UNIVERSITETET I OSLO
Institutt for informatikk

The Mobile Phone as Doorkeeper

Masteroppgave
(60 studiepoeng)

Haakon Eikenes

01. August 2006

Forord

Denne masteroppgaven er gitt av Universitetet på Keller ved Josef Noll.

Jeg vil benytte anledningen til å takke min veileder Josef Noll, for hans dyktighet og veiledning under oppgaven. Takk for lån og tilrettelegging av ressurser, uten dette hadde ikke oppgaven latt seg gjennomføre.

Jeg vil også takke Kjell Myksvoll, som arbeider ved Telenor Research & Development, for hans støtte under programmeringen. Han har vært til stor hjelp de gangene jeg har hatt tekniske spørsmål omkring utviklingen.

Til slutt vil jeg takke Thomas Halvorsen for et fint samarbeid gjennom hele oppgaveperioden. Mange diskusjoner og meningsutvekslinger har vi hatt, noe som har vært med på å forme utviklingen av systemet og skrivingen av oppgaven.

Haakon Eikenes

25. Juli 2006

Abstrakt

Dette er en mastergradsoppgave ved Institutt for Informatikk, Universitetet i Oslo. Oppgaven er en utforsking av Near Field Communication (NFC) satt i sammenheng med bruk av mobiltelefon. En del av oppgaven har vært å programmere et system som beviser at det er mulig å distribuere adgangsnøkler, ved hjelp av Short Message Service (SMS), til en mobiltelefon som igjen gir adgang til en fysisk dør. Teknologien er i startfasen, men mye tyder på at det finnes et potensial som ennå ikke er fullt utnyttet. Studien gir en oversikt over teorien, hva som finnes i dag og muligheter og utfordringer knyttet opp mot både systemet og teknologien, samt mulige løsninger.

Innholdsfortegnelse

Figurliste

Tabelliste

1. Introduksjon

En selvfølge for de fleste av oss er krav til rask tilgang til informasjon og elektroniske tjenester. En hverdag der tilgjengelighet og brukertilfredshet er sentrale temaer for tjenesteleverandører av mobile tjenester vil nye og bedre applikasjoner og teknologier vokse frem. For få år siden var internett det store satsingsområdet, mens vi dag ser en dreining mot tilgjengelighet og mobilitet. Derav er tjenester og muligheter som også ligger til rette for mobiltelefon sentralt i forhold til fremtidige tjenester som tilbys. Mobiltelefon er ofte noe vi bringer med oss, og SIM-kortet tillater autentifisering gjennom GSM-nettet.
Med dette som utgangspunkt har vi utarbeidet et system som distribuerer nøkler for fysisk adgang, ved hjelp av NFC-teknologien. Teknologien er relativt ny i forhold til etablert kunnskap, derfor var utgangspunktet for oppgaven krevende, særlig i forhold til innhenting av litteratur og tidligere utførte prosjekter.

I oppgaven har jeg beholdt en del engelske ord og uttrykk der hvor ord mangler i det norske, fordi de fleste av disse er integrerte og etablerte.

Tidslinje og aktiviteter
Samarbeidet og møtene med våre to veiledere har fungert bra. Vi startet på oppgaven høsten 2005, men på den programmeringsmessige delen av oppgaven gikk det en del mer tid enn både veilederne og vi hadde planlagt. Mye av grunnen skyldes ny teknologi og endringer av oppgaven underveis, en utfordring har til tider vært å sette grenser under utviklingen.

Vi har også hat en del aktiviteter under oppgaveperioden bestående av:

- Møter ved Unik
- Møter ved Telenor Fornebu
- Møter ved Institutt for Informatikk
- Møter ved Movation [Movation]
- Workshop ved Telenor Fornebu ved Nicolay Bang

- Møte ved Epsys ved Kostas Papadopoulos [Epsys]

1.1 Oppgavens Struktur

Oppgaven presenterer bakgrunnsteori, metode og resultater og drøfting på følgende måte.

Kapittel 1 introduksjon til oppgaven.

Kapittel 2 tar for seg problemstillingen, utgangspunktet for oppgaven, problem- og anvendelsesområdet, fokusområdet og begrensninger.

Kapittel 3 vil fokuserer på bakgrunnsteorien for utviklingen av systemet.

Kapittel 4 vil gi en innføring i hvordan teknologien vi har benyttet fungerer og andre prosjekter som er utført.

Kapittel 5 beskriver de ulike delene av systemet, hvordan de er bygget opp og til slutt hvordan komponentene er satt sammen til et system.

Kapittel 6 presenterer systemet i ulike scenarioer, sikkerhet knyttet til bruk av teknologien og systemet, og til slutt drøftes styrke og svakheter.

Kapittel 7 avslutter oppgaven med å gi en oppsummering og retter et blikk mot utfordringer i fremtiden.

1.2 Near Field Communication Forum

NFC teknologien har dannet sitt eget bransjeforum, NFC Forum. NFC Forum ble grunnlagt av Royal Philips Electronics og Sony Corporation i 2004, mens teknologien er utviklet av Royal Philips Electronics, Sony Corporation og Nokia.
I dag er det flere store selskaper som har inngått samarbeidsavtale med NFC Forum, med forskjellige typer medlemskap. Dette er selskaper som har interesseområder i mobilteknologi, betalingsløsninger, softwareløsninger og lignende.

NFC forum har åpnet for et samarbeid mellom de ulike interessentene om en standardisering og spesifisering av NFC-teknologien. Sammen har de laget standarder for NFC protokollen (NFCIP-1 og NFCIP -2), slik at alle enheter med NFC-teknologi uavhengig av produsent skal kunne

fungere sammen og i tillegg være kompatibel med Sony`s FeliCa™ og Philips MiFare ® teknologien. [Near Field Communication Forum]

Antall medlemmer av NFC Forum er i dag over 50 selskaper, og flere av dem er kjente selskaper rundt om i verden. Sponsorselskapene har medlemmer i styret, mens mindre aktive selskaper har medlemmer i komitéer. Sponsormedlemmene er i dag: MasterCard International, Matsushita Electric Industrial Co., Ltd., Microsoft Corp., Motorola, Nokia Corporation, NEC, Renesas Technology, Royal Philips Electronics, Samsung, Sony Corporation, Texas Instruments og Visa International.

NFC Forum består i dag av fire tekniske arbeidsgrupper, som deler opp arbeidet i fire forskjellige ansvarsområder. Henholdsvis NFC-enheter, anvendelsesrammeverk, sikkerhet og testing.
Innen disse områdene jobber de sammen mot en standard for industrien som produserer enheter og de som utvikler NFC-teknologien, slik at disse bruker felles protokoller, dataformat, tester og sertifisering.

NFC Forum har kommet langt i arbeidet med NFC-protokollen på kort tid. Protokollen har støtte for dataoverføring mellom to NFC enheter og er kompatibel med dagens smartkort som bruker Proximity Card Reader (ISO 15693) protokollen. Videre har den også mulighet til å sette opp en sikker forbindelse mellom to enheter for så å overføre konfigurasjonen til andre protokoller som for eksempel Bluetooth. Dette er hovedsakelig hva som er utviklet av NFC Forum og det vil forklares i detalj i kapittel 3 og 4. Arbeidet som er gjort frem til nå er grunnsteinene for en videre utrulling av NFC teknologien i forbrukermarkedet. I årene fremover (2007/2008) vil det bli utført flere pilotprosjekter og kommersielle NFC-produkter vil komme på markedet, og da særlig mobiltelefoner. En viktig betingelse for den fremtidige utviklingen vil være samarbeid om standardisert NFC-protokoll.

Målet til NFC Forum er en teknologi med kompatibilitet mellom produkter som benytter RF (Radio Frequency) som kommunikasjonskanal.
For brukerne vil det si en intuitiv måte å kommunisere trådløst og sikkert med tjenester ved bruk av mobiltelefonen og andre håndholdte enheter.

2. Problemstilling

Dette har vært en praktisk rettet oppgave, med mye av fokuset på designspesifikasjon og det å få til en prototyp som beviser det vi satt oss som mål. Målet var et system som kunne gi personer fysisk adgang til en eller flere dører ved å sende SMS til en serverapplikasjon som kommuniserte med den elektroniske låsen. Videre skulle dataoverføringen mellom mobiltelefonen og låsen håndteres av NFC-protokollen. Vår oppgave var å få disse komponentene til å fungere sammen, slik at systemet kunne brukes som en prototyp til blant annet demonstrering.

2.1 Utgangspunktet for oppgaven

Historien om lås og nøkkel går flere tusen år tilbake, fra de mest primitive lås mekanismene, hvor låsen var basert på lengden til nøkkelen, den gang en trestokk, til låsemekanismene vi bruker i dag som er alt fra hengelås til fingeravtrykk baserte låser. Grunnregelen den gang var lik den vi har i dag, nemlig sikre verdier.
Det er mange av disse faktaene/poengene som ligger til grunn for oppgaven, nemlig å utvikle et låsesystem som er enklere og sikrere enn mange av de vi har i dag. En viktig faktor her er at et hvert nytt system må være enklere å bruke, og ikke minst gagne brukerne.

Samfunnet er under stadig utvikling og trenger stadig forbedringer og nye løsninger, da er det ofte at problemet eller forbedringen ender med en digital løsning. Dette fordi samfunnet generelt blir mer og mer digitalisert, og fordi en slik løsning ofte øker effektiviteten.
I sammenheng med denne utviklingen har også teknologiutviklingen gitt oss nye muligheter.

Et sentralt begrep er mobilitet, selv om det er et vidt begrep som både kan omhandle menneskers evne til å være mobil, det vil si evnen til å flytte seg fra ulike geografiske plasseringer, til det å definere en enkel enhet som mobil. I følge definisjonen til Hjelm, er en enhet mobil når; den kan følge en person rundt; få plass i lommen; betjenes med en hånd [Hjelm, 2000]. Dette er selvsagt et definisjonsspørsmål, fordi mange ser på bærbar-PC som en mobil enhet. I følge av

teknologiutviklingen som kommer i fremtiden og teknologien som finnes i dag, har vi tatt utgangspunkt i bruken av mobiltelefon som ”Doorkeeper”.

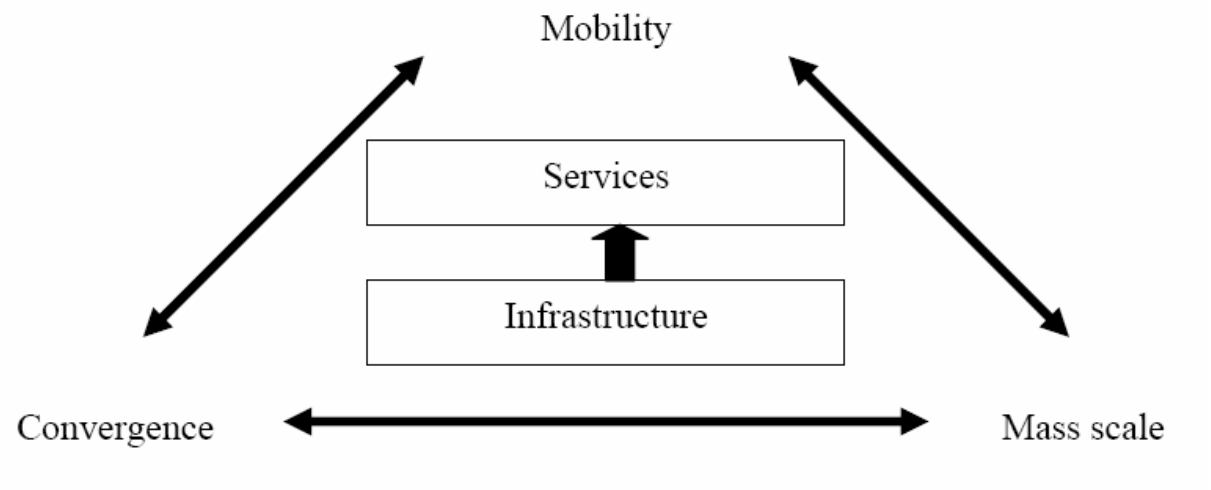
De fleste tar med seg mobiltelefon, nøkler og lommebok når vi forlater hjemmet. Hvordan ville det fungere dersom disse enhetene ble digitalisert og implementert på mobiltelefonen? I denne oppgaven har jeg sett på hvordan det går an å implementere husnøkkelen på mobiltelefonen og i tillegg sett på muligheter i sammenheng med teknologien som er brukt.

Det er ikke lenger slik at en tjeneste er tilgjengelig på et stasjonært område, og at brukeren må dra ditt for å benytte den, i dag ser vi at det blir mer vanlig at tjenestene tilbys der brukeren er, når og hvor han eller hun måtte ønske. Et eksempel vil være kjøp av musikk, man trenger ikke lenger dra til en butikk som selger CD-plater. Har man en PC, PDA eller liknende er tjenesten tilgjengelig der hvor brukeren er.

2.2 Nomadisk informasjonsmiljø

I følge artikkelen “The Next Wave of Nomadic Computing: A Research Agenda for Information Systems Research” skrevet av Lyytinen m.fl. lever vi i et nomadisk informasjonsmiljø. Nomade er en betegnelse på en menneskegruppe som stadig flytter seg mellom ulike fysiske steder. Bakgrunnen for at vi lever i et slik miljø er flere, for det første har nye mobile – og trådløse kommunikasjonsteknologier som WAP, Bluetooth, 3G og NFC blitt utviklet. Dette gir oss mulighet for mange og nye typer kommunikasjonstjenester. For det andre vil håndholdte datamaskiner som PDA, eller digitale mobiltelefoner føre til en mer digitalisert informasjonsflyt. Sett fra forfatternes synspunkt er nomadene her de organisatoriske aktørene. Men jeg mener også at en riktig definisjon vil være at alle mennesker som benytter seg av denne type teknologi kan sees på som en nomade. Det vil si at et hvert individ, enten det er innad i en organisasjon, eller ikke, kan sees på som en nomade i denne sammenheng.

