UNIVERSITETET I OSLO
Institutt for informatikk

The Mobile Phone as Doorkeeper

Masteroppgave
(60 studiepoeng)

Thomas Halvorsen

1. august 2006

Forord

Jeg vil takke hovedveileder Josef Noll som har vært en inspirasjons- og motivasjonskilde av de sjeldne og en som virkelig tar seg tid til studentene selv om han har aldri så mange baller i lufta.
Veileder Kjell Myksvoll fortjener også takk. Han har vært en utrolig god hjelp ved alle tekniske spørsmål.
Haakon Eikenes fortjener til slutt en takk for lærerike samtaler, korreksjoner og godt samarbeid.

Oslo, juli 2006

Thomas Halvorsen

"The future is here.
It's just not widely distributed yet"
William Gibson

"There is no great technology leap involved, it's just that no-one has thought of using the near field before in these ways"
David Stocks

Sammendrag

Near Field Communication er en teknologi for kontaktløs overføring av data. I denne rapporten ser vi på teknologien, muligheter og sikkerhetsaspekter. For å vise potensialet ble en prototyp implementert. Funksjonaliteten består i å sende en elektronisk nøkkel via SMS til en mobiltelefon. Denne lagres i en smartkortkompatibel brikke og gir adgang til en fysisk dør ved NFC utveksling.
Andre funksjoner som kan benyttes i NFC-mobilen er billettering, betaling, identifikasjon og dataoverføring.

Innholdsfortegnelse

Figurliste

1 Introduksjon

I dette kapitlet kommer en innledning til oppgaven og problemstillingen. Jeg sier også litt om året som har gått med til oppgaven.

1.1 Innledning

Høsten 2005 begynte jeg i samarbeid med Haakon Eikenes på lang masteroppgave gitt av Universitet på Kjeller med Josef Noll som veileder.
Kjell Myksvoll, ansatt ved Telenor FoU, har fungert som ekstern veileder.
Lang masteroppgave tilsvarer 1 årsverk (60 studiepoeng) og tas vanligvis med 10, 20 og 30 studiepoeng over tre semestre, mens vi utførte det over to semestre med 30 poeng per semester.

Jeg og Haakon Eikenes har dekket to unike områder i en felles implementering og leverer individuelle rapporter.
Oppgaven var beregnet på 2 – 4 personer og handler om Near Field Communication (NFC) i forbindelse med å gi noen tilgang til hjemmet sitt ved hjelp av mobiltelefonen.
NFC er en relativt ny teknologi og det har tidvis vært vanskelig, spesielt i starten, å finne informasjon og gode artikler om temaet.
Vi utviklet en prototyp med splitter ny teknologi, dette krevde at Javakunnskapene måtte friskes opp og utvides, mange tilleggspakker måtte læres.
Det var tidvis lite eller ingen dokumentasjon på implementeringsproblemene.
Vi kastet oss rett og slett ut på dypt vann.

Oppgaven er praktisk orientert (implementeringsoppgave), dette gjenspeiles i rapporten. Rapportens største kapittel beskriver i detalj implementeringen. Denne blir dermed noe mindre teori-, forsknings- og drøftingsbasert og litt mer teknisk.

Rapporten er skrevet for fagpersoner og personer med teknisk innsikt i IT og telekommunikasjon, men forsøker å forklare de fleste begreper best mulig.

1.2 Problemstilling

Enkelt forklart gikk oppgaven ut på å implementere en prototyp hvor man sender SMS til noen som skal besøke deg. SMS'en installerer seg i mobiltelefonen til gjesten. Når gjesten ankommer må han autentisere seg for dørlåsen ved hjelp av NFC grensesnittet i låsen og telefonen.
Han som venter besøk har muligheten til å få en SMS hvor det står at gjesten er ankommet.

For å få til dette praktiske måtte en del legges til rette:

- Grunnlegge arkitektur med alle nødvendige komponenter, spesielt med hensyn på skaleringsspørsmål
- Hjemmetjener
- SMS sendingsfunksjonalitet
- SMS kommunikasjon med SIM-kortet
- Radio Frequency IDentitification (RFID)/NFC informasjonssikkerhet og informasjonsutveksling. Utveksle riktig informasjon avhenging av tjenestetilbyder og tjeneste. Eksempelvis kan det i tillegg til adgangskontroll være småbetaling hos Narvesen eller kollektivtransport av forskjellig natur:
  a) Månedsbillett
  b) Enkeltbillett
- Smartkort informasjonssikkerhet og informasjonslagring. Se punkt over for eksempler

I tillegg vil risikoer og sikkerheten i konseptet bli diskutert. Hvor er systemet angripelig og kan vi tette sikkerhetshullene?

1.3 Tidslinje og aktiviteter

26 august startet oppgaven. Høsten gikk med til obligatorisk skrivekurs ved UiO (INF5550), og tiden frem til jul ble brukt til å lese, skrive og utføre undersøkelser om "Near Field Communication" (NFC). Dette er beskrevet i kapitlet og kapittel 3 og 4.
Over nyttår 2006 startet implementeringen og i slutten av mai begynte rapportskrivingen.

I løpet av oppgaveperioden har det vært både regelmessige (1 gang i uka) og uregelmessige møter med veileder, ekstern veileder og andre ressurspersoner for å planlegge veien videre, definere og avgrense oppgavene, informere og bli informert, få perspektiv og gode råd.

Eksempelvis har vi:

- Holdt møte med ressurspersoner i Telenor FoU. Disse hadde interesseområder som fremtidens hjem, hjemmeinnhold (musikk, bilder), sømløs aksess.
- Vært med på SIM Authentication Workshop, Telenor.
- Besøkt Kostas Papadopoulos i Epsys, som leverer låsesystemer og NFC/RFID-lesere.
- Vært på seminar hos Telenor. Her ble RFID, NFC diskutert spesielt med hensyn på SIM.
- Vært med på seminar i regi av Abelia og Ericsson i Asker. ”Utvikling av fremtidens mobile tjenester.”
- Holdt uoffisielle demonstrasjoner av prototypen på Movation, Oslo og UniK, Kjeller.

Ettersom det er et relativt nytt område som belyses kom stadig nye momenter på banen under utforskningen og møtene. Oppgaven er blitt omformet underveis. Utfordringen har vært å sette grenser.

1.4 Oppbygging av rapporten

Kapittel 1 starter med innledning og problemstilling.
Deretter følger beskrivelse av metodene som er benyttet til å skaffe oversikt og informasjon til bruk **kapittel 2**.
I **kapittel 3** gis en teoretisk orientering om NFC, og
i **kapittel 4** en mer praktisk tilnærming.
I **kapittel 5** beskrives prototypen, hovedfokuset i oppgaven.
Kapittel 6 gir en oversikt over resultater vi har kommet frem til, før det drøftes i forhold til eksisterende kunnskap i **kapittel 7**.
Kapittel 8 avrunder med konklusjon.

2 Metode

Metodene som ble benyttet under oppgaveperioden er prototyping, imperiske undersøkelser i form av artikkellesing og internettsøk, samt møter og telefonsamtaler med fageksperter.

2.1 Prototyping

Prototyping har vært hovedfokuset i oppgaven. For å kunne implementere prototypen har jeg vært nødt til å lære meg ny og friske opp mye gamle Javakunnskaper. Nye Application Programming Interface (API) måtte læres, hvorav to var nye av året, et lansert så seint som desember 2005. Dette er grensesnitt som gjør det mulig å kommunisere med den spesielle maskinvaren, nærmere beskrevet i kapittel 4. Flere av disse hadde kun medfølgende dokumentasjon og ikke noen ressurser på internett, i form av for eksempel forum eller spørsmål og svar sider. Å stille eksperter i firma som Nokia og Sun spørsmål koster flerfoldige tusen kroner, og var dermed utelukket.

