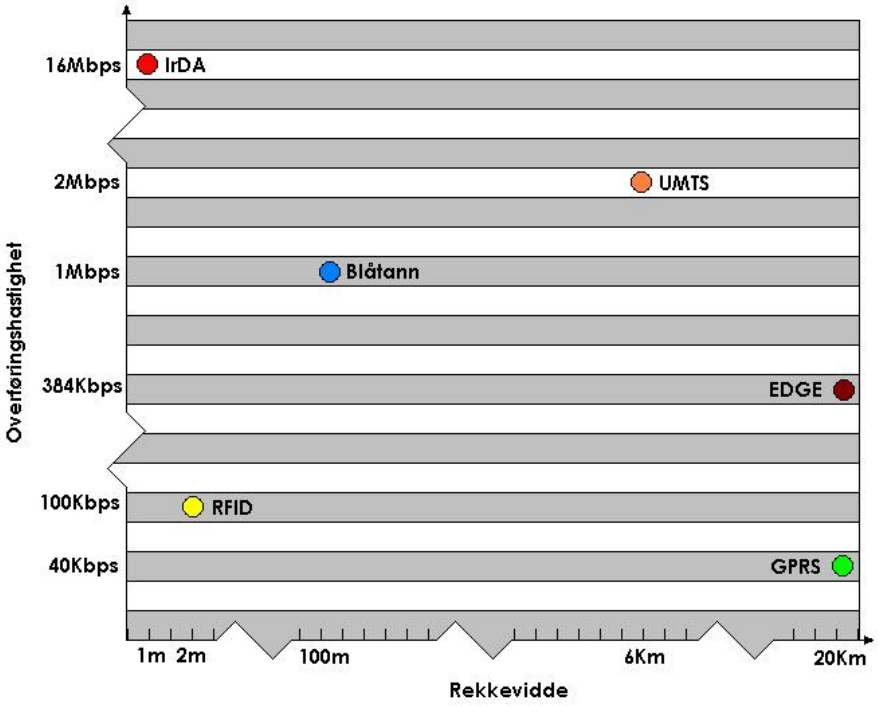
RFID

RFID er liten silikonbrikke med en antenne. Strømtilførsel tilføres trådløst til RFID-brikken via antennen. Det finnes mange forskjellige RFID-systemer. Noen har så kort rekkevidde som 1cm, mens andre har flere meter. De mest vanlige systemene har ca. 1m rekkevidde og en overføringshastighet på 100Kbps.

Tabellen viser de mest vanlige standardene, men det finnes forskjellige versjoner som opererer med annen rekkevidde og overføringshastighet.

Standard	Rekkevidde	Overføringshastighet
Blåtann	10m til 100m	1Mbps
IrDA	<1m LOS	4Mbps til 16Mbps
RFID	<2m	100Kbps
GPRS	<20Km	1Kbps til 40Kbps
EDGE	<20Km	1Kbps til 384Kbps
UMTS	6Km til 10m	144Kbps til 2Mbps

Tabell 1: Overføringsstandarder



Figur 6: Grafisk fremstilling av tabellen over

3.4 Operativsystemer for Mobiltelefoner

Operativsystemet[32] er programvaren som kontrollerer og styrer en datamaskin, smartphone, PDA eller lignende. Operativsystemet fordeler prosessorkraft til de andre programmene som kjøres på systemet. De vanligste operativsystemene til PC er DOS, Windows, Linux og Unix, mens Apple-maskiner kjører et eget operativsystem som heter MAC OS. Mobiltelefoner har som nevnt også operativsystemer. Disse kan deles inn i to grupper; standard mobil operativsystem, og smartphone operativsystem. Hovedforskjellen er at smartphone operativsystemene har en plattform som tillater applikasjonsutvikling på mobiltelefonen, mens standard mobiloperativsystem kommer med standardiserte applikasjoner.

Smartphone

Smartphone er en kategori innen mobilutstyr som kan tilby avanserte muligheter utenom det som er vanlig for mobiltelefoner. På mange måter er dette en kombinasjon av mobiltelefon og PDA. Smartphones har komplette operativsystem som tilbyr et standardisert grensesnitt og en plattform for utvikling av applikasjoner. Eksempel på slike smartphoneoperativsystem er Symbian OS og Windows Mobile for Smartphones. Mobiltelefoner som ikke er smartphone har også et operativsystem, men dette er meget begrenset. Det er ikke mulig å skrive nye applikasjoner som kan knyttes direkte sammen med operativsystemet. Løsningen er blitt Java-applikasjoner for slike mobiltelefoner, også kalt J2ME[33]. Java-applikasjoner krever en JVM[34]-tolker for å kunne blir eksekvert. Dette fører til at Java-applikasjoner ikke har full tilgang til telefonens systemer, og ikke blir like raske. Nokia OS er et eksempel på et operativsystem for telefoner som ikke er en smartphone. Nokia OS Series 20 er en eldre versjon som ikke støtter Java, mens Series 40 er den nye versjonen som har Java-støtte.

Smartphone operativsystem

Verdenslederen innen operativsystemer for smartphone er i dag Symbian OS, men det finnes også andre store aktører som Linux, Windows og Palm, hvor Symbian og Windows er de som er å finne på det norske markedet.

[32] Forkortes OS
[33] Java 2 Platform, Micro Edition
[34] Java Virtual Machine

Sammenligning

Tabellen under sammenligner de forskjellige OS for smartphones. Som tabellen viser har i dag ingen av operativsystemene noen full støtte for RFID, men dette er under utvikling. Stading flere tidsskrifter forteller nå at de store operativsystemene for mobiltelefon vil lansere RFID-støtte i de neste versjonene [RFIDu2005]. Som er resultat av dette er det ikke mulig å utvikle en prototype av den elektroniske lommeboken i en mobiltelefon i dag.

OS	Markedsandel %	J2ME støtte	RFID støtte	Lisensiert utvikling	Blåtann/ IrDA støtte
Windows	14	Ja	Nei	Ja	Begge
Palm	13	Ja	Nei	Ja	Begge
Linux	6	Ja	Nei	Nei	Begge
Symbian	67	Ja	Nei	Valg fritt	Begge

Tabell 2: Sammenligning av mobiltelefon OS

Microsoft Windows Mobile for Pocket PC Phone Edition

Microsofts sitt operativsystem Windows Mobile har flere versjoner. Hovedsakelig er dette laget for lomme PC-er og PDA[35], men de har også laget en Phone Edition som skal brukes i smartphones. Windows Mobile bruker kjernen til operativsystemet Windows CE. Microsoft har valgt å beholde mye av utseende og funksjonalitet fra Windows for stasjonære PC-er, slik at overgangen ble mindre [MSMobile].

Telefoner som benytter Windows Mobile har som oftest store display, og ligner mer på en PDA enn en mobiltelefon. Telefonen på bildet under er et typisk eksempel på en slik telefon. Det er en Samsung SGH-i700, og bruker Windows Mobile. Den har et display med 240 x 320 oppløsning.

Figur 7: Samsung SGH-i700 (Windows)

[35] Personal Digital Assistant

Palm OS

Palm har i en årrekke vært ledende i utviklingen av PDA. Den første Palm ble introdusert i 1996 (Palm Pilot), og Palm trengte da ett egnet operativsystem. Det var ikke mange tilgjengelige løsninger på markedet. Så løsningen var å produsere sitt eget skreddersydde operativsystem.

Det har ikke være brukt som operativsystem for smartphones tidligere, men noen aktører har nå fattet interesse for operativsystemet. Xplore M68 er en smartphone som bruker PalmOS (se bildet under), og flere produsenter som PiTech og Samsung følger nå etter [Kairer 2005].

Figur 8: Xplore M68 (Palm OS)

Linux PDA

Linux er et Open Source operativsystem i Unix familien, utviklet av Linus Thorvalds. På grunn av sin robusthet og tilgjengelighet har Linux blitt veldig populært blant forbrukere og utviklere.

Linux har ikke blitt benyttet som OS for PDA-er i så lang tid, men i den senere tid har det blitt sluppet flere forskjellige OS-er som er Linuxbaserte, både for PDA og smartphones. Motorola er de første som benytter Linux på sine telefoner [Linuxdevices].

Figur 9: Motorola E680 (Linux)

Symbian

Symbian er i dag det mest brukte operativsystemet for håndholdte enheter (mobiltelefoner og PDA). Symbian ble etablert som et privat uavhengig firma i juni 1998. Det er eid av Ericsson, Nokia, Panasonic, Motorola, Psion, Samsung Electronics, Siemens og Sony Ericsson. Hovedkontoret ligger i Storbritannia, med avdelinger i Japan, Sverige og USA. Symbian har visjonen *"Symbian OS on every phone"*, og ser seg selv midt i sentrum av den teknologiske revolusjonen som skjer innenfor mobiltelefoner og håndholdte enheter i disse dager.

Figur 10: Siemens SX-1 (Symbian)

Ideen var å lage et felles operativsystem for håndholdte enheter fra forskjellige produsenter, slik at utvikling av programmer ville bli lettere. Likevel er programmer skrevet for en Symbian-telefon ikke nødvendigvis kompatibelt med en annen Symbian-telefon. Dette er fordi telefonene kan være forskjellige. Noen telefoner benytter en trykkfølsom skjerm hvor brukeren benytter en penn for å bruke telefonen, mens andre benytter et tastatur. Vi kaller dette ofte UI[36]. Det er likevel stor likhet i utviklingen av programmene, og en bedrift trenger ikke ha en ny opplæringsfase for sine utviklere, dersom de vil gå fra et UI til et annet. De fleste store produsentene er medeiere, dette øker troverdigheten til Symbian OS.

Symbian OS er et 32-bit multitasking operativsystem som er basert på EPOC. EPOC software arkitektur ble laget av Psion i 1990. EPOC ble benyttet på flere av Psion sine håndholdte enheter som Revo, Series 5mx, Series 7 og Netbook. EPOC ble etter vært videreutviklet mot smartphonemarkedet og omdøpt til Symbian.

Ericsson R380 Smartphone var den første som brukte Symbian OS, og ble lansert i 2000, mens det teknisk sett fortsatt var EPOC. De fleste nye mobiltelefoner kommer nå med Symbian OS. Nokia har for tiden flest Symbian-telefoner på markedet, og satser stort på sin hovedplattform Series 60 som bygger på Symbian OS. Businessmodellen til Symbian er svært enkel. Produsenter betaler en lisens til Symbian for hver solgte enhet som benytter Symbian plattformen [Symbian].

[36] User interface, Norsk: brukergrensesnitt

3.5 SIM-kort

Smartkort (Se vedlegg 1) som blir brukt i mobiltelefoner kalles SIM-kort, dette brukes til å lagre informasjon om telefonnummer til abonnenten, private krypteringsnøkler og støtter krypteringsprosessen. Et SIM-kort kan flyttes fra mobiltelefon til mobiltelefon uten at kunden må utføre noen endringer. Den sikre kommunikasjonen kan deles inn i 2 grupper: Den første delen tillater mobiltelefonen å koble seg opp mot nettverket for å identifisere seg og å opprette en forbindelse. Den andre delen tillater kommunikasjon mellom telefoner å være kryptert.

Dersom noen skulle få tak i en brukers SIM-kort og får laget en kopi, kan de bruke kortet dersom de kjenner brukerens PIN-kode. PIN-koden er ikke lagret på SIM-kortet, så det er derfor viktig at brukeren holder dette hemmelig. Skulle noen klare å lage en kopi samt å finne PIN-koden, kan de ringe gratis på brukerens regning.

3.5.1 Operativsystemer for smartkort

Smartkort har også et operativsystem slik som PCer eller smartphones. De tre vanligste operativsystemene for smartkort et BasicCard, JavaCard og MultOS.

Sammenligning

Tabellen under viser en sammenligning av smartkortoperativsystemenes egenskaper.

OS	Markedsandel	SIM-toolkit støtte	Multiapplikasjons støtte	Lisensiert utvikling
BasicCard	Minst	Ja	Nei	Gratis
JavaCard	Største	Ja	Ja	Gratis
MULTIOS	Mellomst	Ja	Ja	Lisensiert

Figur 11: Smartkort operativsystem

BasicCard

BasicCard er et meget enkelt, men kraftig operativsystem som tillater brukere å programmere smartkortet i BASIC. Med et OSX for Visual Basic, API-er[37] for C og Delphi. Kortene er Tilgjengelig med 1KB, 2KB, 8KB EEPROM[38] størrelser.