I sammenheng med denne oppgaven vil jeg forsøke å se på de to definisjonene, og hvordan de kan settes i sammenheng med den praktiske delen av oppgaven.



Figur 1 - Rammeverk for nomadisk informasjonssystemer

Videre i artikkelen [Lyytinen m.fl., 2002] diskuteres tre viktige faktorer som til sammen utgjør rammeverket for et nomadisk informasjonssystem, mobilitet, digital konvergens og utbredelse (”Mobility”,”Convergens” og ”Mass scale”, se figur 1).
Mobilitetsbegrepet deles igjen opp i sosial og fysisk mobilitet. Med den sosiale mobiliteten menes evnen til å bevege seg fritt mellom ulike sosiale kontekster. Fysisk mobilitet er evnen til å flytte seg fra et geografisk sted til et annet. Felles for de to er at brukeren skal ha tilgang til den samme teknologien og de samme tjenestene uavhengig av geografisk plassering.

Artikelen ”Expanding the ’Mobility’ Concept” skrevet av Kakihara m. fl. i 2001 deler videre opp mobilitetsbegrepet i tre deler; tid, rom og kontekst, noe jeg vil bruke i drøftingen.

Digital konvergens

Mange medier konverterer til digitale løsninger fordi digitalisering generelt blitt billigere de siste årene, mye på grunn av åpne standarder som Bluetooth, 3G og TCP/IP (v6).
I tillegg er trådløse og mobile enheter essensielt for dette rammeverket [Lyytinen m.fl., 2002].
Det er også et poeng her at nye og gamle teknologier smelter sammen og danner nye hybrider. Tidligere var det ikke mulig å sende tekst, bilde eller filmer, som nå er gjort mulig ved hjelp av SMS og MMS. Et eksempel vil være SMS, en bruker av denne tjenesten vil ha ulike behov avhengi av kontekst og geografisk plassering. I jobbsammenheng ønsker brukeren kanskje også å motta private SMS.

Utbredelse i et nomadisk informasjonsmiljø betyr at ulike typer tjenester blir tilgjenglige med både nye og flere brukere. Infrastrukturen er med på å bestemme hvilke tjenester som de fremtidige brukerne vil benytte. Når nomadiske systemer blir vanlige vil resultatet i all hovedsak føre til utbredelse av tjenestetilgang og flere kommunikasjonstjenester [Lyytinen m.f., 2002].

I henhold til min videre utgreining av definisjonen til Lyytinen og Yoo, vil jeg studere bruken av ny teknologi i et nomadisk informasjonsmiljø. Jeg vil se på hvordan systemet vi har utviklet kan fungere for private hjem, bedrifter og i ulike typer organisasjoner.

2.3 Problem- og anvendelsesområdet

Dersom vi ser på dagens situasjon, det vil si bruken av lås og nøkkel, i forhold til vår visjon vil anvendelsesområdet ikke bli forandret, mens problemområdet vil bli forandret, og etter min oppfattning enklere enn slik den er i dag [Mathiassen m. fl., 2000].

2.4 Problemområdet

Problemområdet ligger i selve låsen, og bruken av nøkler. Låsene vi har i dag, særlig i det offentlige, har en stor ulempe - dersom man mister en nøkkel må kanskje mange låser byttes. Ser man for eksempel på hjemmehjelp tjenesten vil de ha en universalnøkkel som passer alle dører til pasienter de besøker, dersom denne blir borte må sannsynligvis alle dørlåser hvor nøkkelen kan brukes, byttes ut. Det vil bli både tids- og kostnadsmessig dyrt.
På samme måte vil det være for et privat hjem, dersom en nøkkel blir borte vil det ofte være at låsen på inngangsdøren må skiftes ut.

2.5 Anvendelsesområdet

Definisjonen på anvendelsesområdet er brukerne av låsene med tilhørende nøkler. Dette gjelder uavhengig om det er privat- eller organisasjonsmessig.

De fleste låser har i dag en eller flere nøkler, dersom en av disse kommer på avveie vil det ofte være behov for å skifte lås. Ved en eventuell innføring av systemet vi har utviklet vil problemområdet bli forandret, det vil da bli mulig å sperre de digitale nøklene til låsen, på den måten trenger ikke låsen skiftes ut, og en nøkkel kan enkelt erstattes, mens brukerne er de samme.

2.6 Fokusområde

Hovedfokus for denne oppgaven tar for seg serverdelen av systemet, hvordan vi har utviklet systemet, to mulige løsninger for kommersialisering og hva en kommersialisering av systemet vil si med hensyn på organisasjoner og i privat sektor.
Utviklingen er gjennomført i samarbeid med Thomas Halvorsen. Thomas sin oppgave har vært programmering av mobiltelefon og låsen, mens min oppgave har vært programmering av serverdelen. Til sammen utgjør det systemet jeg skriver om, det er derfor også nødvendig at alle delene blir presentert i oppgaven.

Utgangspunktet for den praktiske delen av oppgaven var, kort fortalt, å konstruere et system som kan erstatte dagens dørlås systemer. Løsningen ligger i all hovedsak i NFC-teknologien. Vi har også benyttet annen teknologi som Java (servlets, J2ME, J2SE), GSM (SMS), Tomcat webserver og Program for Advanced Telecom Services [PATS], for å realisere oppgaven. Jeg vil komme nærmere inn på de ulike teknologiene senere.

Systemet er i all hovedsak en prototyp, men for videre utvikling er dette en teknologi og et system som har mange bruksområder og et stort potensial slik jeg ser det. Når det nevnes prototyp her er det nettopp fordi noe av den teknologien vi har anvendt også er på prototyp stadiet, bland annet mobiltelefonen. Systemet har jeg valgt å dele i to scenarioer, som igjen kan deles opp i undersystemer. Den første delen jeg vil se på er hvordan et slikt system kan fungere i et privat hjem. Det andre jeg vil se på er hvordan systemet kan fungere i ulike typer organisasjoner og bedrifter. Utgangspunktet for systemene i de ulike scenarioene er teknologien vi har i dag, men vil også forsøke å bringe inn ny teknologi som kommer og forbedrer noe av det vi benytter i dag.

Når jeg her nevner undersystemer vil det si at jeg vill se på hvordan et slikt system kan fungere med kun en frittstående lås, og hvordan det fungerer med en server som styrer det hele. Det vil også selvsagt være en applikasjon og/eller en tjenesteleverandør som tar i mot SMS`ene fra lås eieren, og sender ut nødvendig data i form av SMS.
I hovedsak vil jeg se på hva en kommersialisering av systemet vil si for oss som individer og organisasjoner i et nomadisk informasjonsmiljø.

2.7 Avgrensning

Det er alltid knyttet en del utfordringer opp mot de fleste prosjekter som tar for seg utviking av programvare. Særlig når det kommer til brukergrensesnitt, kvalitetssikring, innovasjon, effektivitet, forretningslogikk og ikke minst sikkerhet. Det finnes selvsagt mange heuristikker og bevis fra ulike forskere som forklarer forskjellig løsninger på disse utfordringene. Vi har forsøkt å bruke gode løsninger og heuristikk gjennom hele prosessen, men en tidsramme vil alltid sette begrensninger. Alle disse utfordringene er som nevnt viktige og tett knyttet opp mot systemet, noe som gjør at vi har forsøkt å presentere de viktigste aspektene av utfordringene, men ikke hatt mulighet til å gå i dybden på alle.

I forhold til de økonomiske problemstillingene har vi ikke mulighet til å sammenligne med andre tilsvarende systemer da det ikke finnes. Dette har heller ikke vært en del av oppgaven.

3. Bakgrunnsteori

For lettere å kunne forstå hvordan NFC-teknologien fungerer vil dette kapittelet ta for seg teorien bak NFC, og andre teknologier som NFC er en del av. I tillegg vil jeg presentere smartkort av typen smartMX som også er essensielt for vårt system og en videreutvikling av teknologien og systemet.

3.1 Radio Frequency Identification og Near Field Communication

NFC teknologien er en videreutvikling av RFID (Radio Frequency Identification) og annen trådløs kommunikasjonsteknologi. RFID på sin side er utviklet for distribusjonsnettverk, for å holde kontroll over varer og lignende. En brikke plasseres på varen og den registreres når den flyttes forbi en leser. NFC er kompatibel med en slik løsning, men den er også videreutviklet til å kunne opprette en peer-to-peer kommunikasjon mellom to enheter. Begge teknologiene er basert på radiofrekvens som kommunikasjonskanal. RFID dekker en hel rekke frekvenser, mens NFC bare tar for seg en av dem, 13,56MHz.

3.2 Radio Frequency Identification

RFID teknologien består av to komponenter, en leser og en brikke. Hensikten til leseren er å sende spørresignaler til brikken, som da vil svare leseren. En brikke består av tre hoveddeler; en antenne, en silisium chip og et omslag.

Det finnes hovedsaklig to typer RFID brikker; aktiv og passiv. Den enkleste er den passive brikken, en slik brikke er avhengig av strøm fra leseren. Det vil si at den passive brikken mottar strøm og et spørresignal fra leseren, slik at brikken kan generere et svar og sende tilbake ved hjelp av strømmen den har mottatt. Slike brikker blir benyttet der leseavstanden er kort. Den enkleste kommandoen en RFID brikke kan bli gitt er å fortelle leseren hva dens unike ID er.

Den aktive brikken vil i tillegg ha en strømkilde, slik at den kan programmeres til å inneholde mer enn dens unike ID. Disse brikkene vil ha en kortere levetid.
Både den passive og den aktive brikken kan inneholde kryptert informasjon.
Det finnes i tillegg en semipassiv brikke som er veldig lik en aktiv brikke, men i motsetning til den aktive brikken vil den kun aktiviseres ved et signal fra leseren. Signalet fra leseren aktiviserer sending og mottak i brikken, slik at batteriet i den semipassive brikken kun benyttes når den mottar signaler noe som vil øke levetiden.

Radio Frequency Identification og bruksområder

Bruksområdene til RFID er i dag mange, og under en stadig utvikling for nye områder. Hovedsakelig benyttes RFID der hvor det er viktig å kunne spore og identifisere ulike typer objekter. Teknologien egner seg godt til å skape en bedre informasjonsflyt enn hva vi har i dag, RFID vil på mange områder effektivisere informasjonsflyten og fjerne ledd av usikkerhet.

Noen av dagens bruksområder:

- Bil med startsperre vil ikke starte uten at en nøkkel med riktig ID settes i tenningslåsen
- Husdyr kan merkes med en brikke slik at dyret kan spores tilbake til sin rette eier
- Merking av varer og kolli slik at bedrifter til en hver tid har kontroll på sitt lager

3.3 Near Field Communication Standardiseringen

NFC-teknologien er kommet som en videreutvikling av RFID og andre teknologier for å få en standardisering som kan brukes i ulike teknologier som benytter trådløs dataoverføring. Ved å innføre en standardisering vil ulike produkter fra forskjellige produsenter kunne kommunisere. NFC Forum består i dag av mange forskjellige selskaper med interesse for trådløs kommunikasjon. Sammen har de utarbeidet standarder for NFC-teknologien, og samarbeidet resulterte i flere ISO/IEC og ECMA (European Computer Manufacturer`s Association) standarder etter kun 14 måneder.

NFC standard protokoll

ECMA-340 Near Field Communication—Interface and Protocol l (NFCIP-1)

Protokollen beskriver data flyten mellom to NFC enheter, altså en peer til peer kommunikasjon. Spesifiserer også kommunikasjon mellom to aktive enheter samt en aktiv og en passiv enhet. Ble i 2003 en ISO standard (ISO 18092) [Near Field Communication White Paper].

NFC standard protokoll 2

ECMA 352 Near Field Communication Interface and Protocol – 2 (NFCIP-2)

Standarden spesifiserer kommunikasjon metoder mellom NFC enheter og andre enheter som er ISO 14443 kompatible (ISO 21481) [Near Field Communication White Paper].

ECMA 356

Standard for RF test metoder for NFCIP 1 enheter med antenne innen for det rektangulære området 85 mm x 52 mm.

ISO 14443

Standard som spesifiserer kommunikasjonskanal og protokoll mellom SmardCard og betalingsterminal, med frekvensområde 13,56MHz, som for eksempel Philips MyFare® og Sony`s FeliCa™.

Tekniske data

En oversikt over de tekniske dataene til NFC-teknologien.

Signal:	Frekvens på 13,56 MHz
Hastighet:	106kbits/s, 204kbits/s, 424kbits/s. Arbeider med 848kbits/s Maksimalt 3MB/min
Distanse:	0-10 centimeter, avhengig av størrelsen på antennen
Protokoll:	Halv-duplex

Tabell 1 - NFC tekniske data
[Near Field Communication White Paper]

4 Near Field Communication teknologien

Dette kapittelet vil ta for seg NFC-teknologien, hvordan den fungerer i praksis, områder hvor den er i bruk i dag og litt om hva fremtiden kan bringe.

NFC-teknologien er en utvidelse av RFID og andre sammenkoblingsteknologier. NFC er på samme måte som RFID en teknologi som er utviklet for kontaktløs identifikasjon. For at to NFC-enheter skal oppnå kontakt må de fysisk holdes mot hverandre, med kun noen få centimeters avstand, og det er dette som er spesielt for NFC teknologien.
I motsetning til for eksempel Bluetooth protokollen som alltid er aktiv så fort brukeren har slått den på. Da vil hvem som helst kunne finne denne enheten kun ved å søke den opp.

Enheter som bruker NFC-teknologien vil inneholde en unik ID, samt en eller flere applikasjoner. Denne ID vil være unik for brukeren og må derfor krypteres når den sendes. Applikasjon(er) på mobilen henter ut ID, krypterer og sender informasjonen til leseren. Brukeren vil da kunne gjøre seg til kjenne ved hjelp av enheten der hvor det kreves autentifisering for å få adgang til dører, PC`er og liknende.

En annen mulighet med NFC-enheter er at protokollen først oppretter en sikker peer-to-peer kommunikasjon. Deretter kan de to enhetene overføre konfigurasjonen til andre protokoller som Bluetooth, Wireless Ethernet, mellom forskjellige enheter som TV, mobiltelefon, PDA, bærbar-PC og lignende.