Verdifull informasjon kan bli høstet av prototypen. Mye av denne informasjonen er praktisk av natur. En prototyp kan si mye om hvor dyrt, utfordrende og lønnsomt (ikke nødvendigvis økonomisk) en fullstendig utvikling vil være.
Av det mer teoretiske kan vi trekke slutninger på spørsmål rundt nøkkeldistribusjon ved hjelp av tekstmeldinger. Dette finnes det tilnærmet ingen informasjon om. Det nærmeste man kommer er autentisering med smartkort eller public key infrastructure (PKI).
Nyttige tilbakemeldinger får man fra fagpersoner som ser på og prøver prototypen.

2.2 Imperiske undersøkelser

Artiklene som er blitt sitert og direkte brukt er listet opp i kildehenvisningene. I tillegg har vi møtt og pratet med ressurspersoner
Litteratursøk er foretatt med elektroniske søkeverktøy som IEEE database- og tidsskriftsøk, Google scholar søkemotor som søker i akademiske og faglige utgivelser, og X-port ved UiO

som søker i databaser og tidsskrifter av samme natur som Google scholar, men med autentisering fra UiO så man har tilgang på databaser som er stengt for allmennheten.

Mye informasjon har blitt trukket ut av møter og seminarer med veileder og andre fageksperter. Under slike seanser får man også stilt direkte spørsmål og ryddet opp i uklarheter og feil.

2.3 Oppsummering

Når det gjelder hvorfor disse metodene er benyttet er det fordi NFC og elektronisk nøkkel i mobilen er et nytt emne som det kan være vanskelig å få informasjon om. Vi fant ingen informasjon om å sende elektroniske nøkler med tekstmelding, prototypen er derfor en viktig ressurs. Fagartikler har utelukket vært på engelsk, noen artikler på nyhetsnettsteder har vært på norsk. Jeg har forsøkt å finne artikler så tett opptil problemstillingen som mulig, men de belyser sjelden alle momentene.

Man skal være kritisk til informasjon man finner på internett. Jeg har ikke basert noen påstander eller argumenter på diverse sider funnet på nett, kun artikler. Artiklene har holdt høy kvalitet og flere er publisert i IEEE og på universiteter.

3 Eksisterende kunnskap

I dette kapitlet vil jeg gi en innføring i Near Field Communication forumet som forvalter og fremmer NFC teknologien, NFC i seg selv og RFID som NFC bygger på.

3.1 Near Field Communication Forum

NFC Forum ble dannet av Philips, Sony og Nokia tidlig i 2004 og er et samarbeidsorgan hvor forskjellige firmaer fra relevante bransjer samarbeider om å utvikle, standardisere, markedsføre og implementere teknologien NFC. Blant medlemmene finner vi blant andre Mastercard, Microsoft, Motorola og Texas Instruments. Ved at så mange og store aktører går sammen i et slikt forum gir som resultat stor levedyktighet og et bredt spekter av bruksområder.

Når NFC har fått et eget forum er det et kjennetegn på at teknologien har kommet for å bli. I februar 2005 økte antallet medlemmer fra 5 til 25, og per november 2005 var det 47 medlemmer.

NFC Forum dannet tidligere i år fire arbeidsgrupper med hvert sitt fokusområde og underliggende oppgaver og problemer.
Fokusområdene er enheter (maskinvare), applikasjonsrammeverk (programvare), sikkerhet og testing. De aktive, tekniske medlemmene av NFC Forum velger den eller de gruppene de kan bidra i.

3.2 Near Field Communication

Dette underkapitlet tar for seg NFC (Near Field Communication), en kommunikasjonsteknologi som ved hjelp av radiobølger opererer mellom enheter over meget korte avstander. Dette åpner for mange nye muligheter og funksjoner, og har samtidig potensialet til å samle mange tjenester i en håndholdt enhet, som mobiltelefonen man som regel alltid har med seg. Typiske tjenester er elektronisk nøkkel, betaling, billetthåndtering osv. Sikkerhet og personvern kan ivaretas gjennom kryptering og smartkort.

NFC er en standard i utvikling og består av en protokoll og et grensesnitt basert på trådløs kommunikasjon over meget korte avstander, typisk 0 - 2 cm, maksimalt opptil 10 cm. Ideên er en videreutvikling av teknologien fra smartkortene Sony FeliCa og Philips MiFare. Kommunikasjonen utføres ved hjelp av radiobølger på samme frekvens som smartkortene og RFID (mer om RFID i avsnitt 3.3) 13,56MHz. Dette er en globalt åpen frekvens, men noen land har restriksjoner på hvor stort geografisk område signalet er lov til å sende. Den korte avstanden teknologien opererer over tilsier at en frekvens er nok og at radiorommet ikke blir overfylt [5].
Hensikten er å utveksle informasjon eller opprette et midlertidig (ad-hoc) nettverk mellom to enheter (både mellom ”smarte” enheter, for eksempel mobiltelefon, og mellom smarte og ”dumme” enheter som TV) kun ved å holde de i nærheten av hverandre, uten noen form for oppsett. Informasjonen skal kunne brukes til identifisering, autentisering, betaling, utveksling av data eller oppsett av andre kommunikasjonsformer.

I praksis består NFC av en RFID-leser integrert i forskjellige enheter, sammenknyttet med prosessor og minne. Selv om det heter RFID-leser, har NFC også full mulighet til å sende/skrive. Teknologien kan brukes mer avansert ved hjelp av applikasjoner. Man tenker seg at NFC kan brukes i mobiltelefoner, PDA’er, PC’er, dørlåser, betalingsautomater, biler, TV, kjøleskap og så videre.
Funksjoner som allerede finnes eller man tenker seg spenner vidt:
-identifikasjon
-autentisering
-elektronisk nøkkel
-betalingsmiddel
-billett
-overføring av data, for eksempel bilder, musikk, forretningskort, filer
-oppsett (bootstrapping) av andre kommunikasjonsprotokoller som Blåtann eller Wi-Fi

NFC enheter skiller mellom å operere i aktiv og passiv modus. I den aktive modusen vil enheten generere sitt eget signal ved hjelp av en strømkilde, mens i passiv modus svarer den kun på ”anrop” fra en annen enhet (i aktiv modus) og modulerer dennes radiobølger til svar. Dette gjør den ved å skrive til en innebygd RFID eller smartkort kompatibel krets. En enhet i passiv modus som blir anropt kan også skifte modus til aktiv før den svarer. Aktive RFID-

enheter trenger naturligvis også en strømkilde, men kan også ha muligheten til å skifte over til passiv modus og vil da trenge svært lite strøm og dermed blir ikke batterilevetiden en flaskehals. I aktive RFID-enheter som ikke har ekstra minne eller prosessor knyttet til seg er allikevel ikke batterilevetiden et stort problem, Autopass sine brikker, brukt i bomringer i Norge, har en levetid på 10 år eller mer. Alle NFC enheter har muligheten til være både i aktiv og passiv modus, i motsetning til RFID-brikker som kan produseres til å være bare det ene eller det andre (i tillegg til både og).

I motsetning til vanlig RFID som oftest benyttes over lengre avstander (meter) trenger ikke NFC enheter i passiv modus strøm for å forsterke signalet siden det kun skal benyttes over korte avstander, men man kan anta at de fleste NFC enheter opererer i samarbeid med en applikasjon som kjøres på en prosessor som igjen trenger strøm. Derfor vil NFC enheter alltid sett trenge en strømkilde.

En NFC forbindelse skjer kun mellom 2 enheter. Den som tar initiativet, eller først blir registrert dersom flere prøver å starte en forbindelse samtidig, kaller vi initiativtaker og mottageren blir kalt mål. Det er alltid initiativtakeren som kontrollerer dataoverføringen. Dersom det er flere enheter som er aktive og ber om å være initiativtaker i samme radiorom eller er kollisjoner av noe slag er det i protokollen innarbeidet en ”lytt-før-snakk” prosedyre. Når alle først lytter etter overføringer og tar hensyn til disse får man ikke kollisjoner.