Figur 12: BasicCard logo

Aptura Java Card®

Aptura Java Card® plattform-baserte smartkort kjører Java teknologibaserte applikasjoner i form av byte-kode. Disse er lastet inn i minnedelen av smartkortets mikroprosessor hvor de kjøres av virtual machine. Den eksekverbare koden er derfor plattformuavhengig, slik at alle kort med en Java Card[a] technology-based tolker kan kjøre de samme applikasjonene. Kortene er tilgjengelig med 16KB og 32KB EEPROM størrelser på Hitachi chips.

Figur 13: Java logo

MULTOS®

MULTOS® ("Multiple Operating System") er et OS som tillater flere (multiple) applikasjoner å bli installert og forbli separate og sikkert lagret på smartkortet. Hvert program er isolert av operativsystemet slik at ingen applikasjoner påvirker andre. Gamle smartkortsystemer tillot ikke nye applikasjoner å bli installert, eller at gamle ble slettet, MULTOS® gjør dette mulig. Det er også mulig å installere oppdateringer etter behov. Hver applikasjon er plattformuavhengig takket være implementeringen av virtual machine. Utviklere skriver applikasjoner for MULTOS® smartkort med MEL[39]. Kortene er tilgjengelig med 16KB og 32KB EEPROM størrelser fra Hitachi.

Figur 14: MULTOS logo

[37] Application Programming Interface
[38] Electrically-Eraseble Programmeble Read-Only Memory
[39] MULTOS® Executable Language

3.5.2 SIM-toolkit

SIM-toolkit er en ETSI standard for blant annet e-handel som tillater bruk av mobiltelefoner til å utføre transaksjoner. SIM-toolkit er programmert inn i mobiltelefonens SIM-kort, som gjør at SIM-kortet kan styre mobiltelefonens grensesnitt og utføre kommandoer uavhengig av mobiltelefonen og telenettet.

3.5.3 Andre anvendelsesområder for smartkort

Det finnes flere bruksområder for smartkort. Den mest vanlige bruken av smartkort er i dag SIM-kort for mobiltelefoner, men smartkort som bankkort forventes å bli mer vanlig.

Adgangskort

Disse kortene kan brukes og implementeres på mange forskjellige måter. De kan brukes til å generere adgangstegn for fysisk tilgang til deler av en bygning eller elektronisk tilgang til for eksempel ulike bankkonti. Disse kortene har vanligvis en innebygd krypteringsfunksjon som tilbyr hashing, digital signatur og krypteringsmuligheter på kortet. Det er ofte vanlig med en PIN eller passord for å kunne få tilgang til sine data/konti. Under er et eksempel på slikt kort:

- Tilgang til ansatte med sikre passord og mulighet for å benytte biometriske metoder for å beskytte tilgang til datasystemer.

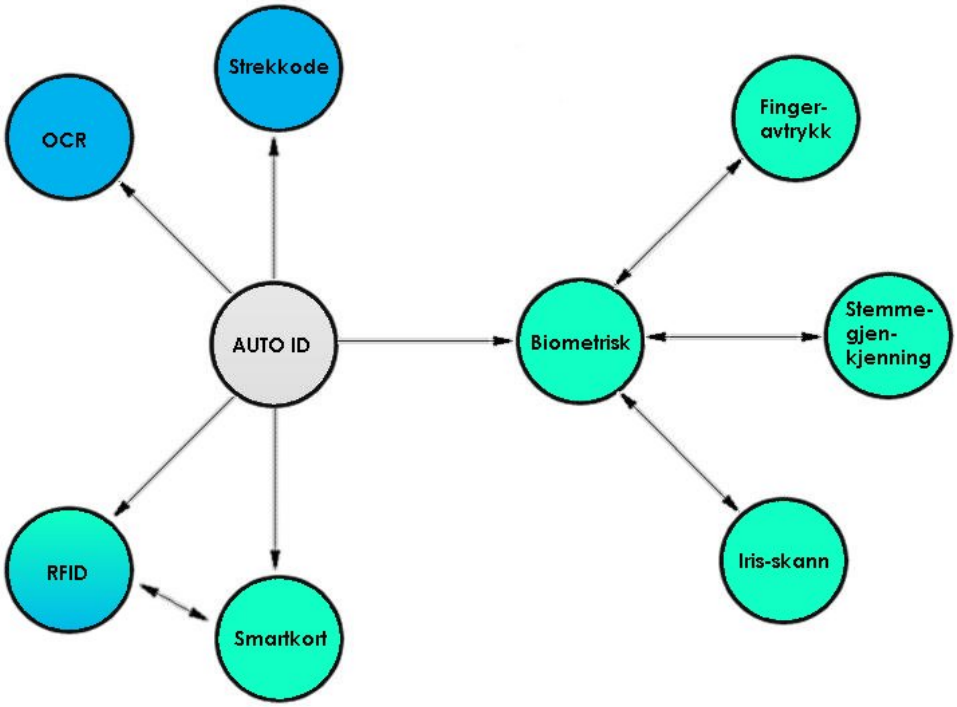
Multifunksjonssmartkort

Disse kortene tilbyr at samme kort kan bli brukt av forskjellige applikasjoner. Slike kort inneholder en CPU som ikke bare har basissikkerheten for lagring/skriving av informasjon, men også støtte for kundespesifiserte applikasjoner. Under er noen eksempler på slike kort som eksisterer idag:

- Flerfunksjonelle student ID-kort som inneholder ulike applikasjoner som elektronisk cash, bibliotekskort og kantinekort.
- Ha oversikt over kundens bonus og lojalitetspoeng på eget smartkort som brukes hver gang man benytter selskapets tjeneste

4 Automatiske ID-systemer

Automatisk identifikasjonsprosedyrer finnes til forskjellige formål, som adgangskontroll, kjøp og salg, personidentifisering og bokstavgjenkjenning. Biometriske-ID prosedyrer brukes ofte til adgangskontroll. Figuren under viser de mest vanlige prosedyrene. De blå feltene viser prosedyrer for identifisering av gjenstander, mens de grønne viser autentifisering av personer. Som figuren viser har RFID et utvidet bruksområde.



Figur 15: ID-prosedyrer

4.1 Adgangskontroller

Når det kommer til sikkerhet på datamaskiner, er de fleste kjent med bruken av passord, PIN-koder og kodekalkulatorer. Kalkulatoren er meget populær, men er et meget dyrt alternativ. Problemet med slike løsninger er at de kun kan brukes til adgangskontroll, og ikke til digital signering. Et annet problem er at slike løsninger ofte er mellom kunde og èn leverandør. Dette betyr at internettbrukere vil måtte holde orden på mange passord, PIN-koder og kalkulatorer

Biometriske prosedyrer

Biometri er definert som vitenskapen av måling- og sammenligningsprosedyrer av levende vesen. Dette vil si prosedyrer som kan identifisere personer ut i fra individuelle personlige kjennetegn, som fingeravtrykk, håndskrift, stemme og iris-skanning.

Stemmegjenkjenning

I det siste har det kommet systemer som identifiserer personer med stemmegjenkjenning. Personen snakker i en mikrofon som er koblet til en datamaskin. De talte ordene blir konvertert til digitale signaler som igjen blir evaluert av et identifikasjonssystem.

Fingeravtrykkslesere

Kriminaletterforskere har siden tidlig på nittenhundretallet brukt fingeravtrykk for identifikasjon av kriminelle. Teknikken går ut på å lese av de karakteristiske trekkene på fingertuppene. Disse trekkene kan fåes fra selve fingeren, men også av gjenstander som vedkommende har rørt.

Når fingeravtrykkslesing er brukt til identifikasjon, er det vanligvis for adgangskontroll, men i senere tid også som innlogging til datamaskiner. Brukeren plasserer da fingertuppen på en spesialleser. Systemet kalkulerer en binær datastreng, og sammenligner den med de som er i arkivet. Moderne systemer kan gjøre denne jobben på under et halvt sekund. For å unngå brutale forsøk på innbrudd, har det også blitt utviklet systemer som kan avgjøre om fingeren som blir plassert på leseren tilhører en levende person.

4.2 Kjøp og salg

I nyere tid har automatisk identifikasjonsprosedyrer blitt svært populært innen service-industrien. Salg, distribusjon, logistikk og produksjon er noen av de som har benyttet denne teknologien mest. Strekkoden, som gjorde revolusjon på slutten av 70-tallet, er ekstremt billige, men har to vesentlige ulemper. De har alt for liten lagringskapasitet, og de har ikke mulighet til å bli omprogrammert.

Det optimale hadde vært en løsning hvor data kunne lagres på en silikonbrikke. Dette løser både problemet med lagringskapasiteten og omprogrammeringen. Den mest vanlige løsningen av denne type i dagliglivet er smartkortet. Ulempen er at de vanlige smartkortlesere har behovet for metallisk kontakt for å kunne lese innholdet. En kontaktløs overføring hadde vært mye mer praktisk. Dersom silikonbrikken skulle kunne sende sitt innhold trådløst til leseren trenger den også strøm, og det ville være svært upraktisk om brikkene kunne gå tom for strøm. Løsningen er at leseren sender et signal til silikonbrikken som aktiverer den. Energien som brikken behøver blir altså levert trådløst av leseren. Slike systemer kalles RFID, og blir stadig mer populære.

På verdensbasis ble det i 2000 solgt RFID-teknologi for ca. 900 millioner $US, og i 2005 ventes dette tallet å stige til over 2650 millioner $US [Finkenzeller 2003]. På grunn av den store etterspørselen har prisene sunket. En RFID brikke som brukes i tyverialarmer kan man i dag få helt ned i 20 cent [Collins 2004].

Strekkoder

Strekkoder er en binærkode representert av parallelle streker. Tykkelsen på strekene og størrelsen på mellomrommene forteller hvilke siffer de representerer. Figuren under viser en typisk strekkode.

Figur 16: En strekkode

Strekkoden leses med en optisk laserskanner, som måler refleksjonene fra de hvite og svarte feltene i strekkoden, og dermed tolker de som binærkoder. De fleste strekkoder ser for det blotte øye svært like ut, men det finnes i alt ca. 10 forskjellige strekkodesystemer i bruk i dag. Det mest brukte systemet heter EAN[40], som ble utviklet for å møte kravene til matvareindustrien i 1976. EAN er en videreutvikling av UPC[41], som ble utviklet i USA så tidlig som 1973 [Barcode].

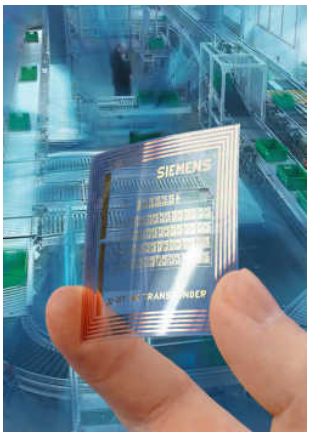
EAN-koden består av 13 siffer som er delt inn i 4 bolker: landskode, produsent-ID, varenummer og et kontrollsiffer til slutt. Figuren under viser hvordan de er inndelt. L1-L2 (land), P1-P4 (produsent), V1-V6 (varenummer) og K (kontroll-sum).

Figur 17: EAN-inndeling på strekkoden

[40] Europeisk Artikkel Nummer
[41] Universal Product Code

RFID

RFID har mye til felles med smartkort som er beskrevet i vedlegg 1. Den vesentlige forskjellen er at smartkort trenger en galvanisk kontakt med leseren hvor strømtilførsel og dataoverføring skjer. Med RFID skjer denne overføringen via magnetiske eller elektromagnetiske felt. Noe som gjør at RFID er en trådløs teknologi. Dette er en kjempefordel for svært mange brukere, og er hovedgrunnene til at RFID salget i den senere tid har tatt av. Ved å integrere RFID brikken på et plastkort (slik som med smartkortene) har man et kontaktløst smartkort.