Hvis man skal overføre større mengder med data mellom to trådløse enheter, for eksempel en bærbar og en stasjonær PC, vil NFC-båndbredden gå for sakte. Dersom vi velger å benytte Bluetooth som protokoll må dette settes opp manuelt med passord som beskyttelse. Ved å bruke NFC kan denne kommunikasjonen settes opp kun ved hjelp av et enkelt tastetrykk. De to enhetene føres mot hverandre slik at de oppnår kontakt, deretter aksepteres brukeren og de vil opprette en sikker kommunikasjon. Bluetooth kommunikasjonen blir opprettet som det neste steg av prosedyren ved at konfigurasjonen utveksles. Nå kan de to enhetene flyttes fra hverandre, men

de fortsetter da å bruke den opprettede Bluetooth forbindelsen [Near Field Communication White Paper].

I følge NFC Forum er det spesielt to egenskaper ved NFC-teknologien som gjør den unik i forhold til andre typer trådløs kommunikasjon. Protokollen er basert på en kort overføringsdistanse, dvs. bare noen få centimeter. For det første mener de at sikkerheten er ivaretatt nettopp fordi avstanden mellom to enheter er veldig kort, og at det er lett å kontrollere kommunikasjonen ved å føre enhetene mot hverandre eller fra hverandre. For det andre mener de at denne type kommunikasjon er lik den vi mennesker har oss imellom. Når vi kommuniserer står vi som regel ikke og roper til andre langt borte, men vi går bort til personen vi skal kommunisere med. Det vil derfor være en kommunikasjonsmetode vi mennesker er kjent med, og kjenner oss igjen i [Near Field Communication White Paper].

NFC-teknologien gir oss mange nye utfordringer, en av de viktigste vil være dette med sikkerheten. Protokollen i seg selv skal være sikker fordi overføringsdistansen kun er noen få centimeter.

Det vil alltid være en viss fare for avlytting når data overføres trådløst. Selv om NFC-standarden kun tillater få centimeter mellom enhetene vil det være steder der man står i kø eller tett i folkemengde hvor en dataoverføring vil kunne avlyttes. Dette er teoretisk mulig, men praktisk nesten umulig, fordi med NFC-teknologien på mobiltelefonen er dette kun en leser, som ikke sender ut informasjon.
Sikkerheten er viktig her nettopp fordi enhetene kan inneholde virtuelle penger, nøkler og annen personlig informasjon om brukeren. Det at dataene overføres trådløst setter ekstra krav til sikkerhet, på grunn av fare for avlytting.

Near Field Communication Interface and Protocol 1
NFC protokollen er basert på en trådløs forbindelse mellom to parter, altså en peer-to-peer kommunikasjon. Selv om det er en trådløs forbindelse er rekkevidden som før nevnt ikke særlig lang.

Protokollen er laget slik at når to enheter er innenfor rekkevidde vil de straks oppnå kontakt, men det vil alltid være brukeren som godtar dataoverførsel og det gjøres med et enkelt tastetrykk. Det vil si at brukeren ikke trenger å konfigurere noe, og at sikkerheten er ivaretatt. Protokollen er sikker fordi data krypteres og avstanden mellom to enheter er såpass kort.

På samme måte som RFID skiller NFC-teknologien på leser og brikke. Forskjellen er at med en NFC-enhet vil man ikke bare ha en lesende enhet, men en enhet som kan både motta og sende informasjon (halv-duplex), som igjen fører til at NFC-teknologien kan brukes til overføring av filer mellom for eksempel en mobiltelefon og en PC og omvendt. I motsetning til RFID er det altså ikke konstruert brikke og leser, disse rollene kan byttes om på en og samme enhet. NFC-teknologien skiller på hvilke av de to enhetene som er initiativtakeren og mottager. Initiativtakeren sender ut spørring som mottageren svarer på og når kommunikasjonskanalen mellom to enheter er opprettet vil allikevel ikke initiativ- og mottager- rollene kunne byttes om.

En liket med RFID er at NFC-protokollen skiller på aktiv og passiv kommunikasjonsmetode. Ved aktiv kommunikasjonsmetode har begge enheter generert sitt eget RF-signal hvor de utveksler data. Passiv kommunikasjonsmetode vil si at kun en av enhetene har generert RF-signal og den andre bruker dette når den sender svar tilbake. NFC-protokollen spesifiserer at den av enhetene som er initiativtakeren er den som er ansvarlig for å opprette RF-signalet.

Protokollen etablerer forbindelsen mellom to NFC-kompatible enheter. Det er initiativtakeren som sender ut et spørresignal som leseren oppfatter og tar imot. Videre vil det være initiativtakeren som kontrollerer overføring av data og hastighet. Leseren, den passive brikken, vil da svare ved å sende data tilbake i samsvar med spørringen.
Overføringen stanses ved at applikasjonen i brikken avslutter, eller ved at brikken fysisk flyttes bort fra leseren.

Near Field Communication Interface and Protocol 2

Det finnes flere ISO/IEC standarder som benytter samme radio frekvens (13,56MHz) som kommunikasjonskanal. Det er derfor utviklet en NFC protokoll som gjør det mulig at disse tre standardene kan kommunisere. De tre standardene er:

- NFC (Near Filed Communication) - ECMA-340
- PCD (Proximity Card Reader) - ISO 15693
- VCD (Vicinity Card Reader) - ISO 14443

NFCIP 2 protokollen spesifiserer hvordan enheter med de ulike gateway(ene) oppnår kontakt med hverandre, og hvilken av de tre som skal benyttes. En prosedyre er satt opp for hvordan enhetene skal gå frem for å oppnå kontakt [Near Field Communication White Paper].

Hvis vi har en mobiltelefon med NFC-teknologi som forsøker å oppnå kontakt med et smartkort vil ikke NFC-standard protokollen klare å håndtere kommunikasjon mellom disse, fordi smartkort benytter PCD. Dersom mobiltelefonen har støtte for NFCIP 2, vil den allikevel først forsøke å oppnå kontakt med NFC-standard protokoll, deretter vil den gå over til VCD, og så PCD før den vil oppnå kontakt. Nå har de to enhetene opprettet en kommunikasjonskanal.

4.1 Smartkort

I den virkelige verden har vi flere typer håndfaste identitetsbevis, utsendt av for eksempel stat eller en bank, dette er et fysisk bevis på at du er deg. I den virtuelle og digitale verden er identifisering mer komplekst å håndtere. Spesielt innen den virtuelle verden, hvor det i dag ofte er kun et skjema som fylles ut (av hvem som helst) og man får tildelt et brukernavn og passord.

Avsnittet ” SmartMx brikken og MiFare smartkort emulering” er skrevet av Thomas Halvorsen.

Det finnes i dag mange teknologier som hjelper oss med elektroniske identitetsbevis som for eksempel magnetstripe, strekkode og RFID. De to førstnevnte er kostnadsmessig billige alternativer, men fordi sikkerheten ikke er særlig god sett i forhold til et smartkort er de to ikke lenger så relevante i forhold til identitetsbevisutviklingen. Et eksempel på dette er det nye biometriske passet. Fra 2004 ble alle nye pass utstyrt med en maskinlesbar strekkode, men fra 1. oktober 2006 vil nye pass også inneholde et biometrisk kjennetegn. Den mest kjente typen for

biometriske kjennetegn er fingeravtrykk, men også personens ansiktsform, og iris kan benyttes [Politi]. Disse kjennetegnene blir kryptert og lagret elektronisk i en RFID brikke på passet.
En strekkode må være synlig for at den skal kunne leses av, og derfor veldig lett og kopiere noe som gjør den uegnet som identitetsbevis.
Et kort med magnetstripe på sin side er noe bedre sikret, dataen som er lagret her er ikke mulige å se, de må leses av ved å dra kortet over et lese hode. Magnetstripekort har vanligvis tre spor, hvorav spor 1 og 2 vanligvis brukes. Spor 3 er et lese/skrive spor som inkluderer en kryptert PIN (Personlig Identifikasjons Nummer), landskode, valuta, maksimumsgrense, men denne er ikke standardisert hos de ulike bankene. Dataen på magnetstripen er ofte dårlig sikret og en stor svakhet er at de kan kopieres (skimming). Magnetstripen sammen med en personlig fire siffer kode er i dag en standard for betalingssystemer.

En elektronisk lommebok i form av smartkort, vil ligne på de kredittkortene vi har i dag, med påtrykt bilde og signatur (se figur 3). Chipen inneholder mikroprosessor, minne og operativsystem, hvilket gjør at den kan behandle og lagre data. Smartkortet kan kontrollere både data som behandles og hvem som har tilgang til hvilken data. En viktig del av smartkortet er muligheten til intern kryptering/dekryptering i tillegg til PIN.

Påtrykt bilde og signatur vil selvsagt ikke bli mulig på samme måte når smartkortet integreres i en mobiltelefon. Identitetsbeviset må da digitaliseres (digitalt sertifikat). Digitale sertifikater kan benyttes for å kontrollere at en digital signatur er ekte. Mobiltelefonen og Globalt System for Mobilkommunikasjon (GSM) støtter følgende sikkerhetsfunksjoner [GSM-world]:

- Public key infrastructure (PKI)
- One-Time-Password (OTP)
- EAP (Extensible Authentication Protocol)/SIM identifikasjon

Ved hjelp av disse sikkerhetsfunksjonene, og applikasjoner på smartkortet vil sikkerheten av dataoverføring (sende/motta) bli ivaretatt. EAP mekanismen støtter:

- SIM identifikasjon
- Anonymitet
- Reverifisering

Det innebærer at penger som er lagret på smartkortet blir betraktet som elektroniske kontanter. Elektroniske kontanter har da de har samme egenskapen som kontanter, de tillater anonym og gebyrfri betaling. I første omgang er det beregnet på kjøp av varer under 2-300 kroner. Ved kjøp av varer over en slik sum vil det kanskje bli aktuelt med en signering i tillegg.
Ved en hver transaksjon følger det med en kvittering, denne kan lagres som elektronisk kvittering på smartkortet.
PKI på sin side krever en tiltrodd tredjepart som garanterer at brukerens sertifikat er ekte og gyldig. Brukerstedet sjekker da gyldigheten av sertifikatet ved hjelp av en henvendelse til sertifikatutsteder eller en verifiseringsautoritet.

Smartkort typer

Det finnes i dag en rekke store aktører som er ute på markedet med både egne løsninger og åpne standarder på smartkort. Jeg har tidligere nevnt Philips sin MiFare®, og Sony sin Felica™ løsning. Disse er kompatible med NFC-teknologien. I tillegg til disse finnes det flere standarder som Java Card® og MULTIOS®.
Java Card er en åpen standard av Sun Microsystems, hvor det er en virtuell maskin som kjører på operativsystemet.

SmartMx brikken og MiFare smartkort emulering

Figur 2 - Mobiltelefon med SmartMX brikke

SmartMx brikken er et smartkort som består av en prosessor og 72KB skrivbare EEPROM2 (veldig lite ikke-flyktig minne), her lagres applikasjoner og informasjon som trengs av tjenestetilbydere som banker, transportfirma og lignende. Den har et lite operativsystem, Java Card, og prosessoren kan kjøre applikasjoner kalt Java Card Applets.
Applikasjonene bør helst lastes ned OTA (over the air) det vil si over GPRS eller WAP. Telefonen vi utviklet prosjektet på måtte bruke en Java MIDlet som mellomledd mellom OTA-kommunikasjonen (som bestod av SMS, ikke ”ekte” OTA) og minnet på SmartMx.
Den store fordelen med OTA installering er at når kunden skal tilføye funksjonalitet, for eksempel Oslo Sporveiers nye elektroniske billettsystem, trenger han ikke å oppsøke Oslo sporveiers billettluke.
For enklere å tilby tjenester emuleres MiFare 1k smartkort på SmartMx. Dette er en av verdens mest brukte og godt dokumenterte smartkortstandarder. Denne er benyttet fordi den er hensiktsmessig i prototypen.
Skal man bruke en NFC-terminal eller -lås som støtter MiFare vil SmartMx kunne være transparent og fremstå som et ordinært Mifare smartkort.
For at SmartMx brikken skal være sikker kan den ikke aksesseres helt uten videre, man trenger såkalte A (lese) og B (skrive) nøkler for å få tilgang til hvert enkelt element. Dermed kan man opprette forskjellige områder og applikasjoner med ulike tilgangsalternativer:
- Lese, men ikke skrive
- Skrive, men ikke lese
- Lese og skrive
- Verken lese eller skrive

For økt sikkerhet trenger man en sikkerhetsID for å installere og slette applikasjoner i tillegg til A og B nøklene. Enda en sikkerhetsmekanisme er støtte for kryptering av typen 3-DES og RSA. Dette gjør at uvedkommende ikke får tilgang til verken å installere applikasjoner eller utføre avlesning og eventuelt skriveoperasjoner.

Figur 3 - Visa med smartkort

Neste generasjons SIM-kort

Mobiltelefonens SIM-kort er et smartkort på lik linje med de som finnes på mange kreditt/debet-kort i dag (se figur 3). Det er derfor mulig å integrere informasjonen fra for eksempel bankkortet over på mobilens SIM-kort.

Før NFC kan implementeres på mobiltelefoner er det flere viktig punkter som gjenstår, hvordan smartkortet skal kommunisere med NFC-modemet, hvordan smartkortet skal integreres på mobiltelefonen, hvem stiller som verifiseringsautoritet dersom PKI skal benyttes og hvordan data skal lagres på SmartMX chipen? En løsning er NFC og sikkerheten som er tilgjengelig i SIM-kortet. Da vil SIM-kortet lagre applikasjonene og nøklene. En mulig løsning for kommunikasjon mellom NFC-modemet og smartkortet er Philips sitt S^2C [Philips] grensesnitt, men det arbeides for å få til en standardisering. Den andre løsningen er å gå utenom SIM-kortet, ved å implementere et smartkort i f. eks. dekslet, kretskortet eller som et digitalt kretskort på mobiltelefonen. Ved å implementere NFC i et eget digitalt kretskort som fysisk kan fjernes gir det brukeren mer kontroll over bruken. Dette innebærer at teleoperatørene ikke lenger har full kontroll over smartkortet. Når applikasjoner og oppdateringer skal installeres må det håndteres av en Java applikasjon på SIM-kortet dersom data skal sendes trådløst. Et annet alternativ er at brukeren må dra til tjenesteleverandøren for å få installert applikasjonen via kabel, men jeg vil ikke tro at det blir noe reelt alternativ.