NFC opererer på hastighetene 106, 212 og 424 kbit/s (maksimalt 3MB/min), og arbeid er i gang for å øke maksimalhastigheten først til 848kbit/s og senere 2Mbit/s. Hastigheten tilpasses under kjøring ved at enhetene snakker sammen. Disse hastighetene tilsier at NFC ikke egner seg til å overføre større mengder data. Dersom dette er et behov fokuserer NFC på å være en protokoll som uten brukers påvirkning kan opprette Blåtann eller Wi-Fi forbindelse mellom enhetene (”interface of interfaces”, kan tolkes både bokstavlig, som ment her, og i betydningen det beste grensesnittet). NFC bruker radioteknologi mellom enheter i samme frekvensrom, derfor kan man kun operere på halv dupleks. Det vil si at enhetene sender og mottar data på tur og ikke samtidig.

Standardene som beskriver NFC er:
ECMA-340 / NFCIP-1 “Near Field Communication Interface and Protocol”, adoptert av ISO/IEC 18092, og

ECMA-352 / NFCIP-2 Near Field Communication Interface and Protocol, adoptert av ISO/IEC 21481.
NFC er også kompatibel med smartkort av standarden ISO 14443 A (Philips MiFare og Sony FeliCa).

NFCIP-1 beskriver protokollen og grensesnittet. Det vil si det som er beskrevet i dette kapitlet.

NFCIP-2 beskriver hvordan NFC kan kommunisere med liknende standarder og automatisk velge riktig standard. Standarder NFC kan kommunisere med er VCD (lenger rekkevidde) og PCD (kort rekkevidde), sistnevnte brukes av smartkortene FeliCa og MIFARE. NFCIP-2 sørger for at NFC-enheter ikke forstyrrer pågående kommunikasjon og bruker den nevnte ”lytt-først” prosedyren, samt det å være grensesnittet.

ECMA-356 (juni 2004) er en standard for testing av NFC sitt RF grensesnitt med antenner med fysiske dimensjoner mindre enn 85 x 54mm.
ECMA-362 (desember 2004) er en standard for testing av NFC protokollen, både på initiativtaker- og målsiden.

Det med å bruke (nesten-) berøring når du vil kommunisere er ifølge NFC Forum [1] både naturlig og innovativt. Det er lett å sette seg inn i følgende situasjon: du vil prate med noen du ikke har øyekontakt med. Da er en berøring på skulderen eller armen en vanlig måte å ta kontakt. Denne psykologiske bekvemmeligheten er viktig idet det store markedet skal involveres. De store massene er mer interessert i funksjonaliteten (og designet) til enheter og vil ikke streve med parametere og teknisk oppsett. Dermed kan produkter som i dag ikke enkle nok bli tilgjengelige for større og helt andre grupper mennesker. Kanskje vil ny teknologi for en gangs skyld ikke føre til fremmedgjøring.

3.3 Radio Frequency Identification

RFID (Radio Frequency Identification) er radiobasert kommunikasjon av data med lav- (125/134,2MHz), høy- (13,56MHz) og ultrahøyfrekvens (868 – 956MHz), men det finnes også RFID på mikrobølgenivå (2,45MHz) og i andre frekvensområder. Dette er stort sett

”åpne” frekvenser, det vil si fri for restriksjoner, annet enn at hvor langt (sterkt) et signal kan sendes (gitt nasjonalt). Det hersker uenighet om når RFID teknologien ble oppfunnet, noen sier 1920-årene, men andre hevder 1942. Wikipedia [6] forteller oss at teknologien ble brukt til avstandsmåling og identifikasjon av fly under andre verdenskrig. Det som vi i dag forbinder med RFID stammer fra 1970-årene og det er særlig logistikkbransjen som har tatt teknologien i bruk der den blant annet erstatter strekkoden. Den brukes også ofte i bomstasjoner, billettsystemer, betalingssystemer og som bilnøkkel.

RFID-lesere og RFID-brikker består begge av en antenne (lesere kan ha flere) for å motta og/eller sende radiobølger og som navnet antyder en ID. Den enkleste formen for ID er et lite minne (2kB) med en tekststreng bestående av produkt-id og serienummer, men minnet kan også være langt større. Disse billigste brikkene er på størrelse med et SIM-kort og er nylig blitt svært billige. De minste RFID-brikkene man kan produsere tar omtrent like stor plass som et sandkorn. Lesere må ha en strømkilde og bruker alltid strøm når den er slått på, rekkevidden kan være mange hundre meter.

Man skiller mellom aktive, passive og semipassive brikker. De aktive brikkene har en strømkilde og lager sitt eget radiosignal, mens passive kun modulerer signalet det mottar fra en leser. Det vil si at de mottar radiobølger fra en RFID-leser, omgjør bølgene og sender ut innholdet sitt. De semipassive brikkene er passive til en leser avleser de, da sender de et strømforsterket signal tilbake som har mye lenger rekkevidde enn et passivt svar. Aktive brikker kan ha større lagringsplass, mer funksjonalitet og mye lengre rekkevidde, opptil over flere hundre meter, men de trenger en strømkilde, oftest et batteri.

Siden RFID er basert på radiobølger trenger ikke sender og mottaker vanligvis å ”se” hverandre, slik som ved bruk av for eksempel infrarød overføringsteknologi, men dersom det kommer for mange hindringer som vegger, metall eller vann i mellom enhetene kan det hende signalene ikke når frem. Dette, pris og rekkevidde avgjøres i størst grad av frekvensområdet. Lav frekvens gir lav pris og rekkevidde, høy frekvens gir lang rekkevidde, men er dyrere. Lang rekkevidde åpner for flere bruksområder enn kun erstatning av strekkoden, for eksempel overvåking av øremerkede dyr ute i naturen.

I dag er RFID-brikker som nevnt mest brukt til merking av varer i transport og elektronisk styring av lagerbeholdning. Ved hjelp av RFID-brikker, lesere på forskjellige stasjoner og

internett er det mulig å spore et enkelt kolli eller en hel forsendelse for både avsender og mottaker, likt Postens pakkesporing. Arbeidet med å identifisere/spore pakkene på Postens stasjoner i dag er typisk gjort ved hjelp av strekkodelesere og er ensformig arbeid. I forhold til RFID er strekkoden avleggs, så hvorfor er ikke RFID rullet ut i stor skala?
RFID-produsentene har hatt problemer med å presse prisene ned. Prisen på RFID-brikkene går ikke ned før produksjonen skyter i været, og produksjonen tar ikke av fordi få vil kjøpe brikkene til dagens pris.
Noen er allikevel pådrivere, Wal Mart og den amerikanske hær får mye ære for at prisene nå går ned fordi de tvinger vareprodusentene til å levere varene merket med RFID-brikker og det er snakk om meget store kvantum. I 2006 tar salget vil ta av. Man sier at man vil ta i bruk 3 ganger flere brikker dette året enn i de foregående 60 årene teknologien har eksistert.

4 Near Field Communication i praksis

NFC- og RFID-teknologien er økende i popularitet og kommer til å bli veldig utbredt. Bruksområdene og mulighetene er mange og prisen synkende. Mange tjenester vil bli samlet i små, bærbare enheter, sannsynligvis blir mobiltelefonen mest populær. For å bli godt tatt imot kreves høy sikkerhet og brukervennlighet og NFC legger alt til rette for dette. Det utvikles verktøy og løsninger for å kunne utnytte teknologien i stor skala. Vi kommer til å se mer og mer til enheter med NFC i kommende år, og flere og mer standardiserte tjenester.

4.1 Status quo

NFC er en teknologi i barndomsstadiet som har fått mye oppmerksomhet. Ideên er enkel, man holder enheter som mobiltelefoner, smartkort eller bærbare PC'er inntil hverandre og de kommuniserer, nesten som et håndtrykk. Man trenger verken å sette opp parametere eller taste inn data. Overføring av parametere og data skjer ved hjelp av radiobølger som sendes og mottas mellom enhetene. Bruksområder spenner fra betaling, elektronisk billett, overføring av data, automatisk oppsett av WLAN til å vise familien bilder fra digitalkameraet på TV, uten behov for en ledning.