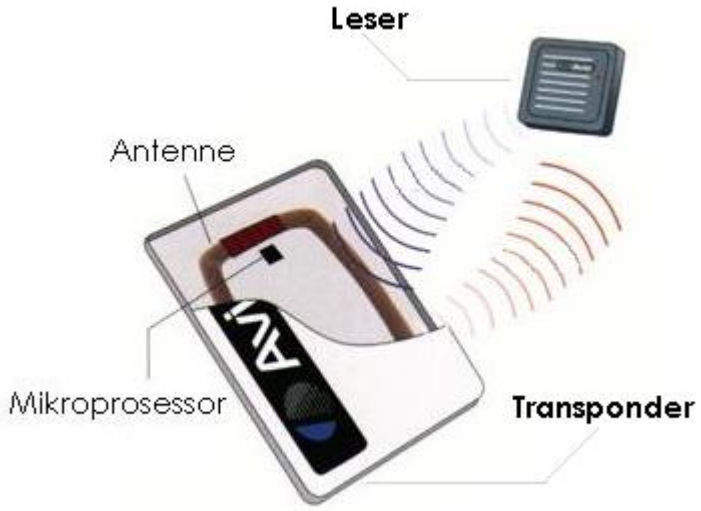


Figur 18: En RFID-brikke

5 Virkemåten til RFID

RFID-systemer består av to deler; en leser og en transponder. Transponderen er den delen som legges inn i et smartkort, en køfri-brikke[42], tyverialarm eller opereres inn under huden til et dyr. Leseren er den delen som leser informasjon ut fra transponderen. NFC[43] er en standard som blir utviklet av Nokia, Philips og Sony. NFC er en videreutvikling av RFID hvor leser og transponer er i en og samme brikke. Denne standarden er laget spesielt for håndholdte enheter som mobiltelefon og PDA [NFCforum].

Oppgaven vil bruke betegnelsene RFID-transponder og RFID-leser i stedet for NFC-brikke for å klargjøre hvilken komponet det er snakk om, men for utvikling vil en NFC-brikke utfylle rollen bedre siden alt her er integrert i en brikke.

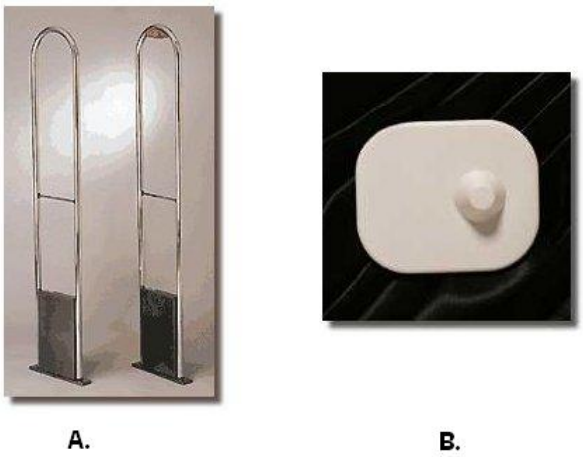


Figur 19: RFID-systemet

Sikkerhet

Mange har vært skeptiske til bruk av RFID. Frykt for at persondata skal kunne bli leset av andre og misbrukt er årsak til skepsisen. Philips har derfor utviklet hva de kaller andre generasjons RFID-teknologi. Ved å bruke kryptert transmisjon[44] vil eventuell avlyttet data være ubrukelig. Slike RFID-brikker vil kunne bli benyttet i systemer som krever strengere sikkerhet. Det norske Datatilsynet mener at det er tilstrekkelig med en DES-algoritme og 56-bits nøkkelrom, men anbefaler 112-bits effektiv nøkkel [Datatilsynet].

[42] Abonnenter i bomringene bruker køfri-brikker
[43] Near Field Communaication
[44] Se kapittel 2 for mer informasjon om kryptering



Figur 20: EAS-leser (A) og EAS-sender (B)

Det er transponderen det stilles størst krav til, siden den skal kunne masseproduseres billig. De skal ofte kunne være omprogrammerbare og ha en lang levetid. Den må i mange tilfeller være så liten og tynn at den får plass på baksiden av en prislapp. De brikkene som må være minst har ofte ikke plass til en egen strømkilde, som et batteri. Dette løses ved at transponderen kan trekke elektrisk kraft ut av signalet fra leseren. Dette betyr at så lenge leseren er i nærheten av transponderen, så har transponderen kraft. Så snart leseren trekkes unna forsvinner kraftkilden til transponderen, og den skrues av. Figuren under viser hvordan data, energi og klokkepuls sendes mellom leser og transponder. Klokkepulsen brukes til å synkronisere leseren og transponderen.

Figur 21: Transmisjon som sendes med RFID

For at transponderen skal kunne trekke elektrisk kraft fra leseren, trenger vi et RF-felt[45]. Dette feltet blir generert ved at et vekselspenningssignal (AC) sendes til en antenne. Det dannes da et magnetisk felt rundt antennen. Siden avstanden mellom leseren og transponderen er så kort, og strømforbruket til transponderen er så lite, er disse lavfrekvente magnetiske bølgene nok til å gi transponderen den elektriske kraften den trenger.

[45]Radio frequency, Norsk: radio frekvens

5.1 De forskjellige RFID-systemene

Det finnes utallige varianter av RFID-systemer, og nesten like mange produsenter. Dersom man skal kunne få en oversikt over RFID-systemene må man første finne ut hva som skiller systemene fra hverandre.

Anvendelser

Tabellen under gir en oversikt over de viktigste forskjellene på noen av de mest kjente RFID-system. Dataene gitt under vil variere blant de enkelte produktene, så et ca. snitt er angitt.

	Alarm EAS	AutoPASS OBU	Dyre-merking	Vare-merking	Skidata
Lagringskapasitet	1bit	64bit	512bit	512bit	64bit
Programerbar	Ja	Nei	Ja	Nei	Ja
Strøm	Passiv	Aktiv	Passiv	Passiv	Passiv
Rekkevidde	>2m	>2m	1cm	1m	1m
Innkapsling	Liten	Stor	Liten	Liten	Liten

Tabell 3: Forskjell mellom RFID-systemer

Overføringsmetode

Alle RFID systemer opererer med en av to virkemåter: full dupleks (FDX)/ halv dupleks (HDX) og sekvensiell (SEQ).

I halv og full dupleks blir transponderens svar sendt når leserens RF-felt er på. Dette fordi transponderens signal kan være veldig svakt sammenlignet med leserens signal, og man må unngå at signalene blandes. I praksis benyttes load-modellering.

Motsetningen er sekvensiell overføring. Der blir leserens RF-felt skrudd av med korte mellomrom. Dette mellomrommet registreres av transponderen som benytter sjansen til å sende data til leseren. Når leserens RF-felt er skrudd av, forsvinner også strømtilførselen til transponderen. Dette betyr at batterier eller kondensatorer må benyttes ved sekvensiell overføring.

Lagringskapasitet

Lagringskapasiteten kan variere fra et par byte, til flere kilo-byte. Unntaket er 1bits transponderen. 1 bit er nok til å signalisere (av/på eller ja/nei). Denne varianten trenger ikke noen lagringsenhet, og kan derfor produseres til en brøkdel av prisen. Denne typen RFID benyttes i EAS[46] blant annet til å beskytte varer i butikker. Dersom noen kjøper en varer, blir transponderens bit endret, slik at leseren ved utgangen ikke reagerer. Dersom en kunde forsøker å stjele varen, registrerer leseren ved utgangen at transponderen ikke har blitt deaktivert, og starter alarmen.

[46] Elecrtonic Article Surveillance

Figur 22: EAS-brikke

Programmerbar

Muligheten for programmering av RFID-brikken gir oss nok en mulighet til å klassifisere RFID-systemer. I de enkleste systemene inneholder transponderen et datasett som det får innprogrammert ved produksjon, dette er vanligvis et serienummer, og kan ikke endres. I programmerbare systemer derimot, kan leseren endre innholdet til RFID-brikken. Det finnes tre forskjellige lagringsmåter for programmerbare respondere. Forskjellene er strømforbruk og levetid.

- EEPROM Dette er den mest brukt typen. Ulempen er at den bruker mye strøm, og har et begrenset antall omprogrammeringer (mellom 100 000 og 1 000 000). Til de fleste bruksområder er dette tilstrekkelig.
- SRAM[47] Mest vanlig i mikrobølgesystemer. Denne brikken kan utføre meget raske skrivesykluser, men har den ulempen at den trenger konstant strømtilførsel av et batteri eller lignende.
- FRAM[48] har blitt benyttet i noen testprosjekter, men det er fortsatt noen problemer som hindrer utbredt bruk. Strømforbruket blir redusert med en faktor på 100 i forhold til EEPROM, og skrivetiden reduseres med 1000 ganger. Det foreligger ingen begrensninger i antall ganger den kan omprogrammeres.

Strømtilførsel

Transpondere uten egen strømkilde kalles passive transpondere. Disse trekker strømmen fra leserens RF-felt. Aktive transpondere har et eget batteri.

[47] Static RAM
[48] Ferromagnetic RAM

Frekvens

Når vi snakker om RFID-brikkens frekvens, er det leserens frekvens man mener. Dette er fordi transponderen sitt signal er så veldig mye svakere. Vanligvis benytter de også samme frekvens. Det er stor forskjell mellom frekvensene som brukes av forskjellige RFID-brikker. Vi deler frekvensbandene opp i klasser [Finkenzeller 2003]:

- LF (lav frekvens) 30-300kHz
- HF (høy frekvens) 3-30MHz
- UHF (ultra høy frekvens) 300MHz-3GHz
- Mikrobølge >3GHz

RF-Felt

Leseren i et RFID system bruker ikke galvanisk kontakt til å overføre strøm og data, men bruker et magnetisk (induktive) eller elektromagnetisk felt. Nesten 90% av alle RFID-system som selges i dag er induktive [Brain 2000].

Rekkevidde

Det er stor forskjell på rekkevidden til RFID-brikkene. Brikkene kan designes med den rekkevidde som måtte være ønskelig for bruksområdet. Vi kan også her dele opp i klasser:

- Nær-lesing: Opptil 1cm
- Avstands-lesing: Opptil 1m
- Lang-lesing: Over 1m

Nær-lesing krever at transponderen og leseren i praksis er borti hverandre. Det kan her brukes både magnetiske og elektriske RF-felt, og frekvenser opp til 30MHz. En slik kort avstand gjør at strømtilførselen til transponderen er meget stor. Dette gjør at en mikroprosessor kan brukes på et slikt system selv uten en egen strømkilde som et batteri. Dette gjør at slike løsninger ofte brukes der sikkerhet er en viktig faktor, som ID-kort og nøkkelkort. ID-1 er et trådløst ID-kort (ISO 10536) som bruker nær-lesing.

Avstands-lesing kan ha en avstand opp til ca. 1m, og bruker induktive felt. Dette er i dag de mest vanlige. Frekvensen som normalt brukes er 13.56MHz (ISO 14443, contactless smart card).

Lang-lesing kan benyttes opp til 15m, og i enkelte tilfeller enda lenger. Det benyttes bare elektromagnetiske bølger i UHF og mikrobølger. Systemer som har en rekkevidde på 3m er nå laget uten batteri. På systemer med lenger rekkevidde benyttes batteriet til å styre mikroprosessoren og ikke til selve transmisjonen.

Transponder respons

Det er forskjellige måter for en transponder å svare på. Det er også her tre forskjellige måter:

- Lik frekvens: transponderen svarer med samme frekvens som leseren (1:1)
- LM[49]: leserens frekvens blir påvirket av transponderen (1:1)
- Underharmoni: transponderen svarer med underharmoniskebølger (1:$\frac{1}{n}$)

Innkapsling

Det finnes mange forskjellige innkapslingsmåter av RFID-transpondere. De forskjellige innkapslingene har også forskjellig bruksområder. Brikker som legges under huden til dyr for identifikasjon bruker en glassinnkapsling. Tyverialarmer for butikker kan benytte store plastikktranspondere som festes til klær, men det finnes også såkalte smartlabels som er 0.1mm tykke plastfilmer som inneholder RFID-transpondere. Disse kan festes i bøker og på flasker. De brukes ofte på baksiden av strekkodene. Figuren under viser noen av de mange typene innkapsling for lesere og transpondere.