Den enkleste løsningen slik jeg ser det er smartkort integrert i SIM-kortet, både fordi det er enklere for teleoperatørene og tjenesteleverandørene, og fordi man slipper Java applikasjonen som videresender data til smartkortet.
En løsning på hvem som stiller som verifiseringsautoritet kan være teleoperatørene, fordi GSM-nettet og mobiltelefonen støtter PKI.
En annen utfordring med hensyn på integrasjon av NFC på mobiltelefonen er samarbeid mellom de ulike tjenesteleverandørene. Hvordan skal de ulike applikasjonene fra tjenesteleverandørene installeres på SmartMX chipen? Nøkler sikrer at andre ikke får skrive- og lesetilgang til et område på chipen hvor det allerede er installert en applikasjon. For at dette ikke skal skje må det lages en standardisering eller algoritme som håndterer applikasjoner etter hvert som de installeres.

Den tekniske kompleksiteten til mobiltelefoner i dag øker stadig som følge av utvikling av nye funksjoner. Kamera og mp3-spiller på en mobiltelefon blir stadig mer vanlig. Flere aktører som BenQ lanserer også mobiltelefoner med Windows operativsystem. Mye av tankegangen bak NFC-teknologien er at den kan implementeres i en mobiltelefon.

Når det kommer til bruken av et slikt system satt ut i praksis er det som tidligere nevnt tre fokusområder jeg vil se nærmere på. Hvordan det kan fungere i et privat hjem, en bedrift og i en organisasjon. Systemet slik det er i dag har flere betingelser som gjør at det fungerer,

- smartkort i dekslet på telefonen
- applikasjon på telefon forhånds installert

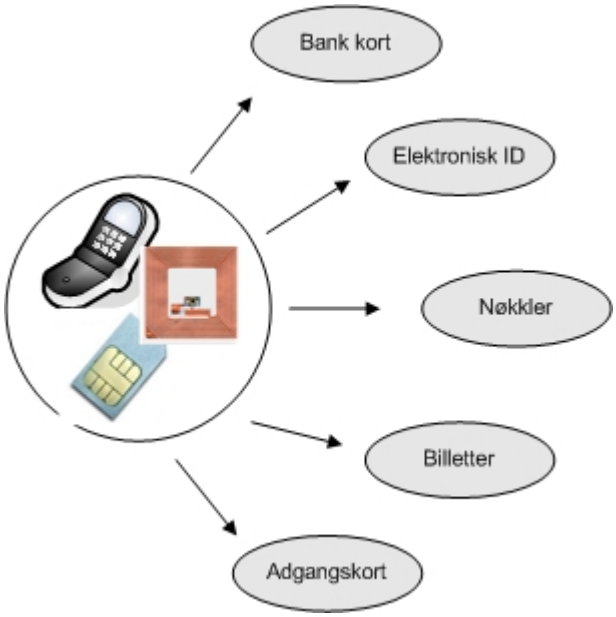
I en fremtidig utgave av et slikt system vil det også være betingelser for en optimalisering av dette:

- lagring av data på SIM-kort
- SIM-kortet er et sikkert sted å lagre data
- Behov for verifiseringsautoritet
- Samarbeid mellom verifiseringsautoriteten og tjenesteleverandørene

4.2 Subscriber Identity Module og Near Field Communication

Ved å implementere NFC i mobiltelefonen (SIM) gir det en rekke fordeler, installasjon, og ”oppdateringer” kan sendes til SmartMX chipen som er integrert på SMS-kortet. På samme måte som det er i dag med en et kort for betaling og et annet for adgang til kontoret vil det bli med de installerte applikasjonene på SmartMX chipen. Brukeren vil ha en ID for hver tjeneste. Tjenesteleverandøren sender applikasjonen brukeren trenger, og den lagres automatisk på SmartMX chipen, autentifikasjon av bruker kan formidles mellom teleoperatør og tjenesteleverandør.
GSM systemet tillater også sperring av SIM-kortet, noe som vil være helt nødvendig dersom en telefon mistes, eller blir stjålet. Brukeren må ha mulighet til å kontakte sin tjenesteleverandør av mobilnett slik at SIM-kortet kan sperres. Det betyr at data på smartkortet blir utilgjengeliggjort.

En slik løsning åpner for en rekke nye muligheter. De fleste smartkort baserte betalingssystemene i Europa benytter ISO14443 standarden, som NFC er kompatibel med. Etter hvert vil også AS Oslo Sporveier starte nytt elektronisk billett system som baserer seg på ISO14443 standarden [Sporvien].
Billettsystemet under fotball VM 2006 benytter også RFID baserte billetter, dersom en kjøper av en billett mister billetten, kan denne slettes og kjøperen kan få en ny billett. Dette er bare noen eksempler som viser at denne type teknologi er i bruk i dag. Ved å integrere NFC i mobiltelefonen vil disse funksjonene bli tilgjengelig fra en og samme enhet. SIM-kortet kan bli nøkkel komponenten som kan inneholde sensitiv informasjon for brukeren; bankkort, elektronisk ID, nøkler, billetter, og adgangskort (se figur 4).



Figur 4 - Muligheter med NFC integrert på mobiltelefon

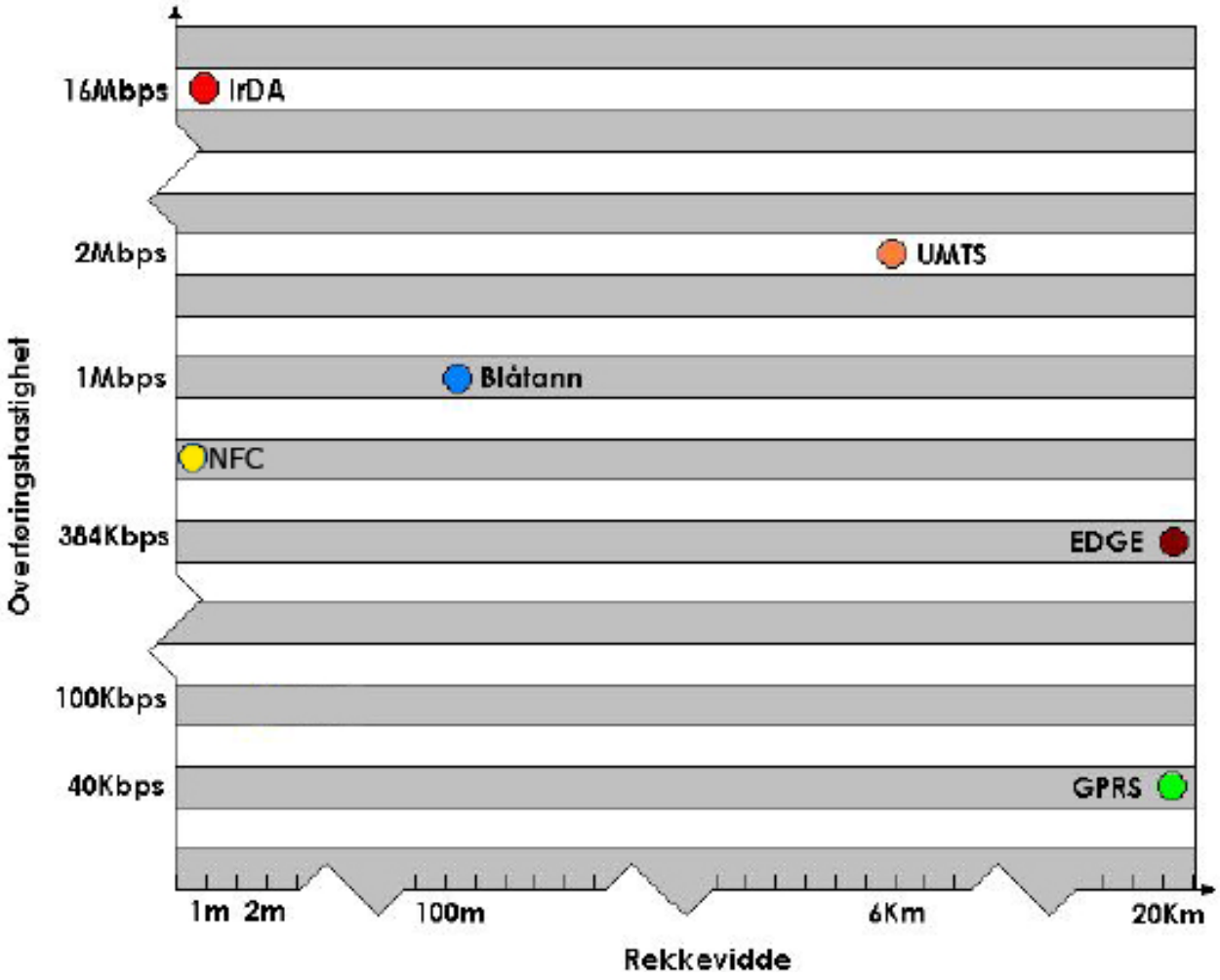
Tabellen viser en oversikt over de mest vanlige standardene. Jeg har valgt å ikke ta med RFID i denne tabellen fordi rekkevidden på en RFID brikke avhenger av flere ting som: aktiv eller passiv brikke, hvilke frekvensområde, energieffekten og så videre.

Standard	Rekkevidde	Overføringshastighet
Blåtann[1]	0 til 100m	2Mbps
lrDA[2]	< 1m	2.4Kbps til 16Mbps
GPRS[3]	<20Km	<160Kbps
EDGE	<20Km	<384Kbps
UMTS[4]	10m til 6km	<2Mbps
NFC[5]	0 til 10cm	<424Kbps

Tabell 2 - Kommunikasjonskanaler

Tabellen er ment som en oversikt over de vanligste overføringsmetodene innen mobilteknologi. Det er spesielt med tanke på hvor i den grafiske fremstillingen NFC befinner seg i forhold til andre standarder. Det vi kan se ut i fra grafen er at NFC ikke er basert på dataoverføring over store avstander, og at den teoretiske overføringshastigheten er høyere enn både GPRS og EDGE.

[1] http://www.bluetooth.com/bluetooth/
[2] http://www.irda.org
[3] http://www.3gpp.org
[4] http://www.elektroikt.no/dokumenter/UMTS_innforing.pdf
[5] http://www.nfc-forum.org



Figur 5 - Grafisk fremstilling av tabell 2

4.3 Andre prosjekter

NFC teknologien er relativt ny, mens RFID som NFC bygger på har vært en utviklende teknologi siden 1942. RFID ble først tatt i bruk under andre verdenskrig, da engelskmennene ville skille mellom flyene slik at de lettere kunne vite om flyet var fiendtlig. Flyene fikk festet en transponder på seg slik at de viste et signal på radaren. Systemet ble kalt IFF (Identification Friend or Foe) [History of RFID].

.

Bruken av RFID er i dag stor, og mulighetene enda større, men RFID teknologien setter flere begrensninger på områder. Det er på disse områdene NFC og en eventuell SmartMX chip integrert i SIM-kortet har sitt potensial.
Et av områdene hvor NFC har gjort suksess er innen mobiltelefoner. Dette skyldes at flere verdenskjente mobiltelefonprodusenter har gått inn som medlem av NFC Forum og er med i utviklingen. Det er selskaper som Nokia, Motorola og Samsung.

I dag

I 2004 ble forgjengeren til NFC, nemlig Sony`s FeliCa, implementert i mobiltelefoner i Japan og Korea. Dette har blitt godt mottatt, og er i dag i bruk til flere formål. Under et år etter lanseringen i juni 2004 har det Japanske selskapet NTT DoCoMo solgt over 3.3 millioner FeliCa enheter og over 20.00 terminaler er stasjonert rundt i butikker, flyplasser, jernbanestasjoner, kinoer og teater [RFID evolves into Near Filed Communication (NFC) to create substantial new revenue opportunities].

FeliCa teknologien er i bruk på flyplassene i Japan, der reisende som har trådløs billett på mobiltelefonen kan ”touch and go”. De slipper lange køer som innsjekking, og dermed går ombordstigningen raskere [JAL`s expands ‘Touch & Go’ boarding throughout Japan].

Det amerikanske firmaet VIVOtech har sammen med Philips utviklet et betalingssystem hvor NFC telefoner kan brukes som betalingsmiddel. Systemet fungerer ved at VIVOtech leseren er koblet opp til butikkens kassaapparat, hvilket gir mulighet for trådløs betaling gjennom selvbetjening. Ved en transaksjon mottar leseren en unik ID samt en sikkerhetskode. Signalet kan komme fra et vink med en NFC-mobiltelefon, et NFC-betalingskort i stil med SpeedPass, PayPass eller ExpressPay [Vivotech].

I morgen

“Near Field Communication - the new handshake” [6]

[6] http://www.unmediated.org/archives/2004/10/near_field_comm.php

Tiden da det gode, gamle håndtrykket var måten å hilse på folk er forbi, nå er NFC den nye måten å presentere seg på. Ved hjelp av mobiltelefonen overfører du data, med kun et tastetrykk og personen kan lese hvem du er.
Dette er selvsagt satt på spissen, men ingen umulighet om vi skal tro forventingene til selskapene bak NFC. Innen år 2009 antas det at 50 % av alle mobiltelefoner som selges vil være utstyrt med NFC, basert på en rapport fra analysebyrået AIB [Your phone is your swipe card].