Per i dag er teknologien standardisert men bare så vidt begynt å bli tatt i bruk. Det er mange fordeler som taler for bruk, for eksempel å klare seg med kun mobiltelefon for å betale kaffen på kiosken, låse seg inn på jobb og se en film på kino med elektronisk billett. Kneika kan være at man må utvikle systemer og standarder som passer alle og sikkerheten må ivaretaes. Ulempen med RFID som NFC er basert på er blant annet at radiobølger kan avlyttes og kryptering i teorien kan knekkes. Mottiltak som at du skrur NFC på når du trenger det og at informasjon kan ligge på et meget sikkert smartkort gjør allikevel at sikkerheten ikke blir en akilleshæl.

Det er mobiltelefonen som vil bli en av de største driverne for NFC, de første er allerede i salg. Noen av de største bidragsyterne i utviklingen av NFC er mobilselskaper. Mobilen vil man kunne benytte den som et regelrett smartkort eller installere applikasjoner som gjør andre

oppgaver. Også enheter som man ikke forbinder med kommunikasjonsteknologi, som TV og digitale kamera, vil godt kunne bruke teknologien. Ikke minst vil det enkle brukergrensesnittet, fysisk nærhet, kunne bidra til stor utbredelse og at mennesker med mindre teknisk innsikt vil kunne bruke enhetene.

4.2 State of the art

NFC er på barnestadiet: teknologien finnes og er standardisert, men er foreløpig ikke rullet ut i stor skala. Det første NFC-produktet i produksjon er en mobiltelefon fra Nokia, mobiltelefonen 3220 med en NFC-leser i dekselet. Det er riktignok svært lite den kan brukes til foreløpig, men en fotballstadion i Nederland har tatt teknologien i bruk. Tilhengerne av Roda JC kan bytte ut supporterkortene sine og i stedet lade mobilen med virtuelle penger og bruker kun den for å komme inn på kampene, kjøpe mat og drikke, samt supporterutstyr. Også et stort transportselskap i Tyskland, Rhein-Main-Verkehrsverbund (RMV) [3], prøver ut denne telefonen som betalingsmiddel. I Asia, spesielt Japan og Korea, er smartkortene FeliCa og MiFare i full bruk og brukes til å betale transportbilletter på tog og buss. Disse finnes det allerede millioner av på markedet og å portere disse til en NFC mobilen er enkelt som følge av 100 % kompatibilitet. Dermed slipper man å ta med seg annet enn mobilen.
Disse prosjektene viser at teknologien virker og er fullt mulig å bruke i praksis. Det er seriøse aktører som står bak og det er få grunner til at det ikke skal bli tatt i bruk.

Enheter som mobiltelefoner, PDA'er og bærbare PC'er har i dag muligheter for utveksling av data seg i mellom, men det er liten mulighet for trådløst samarbeid/datautveksling mellom disse og mindre "smarte" enheter som video, TV, kamera eller klokke. NFC Forum bruker som eksempel å vise bilder tatt med PDA på TV ved å føre de i nærheten av hverandre. Slike funksjoner er i dag spesielt designet, ofte dyre og man må typisk kjøpe enheter fra samme produsent. Funksjonene er sjelden trådløse, men heller basert på flytting av minnekort eller tilslutning med kabel.

I dag er det WLAN på bærbare PC'er og GPRS på mobiler som er måten flest bruker for å koble seg til internett på. For å utveksle data mellom disse enhetene brukes oftest Blåtann. NFC er ikke ment å være en konkurrent for disse, snarere tvert imot. Et av NFC Forums hovedideer er bootstrapping av Blåtann og WLAN. For å sette opp WLAN og Blåtann må

man klikke seg frem i ikoner og menyer, og taste inn tekniske parameter. Mannen i gata er ikke interessert i å fikle med disse parameterne og prøve seg frem, han eller hun vil at enheten skal virke fra det øyeblikk den er ute av esken. NFC vil gjøre det mulig for to enheter å koble seg til hverandre i Blåtann eller WLAN nettverk kun ved å føre enhetene sammen og la NFC ta seg av oppsettet.

Et scenario som Nokia bruker for å markedsføre sin første NFC-telefon er muligheten for å lese en RFID-brikke som er integrert under en filmplakat. Med det som utgangspunkt skal man kunne få ringetone, videosnutter og grafikk, bestille kinobilletter og dele reklamen med venner. Det er ikke nok minne i de enkle RFID-brikker til at de kan inneholde mediedata og RFID-brikker med mer minne koster altfor mye å produsere for slike bruksområder. En løsning på problemet er å la RFID-brikkene inneholde en link til et webområde med innholdet som brukeren kopierer over på mobilen sin, deretter bruker han eller henne GPRS for å laste det ned.

4.3 Utfordringer og muligheter

Trendene beveger seg fra at man har mange forskjellige enkeltbruksenheter til færre flerbruksenheter. I tillegg går enhetene fra å være isolerte til å ha nettverksmuligheter. Eksempelvis er almanakk, digitalkamera, mp3-spiller og internettlesere allerede integrert i mobiltelefonen, som ikke lenger bare kommuniserer over GSM og andre mobilnett men også ved hjelp av Blåtann og Wi-Fi. Når NFC og annen ny kommunikasjonsteknologi blir utbredt vil enheter lettere kunne dele ressurser. Dersom en klokkeprodusent ønsker at en nytt armbåndsur skal kunne stille seg selv, kan den kommunisere med NFC-telefonen som kan hente nøyaktig klokkeslett fra en server over GPRS. Jakken din kan ha sensorer som måler temperaturen, men det er ikke funksjonelt med skjerm på jakken, den kan derfor isteden bruke skjermen på mobilen og vise hvor mange grader det er.
NFC kommer til å være prismessig konkurransedyktig, sier Christophe Duverne, styreformann i NFC Forum [5]. Han får støtte av analysebyrået ABI research [2] som sier at i 2009 vil 50 % av alle mobiltelefoner ha NFC og Kay Irwin i inCode som sier at NFC vil være standard på de fleste mobiler om fire år.

Videre spår Duverne at det er mobilen som blir den store NFC enheten. Vi vil også få se streamet høykvalitetsvideo, forlenget batterilevetid, enten ved forbedret eller ny teknologi, mobilen vil få harddisk og minne i gigabyte størrelse. Som nevnt i avsnittet om NFC Forum står det såpass mange og store aktører bak teknologien at den sannsynligvis vil bli brukt i stor skala.

Noe helt annet som også har potensial i fremtiden er såkalt PAN (Personal Area Network). Enheter på eller i nærheten av kroppen (eksempelvis klærne) kommuniserer ved hjelp av kroppens spenningsnett. Gjør det for eksempel mulig å utveksle forretningskort via håndtrykk [13]. Denne fremtidsvisjonen støtter opp om at utveksling av informasjon sannsynligvis vil bli mer fysisk og tilpasset allmennheten.

4.4 Bruksområder og applikasjoner

Det man i dag bruker (kontaktløse) nøkkelkort og nøkler til kan man i nær fremtid utføre med mobiltelefonen, men for at dette skal være mulig må brukervennlighet, sikkerhet og mangfold av tjenester være ivaretatt. Dette må også gjelde på applikasjonsnivå. Når vi snakker i en mobil kontekst er det Java ME som er interessant å se på med hensyn på applikasjoner fordi det programmeringsspråket er mest utbredt.