Figur 23: Forskjellige innkapslinger

[49] Load modelering

5.2 Eksempel på dagens RFID bruksområde

RFID er en teknologi som har vært benyttet i flere år. Under er noen eksempel på de mange bruksområdene RFID har i dag.

Q-Free

Det norske Trondheims firmaet Q-Free har utviklet komplette systemer innen toll, trafikkinformasjon, parkering, billettering, tilgangskontroll, logistikk og mye mer.

De er Norges største innen bruk av RFID-teknologi, og deres mest kjente produkt er kanskje AutoPASS. AutoPASS er en løsning for passering av bomringer, hvor abonnentene har en RFID-transponder i bilen som registreres av en leser i bomringen. Q-Free kaller denne enheten en On-Board Unit (OBU). Fordelene er flere; man slipper å stoppe i bomringene for å betale eller å ha vekslepenger. På engelsk kalles dette Electronic Fee Collection (EFC).

Q-Free har totalt levert over 1.000.000 OBUer og installert mer enn 300 lesere i bomringer. Den første bomringen som ble utstyrt med AutoPASS, var Ranheim Tollstasjon øst for Trondheim i 1988.

Offshore

Offshore industrien har sett muligheten i å benytte RFID-teknologien kombinert med sensorer som registrerer temperatur, luftfuktighet, støtstyrke og sikkerhetsdeteksjon. Disse RFID-brikkene med flere sensorer koster mye idag, slik at de ikke er stort utbredt, men bare i bruk på helt nødvendige anvendelsesområder. Et annet problem som oppstår med å integrere RFID og ulike sensorer er at brikken blir for stor til å kunne benyttes i spesielle tilfeller. RFID brukes også i adgangskort på plattformer.

Dyremerking

RFID-transpondere finnes i så små utgaver at de kan plasseres i små kapsler som vist på bildet under.

Figur 24: RFID-kapsel for dyremerking

Disse brikkene kan inneholde mye informasjon om dyret. Bonneville Power Administration (BPA) startet å benytte RFID-teknologi i 1986 for å overvåke bevegelsene til fisk ved å plassere lesere i flere demninger. Teknologien er i dag meget utbredt, og benyttes til sporing av dyr, og til å lagre informasjon om dyr.

Deichmanske bibliotek

Det Deichmanske bibliotek har startet et RFID-prosjekt med å merke 850.000 bøker. Hensikten med dette er å forhindre at bøker blir stjålet. Hver bok får en liten RFID-brikke på coveret og hvis den taes ut av døren piper en alarm. En annen side der RFID-merkingen av bøkene hjelper det Deichmanske bibliotek er på redusering av personalkostnader og bedre forvaltning. RFID-brikkene tillater en større form for selvbetjening når man skal låne bøker, noe som gir betjeningen større rom for rådgivning.

Skidata

Skianlegg verden rundt har begynt å bruke RFID-tekonologien i adgangskort til heisene (dagskort, sesongkort o.l). Disse kontrollørene leser kortene gjennom klær, slik at skiløperen ikke trenger å fremvsie kortet. Ski og snowboard begynner å komme på markedet med integrert RFID-transponder som inneholder et unikt serienummer. Ved at skianlegget har RFID-lesere ved heisen, kan de raskt og enkelt lese dette serienummeret, og hvis utsyret er meldt stjålet kan sikkerhetstiltak fra anlegget bli eksekvert.

Figur 25: Skidata

6 Vår løsning

Det er flere problemer med dagens m-handelsløsninger. Før det første er det et for stort skritt å starte og bruke tjenestene. For det andre er det for få tjenesteleverandører som støtter m-handelsløsningene. Det er også et problem at brukeren må gjennom mange tastetrykk for å skrive inn en URL, deretter må det flere tastetrykk til for å bestille en vare.

For å kunne rekruttert tjenesteleverandører til m-handelsløsningen, må man kunne vise til en viss brukermasse. Problemet er at brukerne på sin side ikke blir medlemmer av løsningen dersom det ikke allerede er et bredt spekter av tjenesteleverandører. Dette kalles "kritisk masse", og er et velkjent problem ved lansering av ny teknologi.

For å unngå hele problemstillingen med å rekruttere tjenesteleverandører og brukere, kan man knytte seg til en allerede eksisterende infrastruktur. Norge er et av de landene i verden som bruker betalingskort mest, og 9 av 10 (dvs. 60.000) norske betalingsterminaler støtter Bank-Axept [BankAxept]. Dersom m-handelsløsningen kunne benytte denne infrastrukturen ville man allerede ha et stort nett av tjenesteleverandører og brukere.

Betaling med mobiltelefonen

Mobiltelefonens SIM-kort er et smartkort på lik linje som de mest moderne bankkort (debet og kreditt). Det er defor mulig å integrere informasjonen fra bankkortet over på mobiltelefonens SIM-kort. Ved å plassere en RFID-transponder i mobiltelefonen, og en RFID-leser i betalingsterminalen kan vi oppnå trådløskontakt mellom bankkortet (inne i SIM-kortet) og betalingsterminalen. Dette er bare en utvidelse av bankterminalen. Man kan fortsatt benytte vanlige kort til betaling.

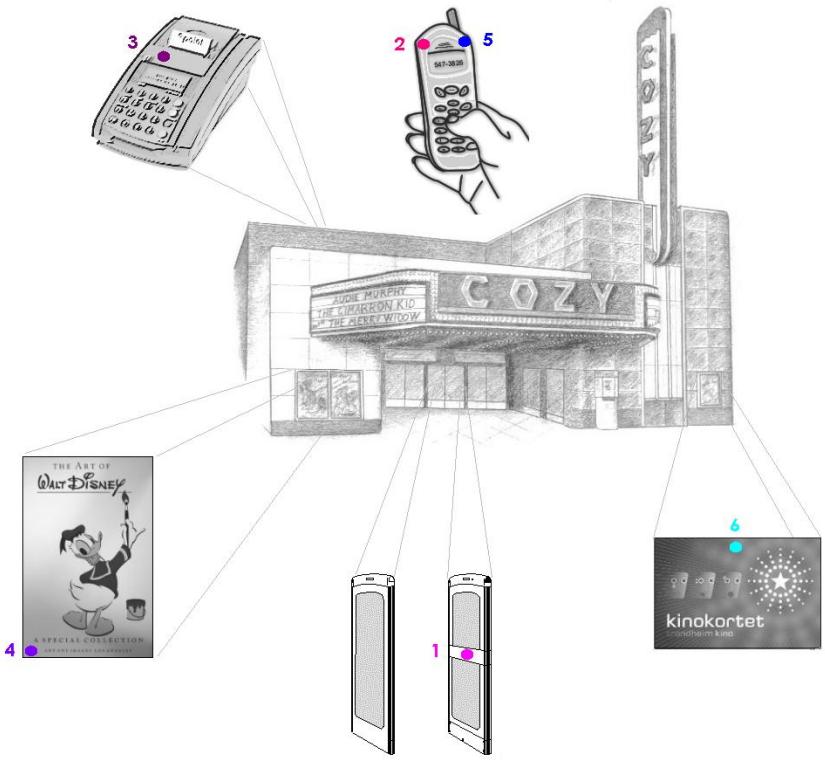
En slik løsning vil ikke by på store endringer i den allerede eksisterende infrastrukturen. Den eneste forskjellen er at brukere nå ikke trenger å dra et kort gjennom betalingsterminalen, men kan holde mobiltelefonen inntil terminalen i stedet. Sikkerheten vil ivaretas ved at rekkevidden til RFID-transmisjonen bare er noen få cm. Dette gjør at det blir svært vanskelig å avlytte transmisjonen. Informasjonen er kryptert[50], slik at skulle likevel noen klare å lese informasjonen som blir transmittert, vil den være verdiløs uten nøkkelen.

Figur 26: Betaling med RFID-telefon

[50] Se vedlegg 2 for mer informasjon om kryptering

Eksempel

Figuren under viser forskjellige områder hvor RFID-teknologi kan benyttes. 1, 2 og 3 er RFID-lesere, mens 4,5 og 6 er RFID-transpondere.



Figur 27: Eksempel på bruk av RFID

1. RFID-leser i billettkontroll må ha en rekkevidde som gjør at alle som passerer blir kontrollert. Ca. 2m
2. RFID-leser i mobiltelefon må kunne lese transpondere i nærheten. Ca. 1m
3. RFID-leser i bankterminal må ha en rekkevidde som er så kort at kun den første kunden har kontakt. Ca. 15cm
4. RFID-transponder i plakat må ha en rekkevidde som er så kort at kun de som aktivt går inn for å få kuntakt får det. Ca. 10cm
5. RFID-transponder i mobiltelefon må ha en kort rekkevidde. Ca. 15cm
6. RFID-transponder i reklame må ha en rekkevidde som gjør at de som er nær reklamen får tilbud. Ca. 2m

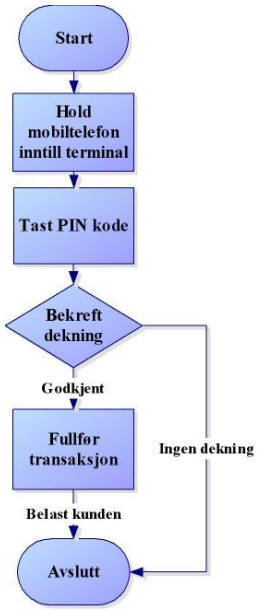
Elektronisk lommebok

Siden betaling med mobiltelefonen og betalingsterminaler ikke er så veldig forskjellig fra vanlig betaling med kort, vil dette sannsynligvis ikke være så stor overgang for kundene. Når kundene har blitt vant til å benytte mobiltelefonen som et betalingsmiddel, kan man gradvis innføre nye tjenester, hvor helheten blir en elektronisk lommebok (som beskrives i kapitel 2). Den neste tjenesten man kunne tenke seg er elektroniske kontanter. Fordelen med å betale med elektroniske kontanter er fra brukerens side at betalingen er anonym og gebyrfri.

Det vil finnes flere måter å overføre elektroniske kontanter til den elektroniske lommeboken. Det vanligste vil være en overføring fra en bankkonto til den elektroniske lommeboken, men man kan også tenke seg at disse kontantene kan overføres mellom to elektroniske lommebøker.

De elektroniske kontantene lagres på SIM-kortet, hvor de er beskyttet av SIM-kortets PKI. Dersom noen skulle stjele mobiltelefonen vil de elektroniske kontantene gå tapt, men tyven vil ikke kunne bruke dem siden man må benytte PIN-kode for å benytte de.

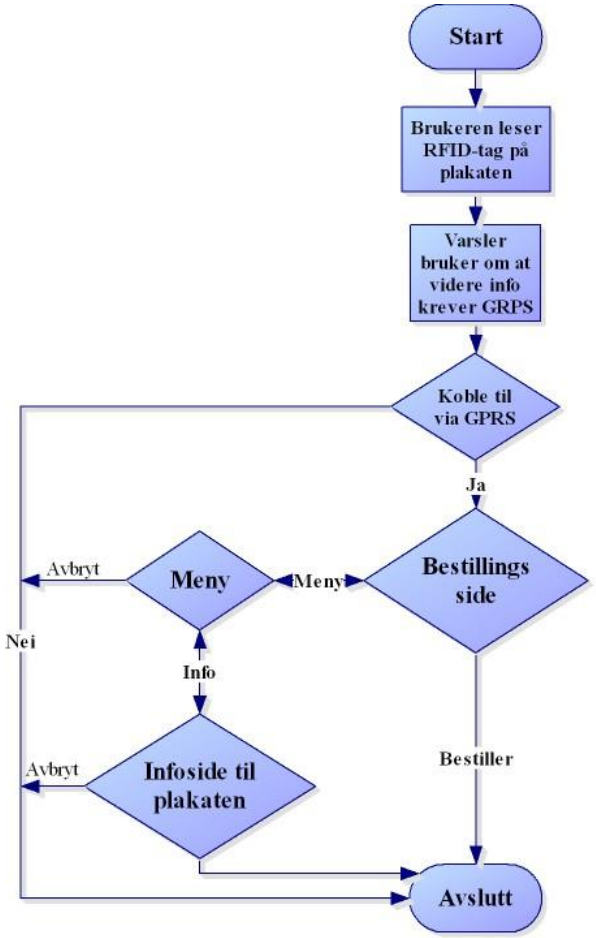
Den elektroniske lommeboken har nå et komplett betalingssystem, både debet, kreditt og kontant, man kan utvide betalingsløsningene med lojalitetspoeng, mikrotransaksjoner, og kvitteringshåndtering. Videre utvidelse av den elektroniske lommeboken, kan være elektronisk identifikasjon og personlige agenter.