Mange pilotprosjekter er utført i samarbeid med selskaper som er medlem av NFC Forum. De som er nevnt her er bare noen av dem, og flere av pilotprosjektene er allerede tatt i bruk flere steder i Asia og USA. For Sony og Philips som allerede er på markede med sine respektive teknologier Felica og MiFare vil samarbeide om NFC-teknologien kanskje være starten på en ny suksess, som Sony og Philips hadde på 1980 tallet med Compact Disc Digital Audio teknologien. Potensialet til hva NFC teknologien kan gi oss er altså stort, trolig er det kun et spørsmål om tid før det vil komme i stor skala her i Norge og resten av Europa.

5. Metode og resultater

For å komme frem til en løsning og forstå problemstillingen har vi i begynnelsen snakket mye med veilederne og har i løpet hele av prosessen hatt løpende kontakt, kunnet stille spørsmål og fått tilbakemeldinger på våre løsninger.

Artikler, empiriske undersøkelser og andre kilder er lest og brukt i rapporten for å kunne bruke andre sine meninger og undersøkelser der hvor det har vært relevant.

Valg av metode går ut på hvordan gå frem får å innhente kunnskap og hvordan metoden anvendes på problemet. Denne oppaven baserer seg på ”Proof of concept” da utgangspunktet var å bevise at distribusjon av nøkler ved hjelp av SMS og overføring av nøkkelen fra mobiltelefon til en RFID basert lås, var mulig. Resultatet har munnet ut i en fungerende prototyp.

Avsnittene i dette kapittelet som omhandler implementering av mobiltelefon og låsen er skrevet av Thomas Halvorsen, de er tatt med for et mer helhetlig bilde av resultatet.

Prototyp

Mange private hjem er påvirket av den digitale konvergensen, gamle teknologier skiftes ut og nye digitale løsninger tar over. Alle disse nye teknologiene genererer data av ulik format, og det trengs ofte et sted hvor disse kan lagres. Med nye teknologier mener jeg her, digital kamera, overvåkningskamera, mp3-spillere og så videre. Mye av slik data lagres i distribuerte systemer. Brukere ønsker å aksessene disse dataen fra forskjellig typer digitale enheter, uavhengig hvor brukeren befinner seg; hjemme, jobb osv. Til sammenlikning er ikke systemet vi har utviklet så fjernt fra de teknologiene som allerede finnes. Ved å dele opp vårt system ser man i dag flere eksempler på bruken av for eksempel RFID-teknologien. MasterCard har utviklet er betalingssystem, PayPass [PayPass], som bruker RFID-teknologien. Dette systemet gjør det mulig å betale med en smartkort løsning uten og dra kortet slik at magnetstripen leses, da data overføres trådløst. På samme måte som nøkkelen blir digitalisert og overført trådløst i vår prototyp.

SMS på sin side er en enkel tjeneste som de fleste kjenner til, den gir oss muligheten til å sende tekstmeldinger på maksimalt 160 tegn mellom to mobiltelefoner. Et godt argument for å satse på SMS som kommunikasjonsmiddel i dette systemet er at det i 2005 var 103 mobilabonnenter per 100 innbyggere i Norge [ITU 2005].

Aksess til systemet for distribusjon av nøkler kan skje uavhengig av hvor huseier/administrator befinner seg. Eneste kriteriet er mobildekning for sender og mottaker.

5.2 Software bruk og utvikling

Server delen av systemet består av flere komponenter med Microsoft 2003 Server i bunnen. Det er i hovedsak to applikasjoner som kjører her. Den første er en frittstående Java applikasjon som lytter til SMS, den andre er en servlet som kjøres av Tomcat 4.1. I tillegg er det satt opp en database som håndterer lagring av data.

Jeg vil forklare hvordan de forskjellige komponentene fungerer i de neste avsnittene.

5.3 Program for Advanced Telecom Services

Forkortelser og forklaringer

CPA	Content Provider Access – Gateway for SMS mellom tjenesteleverandør og bruker
CP	Content Provider – Tjenesteleverandør av SMS applikasjonen
JMS	Java Messaging Service – Java API som håndterer kommunikasjonen mellom CPA plattformen og CP
Q	Queue – Kø av SMS
MQ	Message Queue – Sytem for kø håndtering av SMS
SMSC	Short Message Service Centre – Server for prosessering av SMS (her PATS)

Tabell 3 - Ordforklaringer

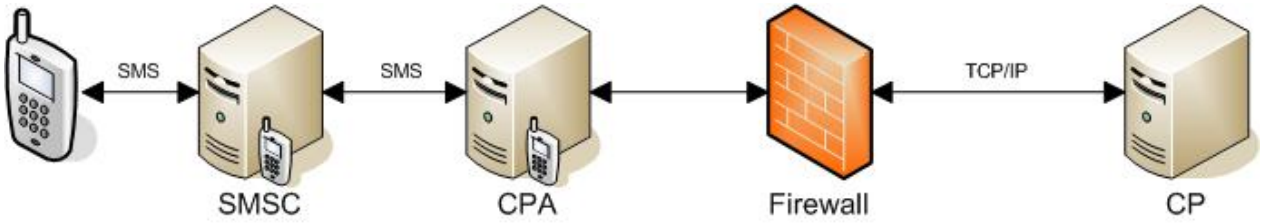
For håndtering av SMS i systemet har vi benyttet Telenor PATS innovasjons laboratorium. PATS er et samarbeid mellom Norges tekniske-naturvitenskaplige universitet (NTNU), industri- og telekommunikasjonsbedrifter [PATS]. De tilbyr i dag en rekke tjenester for utviklere av telekommunikasjon.
Vi har benyttet Telenor Mobil sin CPA protokoll som hjelper oss med håndteringen av SMS, dette grensesnittet støtter også andre funksjoner som posisjonering, men jeg vil ikke gå inn på disse funksjonene her. CPA er en gateway mellom to parter. Den ene er innholdsleverandør av en tjeneste, og den andre parten er mobiltelefonbrukeren. For systemet vårt vil det si at SMS-håndtereren kan sees på som en innholdsleverandør, videre kan brukeren av mobiltelefonen med NFC-applikasjonen sees på som *brukeren*.

Etter hvert som SMS tjenester har blitt mer etterspurt, har etter hver blitt en tredjepart som utvikler de ulike tjenestene, mens kontrollen av trafikken styres av teleoperatørene. Dette er tjenester som for eksempel ringetoner, bilder, spill, nyheter, trafikkinformasjon, horoskop, vitser osv, som tilbys mobilkunder gjennom SMSC (for eksempel 1999 eller 2034). En SMS blir prosessert av SMSC til en teleoperatør og så sendt videre til CP via CPA plattformen.
Når det kommer til betaling av slike tjenester er det innholdsleverandørene som setter prisen på sine produkter, abonnenten blir belastet for tjenestene på sitt abonnement, teleoperatørene på sin side trekker da en avgift fra prisen på tjenesten.

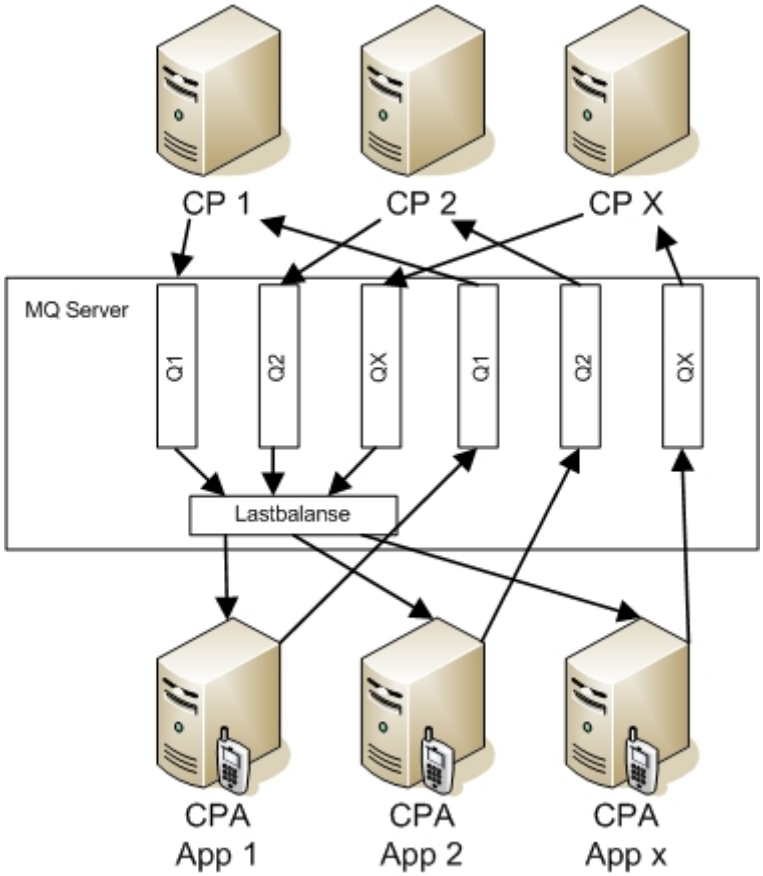
mPay kan sees på som både innholdsleverandør og en betalings løsning som tilbyr tjenester for brukere av mobiltelefon. Dette systemet gir brukere tilgang til å betale for parkering via mobiltelefonen [mPay]. Tanken bak konseptet er at brukere av parkeringsplasser slipper å ha småpenger tilgjengelig for parkometeret, men heller kan betale ved å sende SMS.

Distribusjon av mobiltjenester er ofte basert på SMS og WAP, hvor SMS kan sees på som en ordre og WAP kan sees på som ”applikasjonsprotokollen”. Applikasjonsserveren er da ofte en virtuell maskin som tilgjengeliggjør sine applikasjoner på internett via XML grensesnittet. For

aksess til applikasjonene, sendes en SMS som går via en SMS gateway som for eksempel Push Access Protocol (PAP). Et eksempel på dette: En bruker sender en SMS til 1111 med et kodeord for et gitt spill. CPA plattformen gjenkjenner dette nummeret og vet da hvilken CP som skal ha forespørselen, det sendes videre en spørring mot en URL til det gitte spillet.
Applikasjonsserveren får så denne URL og genererer en PAP. En SMS sendes ut til brukeren med URL`en og spillet kan lastes ned via WAP.



Figur 6 - Arkitektur



Figur 7 - Oversikt over CPA, sett fra CP

Et alternativ til PATS er Kannel [Kannel]. Denne fungerer på samme måte som PATS, ved at det er en gateway mellom SMS applikasjon og inn- og utgående SMS'er. I starten av utviklingen benyttet vi Kannel applikasjon ved Telenor. Forskjellen er at Kannel må ha tilgang til et SIM-kort, altså et åttesifret nummer, mens PATS på sin side har et firesifret nummer pluss et kodeord. PATS alternativet er også nærmere en reell løsning.

5.4 Subscriber Identity Module håndtering

Applikasjonen som håndterer SMS i vårt system kommuniserer med en tredjepart som er vist i figur 5.

Når en SMS sendes fra Telenor Mobil sitt nett til en CPA server, blir den videre lagt i en kø. Vår applikasjon som håndterer SMS trenger ikke hente ut meldinger (PULL) fra denne køen,

applikasjonen lytter på en bestemt kø, i vårt tilfelle er det alle meldinger som starter med Rfid. Når en SMS med kode ord rfid blir lagt i køen opprettes en hendelse og SMS`en blir gjort tilgjengelig for CP. MQ serveren håndterer kø systemet for sendte og mottatt SMS, denne er kompatibel med JMS apiet til Java. SMS`er som kommer inn sendes til Telenor Mobil sin CPA via SMSC (her PATS) som tar i mot meldinger på nummer 2034.

Kommunikasjonen mellom CPA og CP foregår over en TCP/IP tilkobling, CP kobles opp mot en IP adresse hos Telenor og autentifiseringen skjer ved hjelp av brukernavn og passord. Tilkoblingen vil vare til enten klienten eller serveren lukker den. For tilgang til PATS er det satt opp en Trustix Linux server ved Unik, den fungerer da som en gataway mellom Unik og PATS.

Når en SMS sendes ut fra CP kjøres et kall på en metode gitt av MQ klient API'et (se figur 8), den blir så lagt i en kø før den sendes ut via Telenor Mobil sin CPA.

```
public boolean sendSMS(String to, String txt)
        {
                try {
                        javax.jms.Message message = cpa.createMessage();
                        message.setStringProperty("msn",to);
                        message.setStringProperty("pricegroup","CPA000");
                        message.setStringProperty("sno","2034");
                        message.setStringProperty("messageid", Integer.toString(messageid++));
                        .
                        .
                        .
                cpa.sendMessage(message);
```

Figur 8 - Java kode utdrag

5.5 Låsen

NFC-leser

SCR331-DI er en kombinert smartkort- og kontaktløskortleser med USB grensesnitt. Med drivere kan vi bruke denne koblet til PC'en. Ved hjelp av et API kalt JPC/SC (Java PC / SmartCard) for Java kunne vi programmere en applikasjon som simulerte en dør tilknyttet en NFC-lås. JPC/SC kan kommunisere med PC/SC kompatible enheter. Denne benytter også APDU kommandoer for å kommunisere med smartkort.

5.6 Mobiltelefonen

Mobilen er en vanlig 3220 levert av Nokia. Det som imidlertid er spesielt, er dekselet. Dekslet har innebygd NFC modem (RFID/NFC modem med lese- og skrivefunksjonalitet) og smartkortkompatibel chip kalt SmartMx. Dette dekslet kommuniserer med telefonen ved hjelp av datakontakter.

5.7 Subscriber Identity Module applikasjon

Subscriber Identity Module applikasjonen kjører på pats1.unik.no serveren og kan sees på som CP (se figur 6). Det er denne applikasjonen som håndterer inn utgående SMS'er i systemet. Applikasjonen håndterer også utgående SMS'er, men dette kan også skje fra servleten. Når en

SMS sendes fra administrator til 2034 blir den langt i en kø hos CPA, så opprettes en hendelse i applikasjonen. Først sjekkes det at avsender har rettigheter, hvis ja, sjekkes innholdet i forhold til designspesifikasjon (se vedlegg 1). Deretter lagres den nye adgangen i databasen, og tidligere adganger som er gitt blir slettet dersom de er gått ut på dato. Så sendes det en informasjonsmelding til gjest, som sier hvor og når det er gitt tilgang samt hvilken dør. Det sendes også ut en adgangs SMS som nå må godkjennes av gjest, men denne vil bli transparent for brukeren når kommunikasjonen mellom NFC modemet og smartMX chipen blir standardisert. Adgangs SMS`en blir omgjort til heksadesimal kode, og sendt til port 45454 på mobiltelefonen, slik at den blir transparent for mottaker.
Applikasjonen er utviklet i Java (1.4.2SDK) for enkelt å kunne kommunisere JMS apiet til PATS.