Brukervennlighet er nærmest NFC sitt varemerke og har blitt snakket om tidligere i rapporten, men det må også gjelde på applikasjonsnivå. Noen vil kanskje si at brukervennlighet er gode skjermbilder, layout, knapper og menyer, men virkelig god brukervennlighet kan være fraværet av behovet for å interagere med tradisjonelle IO-enheter som skjerm og knapper. Kun meget enkle valg og inntastinger, som valg av profil, ja/nei og PIN-kode bør være nødvendig i en NFC-applikasjon. Mye av informasjonen applikasjonen får bør være usynlig for brukeren.

En stor del av sikkerhet blir ivaretatt på NFC enheter ved at de må være nærmest helt inntil hverandre for å kommunisere, men det er fortsatt mulig å avlytte eller få informasjon på falske premisser. Kryptering av data er en elementær sikkerhetsforanstaltning når det kommer til datakommunikasjon og kommet til å være sentralt i implementering av applikasjoner i NFC-telefoner. PKI forum [4] fremmer Public Key Infrastructure, som er en standard for

kryptering ved hjelp av elektronisk legitimasjon og signatur og som går for å være veldig sikker. Denne er spesifisert i JSR-177 Security and Trust Services API for Java ME og kan dermed brukes i mobilapplikasjoner.

Når en enkelt enhet (NFC-mobiltelefon) skal brukes i mange sammenhenger (kjøpe kinobilletter, betale for kaffe, nøkkel til PC'en og så videre) kan ikke telefonen sende samme data til alle de forskjellige mottakerne. Det går kanskje til en viss grad å sende en statisk, standardisert kryptert streng som identifikasjon, men dermed har du bare en nøkkel og alle "låser" må tilpasses deg. Dersom en avlytter signalet og bryter krypteringen eller en utro tjener stjeler telefonen/identiteten din vil personen ha tilgang til alt du har tilgang til. Slik det ser ut i dag vil man snart kunne lese ut en identifikasjonsstreng fra SIM-kortet dermed kan en applikasjon som er kontekstsensitiv krypterer denne med en nøkkel som svarer utelukket til mottageren. Dermed er det bare riktig mottaker som kan lese dataen.

Når man har tenkt igjennom disse punktene og skal i gang å lage applikasjoner for NFC-mobiler er det Java Micro Edition (Java ME) som er det programmeringsspråket som er mest utbredt i denne verdenen. Dette er en lettere versjon av Java standard edition som egner seg godt for enheter med begrenset minne og prosessorkraft. Sun, som står bak språket, jobber hele tiden med å videreutvikle det i samarbeid med eksperter og interessenter (både firma og privatpersoner), slik at ny teknologi som NFC kan taes i bruk. De samarbeider i noe som heter Java Community Process (JCP) og her lages og endres spesifikasjoner. Nylig har det kommet nye spesifikasjoner som støtter smartkort (NFC kompatibelt) som er spesielt sikkert og interessant med hensyn på betaling og autentisering.

JSR – Java Specification Request

JSR-177 Security and Trust Services API for J2ME (SATSA)	-final release
JSR-185 Java Technology for the Wireless Industry (JTWI)	-final release
JSR-257 Contactless Communication API	-early draft

En JSR er som navnet røper en anmodning om ny eller forandring av eksisterende spesifikasjoner i Java. Den mest interessante i dag er JSR-177 som tar for seg smartkort standarden (Nokia's SmartChip API er et undersett/basert på JSR-177). Denne er fullt utredet og i bruk. Denne tar for seg kommunikasjon mot smartkort som mange NFC-enheter vil

benytte seg av, spesielt NFC-mobiler. I tillegg sørger den for muligheter til kryptering, vedlikehold og andre oppgaver knyttet til smartkort.
Per i dag finnes det ikke et NFC API som er allment tilgjengelig. JSR-257 er i utviklingsfasen og tar for seg flere former for kontaktløs kommunikasjon, herunder NFC. Når denne spesifikasjonen blir tilgjengelig vil hvem som helst kunne programmere NFC-enheter som har kontakt med Java-kjørende prosessorer. Tilsvarende API vil også komme for andre språk/plattformer. Flere aktører, for eksempel Nokia, har utarbeidet egne API'er, men disse er ikke tilgjengelige for allmennheten eller uten spesielt grunnlag. Foreløpig må man enten smøre seg med tålmodighet eller ha tilgang til disse API'ene.

5 Utviklingsarbeid

Dette kapitlet tar for seg prototypen som ble implementert. Kapitlet går fra å skumme i overflaten til å dykke i dybden på utviklingsarbeidet. Avsnittet serverimplementeringen er skrevet av Haakon Eikenes og er tatt med fordi det er en sentral del av implementeringen.

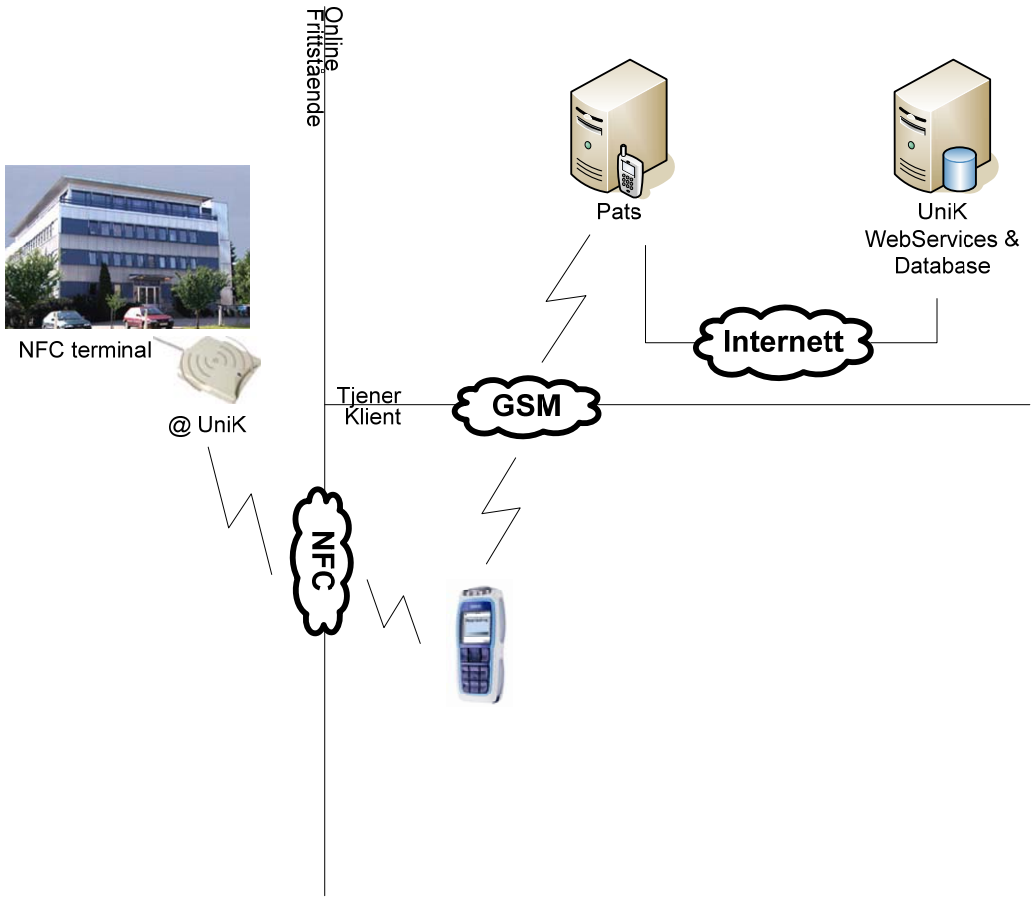
Oppgaven skulle som det stod i oppgavebeskrivelsen ende opp i en fungerende prototyp. Min del av implementeringen var mobildelen. Haakon Eikenes tok for seg serverdelen. Implementeringen er laget for å være mest mulig realistisk.