Figur 28: Betaling med RFID-telefon

M-handel

Mobilhandel er et supplement til e-handelen hvor informasjonsinnhenting og kjøp foregår via mobiltelefon [Davidsen & Tepfers 2002]. Dette betyr at dersom man betaler med mobiltelefonen i en betalingsterminal er det ikke m-handel. RFID kan likevel være et hjelpemiddel i m-handel. Et problem var blant annet at det måtte så mange tastetrykk til får å skrive inn URLer og bestille varer. RFID-brikker kan inneholde informasjon som URLer, epost-adresser, telefonnummer og lignende. Ved å implementere slike RFID-brikker i reklameplakater og brosjyrer forenkles kjøpsprosessen. Når brukeren leser RFID-brikken vil mobiltelefonen starte en nettleser, og åpne bestillingssiden for varen. En personlig profil kan videre forenkle kjøpsprosessen ved å automatisk fylle ut kundeinformasjonen riktig.

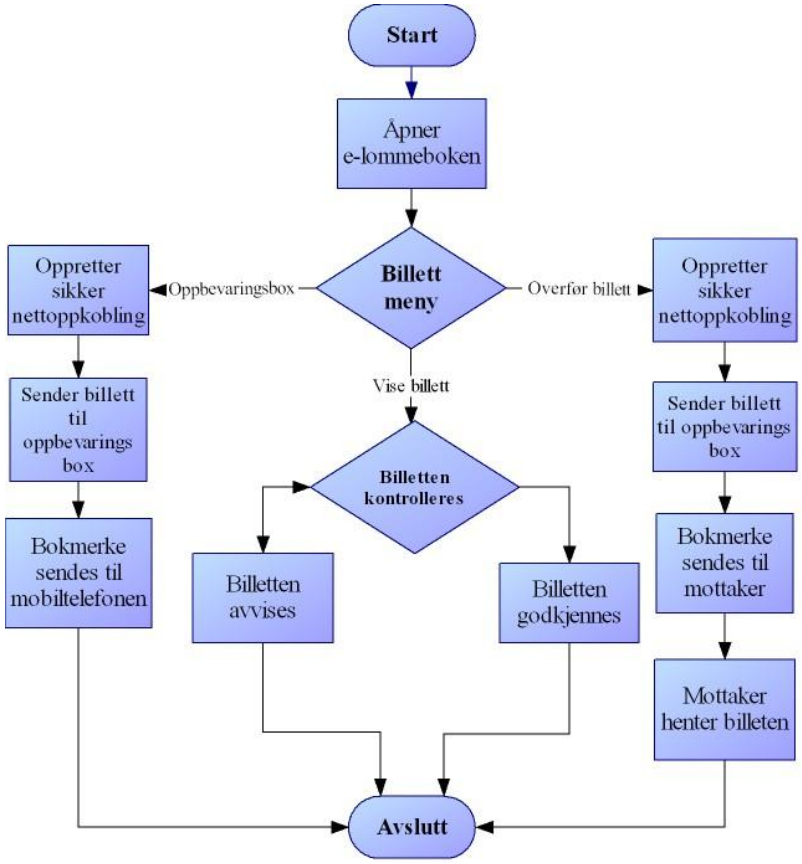


Figur 29: Eksempel på m-handel med RFID

Elektronisk billett

En elektronisk billett lagret på en mobiltelefon vil ha flere fordeler fremfor papirbilletter. For det første vil kunden få en bedre oversikt over billettene sine, men enda viktigere er sikkerheten. Billettutstederen vil med en elektronisk billett være mye sikrere mot kopiering. Den elektroniske billetten lagres i SIM-kortet til mobiltelefonen, som fra før har PKI-støtte. Billetten inneholder en kryptert kode. Denne koden kan bare leses av billettkontrolløren. En slik billettkontroll kan ha store likeheter med metalldetektorer på flyplasser; har kunden billetten i orden er det bare å finne plassen inne i lokalet. Skulle derimot billetten mangle, så reagerer systemet.

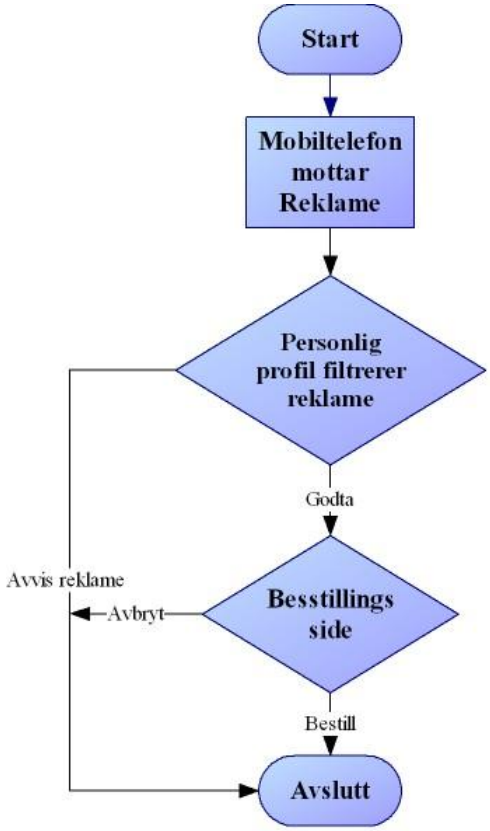
Billetten kan selges eller gies bort til andre, men dette fører ikke til at det blir to kopier av billetten. Den originale billetten blir automatisk slettet når den gies videre til andre, eller når den vises i billettkontrollen. Det eneste som blir igjen er en kvittering som sier hvem billetten ble gitt til, og når den ble gitt.



Figur 30: Elektronisk billett

Personlige tilbud

Butikker har behov for å reklamere til kundene får å gjøre tilbudene sine kjent, men for mye reklame kan skremme kunden. Ved hjelp av en personlig profil kan kunden selv bestemme hvilke tilbud som skal kunne videreformidles. Som eksempel kan en kunde fortelle i sin personlige profil at tilbud om sykler er av interesse. Når kunden så går forbi en sportsbutikk kan RFID-leseren i kundens mobiltelefon plukke opp eventuelle sykkeltilbud som sportsbutikken sender ut. Dersom tilbudet passer innenfor kundens krav (pris og lignende) vil kunden bli gjort oppmerksom på dette av telefonen. Alle andre tilbud avviser den personlige profilen. Ved at profilen har en alderskontroll innebygget, vil upassende tilbud automatisk bli avvist dersom brukeren ikke oppfyller kravet til aldersgrense.



Figur 31: Personlige tilbud

7 Systemkrav

For å kunne lage en prototyp av betalingssystemer med RFID, trenger man en mobiltelefon med RFID, og mulighet til å skrive programmer for mobilen som benytter RFID leser/sender.

Under er en liste over kravene som stilles til mobiltelefonen, elektronisk lommebok, telenettet, betalingsterminaler og RFID-brikkene som plasseres i plakater, varer og lignende.

Numenklatur

Denne delen beskriver terminologien som er benyttet i systemkravene og hvordan de er kategorisert. Alle kravene er beskrevet i tabeller som vist under.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer

Krav ID

Krav tildeles i flere underkategorier, som har hver sin løpende nummerering.

Beskrivelse av krav

Her kommer en presis og konkret tekstlig beskrivelse av kravet.

Prioritet

Hvert av kravene gis prioritet, etter hvor viktige de er for utvikling av systemet. Følgende prioriteter benyttes:

- Høy: Er svært viktig for at systemet skal kunne fullføre sin hensikt
- Middels: Er ikke kritisk for systemet, men sees på som en stor fordel
- Lav: Er ikke viktig for funksjonaliteten, men kan forenkle en del prosesser

Avhengig av

Her listes de krav som dette kravet er avhengig av for å kunne implementeres.

Nødvendig for

Her listes de krav som er avhengig av dette kravet for å kunne implementeres.

Eksisterer

Her beskrives det om teknologien, infrastrukturen og lignende eksisterer i dag, eller om det finnes noen kjente pilotprosjekter på dette.

7.1 Mobiltelefonen

Mobiltelefonen er kjernen i m-handel. Under beskrives kravene som stilles til operativsystem, SIM-kort, RFID, elektronisk lommebok, peronlig profil og overføring.

OS

Mobiltelefonen må ha et operativsystem som tillater installasjon av nye applikasjoner og utviklingsspråket må kunne få tilgang til RFID brikken. I tillegg er det en fordel om det er J2ME støtte og WAP på telefonen.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
M_OS_01	Mobiltelefonen har er Smartphone OS	Høy		M_OS_04	Ja
M_OS_02	Mobiltelefonen støtter J2ME	Medium		N_PP_02	Ja
M_OS_03	Operativsystemet støtter WAP	Medium	M_OF_04		Ja
M_OS_04	Operativsystemet har tilgang til RFID-transponder og leser	Høy	M_OS_01		Nei

Tabell 4: Krav til operativsystem på mobiltelefon

SIM-kort

SIM-kortet må ha støtte for eksekvering av flere applikasjoner på samme tid, slik at enkelte funksjoner til en elektronisk lommebok kan ligge på kortet. Kortet må også støtte SIM-toolkit.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
M_SK_01	Multi-applikasjonsstøtte på SIM-kort	Høy	M_EL_01 M_EL_03 M_EL_04		Ja
M_SK_02	Tilgang til SIM-toolkit	Høy			Ja
M_SK_03	Støtter integrering av RFID-transponder	Medium	M_RT_04		Ja

Tabell 5: Krav til SIM-kort

RFID-leser

RFID-leseren må ha en rekkevidde på 1 meter, dette er fordi at en altfor kort rekkevidde vil gjøre at brukeren må anstrenge seg for å få kommunikasjon, mens en for lang rekkevidde, vil kunne få kontakt meg flere sendere, og dermed feil kilde. RFID-leseren kan benytte telefonens batteri som strømkilde slik at leseren ikke trenger et nytt batteri.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
M_RL_01	RFID-leseren må ha en rekkevidde på 1 meter	Høy			Ja
M_RL_02	RFID-leseren bruker batteri som strømkilde	Høy			Ja
M_RL_03	RFID-leseren er integrert i mobiltelefonen	Høy			Nei
M_RL_04	RFID-leseren støtter PKI	Høy			Ja

Tabell 6: Krav til RFID-leser i mobiltelefon

RFID-transponder

Mobiltelefonen trenger også en RFID-transponder, slik at data kan sendes fra telefonen til andre telefoner, billettkontroller eller betalingsterminaler. Rekkevidden her bør vært svært kort, ca. 10cm. Dette slik at ingen andre skal kunne lese informasjon som sendes mellom telefon og betalingsterminal. Lagringskapasitet på brikken må være mer en 1KB. Brikken må også være programmerbar, slik at forskjellig informasjon kan sendes til forskjellige formål. Strømtilførselen kan også her være telefonens batteri. RFID-transponderen kan plasseres i selve telefonen eller på telefonens SIM-kort. Vi anbefaler plassering i SIM-kortet, slik at eventuelle brikker med funksjonsfeil kan byttes lettest mulig.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
M_RT_01	RFID-transponderen må ha en rekkevidde på 15cm	Høy			Ja
M_RT_02	RFID-transponderen må ha en lagringskapasitet på over 1KB	Høy			Ja
M_RT_03	RFID-transponderen må være omprogrammerbar	Høy			Ja
M_RT_04	RFID-transponderen er integrert i mobiltelefonens SIM-kort	Medium	M_SK_03		Nei
M_RT_05	RFID-transponderen har en strømkilde	Lav			Ja
M_RT_06	RFID-transponderen støtter PKI	Høy			Ja