5.8 Servlet

For utvikling av et webbasert brukergrensesnitt har jeg benyttet servlets fordi en slik Java applikasjon håndterer kommunikasjon og tekstformatering. Servlets tillater utvikling av dynamiske webapplikasjoner bestående av applikasjonslogikk, nettopp fordi den kan kommunisere med andre entiteter som databaser. Servleten er utviklet i Java 1.4.2 SDK, samme som den frittstående SMS håndtereren.
Servleten oppretter en oppkobling mot databasen, og leser/skriver informasjon som den blir spurt om fra klienten. Applikasjonen oppretter også en oppkobling til PATS når det sendes ut SMS. Klienten sender forespørsler ved bruk av POST-metoden, slik at alle parametere som sendes ikke vises i klartekst.
HTML kodingen i servletene er også XHTML 1.0[7] godkjente, for en ryddigere kode, og det gjør det lettere for mindre prosessorkraftige enheter å lese, som for eksempel PDA og mobiltelefon. Servleten tilbyr den samme funksjonaliteten som den SMS baserte applikasjonen. Brukeren kan her logge seg inn og legge til nye brukere samt gi ny/oppdatere adgang. På samme måte som den SMS baserte applikasjonen sendes det ut en SMS til den gitte brukeren som gir adgang.

[7] http://www.w3schools.com

5.9 Database

Relasjonsdatabasen er ofte en essensiell komponent i en moderne applikasjon. SQL er en standardisert plattform utviklet for lagring og utveksling av data mellom applikasjoner. Systemet bruker en MySQL 5.0 server for lagring av data, fordi det er støttet av blant annet innen Java og webutvikling.

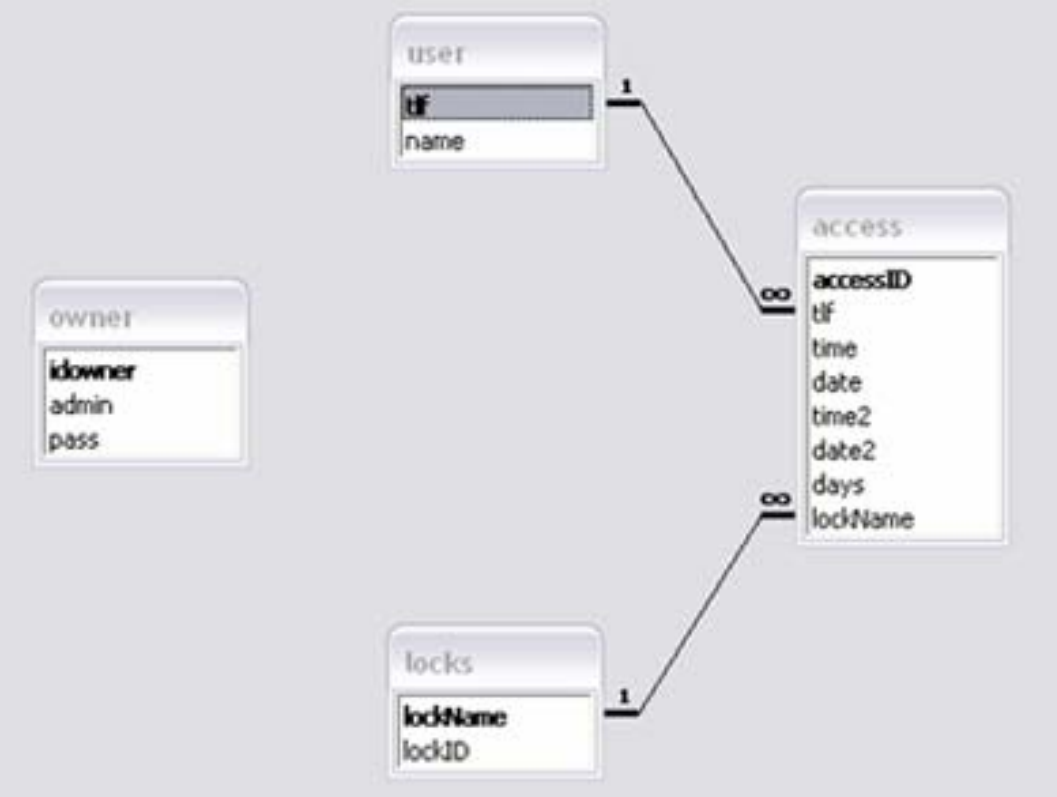
Jeg har tidligere omtalt at vi har delt opp systemet i to sub systemer, hvor vi ser på hvordan systemet fungerer med og uten server. Når det kommer til bruk av relasjonsdatabasen, blir denne benyttet i begge tilfellene. Applikasjonen som håndterer SMS benytter den samme databasen som servleten.

Følgende tabeller har blitt brukt:

- user (tlf, name)
- owner (idowner, admin, pass)
- locks (lockName, lockID)
- Access (accessID, tlf, time, date, time2, date2, days, lockName)

ER- diagram

ER- diagrammet viser relasjon mellom de forskjellige tabellene.



Figur 9 - ER diagram

5.10 Systemet

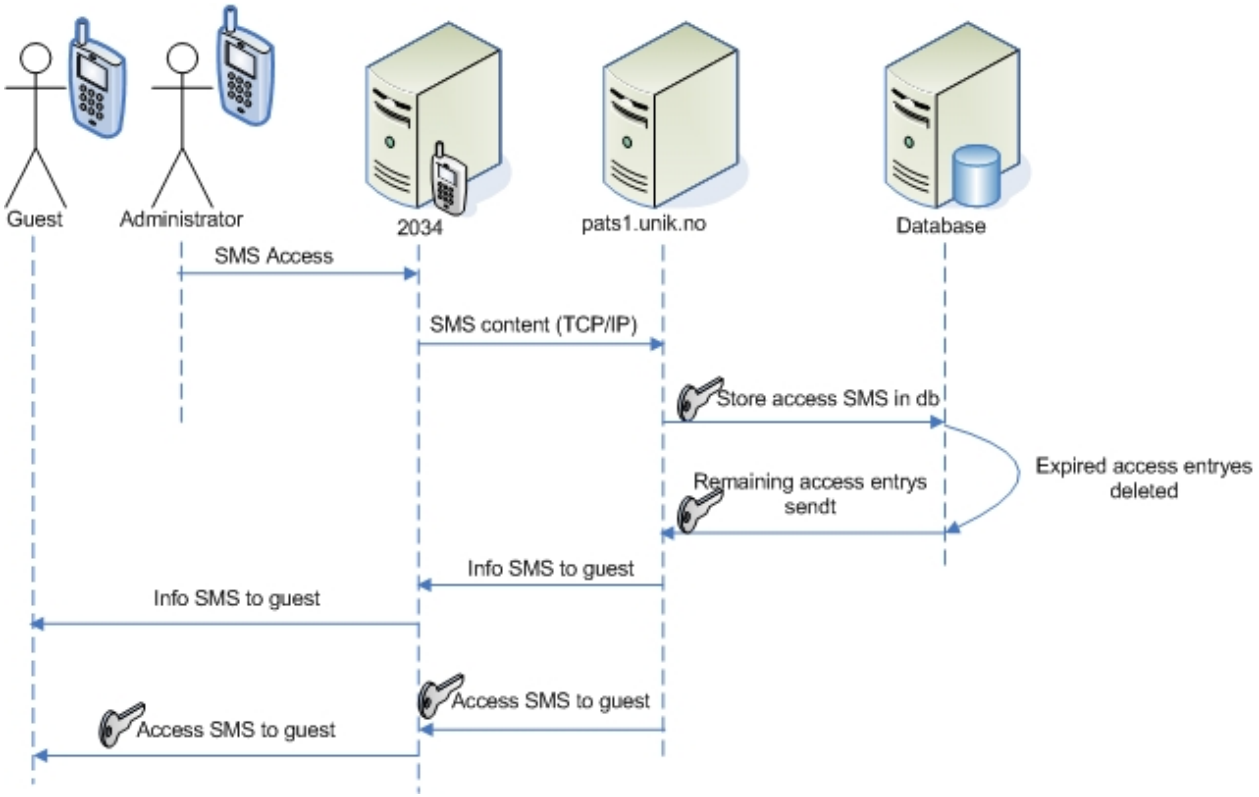
Avsnittene over beskriver de enkelte komponentene av systemet vi har utviklet. Utgangspunket var to mulige løsninger med tanke på ulike bruksområder.

Den første løsningen består av en SMS håndterer applikasjon, database, NFC lås og en mobiltelefon med NFC teknologi. Det betyr at låsen er frittstående og at adgang sjekkes mot en klokke i låsen, som igjen betyr at låsen er avhengig av strøm.

Den andre løsningen har i tillegg mulighet til å håndtere flere låser. Hvilket betyr at låsene må være koblet opp mot serveren slik at informasjon enten kan lastes opp til låsene, eller at det

sjekkes direkte mot server i sanntid. Opplasting av informasjon til låsene i systemer, krever intelligente låser, det vil si at data kan lagres og oppdateres.
En slik løsning er mer kompleks men gir også mer kontroll, det er enklere å styre tilgang til alle dører og hvem som har adgang.

Etter å ha vært i kontakt med Bewator per telefon fikk jeg opplyst at det alltid er backup på elektroniske låser enten i form av UPS eller batteri. Hvor mange batterier som trengs er avhengig av antall låser og hvor lang tid man ønsker backup strøm.



Figur 10 - Sekvensdiagram for aksess distribusjon

Scenario

a) Hansen jobber overtid, han får besøk hjemme av Olsen som ikke har nøkkel.
b) Hansen sitter på kontoret så han har PC`n foran seg, han åpner en nettleser og logger seg inn på webapplikasjonen. Hansen legger til Olsen som en ny bruker.

c) Deretter legger Hansen inn data som gir Olsen tilgang til leiligheten

d) To SMS`er sendes ut til Olsen, en som sier at han får tilgang til leiligheten i et gitt tidsrom, den andre installeres automatisk i smartkortet på telefonen.

e) Olsen kan nå gå inn i leiligheten til Hansen.

Et punkt i scenarioet vil være at Hansen får en SMS i det Olsen går inn i leiligheten.

Scenarioet beskriver hvordan den første løsningen av systemet kan fungere.

Område	Løsning
Privat bolig	1 / 2
Hytte	1
Bedrift/Organisasjon	2
Bil	1
Betaling (VISA o.l.)	2
Betaling (ladekort)	1

Tabell 4 - Bruksområder

Figur 11 - Simulering av NFC-lås

6. Drøfting

I dette kapittelet drøfter jeg de to utgavene av systemet satt i sammenheng med scenarioer i både det private og ulike typer organisasjoner. Jeg vil beskrive potensialet ved en eventuell innføring samt utfordringer som gjenstår før det kan kommersialiseres.
Det er ofte at ny teknologi og digitalisering fører til skepsis, særlig på grunn av sikkerhet, og det at det fysiske og håndfaste ikke lenger er til stede. Men med NFC teknologien implementert, for eksempel i mobiltelefonen mener jeg at det er med på å bringe den fysiske og digitale verden nærmere hverandre fordi da må brukeren holde mobiltelefonen mot for eksempel en betalingsterminal, for at overføring av data skal kunne skje. Jeg tror dette er en viktig faktor for at NFC teknologien skal bli akseptert, fordi det gir brukeren en følelse av kontroll.

6.1 Mobilitets konseptet

Videre kan mobilitetsbegrepet i følge artikkelen ”Expanding the ’Mobility’ Concept” skrevet av Kakihara m. fl. i 2001. deles opp i tre dimensjoner; geografisk plassering, tidsperspektiv og kontekst. Artikkelen tar for seg samhandlingen mellom mennesker og teknologi. For lettere å kunne analysere alle sider ved samhandlingen deler de bruken av teknologi i de tre nevnte dimensjonene.

Jeg vil også drøfte muligheter og utfordringer med hensyn på oss som individer, bedrifter og organisasjoner i forhold til en implementering av systemet.

Geografisk plassering

Dagens bruk av lås og nøkkel er noe vi kjenner godt. For private husstander er det vanlig med den fysiske nøkkelen, mens større bedrifter og organisasjoner i større grad benytter magnetstripekort. Felles for bruksmåten er at hvert enkelt individ har sin egen nøkkel. For private husstander må et besøk planlegges, slik at det er noen hjemme eller at nøkkelen overrekkes til den eller de som kommer på besøk. I større bedrifter og organisasjoner må besøk ofte meldes fra til personen som sitter i ekspedisjonsdisken, slik at når personen kommer blir det sjekket opp mot en besøksliste. Systemet vi har utviklet vil kunne forenkle disse prosessene. I en privat husstand

kan en SMS gi tilgang til besøkende uavhengig hvor huseier befinner seg. Bedrifter og organisasjoner kan enkelt sjekke om personen har mottatt en invitasjon ved at besøkende holder mobiltelefonen mot NFC leseren. Nøkler kan lett distribueres uavhengig hvor sender og mottaker befinner seg.
Et annet viktig punkt er at NFC teknologien tillater en bruker å kjøpe ulike tjenester og varer der hvor brukeren befinner seg. Et eksempel på dette er kjøp av kinobilletter, du ser en reklameplakat for en kinofilm du ønsker og se, ved å holde mobiltelefonen mot reklameplakaten vil man enkelt kunne bestille billetter. Dette vil gradvis være med på å bringe den digitale og fysiske verden nærmere hverandre, fordi tjenester er tilgjenglig der hvor brukeren er og fordi brukeren må holde mobiltelefonen mot leseren.