5.1 Overordnet funksjonalitet og arkitektur

Arkitekturen består av

- Tjener med nettjenester, database og administrasjonsverktøy
- Pats, SMS Gateway
- Mobiltelefon med NFC brikke
- NFC-lås

På figuren under har jeg forsøkt å vise de forskjellige komponentene og hvordan de kommuniserer. Komponentene og data som sendes over de forskjellige kommunikasjonslinjene er beskrevet i tjener- og mobilimplementeringskapitlene. Vi kombinerer standard klient/server arkitektur, database og webservices med telekommunikasjonstjenester. Allikevel er arkitekturen generisk.



Figur 5-1 Overordnet arkitektur

Funksjonene som utføres er

- Administrator registrerer en gjest eller gir en gjest tilgang (se appendiks A). Dette skjer ved å aksessere en webside på UniK eller sende en SMS og oppgi nødvendig data.
    - Dersom administratoren sender en SMS ankommer denne Pats. Tjeneren på UniK mottar dataene.
- Tjeneren på UniK sender en elektronisk nøkkel til gjesten sin mobiltelefon via Pats.
- Gjesten ankommer UniK. Han holder telefonen sin opp mot NFC terminalen ved utgangsdøren som låses opp, da han har tilgang.

Prototypen er utviklet med tanke på å demonstrere at denne teknologien finnes og lar seg bruke, mer enn å lage et system klart for utrulling i stor skala.

5.2 Serverimplementeringen

Funksjonene i serverimplementeringen:

- Webgrensesnitt og webtjenester
- Motta og sende SMS
- Database over brukere og tilgangsrettigheter
- Java-applikasjon

Avsnitt 5.2 er skrevet av Haakon Eikenes.

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.

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)

Ordforklaringer

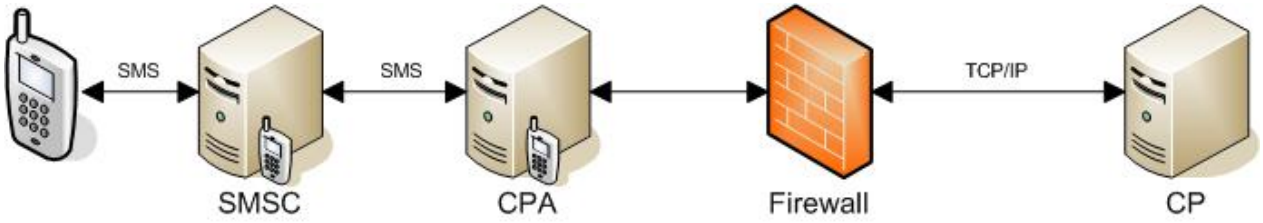
For håndtering av SMS i systemet har vi benyttet Telenor PATS innovasjons laboratorium. PATS er et samarbeid mellom Norges tekniske-naturvitenskaplige universitet (NTNU), industri- og telekommunikasjonsbedrifter. De tilbyr i dag en rekke tjenester for utviklere av telekommunikasjon.
Vi har benyttet Telenor 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.

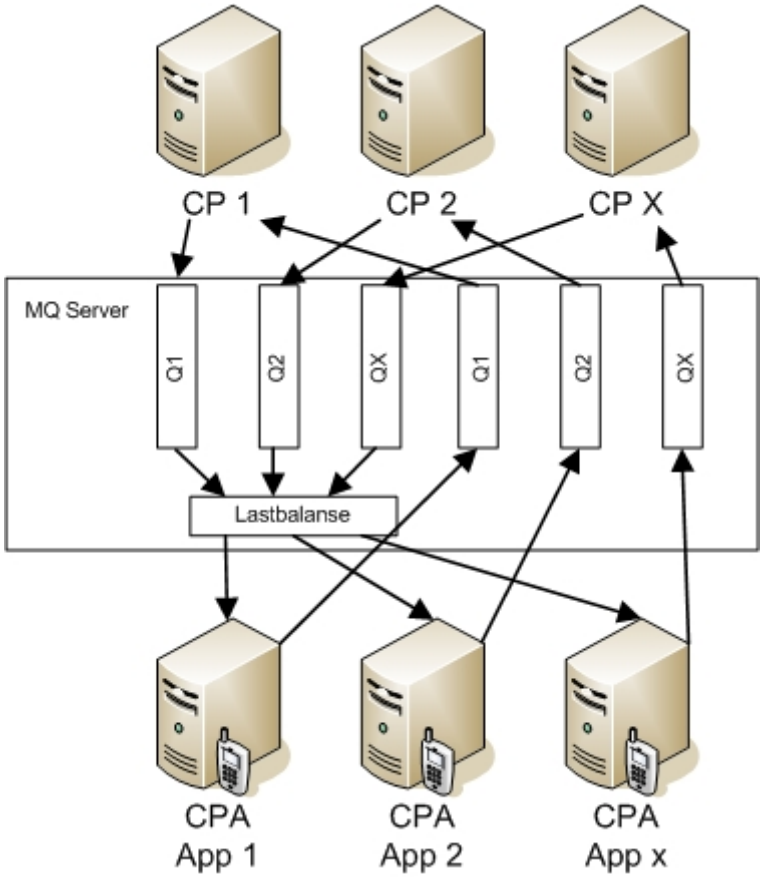
mPay kan sees på som både innholdsleverandør og en betalings løsning som tilbyr tjenester for brukere av mobiltelefon. Dette systemet gir brukere tilgang til å betale for parkering via mobiltelefonen.[1] Tanken bak konseptet er at brukere av parkeringsplasser slipper å ha småpenger tilgjengelig for parkometeret, 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.



Arkitektur



Oversikt over CPA, sett fra CP

Et alternativ til PATS er 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.

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 6), den blir så lagt i en kø før den sendes ut via Telenor Mobil sin CPA.

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 1.0^2 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.

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:

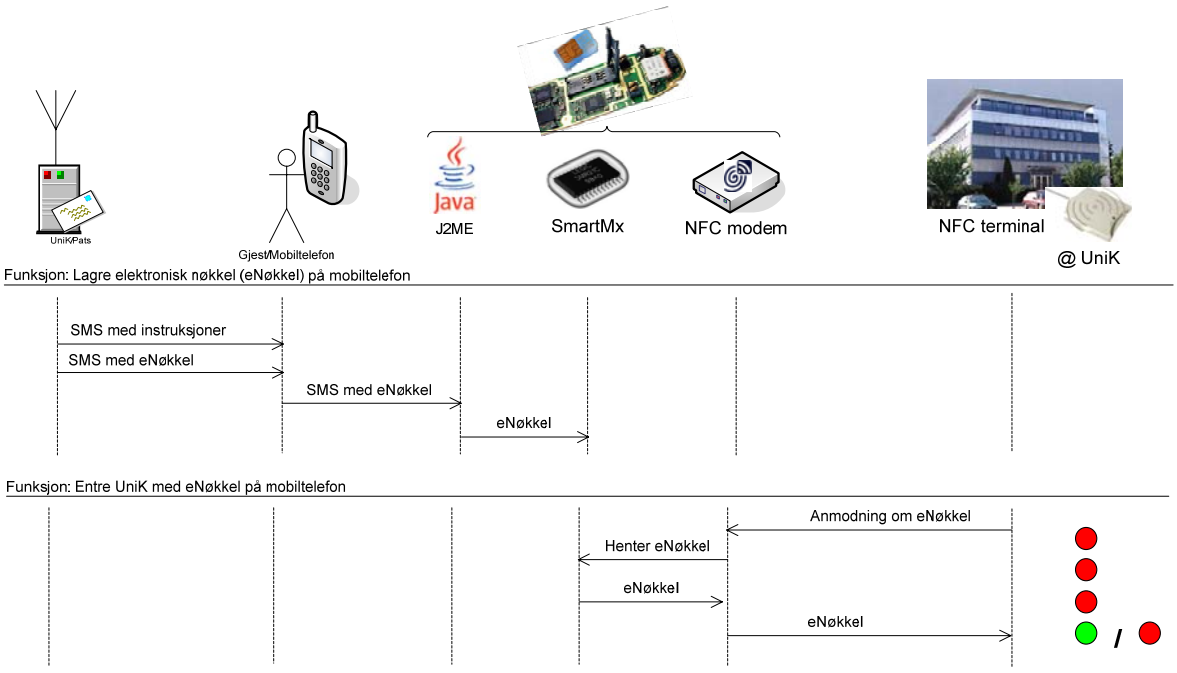
- user (tlf, name)
- owner (idowner, admin, pass)
- locks (lockName, lockID)
- Access (accessID, tlf, time, date, time2, date2, days, lockName)

5.3 Mobilimplementeringen

Min del av den praktiske oppgaven var å sørge for at en prototypmobil kunne motta og sikkert oppbevare en elektronisk nøkkel, samt utveksle denne mot en kontaktløs RFID-/NFC-leser. I tillegg implementerte jeg en NFC-lås simulering.