Tabell 7: Krav til RFID-transponder i mobiltelefon

Elektronisk lommebok

Verdier (penger, billetter) i den elektroniske lommeboken ligger lagret på mobilens SIM-kort, men det må også være mulighet til å overføre de til en sentral oppbevaringsboks. Den elektroniske lommebok må inneholde en funksjon for personlig identifikasjon på lignende måte som førerkort, bankkort og lignende. Den må også ha funksjonalitet til å benytte de ulike betalingsformene som kredittkort, elektroniske kontanter og debetkort.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
M_EL_01	Verdiene i den elektroniske lommeboken må kunne lagres sikkert på mobilen	Høy	M_SK_01		Nei
M_EL_02	Har mulighet for å lagre verdiene i en sentral oppbevaringsboks	Høy			Nei
M_EL_03	Den elektroniske lommeboken må inneholde elektronsik identifikasjon som lagres på SIM-kortet	Høy	M_SK_01		Nei
M_EL_04	Debet og kreditt-kort må være integrert i den elektroniske lommeboken. Lagret på SIM-kortet	Høy	M_SK_01		Nei

Tabell 8: Krav til elektronisk lommebok

Personlig profil

Mobiltelefonnummer er unike i hvert land, og er da en passende ID til bruk i den personlige profilen. Personnummer vil også være et alternativ, men legger den begrensning at brukere med flere mobiltelefoner kun kan ha en personlig profil. En personlig profil kan være lagret lokalt på mobilen og/eller hos en offentlig godkjent TTP. Fordelen med en sentralt lagret profil er at dersom man mister eller ødelegger mobilen, så går ikke profilen tapt, og det gjør det enklere å oppdatere profilen ved å bruke datamaskin via Internett. Ulempen er at hver gang brukeren trenger informasjon fra profilen, så må man koble seg opp til TTP-en for å hente den. Ved å kombinere disse to løsningene får vi det beste fra begge sider. Dette vil si at profilen ligger på mobiltelefonen, og en sikkerhetskopi ligger hos en TTP. Det er kun brukeren selv som skal ha tilgang til å endre profilen. Dette kan gjøres ved at det bare er mulig å oppdatere sikkerhetskopien fra brukerens mobilnummer (profil-ID). En mulig ulempe ved kombinasjonen er at når man oppdaterer den sentrale lagrede profilen, kan det koste penger å kopiere den til mobiletelefonen.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
N_PP_01	Hver personlig profil har en unik standardisert ID	Høy			Nei
N_PP_02	Den personlige profilen skal lagres på mobiltelefonen	Høy	M_OS_01		Nei
N_PP_03	Den personlige profilen skal kunne ha en sikkerhetskopi hos en TTP	Høy			Nei
N_PP_04	Profilen eies av brukeren og er konfidensiell	Høy			Nei
N_PP_05	Profilen må støtte et standarisert ontologispråk	Høy	R_AK_05		Nei

Tabell 9: Krav til personlig profil

Overføring

Mellom to mobiltelefoner som er i nærheten av hverandre trenger man ikke gå veien via telenettet for overføring av data. RFID har for lav overføringshastighet til å kunne utkonkurere IrDA og blåtann når det hjelder ren dataoverføring. RFID har likevel en stor fordel, nemmelig at det kan skape en umiddelbare forbindelse mellom to RFID brikker. Blåtann må på sin side starte et søk som varer i flere sekunder. Vedlegg 3 forklarer hvordan RFID kan benyttes til å koble to tellefoner sammen med blåtann på en mer effektiv måte.

Datakommunikasjon over telenettet er et krev som stilles. GPRS er den standarden med lavest overføringshastighet, og er derfor et minstekrav.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
M_OF_01	Mobiltelefonen støtter IrDA	Lav			Ja
M_OF_02	Mobiltelefonen støtter blåtann	Lav			Ja
M_OF_03	Mobiltelefonen støtter EDGE	Lav	N_MN_02		Ja
M_OF_04	Mobiltelefonen støtter GPRS	Høy	N_MN_01	M_OS_03	Ja
M_OF_05	Mobiltelefonen støtter 3G	Lav	N_MN_03		Ja

Tabell 10: Krav til overføring

7.2 Betalinsterminaler

Betalingsterminalene vil være nesten helt like som de er i dag, eneste forskjell er at de også har en RFID-leser. Denne RFID-leseren vil måtte ha en kort rekkevidde for å være sikker på at bare kunden som står og betaler får kontakt, og ikke de andre i køen. 10-15 cm skulle være tilstrekkelig.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
B_BT_01	RFID-leseren må ha en rekkevidde på under 15cm	Høy			Ja
B_BT_02	RFID-leseren støtter PKI	Høy			Ja

Tabell 11: Krav til betalingsterminaler

7.3 Nett-arkitektur

RFID-teknologi i mobiltelefonen setter noen krav til eierne av RFID-databasen.

RFID-database

Enkelte RFID-brikker kan ha en ID som er registrert i et sentralt register. Flere brikker kan da inneholde samme ID, slik at informasjonen til alle disse brikkene kan endres på et sentralt sted. Dette gjøres ved at IDen kobles mot en RFID-database. Når brukeren leser denne IDen med mobiltelefonen vil IDen sendes til eierne av databasen, som returnerer informasjonen koblet til IDen. Det er viktig at de forskjellige databaseeierne samarbeider om en standard for denne IDen. Denne teknikken benyttes der hvor det er mange brikker som skal inneholde samme informasjon, og informasjonen må holdes jevnlig oppdatert. Telenor har pilotprosjekter på slike databaser. Kravene under er minstekravene som stilles dersom en slik arkitektur skal implementeres.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
N_RD_01	Det finnes en standard som sikrer at IDene i RFID-brikker en unike	Høy			Nei
N_RD_02	Det eksisterer en eller flere godkjente RFID-databaser	Høy			Nei
N_RD_03	RFID-IDer kan registreres i hvilken som helst godkjent RFID-database	Høy		N_RD_04	Nei
N_RD_04	Brukeren mottar riktig informasjon uavhengig av hvilken RFID-database informasjonen er registrert i.	Høy	N_RD_03		Nei

Tabell 12: Krav til RFID-database

Mobilnettet

For datakommunikasjon over telenettet er GPRS den standarden som har lavest overføringshastighet, og er derfor et minstekrav. EDGE og 3G gir høyere hastighet. Tabellen under viser minstekravene til dataoverføring i telenettet.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
N_MN_01	Mobilnettet støtter GPRS	Høy		M_OF_04	Ja
N_MN_02	Mobilnettet støtter EDGE	Lav		M_OF_03	Ja
N_MN_03	Mobilnettet støtter 3G	Lav		M_OF_05	Ja

Tabell 13: Krav til mobilnett

7.4 RFID-reklamebrikker

Disse reklamebrikkene skal kunne plasseres i plakater, brosjyrer, bøker, butikker og lignende. Det er i hovedsak to typer RFID-brikker, de som aktivt oppsøker brukeren og gir tilbud, og de som er passive inntil brukeren selv oppsøker for tilbud og informasjon. Krav til lagringskapasitet, rekkevidde og omprogrammering av disse brikkene vil være forskjellig. Når det kommer til størrelse er det alltid en fordel med flate brikker, slik at de ikke vises og stikker ut. Smartlables er 0.1mm trykke og et fint alternativ.

Passive

De brikkene som er passive inntil brukeren oppsøker dem, trenger ikke mer lagringskapasitet enn størrelsen på IDen. 256Bytes er her en standard som vil holde. Brukeren vil så bli henvist til en webside e.l. for mer informasjon. Den tilhørende informasjonen oppdateres her på websiden, slik at brikken selv ikke trenger å være omprogrammerbar. Når det kommer til strømtilførsel vil de passive brikkene ikke ha egen strømforsyning, men bli aktivert av leseren til brukeren.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
R_PA_01	Tykkelsen på RFID-transponderen er 0.1mm	Høy			Ja
R_PA_02	Lagrings-kapasiteten til RFID-transponderen er 256Bytes	Høy			Ja
R_PA_03	Rekkevidden til RFID-transponderen er 10cm	Høy			Ja
R_PA_04	RFID-transponderen skal ikke være omprogram-merbar	Lav			Ja

Tabell 14: Krav til passive RFID-transpondere

Aktive

De brikkene som aktivt oppsøker brukeren, må ha så stor lagringskapasitet at de kan inneholde all informasjon om produktet de reklamerer for. Dette er fordi at brukere ikke vil aktivt koble seg opp på nettet, dersom de ikke vet noe om reklamen. Informasjonen må lagres på en standarisert måte slik at brukerens personlige profil forstår informasjonen, og kan filtrere. Dersom det skal være mulig å oppdatere informasjonen på brikken, må brikken være omprogrammerbar. Når det kommer til strømtilførsel vil de aktive brikkene ha en egen strømforsyning eller batteri.

Krav ID	Beskrivelse av krav	Prioritet	Avhenger av	Nødvendig for	Eksisterer
R_AK_01	Størrelsen på RFID-transponderen er valgfri	Lav			Ja
R_AK_02	Lagrings-kapasiteten til RFID-transponderen er 8KB	Høy			Ja
R_AK_03	Rekkevidden til RFID-transponderen er 2meter	Høy			Ja
R_AK_04	RFID-transponderen skal være omprogram-merbar	Høy			Ja
R_AK_05	Informasjon på brikken må lagres i et standarisert ontologi språk	Høy		N_PP_05	Ja

Tabell 15: Krav til aktive RFID-transpondere

8 Avslutning

Oppsummering

I dag har vi mange måter å betale for varer på. Vi kan handle med kontanter, kreditt/debetkort, mobiltelefon og internett for å nevne de mest brukte. Problemet med m-handel er å få tjenesteleverandører og en kundemasse samtidig. Kundene vil ikke knytte seg til tjenesten før det er et bredt utvalg av tjenesteleverandører, som på sin side vil være skeptiske til å knytte seg til produkt med lav brukermasse.

Oppgaven introduserer ideen med å integrere RFID-teknologien i mobiltelefonen for å utbrede m-handel. Kjøpsprosessen blir kortere, som er til fordel for tjenesteleverandørene og kundene. RFID-teknologien i mobiltelefonen kan også begrense antall betalingsmidler en kunde trenger konsentrere seg om, da elektronisk lommebok vil støtte elektroniske kontanter og kreditt/debet betaling.

Butikker kan benytte RFID-teknologien til å sende tilbud direkte til brukerens mobiltelefon, når brukeren er i nærheten av butikken. En elektronisk lommebok vil inneholde en personlig profil som vil virke som et egendefinert filter for brukeren. Dette filteret vil skjerme brukeren fra uønsket reklame, og slippe gjennom de tilbudene som er aktuelle for brukeren.

Oppgaven har belyst potensialet som ligger tilgjenglig ved å utnyte RFID-teknologien innen m-handel. Et problem i dag er at ingen produsenter leverer kommersielle varer som støtter RFID i mobiltelefonene, men har pilotprosjekter som omhandler dette.

Konklusjon

Oppgaven viser at RFID-teknologi vil kunne være en viktig faktor innen m-handel. Problemene med liten utbredelse, og for høy inngangsterskel kan forenkles med RFID-teknologi. Også kjøpsprosessen forenkles slik at kunden raskere kan gjøre kjøp.

Som kravspesifikasjonen fremhever, er mange av kravene til en slik løsning allerede klare. Det meste av teknologien er allerede i bruk, men ikke sammen. Det mest kritiske punktet er integrering av RFID-teknologi i mobiltelefonen. Flere mobiltelefonprodusenter jobber nå med prototyper av mobiltelefoner med RFID-teknologi.

Neste steg bør være å integrere RFID-teknologi i betalingsterminaler. Dette vil være en myk overgang til å bruke mobiltelefonen som betalingsmiddel. Videre steg blir å gradvis utvide tjenestene den elektroniske lommeboken kan tilby. Dette inkluderer standarder for elektroniske kontanter, personlig profil, RFID-database og elektronisk identifikasjon.

Videre arbeide med oppgaven vil være en standardisering av ontologien som benyttes i reklamebrikkene, og hvordan den filtreres av den personlige profilen. Oppdatering og vedlikehold av personlig profil må utredes. I fremtiden kan det også utvikles programvare for kommunikasjon mellom mobiltelefon og RFID. I dag selges ingen mobiltelefoner med RFID-leser, og ingen operativsystem har støtte for dette. Men med alt arbeidet som legges ned, og den raske utviklingen som teknologien har hatt, regner man med at standarder snart vil være på plass.