Tidsperspektivet

Et av punktene som blir nevnt i artikkelen er dette med digital konvergens. Det at eldre teknologi skiftes ut med ny teknologi som løser en oppgave raskere. Sett i sammenheng med vårt system vil det ofte være en tidsbesvarelse å sende SMS i forhold til overlevering av nøkler og besøkslister.
Et annet viktig poeng her er hvor lang tid det vil ta før både tjenesteleverandører og brukere vil ta i bruk denne teknologien. I første omgang ligger mye av ansvaret hos tjenesteleverandørene, som igjen må overbevise sine kunder.

Kontekst

Bruken av teknologi er i stor grad avhengig av konteksten som teknologien blir brukt[Brown m.fl., 1994]. For bruken av mobiltelefon vil det si at brukeren velger forskjellige applikasjoner avhengig av kontekst. Å skrive et kalendernotat i et møte, svare på en oppringning når man sitter i trafikken eller skrive SMS på en kald vinterdag er eksempler på at det vil være forskjellige faktorer som beror på sammenhengen mellom miljø og brukers aktiviteter og mål.
Dette er en viktig faktor det bør sees mer på, særlig når det gjelder personen som gir adgang. Vårt system er basert på SMS som nøkkelen til adgang, men i en utvidelse kan det være aktuelt å se på alternativer i forhold til personen som gir adgang og hvilken kontekst personen befinner seg. På en annen side er SMS blitt en ”killer applikasjon” som de fleste kan bruke, og vi har komprimert teksten som skal skrives så mye som mulig, men allikevel ikke mer enn at den er forståelig.

For mottaker gjelder ikke de samme kriteriene, fordi personen som mottar en adgangs SMS, i de fleste tilfellene, har avtalt med huseier/bedriften på forhånd. I tillegg er den første SMS`en en informasjons melding som sier hvor og når personen har adgang. SMS nummer to lagres på mobiltelefonen uten at bruker trenger å gjøre noe.

6.2 Implementering i private hjem

Dersom et slikt system skal implementeres i en privat leilighet er det per i dag to mulige løsninger vi har sett på som nevnt i kapittel 5. Den enkleste løsningen innebærer at det kun installeres en NFC kompatibel lås på inngangsdøren. I tillegg til å kunne gi gjester tilgang, bør det kunne opprettes profiler, slik at huseier/administrator har tilgang hele tiden, så administrator slipper å sende SMS til seg selv for å få tilgang. Det kan også være aktuelt å opprette ulike gjesteprofiler, for venner, familie osv. Disse profilene kan da ha forhåndsbestemte adgangstider, slik at administrator kan sende SMS med et kodeord eller tall som er forhåndsdefinert i låsen. Eks. *"Rfid 95232208 A1"* sendes til 2034, hvor A1 er definert som adgang hver lørdag.
Det bør være CP (Content Provider) sitt ansvar i samarbeid med huseier som definerer de ulike profilene. På samme måte som en del husstander i dag er tilknyttet en alarmsentral betaler de for de ulike tjenester som tilbys.
Folk flest som tar i bruk ny teknologi vil at det skal virke, uten alt for mye konfigurasjon, for mange kan det å stille inn kanaler på TV være nok. I følge artikkelen "Evaluating Wireless Technologies in Mobile Payments – A Costumer Centric Approach" skrevet av Agnieszka Zmijewska nevner hun spesielt seks kriterier som er viktig i forhold til innføringen av ny teknologi; lett å bruke, nytteverdi, pålitelighet, mobilt, kostnad og personlighetspreg [Zmijewska, 2005]. Derfor tror jeg at den beste løsningen er å ha en tredjepart som har ansvaret for serversiden, fordi det ikke krever noen konfigurasjon. I tillegg må tredjeparten garantere operative servere til en hver tid. Huseier trenger kun å vite strukturen på SMS'er som gir adgang. Det vil også være mulig å benytte et webgrensesnitt til å sende ut adgangs SMS'er selv om låsen ikke er koblet opp mot serveren. Ved å la en tredjepart hoste websidene medfølger det ikke noe konfigurasjon her heller, kun et brukernavn og passord for å logge seg inn. Denne innloggingen kan også etter hvert erstattes av NFC-teknologien.

Den andre løsningen hvor serveren er koblet til låsen(e) gir et mer komplett system, og ikke minst gir det flere muligheter. Denne løsningen krever tilgang til databasen, og dersom det er en tredjepart som tilbyr dette systemet vil det bety at det også kreves internett tilgang. Selv om mye av dataen kan lagres lokalt på selve låsen vil de trenge oppdateringer fra serveren.

Dersom det ikke er ønskelig å gi barna mobiltelefon kan applikasjonen installeres på et smartkort, dersom denne nøkkelen kommer på avveie kan ID`en slettes og det kan enkelt opprettes en ny. Nedenfor følger et eksempel scenario på hvordan systemet kan fungere i et privat hjem.

Scenario

a) Ola skal ha besøk av elektriker Kari, han sender en SMS til sin tjenesteleverandør. *"L1 95232208 1000 050506 1200 050506"* (se Vedlegg 1 for forklaring)
b) Tjenesteleverandøren kjenner Ola sitt telefonnummer, det genereres to SMS som sendes til Kari, den første er en informasjons SMS, den andre er en installasjons SMS som installeres automatisk på telefonen til Kari.
c) Kari ankommer boligen til Ola og går inn hovedinngangen ved hjelp av nøkkelen som ligger på NFC telefonen hennes.

For visuell forklaring, se figur 10.

Et annet bruksted kan være hytte, men det er da avhengig av strøm til låsen, noe som ikke alltid er vanlig for alle hytter. Derfor mener jeg at et slik sted er uegnet for et slikt system. Det vil kanskje også være et problem med mobildekning på slike steder. Skal man for eksempel leie ut sin hytte til ukjente vil det kanskje også være en fordel å møte leietaker ansikt til ansikt.

6.3 Implementering i offentlige bedrifter og organisasjoner

En implementering av et system slik som vi har utviklet, i bedrifter og organisasjoner vil i stor grad ikke ha noe å gjøre med innføring av nytt mobilt system. Det er for eksempel ikke et papirbasert spørreskjema som skal byttes ut med et digitalt medium som bærbar PC. Derimot er

det en digitalisering av nøkkelen og overføringen av denne mellom administrator og bruker og mellom bruker og lås. Det er dette som er noe av utfordringen ved innføringen. Samtidig er det ingen brukergrensesnitt for brukere å forholde seg til, derav ingen krav til evaluering, metrikk og felttesting av dette.

Nytten av et slikt system i bedrifter og organisasjoner er flere, særlig der hvor det er utskifting av nøkler og personer som skal ha tilgang eller ikke samt ulike tilgangsnivå. Eksempler på dette er hoteller og båter med lugarer. Nøkkelen overføres til mobiltelefonen når gjesten står i resepsjonen og denne er kun gyldig i perioden det er betalt for. For hoteller kan det også lagres nøkkel til hovedinngangen. Dette vil også være tidsbesparende i forhold til å dele ut nøkler, særlig dersom det er mange gjester som kommer samtidig.

Jeg har tidligere nevnt muligheten til å forhåndsdefinere profiler for familie og venner, for en større bedrift eller organisasjon kan det på samme måte lagres adgangsnivåer. For eksempel vil ”A” bety adgang til alle dører, mens ”A1” betyr adgang til hovedinngang og kontoret samt i et gitt tidsintervall.
En av de store fordelene er altså at digitale nøkler kan sperres og tidstsyres, med en kortleser har man alltid kontroll over hvem som har adgang hvor.

Scenario

a) Hansen avtaler forretningsavtale med Olsen på Hansen sitt kontor. Hansen sender en SMS til 2034 *”L1L9 95232208 1100 010506 1200 010506”*
b) Tjenesteleverandøren genererer så to SMS`er, hvor første er en informasjons SMS som forteller Olsen når og hvor han har tilgang. SMS nummer to blir lagret i applikasjonen på Olsens mobiltelefon
c) Olsen kommer inn hovedinngangen ved å holde mobiltelefonen mot NFC leseren
d) Olsen ankommer så informasjonsdisken og får en forklaring på hvor kontoret til Hansen er

En annen løsning på punkt a) er at alle avtaler lagres i en database, og at utsending av SMS skjer automatisk for eksempel 24 timer før avtale. Dersom avtaler er gjort en stund i forveien il besøkende bli minnet på dette 24 timer før avtalt tid.
Alternativt til punkt d) er at det sendes en SMS til Hansen i det resepsjonisten ber Olsen holde mobiltelefonen mot en leser i resepsjonen. Da får Hansen beskjed om besøket og kan ta imot Olsen.

Det finnes også flere områder der jeg ser fordeler av et slikt system. Hjemmehjelptjenesten er et av disse, her finnes det ofte en universalnøkkel som passer flere dører og et tap av en slik nøkkel kan koste staten mye penger. Dette er også en tjeneste hvor det er masse nøkler i omløp, hjemmehjelpen kan miste, glemme å ta med seg nøkler hjem, ofte har de også med seg nøkler til flere leiligheter. Dersom disse nøklene hadde vært digitalisert er det, som også tidligere nevnt, lettere og ha kontroll på hvilken hjelpepleier som har ansvar for hvilke pasienter. Videre er det enkelt og sende en SMS til en hjelpepleier dersom en ekstra pasient skal besøkes.
For politi og brannvesen vil det også være fordeler ved innføringen av et slikt system. Dersom en patrulje trenger nøkkel til en offentlig bygning kan den enkelt distribueres ut til personene som kommer først til stedet.

Med tanke på kommersialisering av et slikt system er det, som nevnt, utfordringer som gjenstår, men når man ser hvor langt utviklingen er kommet med tanke på smartkort som betalingsalternativ, er ikke skrittet så langt for å få det over på en mobiltelefon med NFC teknologi. Neste skritt på veien er å få overføringen av data til å skje trådløst ved hjelp av NFC protokollen.

6.4 Sikkerhet

Ny teknologi kommer gjerne før det er innført noen lov som setter begrensninger for bruken. RFID og NFC er to slike teknologier hvor det i dag settes flere spørsmål rundt personvern.

RFID og personvern

"RFID tags: Big Brother in small packages" – Declan McCullagh[8]

Anvendelsesområdene til RFID er som nevnt mange, og noen av disse har åpnet for at personvernet kan svekkes. Store selskaper som Gillette, Benneton og Swatch benytter RFID brikker i sine produkter. Mange mener dette kan true personvernet fordi RFID brikken kan brukes til overvåkning. Selv om det i denne sammenhengen ikke er snakk om RFID brikker med personlig informasjon, vil nok mange kunne føle seg overvåket fordi mange av produktene de kjøper inneholder en RFID brikke. Slik kan man altså tenke seg *"Big Brother in small packages"*.

RFID-bruken har i den siste tiden eksplodert, ikke bare på nyttige områder, men også på områder hvor det settes spørsmål omkring personvern. Bruksområdene nevnt i avsnitt 2.3 vil være nyttige områder hvor personvernloven ikke brytes. Men når forbrukere går rundt med produkter som inneholder RFID brikker uten å vite om det, vil det kunne være grunn til bekymring. Forbrukerne vil da ikke vite hvem som leser opplysningene i brikken eller når dette skjer. Folk flest er opptatt av å verne seg mot misbruk av personlig informasjon og kategorisering. Dersom informasjonen om hvordan vi som forbrukere kan verne oss mot misbruk ikke er gjort lett tilgjengelig, vil folk generelt virke aksepterende og likeglade. Det vil være fordi de ikke kjenner til hvilke konsekvenser et eventuelt misbruk kan føre til.

Flere produkter er i dag på markedet; som det nye passet, adgangskort og pasientbrikker som inneholder personlig informasjon som kan hentes opp av en RFID leser. Det er disse brikkene med personlig informasjon det bør settes krav til i forhold til personvernet.

NFC og personvern

Avsnitt 4.1 og 4.2 tar for seg mulige løsninger på hvordan personlig informasjon i en smartMX chip på mobiltelefonen kan krypteres og sperres. Sikkerheten er viktig her nettopp fordi mobiltelefonen kan inneholde virtuelle penger, nøkler og annen personlig informasjon.

[8] http://news.com.com/RFID+tags+Big+Brother+in+small+packages/2010-1069_3-980325.html?tag=st.rn

Spørsmålet omkring personvern kommer inn når de ulike tjenesteleverandørene installerer applikasjoner og oppdateringer. Det gir selskapene mulighet til å logge informasjon om de ulike brukerne, hvor en person befinner seg, hvem personen ringer og hva personen bruker penger på og hvor.
Dersom man gir fra seg sitt bankkort for betaling kan kortets informasjon noteres før det gis tilbake til eieren. Disse opplysningene kan misbrukes uten at korteieren kan kontrollere det. Ved å bruke en NFC enhet til å betale slipper du som bruker å gi fra deg bankkort og signatur. Brukeren behøver kun å holde enheten mot betalingsterminalen, og godkjenne beløpet med et enkelt tastetrykk.

Samtidig må det også nevnes at selskapene som samarbeider om NFC teknologien er relativt store i verdens sammenheng. Nokia, Motorola og Sony står for 60 % av alle mobiltelefoner som selges i dag[RFID evolves into Near Filed Communication (NFC) to create substantial new revenue opportunities], i tillegg står Visa og MasterCard for en stor del av all betaling som skjer med kort. Når disse da går sammen for å utvikle en betalingsløsning med mobiltelefon vil det høyst sannsynlig være en gjennomført og sikker løsning.

6.5 Styrke og svakheter

Utvikling av ny software bringer ofte med seg utfordringer, dette gjelder selvsagt også for dette prosjektet. Derfor vil jeg drøfte noen av de utfordringene knyttet til systemet vi har utviklet og til NFC teknologien.