De forskjellige funksjonene mobilen og MIDlet'en (en Java Micro Edition, J2ME applet) måtte kunne håndtere inkluderte (se figur):

- Motta data som kommer over lufta (over the air) via SMS eller GPRS
- Bruke NFC-modem og SmartMx brikken ved hjelp av API fra Nokia
- Vise meldinger på skjermen til brukeren
- Lese fra og skrive til MiFare emuleringen på SmartMx ved hjelp av Java Card interface



Figur 5-2 Hovedfunksjonene til prototypen

Nødvendig maskinvare

Mobiltelefon

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.

SmartMx brikken og MiFare smartkort emulering

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16			
0																		Line 0:	Title
1																	Block 1	Line 1:	Data
2																		Line 2:	Data
3																		Line 3:	Read/write key
4																		Line 4:	Data
5																	Block 2	Line 5:	Data
6																		Line 6:	Data
7																		Line 7	Read/write key
8																		Line 8:	Data
9																	Block 3	Line 9:	Data
10																		Line 10:	Data
11																		Line 11:	Read/write key

Figur 5-3 Smartkort emulering på telefon og smartkortets oppbygning

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.

APDU

For å kommunisere med smartkortet MiFare/SmartMx gjennom J2ME må man bruke såkalte APDU-kommandoer (Application Protocol Data Unit). Disse skrives som en streng av heksadesimale tall. Når man sender en kommando får man alltid tilbakemelding, en svar-APDU.

Header				Body		
CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	0F	53 69 6A 71 62 65 4A 65 74 5A 2E	00

I Headerfeltet er CLA instruksjonsklassen som skal brukes, INS er instruksjonen som skal gjøres, for eksempel skrive, P1 og P2 er parametere.
Bodyfeltet består av Lc som er lengden på datafeltet, dataene og Le som sier hvor lang response APDU'en får lov til å være (kan være 00 = ubestemt, som i eksemplet).

Gangen i kommunikasjonen er som følger:

- Answer to reset – en terminal vil ha kontakt med smartkortet og ber det svare på anrop.
- Select – leseren velger hvilken applikasjon som skal benyttes, for eksempel vår lese- og skriveapplikasjon
- Lese og skrive applikasjoner utføres. Tilgangsinformasjon sendes for eksempel til NFC-låsen på UniK.
- Deselect - Når oppgavene er utført avvelges applikasjonen.

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.

5.4 Programvare verktøy

En MIDLet er en Java applet for enheter med mindre ressurser enn en vanlig PC, for eksempel PDA'er, skrivere og, som i vårt tilfelle, mobiltelefoner. I motsetning til Java SE og Java EE kommer Java ME (micro edition) med et svært begrenset bibliotek av API'er. Det er derfor vanlig at hver enkelt enheter kommer det begrensede Java ME og de spesielle tilleggs API'ene enheten har behov for.

For å utvikle MIDlet'en for mobiltelefonen tok vi i bruk tilleggsAPI'ene:
Nokia NFC & RFID SDK 1.0,
Nokia Secure Chip SDK 1.0 og
Wireless Messaging 1.1 API (JSR-120),

Wireless Messaging API 1.1 er nødvendig for å motta og sende SMS. Når en SMS kommer på telefonen sjekker den UDH (User Data Header) for å se hvilken port meldingen skal rutes til. Vi har valgt at alle meldinger som kommer på port 45454 skal rutes til MIDlet'en. Dette settes i et register kalt push registry.
Dette starter automatisk MIDlet'en. Meldingen blir så lest av MIDlet'en for så å bli skrevet til SmartMx. Det er Nokia Secure Chip SDK som gjør det mulig å skrive til (og lese fra) SmartMX.

SMS

Header	User Data Header	Message

At meldingen rutes til en gitt port gjør at brukeren ikke ser meldingen og dataene går rett til applikasjonen. Java på mobilen er sikkerhetsmessig sterkt, og for at brukere ikke skal skade innholdet på mobilen ved uhell og at den skal være vanskeligere å åpne/hacke seg inn i for uvedkommende er det ekstra sikkerhetsforanstaltninger. Dette gjør at når brukeren får en melding må han bekrefte at applikasjonen får lov å åpne meldingen. Dette er en fin mekanisme fordi brukeren får kontroll, men dersom avsenderen (sikkerhetsselskap, teleoperatør og lignende) er betrodd bør det være unødvendig.

Sun NetBeans 4.1

NetBeans er et Java IDE (Integrated Developement Environment) fra Sun. Dette er en programpakke bestående av teksteditor, compilator og flere verktøy man trenger under en utviklingssesjon. De fleste elementene man trenger blir inkludert under ett og mye blir automatisert, i tillegg kan mye ”tegnes” (spesielt brukergrensesnitt) istedenfor å kodes. Dette gjør at utvikleren kan konsentrere seg mer om funksjonalitet og spare tid.

For å utvikle mobilapplikasjonen brukte jeg NetBeans, men la også til **J2ME Wireless Toolkit** 2.2 som er en utvidelse av J2ME for utvikling av Java på trådløse (mobile) enheter. Spesielt nyttig her er telefonemulatorene som følger med. Denne støtter virtuelle sms.

Det ble også utviklet en applikasjon som simulerte en NFC dørlås. Denne ble og til i NetBeans,

Figure 5-4 Simulering av NFC-lås

IBM Eclipse og IBM JCOP tools 3.1 plug-in

For å utvikle Java Card applikasjoner for SmartMx (smartkort) har Nokia valgt å ta i bruk IBM JCOP tools (Java Card Open Platform), dermed er dokumentasjonen fra Nokia basert på

dette valget. JCOP tools lar brukeren utvikle blant annet Java Card applikasjoner for er et JavaCard operativsystemet. Dette for å lese fra og skrive til MiFare emuleringen.

Eclipse er i likhet med NetBeans et IDE for Java, men siden IBM utvikler JCOP tools kjører dette verktøyet kun på IBM's Eclipse.
For ikke å gjøre situasjonen vanskeligere enn nødvendig ble både NetBeans og Eclipse benyttet.

Vi baserte vår JavaCard applikasjon på en implementering (SimpleJetZ) skrevet av Myksvoll, ekstern veileder. I denne definerer du a og b nøkkel og kan lese og skrive data til valgte blokker på MiFare emuleringen på SmartMx.

Implementeringen er forsøkt å gjøres så robust som mulig, med "try og catch statements", avbruddshåndtering, tråder og god Java-praksis.

Til tross for dette dukket det opp problemer. Et av disse var blant annet at det tok 0,5 – 1,5 sekunder for applikasjonen å sjekke at NFC dekslet var kolet til mobilen. At dette i tillegg skjedde i en usynkronisert tråd gjorde feilen vanskelig å finne.
Et annet problem var hvordan applikasjonen oppfører seg når den blir grundig utprøvd, for eksempel hva skjer når mobiltelefonen blir sveipet altfor raskt over NFC-leseren eller blir liggende der? Disse scenarioene ble oppdaget i en tidlig demonstrasjon og måtte adresseres.