Ordforklaringer

Forkortelse	Forklaring
2,5G	GSM nettverket, inkludert støtte for GPRS og EDGE
2G	GSM nettverket
3G	(UMTS) Overtar etter GSM-nettverket, og støtter høye overføringshastigheter som muliggjør video over mobilnettverket.
Analog	Den tradisjonelle måten for å overføre signaler på, også brukt i eldre telefoner og mobilsystemet NMT. GSM er digitalt.
Antenne	Brukes på blant annet mobiltelefoner for å optimalisere sende- og mottagersignaler.
API	(Application Programming Interface) et sett med rutiner, protokoller og verktøy for å utvikle applikasjoner
Basestasjon	En sender/mottager som håndterer inn- og utgående samtaler.
Batteri	Mobilens strømkilde.
Bildemelding	Du kan sende og motta meldinger på din mobil som inneholder både tekst og grafikk.
Blåtann	Lavstyrke radioteknologi som blir brukt for at enheter som printere, PCer, mobiltelefoner osv. skal kunne kommunisere med hverandre. Har som regel en rekkevidde på mellom 7-15 meter.
Båndbredde	(Bandwith) En kommunikasjonslinjes evne til å overføre data. Bredbånd er en fellesbetegnelse for båndbredde som ligger over ca. 500-1000kbps
CDMA2000	(Code Division Multiple Access) Digitalt mobilsystem som opererer i 800MHz and 1900MHz båndene.
Data overføring	Overføring av data eller informasjon mellom PCer, mobiltelefoner eller andre eneheter i et nettverk.
Data Transmission	Overføring av data eller informasjon mellom PCer, mobiltelefoner eller andre eneheter i et nettverk.
Dekning	Området hvor en mobiltelefon klarer å oppnå kontakt med nærmeste basestasjon og utføre en inn- eller utgående samtale.
Digital signatur	En elektronisk signatur, kjennetegn, identifikasjon eller særegenhet.
Digitale kontanter	Elektronisk verdi eller valuta som kan blant annet brukes på Internett, telefoner.
Display	Vindu eller skjerm, som på mobiltelefoner har utviklet seg fra å kun vise enkle tegn til å kunne gjengi fargebilder og videoklipp.

Forkortelse	Forklaring
Dual-band	Telefoner som kan nå båndene eller nettverkene GSM900 og GSM1800.
Dupleks / Full dupleks	(Duplex) Toveisoverføring av f.eks en samtale.
Dynamisk minne	Minnet i for eksempel en mobiltelefon er ikke avsatt til hver enkelt tjeneste, men fordeles til de funksjonene eller tjenestene som krever minne. Dette kan være telefonboken, bildegalleri, tekstmeldinger, logoer, ringetoner osv.
EAN	(Europeisk Artikkel Nummer) den mest brukte strekkodestandarden.
EAS	(Electronic Article Surveillance) standard for tyverialarmer.
EDGE	En nyere metode for overføring av signaler og data, som har en teoretisk overføringshastighet på 473 kbps.
EEPROM	(Electronic Eraseble Programable Read Only Memory) minnebrikke som bevarer data selv uten størm.
EPOC	Et operativsystem gir bedre multimediamuligheter for mobiltelefoner.
ETSI	(European Telecommunications Standrads Institue) Organisasjon som utviket GSM i 1982.
FM	(Frekvensmodifikasjon) Radio signal.
FRAM	(Ferromagnetic Random Access Memory) minnebrikke i testfase som kan erstatte EEPROM.
Frekvens	Måles i hertz (Hz), mønsteret en bølge eller et radiosignal har.
GPRS	(General Packet Radio Service) GPRS, eller 2,5G, muliggjør en teoretisk dataoverføringshastighet i GSM-nettet på 171,2 kB/s.
GSM	Telefonsystemet som brukes i Europa og en rekke andre land. Delt opp i ulike nett som 900 MHz, 1800 MHz og 1900 MHz (USA).
HSCSD	Teknologi for GSM-nettet som muliggjør en teoretisk overføringshastighet på opptil 43,2 kbps.
Hz	Måleenheten for frekvens (svingninger per sekund).
Internett-leser	Brukes for å kunne lese blant annet internettsider. En rekke mobiltelefoner har dette innebygget for å kunne lese websider via WAP, GPRS eller annet.
IP	(Internet Protocol) Protokoll for sending av data over Internett.
IrDA	(IrDa) En teknologi som muliggjør overføring av signaler via infrarøde stråler.

Forkortelse	Forklaring
J2ME / Java	Gjør at en kan kjøre Java-applikasjoner som spill og programmer på enheter som inneholder denne programvaren.
Java	Java er plattformuavhengig og brukes av internett lesere og mobiltelefoner for å kunne kjøre ulike Javaprogram.
JVM	(Java Virtual Machine) Programvareimplementasjon av en prosessor som kjører javakode.
Linjesvitsjet	Betyr at det er nødvendig med en konstant oppkobling for at kommunikasjonen skal fungere.
LOS	(Line Of Sight) Fri sikt.
Mbps	(Megabit per sekund) Overføringshastighet som sier hvor mange millioner bit som sendes per sekund.
MEL	(MULTOS Executable Language) Programmeringsspråk for MULTOS smartkort.
m-handel	Mobilhandel.
MHz	(MegaHertz) En million hertz eller svingninger per sekund. Mobil kommunikasjon opererer i 900 MHz, 1800 MHz og 1900 MHz båndene.
MMS	(Multimedia Messaging Service) Melding som kan inneholde både lyd, bilder, tekst og video.
Model	Navn eller nummerbetegnelse for et produkt.
NFC	(Near Field Communication) RFID-standard med leser og transponder i samme brikke.
NMT	Analogt mobilsystem opprinnelig brukt i skandinavia, men er ikke lenger i kommersiell bruk.
OPS	(Open Profiling Standard) En foreslått standard for personlige profiler.
OS	Operativsystem.
OTA	(Over The Air) Trådløs nedlasning av feks ringetoner, SMS, og andre tjenester eller innhold til din telefon.
Packet switching service	Overføringen av data deles opp og sendes i pakker, for siden å settes sammen igjen. Er i motsetning til linjesvitsjet overføring ikke avhengig av en konstant oppkoblet linje.
PDA	(Personal Digital Assistent) Håndholdt enhet / PC som er en mellomting mellom en mobiltelefon og en PC.
PIN	(Personal Identification Number) PIN-kode som brukes sammen med et SIM-kort for å verifisere at rett person bruker telefonen.
PKI	(Public Key Infrastructure) Krypteringsstanderd.
P3P	(Privacy Preferance Project) Standard for bruk av personlig profil.

Forkortelse	Forklaring
Protokoll	Format på f.eks en dataoverføring som brukes ved utveksling av data eller informasjon mellom to enheter.
RF	(Radio Frequency) Radiofrekvens.
RFID	(Radio Frequency Identification) Trådløs kommunikasjonsstandard
SIM	(Subscriber Identity Module) Kort som brukes i alle GSM-telefoner. Kortet har en liten mikrobrikke som inneholder informasjon om eier, telefon og feks kontaktlisten din.
SMS	(Short Message Service) Tekstmeldinger på inntil 160 tegn. Noen telefoner kan sende lengre meldinger, men da deles meldingen opp i flere deler.
SRAM	(Static Random Access Memory) En minnetype
Symbian	Symbian er et operativsystem for mobiltelefoner og PDA, opprinnelig utviklet av Psion, Nokia, Ericsson og Motorola.
TDMA	(Time Division Multiple Access) Teknologi som brukes i digitale, trådløse overføringer. Muliggjør et større antall samtidige overføringer.
Tri-band	En trebåndstelefon fungerer på på nettene GSM900, GSM1800 og GSM1900, og kan dermed brukes i Asia, Europa, Afrika, og Nord-Amerika.
TTP	(Tiltrodd Tredje Part) En offentlig godkjent instans.
UI	(User Interface) Brukergrensesnitt.
UMTS	(Universal Mobile Telephone System) Tredjegenerasjons kommunikasjonssystem. De første telefonene som kan nyttegjøre dette systemet er i salg nå.
UPC	(Universal Product Code) Tidlig strekkode system.
URL	(Uniform Resource Locator) En måte å gi et nettsted eller server en unik adresse på.
W3C	(World Wide Web Consortium) Organisasjon som jobber med Internett standarder.
WAP	(Wireless Application Protocol) Protokoll for overføring av data.
WLAN	(Wireless Local Access Network) Trådløs tilgang til et nettverk fra en datamaskin eller annen enhet.
WML	(Wireless Markup Language) Språk eller protokoll utviklet for trådløse bruk.
XML	(Extensible Markup Language) XML er et språk / format for organisering og struktur av data.

Kilder

"*If I have seen further it is by standing on the shoulders of giants.*"
–Isaac Newton

[BBS]	http://www.bbs.no/bbs/om_bbs/historikk/historikk.cfm
[BankAxept]	http://www.bankaxept.no/bankaxept/baxkort/baxkort.cfm
[Barcode]	http://www.barcode-us.com/
[Bentzen Ernes 2004]	Ann Kristin Bentzen Ernes http://www.digi.no/php/art.php?id=105359
[Bentzen Ernes 2005]	Ann Kristin Bentzen Ernes http://www.digi.no/php/art.php?id=211586
[Brain 2000]	Marshall Brain 2000 http://science.howstuffworks.com/electromagnet.htm
[Brickley og Guha 2004]	Dan Brickley og R.V. Guha 2004 http://www.w3.org/TR/PR-rdf-schema/
[Collins 2004]	Jonathan Collins 2004 http://www.rfidjournal.com/article/articleview/857/1/1/
[Datatilsynet]	http://www.datatilsynet.no/templates/article____889.aspx
[Davidsen og Tepfers 2002]	Davidsen & Tepfers 2002 Fra Buzz til Biz ISBN 82-519-1788-3
[eCash]	http://www.ecash.net/
[eSolutions]	http://www.esolutions.no/index_produkter.htm
[Finkenzeller 2003]	Klaus Finkenzeller 2003 RFID handbook ISBN : 0-470-84402-7

[Frenzel 2002] Louis E. Frenzel 2002
http://www.elecdesign.com/Articles/Index.cfm?AD=1&
ArticleID=2347

[Ganguli2002] Madhushree Ganguli
Getting Started with Bluetooth
ISBN-1-931841-83-7

[Gran 2004] Even Gran 2004
http://www.forskning.no/Artikler/2004/juni/1086785094.34

[HandCash] http://www.handcash.no/

[Hansson 2003] Tone Semmen Hansson
Fordypningsprosjekt NTNU 2003

[Hara2005] Yoshiko Hara 2005
http;//nwm.mobilepipeline.com/161600925

[HowStuffWorks Creditcard] http://money.howstuffworks.com/
credit-card.htm/printable

[Kairer 2005] Ryan Kairer 2005
http://www.palminfocenter.com/view_story.asp?ID=7597

[Lie 2003] Julianne Lie 2003
Handel.no
http://www.handel.no/pkiforum/modules/
module_109/publisher_view_product.asp?iEntityId=963

[Linuxdevices] Linux PDA
http://www.linuxdevices.com/articles/AT8728350077.html

[Longueuil2002] Donald J. Longueuil 2002
Wireless Messaging Demystified
ISBN:0-07-138629-7

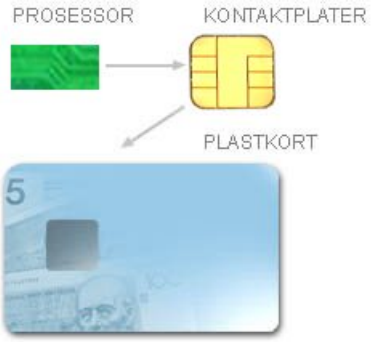
[MSMobile] Windows Mobile
http://www.microsoft.com/windowsmobile/default.mspx