Systemet
Når det kommer til utvikling av prototyp er det flere modeller for utvikling man kan følge, men siden det ikke får noen direkte innvirkning på en brukers arbeidsoppgaver er det vanskelig å evaluere. Mange bedrifter og offentlige organisasjoner benytter allerede magnetstripe kort som adgangsnøkkel. For brukerne er det snakk om et ekstra plastikkort i lommeboken. Forskjellen til systemet vi har utviklet er at nøkkelen lagres på SmartMX chipen i mobiltelefonen i stede for et nytt plastikkort og at data overføres trådløst.
Krav til sikkerhet er helt essensielt for et slikt system, men på grunn av hardware og prioritering i utviklingsperioden har vi ikke implementert det i prototypen. Slik det er i dag kjenner ikke

mobiltelefonen sitt eget telefonnummer (nr. til SIM-kort) med med SmartMX chip integrert i SIM-kortet vil det i fremtiden være mulig å sjekke mot telefonnummer. Mobiltelefonen vi har benyttet, en Nokia 3220 med NFC deksel, støtter ikke uthenting av IMSI (International Mobile Subscriber Identity) som kunne vært en mulighet. En annen mulighet er IMEI (International Mobile Equipment Identity) dette er et 15 sifferet nummer som er unikt for hver mobiltelefon i GSM nettet. Dette nummeret kan sperres fra telefonoperatøren, men sperrer kun mobiltelefonen. Resultatet må uansett være at utsending av nøkkel til feil telefonnummer ikke kan brukes av mottaker, enten ved bruk a PKI, en sjekk mot serveren eller begge.

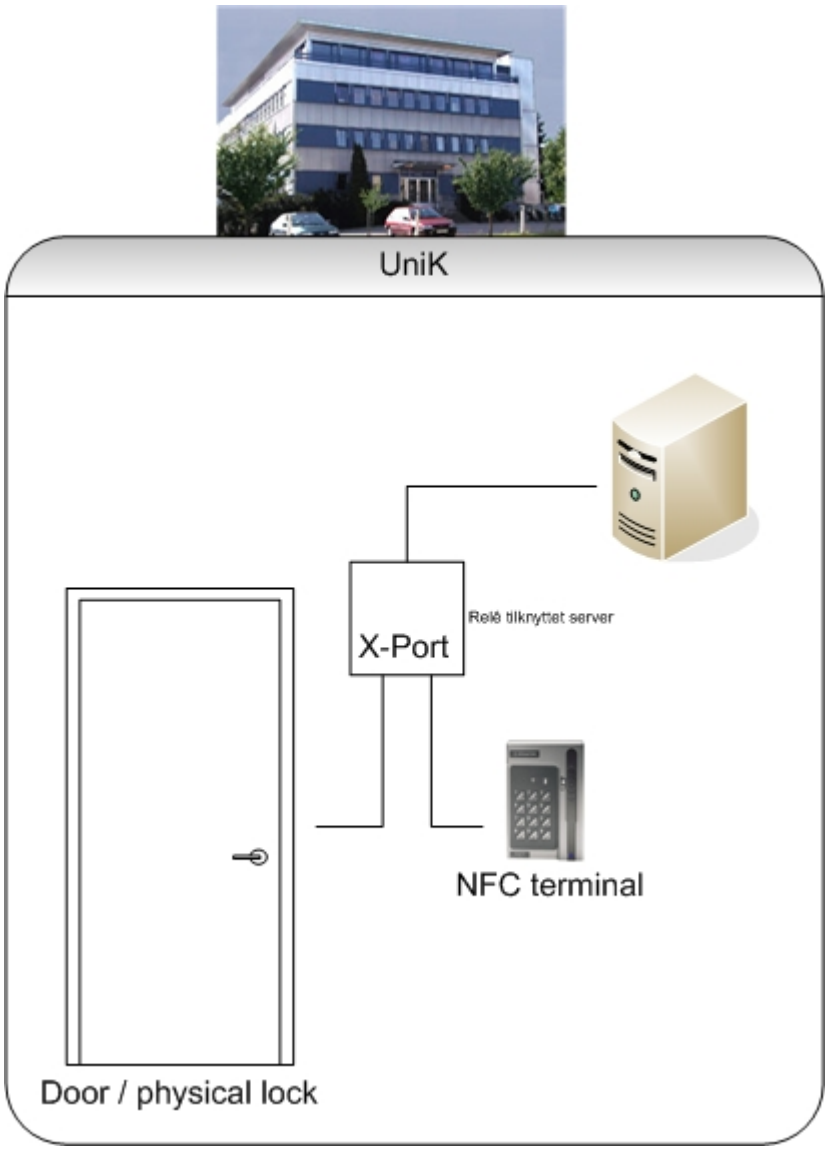
Databasen og låsen er ikke koblet sammen, hvilket betyr at det låsen sjekker mot er at den utsendte ”nøkkelen” er innenfor nåværende tidsrom. Databasen bør også utvides til å håndtere profiler for bruker/administrator, for å styre tilgangsnivå samt være oppkoblet mot låsen(e).

Mange oppfatter kanskje en fysisk nøkkel som mer formelt og håndfast enn en digital løsning. Et neste skritt på veien for videreutvikling av dette systemet kan derfor være en spørreundersøkelse som går på bruk og innføring av systemet i det private, bedrifter og organisasjoner.

Utrulling ved unik

Systemet vi har utviklet er som tidligere nevnt en prototyp, men det er allikevel fullt mulig å implementere og bruke det på en eller flere dører. Et av de neste skrittene for vårt system er nettopp at det skal implementeres på kontordøren til vår veileder, Josef Noll, ved Unik. I den forbindelse er det noen elementer som gjenstår før det er hundre prosent operativt. Under utviklingen har vi ikke konsentrert oss om hvordan den elektroniske låsen fungerer, eller hvordan NFC terminalen kommuniserer med denne. Men etter et møte med Kostas Papadopoulos[Epsys] og e-post utveksling med Rune Madsen[Teknobua] har vi kommet frem til følgende løsning på dørlåssystemet:

Låsen i døren må selvsagt være elektrisk slik at den kan reagere på strøm fra et relé. Løsningen vi har sett på er en X-Port[X-Port] som har TCP/IP grensesnitt koblet opp mot serveren, videre har den tre diskrete inn-/utganger som kobles til dørlåsen og en serieport som kobles til NFC leseren (se figur 12). X-Port er et frittstående system med eget operativsystem.



Figur 12 - Mulig løsning ved Unik

.

7. Konklusjon

Denne oppgaven har sett på muligheter som ligger i NFC teknologien, spesielt et bruksområde som går på distribusjon av nøkler til fysiske dører. Utgangspunktet for et slikt system er muligheten for å bruke mobiltelefon som autentifikasjon i den virtuelle verden ved bruk av sikkerhetsfunksjoner som PKI og NFC som overføringsprotokoll.
En del av oppgaven var å konstruere et system som gir mulighet til distribusjon av adgangsnøkler ved hjelp av tekstmeldinger for så å håndtere overføringen av nøkkelen mellom mobiltelefonen og RFID låsen. Prosessen har resultert i en fungerende prototyp som etter hvert skal implementeres ved Unik.

Første skritt på veien mot en løsning der mobiltelefon kan benyttes som ”Doorkeeper” er på god vei. Bankene har sin egen BankID som er bankenes egen elektroniske legitimasjon for sikker identifisering og signering. Her stiller banken som verifiseringsautoritet overfor andre institusjoner som for eksempel kommunen din. En mulig løsning for at mobiltelefonen kan benyttes som en autentisitet er at telefonoperatørene stiller som verifiseringsautoritet, eller et resultat av et samarbeid mellom disse. Uansett krever denne løsningen samarbeid mellom aktørene som ønsker at mobiltelefonen skal fungere som ”Doorkeeper”, fordi applikasjoner skal installeres og en standard for dette må etableres blant aktørene.

Neste skritt på veien mot suksess vil være aktørenes evne til å påvirke og overbevise brukere om at dette er en sikrere løsning enn den vi har i dag, og ikke minst at det er en løsning som gagner brukerne både når det gjelder håndterbarhet og brukervennlighet.

8. Referanser

[Bewator],
http://www.bewator.com/no/

[Brown m.fl., 1994] Brown, J. S. & P. Dugid,
"Borderline issues: Social and material aspects of design",
Human computer intaeraction, 1994.

[Epsys],
http://www.epsys.no/.

[GSM-world],
http://gsmworld.com.

[History of RFID],
http://www.rfidsurvival.com/HistoryofRFID.html.

[Hjelm, 2000] Hjelm, J.,
"Designing wireless information services",
John Wiley and Sons Ltd, 2000.

[ITU 2005] International Telecommunication Union,
http://www.itu.int/home/index.html.

[JAL`s expands 'Touch & Go' boarding throughout Japan],
http://www.jal.com/en/press/0000090/90.html.

[Kalle m. fl., 2001] Lyytinen K. & Youngin Y.
" The Next Wave of Nomadic Computing:
A Research Agenda for Information Systems",

Case Western Reserve University, 2002.

[Kannel],
http://www.kannel.org/.

[Mathiassen m. fl., 2000] Mathiassen, L. & Munk-Madsen, A. & Nielsen, P. A. & J. Stage,
"Object Oriented Analysis & Design",
Aalborg: Marko Publishers, 2000.

[Movation],
http://www.movation.no/.

[mPay],
http://www.mpay.no.

[Near Field Communication Forum],
http://www.nfc-forum.org.

[Near Field Communication White Paper],
http://www.ecma-international.org/activities/Communications/2004tg19-001.pdf.

[Noll m. fl., 2006] J. Noll & J.C. Lopez Calvet & K. Myksvoll.,
"Admittance Services through Mobile Phone Short Messages",
Unik, N-2027 Kjeller, Norway & Telenor R&D, N-1331 Fornebu, Norway.

[PATS],
http://www.pats.no/index.php/Main_Page.

[PayPass],
http://www.paypass.com.

[Philips],
http://www.semiconductors.philips.com/acrobat_download/other/identification/S2C_survey_10.pdf.

[Politi],
http://politi.no.

[Program for Advanced Telecom Services],
http://www.pats.no/index.php/Main_Page.

[RFID evolves into Near Filed Communication (NFC) to create substantial new revenue opportunities],
http://research.analysys.com/Articles/StandardArticle.asp?iLeftArticle=1941&FROM=arlRHS.

[Sporvien],
http://www.sporveien.no/templates/Page____1215.aspx.

[Teknobua],
http://www.teknobua.no/.

[Your phone is your swipe card],
http://irish.typepad.com/irisheyes/2004/07/your_phone_is_y.html.

[Vivotech],
http://www.vivotech.com/.

[X-Port],
http://www.lantronix.com.

[Zmijewska , 2005] Zmijewska, A.,
“Evaluating Wireless Technologies in Mobile Payments – A Customer Centric Approach”,
University of Technology, Sydney, 2005.

Vedlegg

Vedlegg 1 – Designspesifikasjon

Vedlegg 1: Design Specifications for RFID Doorkeeper

This document describes the design specifications for the RFID doorkeeper application, both for the applet installed on the mobile phone and the application sending SMS.

SMS design

SMS to 2034 "Rfid 90838066 120606 1200"
Will provide user 90838066 access to all locks on 12.06.2006 from 1155-1300 (1 hour access)
SMS to 2034 "Rfid 90838066 L1 L2 L8 120606 1200"
Will provide user 90838066 access to locks L1, L2 and L8 on 12.06.2006 from 1155-1300 (1 hour access)
"Rfid 90838066 L1 120606 1200 140606 1800"
Will provide user 90838066 access from 12.06.2006 from 12:00h to 14.06.2006 18:00h

- Specify the locks through an optional parameter: L1, L2, ..., (L0 for all locks)
- Hour from is set to -5 min (Example 11.00 is set to 10.55)

Add user

SMS to 2034 "rfid reg Thomas 92427178"
Also registers the mobile number in the "white list", but adds a name/reference for easier handling

Give access to a user

SMS to 2034 "rfid 92427178 param[]": you can use either name or number, as long as it's registered in the white list to give someone access. The parameters are described below.

Access from date/time

SMS to 2034 "rfid 92427178 L9 160106 1200"

if param.length == 3 && param[0] == “L9” &&
param[1].length == 6 : DDMMYY &&
param[2].length == 4 : TTMM;

Access from param[1] -5 min -> param[1] + 1 hour
SMS sent to guest’s mobile application: L916010611551601061300

This sends access to mobile phone 92427178, and gives access from 16.01.06 12:00 (-5min) to 16.01.06 13.00 1 hour is preset as a default, but may be changed. The "rfid" trigger word disappears from the message at PATS so param[1] is really 1601061200 in the above

example. L9 specifies which lock the user has access to. We only have one lock so L9 is the name of that.

Access from date/time to date/time

SMS to 2034 "rfid 92427178 L9 160506 1200 160606 1600"

```
if param.length == 5 && param[0].length == “L9”&&
param[1].length == 6 : DDMMYY &&
param[2].length == 4 : TTMM &&
param[3].length == 6 : DDMMYY &&
param[4].length == 4 : TTMM;

Access from param[2] -5 min -> param[4]
SMS sent to guest’s mobile application: L916050611551606061600
```

Access form given date and time to given date and time.

Access on a specific date

SMS to 2034 "rfid 92427178 L9 160506"

```
if param.length == 2 && param[0] == “L9” &&
param[1].length == 6 : DDMMYY;

Access from param[1] 00:00 -> param[1] 23:59
```

SMS sent to guest’s mobile application: L916050600001605062359

Access is given on a specific date.

General access

SMS to 2034 "rfid L9 92427178 AA"

```
if param.length == 3 &&
param[0].toUpper().equals("AA")

Access from NOW to NOW + 1 year
```

SMS sent to guest’s mobile application: L92404060002404070000

Access is given to a user for one year.

Interval access (based on weekdays)

SMS to 2034 "rfid 92427178 L9 12345 1200 1600"

> if param.length == 4 && param[0] == “L9” &&
> param[1].length<8 && param[1].length>0 &&
> param[2].length == 4 : TTTT && param[3] == 4 : TTTT
>
> Access Mon - Fri from 1200 to 1600 each day

SMS sent to guest’s mobile application: L9MTWH31080611553108071600

Access given to a user based on time interval and weekdays.

Mon	1,
Tues	2,
Wed	3,
Thur	4,
Fri	5,
Sat	6,
Sun	7,