[NFCforum] http://www.nfc-forum.org/aboutnfc/

[Post- og teletilsynet 2004]	http://www.npt.no/pt_internet/venstremeny/publikasjoner/telestatistikk/statistikk2004/halvaar.pdf
[RFIDu2005]	RFIDupdate http://www.rfidupdate.com/news/10252004.html
[SF04]	http://intranett.sparebankforeningen.no/wointer/article.asp?Channel_ID=1150&Article_ID=3562
[SSB2000]	http://www.ssb.no/ssp/utg/200006/6.shtml
[Stallings 2003]	William Stalling 2003 Network Security Essentials ISBN 0-13-120271-5
[Statens forvaltningstjeneste 1998]	http://odin.dep.no/nhd/norsk/dok/andre_dok/rapporter/024005-990115/hov003-bn.html
[Symbian]	http://www.symbian.com/technology/technology.html
[TNMH1]	http://telenormobil.no/mobilhandel
[Whatis2005]	http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci214208,00.html
[Wiley2001]	John Wiley & Sons, Ltd GSM, GPRS and EDGE Performance ISBN:0470 84457 4

Vedlegg 1 Smartkort

Smartkort med mikroprosessor ser ut som et vanlig standard plastikkort, men er utstyrt med en integrert Integrated Circuit(IC) brikke. Smartkort kan lagre informasjon, utføre lokal prosessering av data og utføre komplekse kalkulasjoner. Slike kort fines i kontaktløse kort og kontakt-kort varianter. Det finnes flere ulike typer smartkort, men felles for de alle er at de trenger et eksternt grensesnitt for å kunne kommunisere, forsyne strøm og klokkepuls. Alle de ulike smartkortene kan kategoriseres i 2 ulike kategorier: Minnekort og mikroprosessorkort. De store kortleverandørene har utviklet en egen standard for smartkort. Det er satt januar 2005 som frist for europeisk overgang til EMV(EuropayMasterCardVisa) smartkort. I Norge vil dette koste ca. 600 millioner kroner. Innføringen av smartkort vil ikke umiddelbart bety at magnetkortene forsvinner. Vi ser nå at banker utsteder smartkort med magnetstripe. Dette er på grunn av at de nye kortene også skal være brukbare på gamle terminaler, og terminaler i andre land [SF04].



Historie

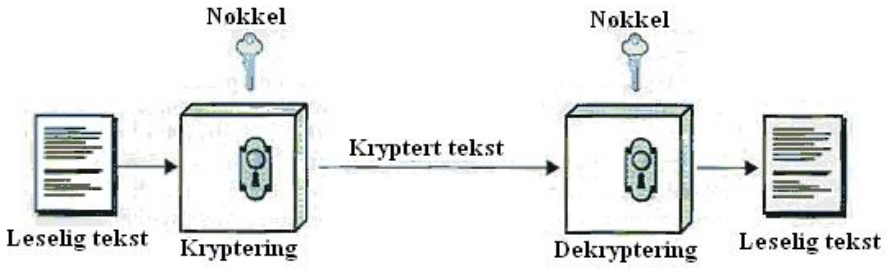
Smartkortet ble oppfunnet og patentert av franskmannen Roland Moreno i 1974. Det tok mange år før smartkortet kom på markedet, men i 1982 kom det første kortet ut på markedet i Frankrike, som et telekort(Telecarte). I 1984 kom det første debetkort med smartkort. Disse kortene ble stadig forbedret og sikkerheten bedre gjennom årene som gikk, og i 1993 klarte man å slå disse 2 kortene sammen til ett kort, et multifunksjonelt smartkort. Europay, MasterCard og VISA gav ut en standard, kalt EMV, i 1994. Tyskland var første land ut med å dele ut helsesmartkort til alle sine innbyggere, noe også Frankrike fulgte opp med noen år senere. I 1995 ble smartkortet(SIM-kort) brukt i mobiltelefonen for å initiere samtaler og lage regninger for samtalene. Det har oppstått flere varianter av smartkort operativsystem i kampen om å skape interoperabilitet(egenskap for at software og hardware fra forskjellige leverandører i heterogene systemer skal kunne kommunisere), og i dag er de 3 største Javacard, MULTOS og Windows SmartCard. I dag har smartkort utviklet seg enda lengre slik at de nå kan komme i både kontakt baserte og kontaktløse baserte kort, og anvendelsesområdene bare vokser og vokser.

Vedlegg 2 Kryptering

Det aller viktigste automatiserte verktøy for nettverkssikkerhet er kryptering. Det finnes to hovedtyper kryptering som er i bruk i dag: symmetrisk (secret key) og asymmetrisk (public key) kryptering. Til bruk i en elektronisk lommebok vil asymmetrisk kryptering være eneste løsning. Dette er også brukt i digital signatur.

Symmetrisk kryptering

Dette var den eneste form for kryptering helt fra til slutten av 1970-tallet. Tankegangen bak denne krypteringsformen er svært enkel. Det finnes èn nøkkel. Denne nøkkelen brukes til å kryptere (låse) et dokument, slik at det ikke lenger er leselig. For å kunne dekryptere (låse opp) dokumentet må man ha den samme nøkkelen [Stallings 2003].



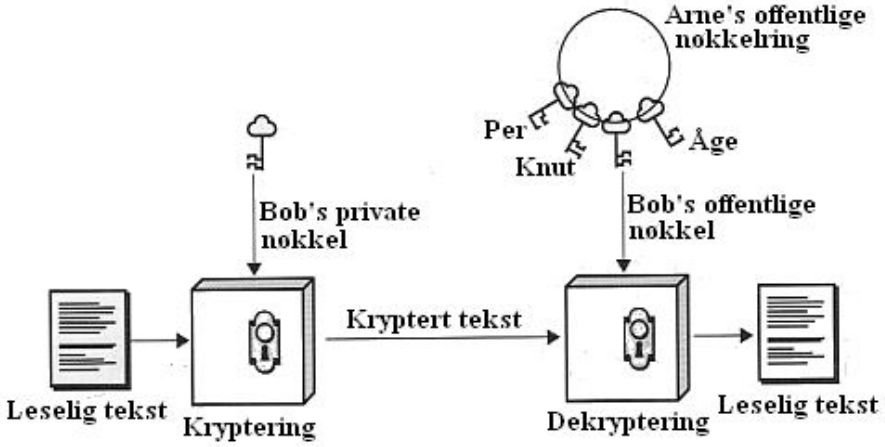
Sikkerheten av denne krypteringsformen avhenger i stor grad av nøkkelen. Problemet er at dersom et kryptert dokument sendes fra en bruker til en annen, så må begge brukerne kjenne nøkkelen. Den første brukeren må ha nøkkelen for å kunne kryptere dokumentet, mens den andre brukeren må ha nøkkelen for å kunne dekryptere og lese dokumentet. Det ble funnet en løsning på denne svakheten på slutten av 70-tallet, da asymmetrisk kryptering ble laget.

Asymmetrisk kryptering

Asymmetrisk kryptering, også kalt "public key", har en litt annen oppbygging. Her er det to nøkler, en privat nøkkel, og en offentlig nøkkel. Dette betyr at sender og mottaker ikke trenger å ha samme nøkkel. Sikkerheten her avhenger, som i symmetrisk kryptering, av at den private nøkkelen holdes hemmelig, noe som i dette tilfellet blir mye lettere. Dette gjøres ved å lagre den hemmelige nøkkelen i kundens SIM-kort, eller smartkort. Den offentlige nøkkelen skal man dele ut til alle som trenger den. Det finnes instanser som sørger for å dele ut disse offentlige nøklene, og å verifisere at den offentlige nøkkelen faktisk tilhører den riktige person [Stallings 2003]. Det er to forskjellige bruksområder av asymmetrisk kryptering; verifisering og kryptering.

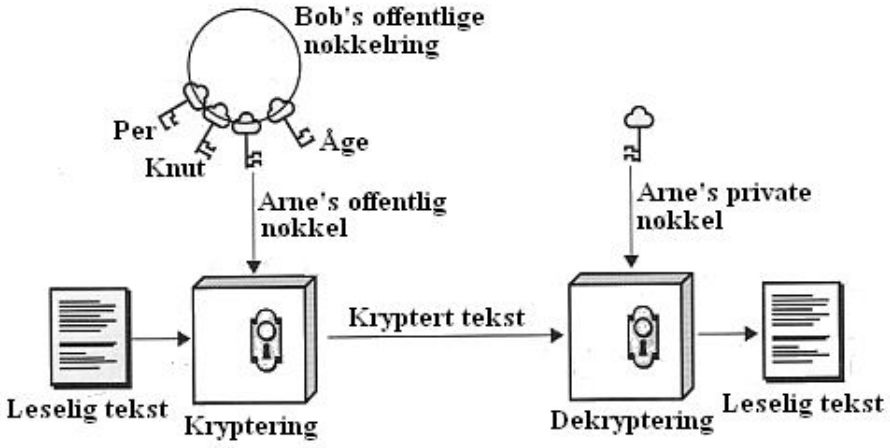
Verifisering

Dersom man krypterer med den private nøkkelen, kan man bare låse opp med den tilhørende offentlige. Dette kan brukes til å verifisere hvem som har kryptert meldingen.



Kryptering

Dersom man vil sende et hemmelig dokument til kun èn person, krypterer man ikke med sin egen hemmelige nøkkel, men med mottakeren sin offentlige nøkkel. Et dokument kryptert med en offentlig nøkkel, kan bare dekrypteres av den tilhørende private nøkkelen, noe som betyr at kun èn person kan lese dokumentet.



Eksempel

Dersom en kunde ønsker å ta opp et lån i sin nettbank, vil banken generere et dokument som inneholder alle regler og juridiske aspekter i forbindelse med lånet. På dette dokumentet vil også lånebeløpet, lånesøkerens navn, nedbetalingsavtalen og lignende informasjon være. Dersom kunden godkjenner dokumentet genererer han en kryptert datafil som knytter han til dette dokumentet. Vi kaller dette for signaturen. Signeringsprogrammer automatiserer denne prosessen, og gjør det lett for brukeren. Ingen andre kan endre på denne signaturen uten å kjenne kundens private nøkkel, ikke engang banken.

Banken kan verifisere at det faktisk var den riktige kunden som kvitterte, ved å dekryptere med hans offentlige nøkkel. Dersom dekrypteringen er vellykket, vet banken at kunden ikke har endret noe i kontrakten, og at rett person har signert den. Kunden vet også at banken ikke kan endre kontrakten etter at han har signert den, siden de ikke kjenner hans private nøkkel. Det er meget plasskrevende å lagre alle signerte dokumenter dobbelt, en i klartekst og en som er signert (kryptert). Derfor lages det ofte et matematisk resymé (hash) av hele dokumentet. Deretter krypteres dette resymeet. For å verifisere en slik signatur må banken også lage en hash av dokumentet for så å sammenligne den med den dekrypterte hashen i signaturen. En hash kan sammenlignes med et fingeravtrykk av dokumentet, mye mindre i størrelse med likevel unikt.

TTP

Spørsmålet mange nå stiller seg er; hvordan vet vi at denne offentlige nøkkelen tilhører kunden? Kan en svindler dikte opp begge nøklene og late som han er en annen person? Til å løse dette problemet trenger vi en tiltrodd tredjepart (TTP) også kalt certification authority (CA). En TTP er en instans som har ansvaret for å vedlikeholde og distribuere de offentlige nøklene. Til dette brukes digitale sertifikater.

Vedlegg 3 Mobil til mobil

Kommunikasjon mellom to mobiltelefoner kan ofte være litt vrient å sette opp. Som figuren til høyre illustrerer må mottakeren manuelt aktivere blåtann før avsenderen kan søke etter enheter. Denne søkeprosessen returnerer alle blåtann-enheter innen rekkevidde, noe som kan være tidkrevende. Avsenderen må finne mottakerens enhet ut i fra en liste. Disse enhetene har ikke alltid logiske navn, så det kan være vanskelig å finne rett. Når mottakeren så har godkjent oppkoblingen og mottatt data må blåtann manuelt avsluttes. RFID-teknologien kan forenkle jobben ved at mobiltelefonene vil inneholde en RFID-transponder og en RFID-leser som kan opprette blåtann og IrDA forbindelser automatisk. Figuren til venstre illustrerer at RFID automatisk kan opprette en blåtann-forbindelse når mottaker godkjenner forespørselen. Data sendes og forbindelsen avluttes automatisk.