5.5 Oppsummering

Prototypen virker tilfredsstillende og har blitt vist blant annet for Telenor, Movation og DailerChrysler. Vi får sendt elektroniske nøkler via sms og webgrensesnittet til telefonen og de kan benyttes i en NFC-lås simulering. Mange verktøy må samarbeide og problemer som dukker opp underveis må håndteres.

6 Resultat

I dette kapitlet sies det litt om hva vi fant ut i løpet av oppgaveperioden, basert både på prototypen, erfaringer og imperiske undersøkelser.

6.1 Scenario

I designfasen eksperimenterte vi med forskjellige løsninger. Spesielt var vi usikre på om vi skulle gå for en servertilknyttet eller frittstående lås (se for øvrig figur 5.2). En servertilknyttet løsning er mer dynamisk og byr på flere fordeler:
- Server har alltid nøyaktig oversikt over hvem som har tilgang og hvilke tidspunkt.
- Man kan lagre bare en identitetskode på mobiltelefonen, istedenfor strenger med hvilke spesifikke låse/dører man har tilgang til og i hvilket tidsrom. En sms har begrenset antall tegn den kan sende (134 – 160 tegn avhengig av formatering), derfor er det en fordel jo mindre data som sendes.
- Besøkende som kommer uanmeldt kan holde sin ”uautoriserte” telefon mot låsen, personen han eller hun vil besøke får så en sms fra serveren som bekreftes elles avkreftes direkte.
- Alt kan logges, fra SMS’er som blir sendt, til hvem gir hvem tilgang, hvem som har tilgang når og når folk kommer og går.
- Personen som får besøk/har gitt en gjest tilgang kan få beskjed via sms, instant message eller lignende når gjesten ankommer bygningen.

Den frittstående versjonen har også sine fordeler. Skal man implementere låsen på ett bygg uten mulighet for å servertilkobling, på hytta eller i en bil er det ikke mulig å basere seg på servertilknytning. Her trenger vi en lås som kan ta avgjørelsene selv.
Denne låsen trenger en innebygd klokke og en applikasjon som kan gjenkjenne data den får fra telefonen. Dette scenarioet krever at hvilken lås og hvilket intervall man har tilgang er lagret i telefonen.

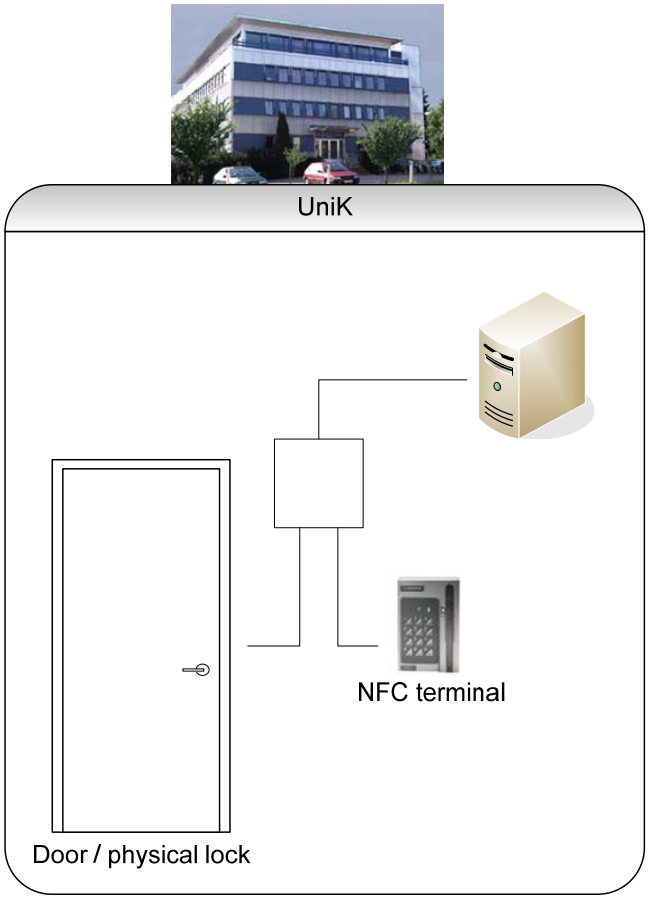


Figure 6-1 UniK NFC-lås konsepttegning

I tillegg til disse to forskjellige løsningene finnes det også en hybrid, en løst servertilknyttet, enkeltstående lås. Magnetkort- og pinbaserte låser er i dag ofte av denne typen. De er tilknyttet en sentral enhet (kan være en PC-server) og en strømkilde (oftest batteri). Serveren sender oppdateringer til låsen når det trengs og låsen tar seg av adgangskontrollen basert på siste oppdatering.

Område	**Scenario I**	**Scenario II**
Privat bolig	X	X
Hytte		X
Bedrift	X	
Bil		X
Betaling (VISA, direkte)	X	
Betaling (ladekort, kreditt)		X

Figure 6-2 viser hvor de forskjellige scenarioene passer

Etter møter, diskusjoner og nyoppdaget innsikt gikk vi mer bort fra kun hjemmetilgang (”home access”) hvor låsen var tilknyttet en tjener som tok avgjørelsene over til en frittstående modell. Et telefonintervju med Trioving [16] opplyser at de fleste låsesystemer ikke kan være avhengige av konstant tjenerforbindelse, det er også dyrt og krever mye administrasjon. Derfor er det vanlig med enten frittstående låser eller tjenertilknyttede låser som kun får oppdateringer iblant. Dette har blitt tatt til følge og lås-implementeringen er derfor frittstående og vi har gått bort fra hjemmetjener.

Når det gjelder betaling og billetteringssystemer vil hvilket scenario som passer være avhengig av om transaksjonen belastes direkte eller om det er et kredittkjøp (inkludert ladekonto på enheten), om det er et småbeløp eller en høykostnadshandel.

SMS kommunikasjon med SIM-kortet

I oppgavebeskrivelsen står det at SMS skal kommunisere med SIM-kortet. Det er flere patentsøknader på området og forskningsprosjekt som undersøker muligheter. Det er teleoperatørene som eier og har kontroll over SIM-kortene. Disse brukes i dag til å lagre brukerinformasjon, telefonnumre og annen telefon/abonnementsrelevant informasjon, ikke brukerdefinert informasjon. Dette gjorde det umulig for å oss å kommunisere med SIM-kortet. Ettersom SIM-kortet er et vanlig smartkort (om enn mindre enn den vanlig kredittkortstørrelsen) og vi fikk tilgang på en mobiltelefon med smartkortet SmartMx regner vi dette for en fullgod erstatning. Alt som implementeres på SmartMx kan i fremtiden implementeres og installeres av teleoperatører (eventuelt andre betrodde tredjeparts selskap).

6.2 Styrker og svakheter ved implementeringen

En av de største styrkene og årsak til at teknologien, og løsninger lignende på implementeringen vår, vil bli en suksess er det fysiske grensesnittet.
NFC blir betegnet det nye håndtrykket.
Alt man trenger blir overført gjennom lufta fra en pålitelig mellommann, dermed er man autentisert til å foreta betaling, kjøre buss og komme seg inn på møtelokalet kun ved å holde mobiltelefonen opp foran terminalen.

Selv om implementering fungerer er det flere ting som kan forbedres og nye muligheter dukker opp i løpet av såpass kort tid at det bør være inkludert i en fremtidig løsning.

Mobiltelefonen Nokia 3220 var den eneste tilgjengelig telefonen med NFC og SmartMx da vi startet implementeringen. Denne er en svært enkel telefon etter dagens standard. Vi kunne ikke hente ut verken telefonnummer, IMEI (unikt telefonID) eller IMSI (unikt SIM-kortID). Flere telefoner kan utlever IMSI til Java Applikasjonen. En ekstra sikkerhetsmekanisme kunne vært å kryptere tekstmeldingene med IMSI som nøkkel. Dette hadde gjort at kun riktig mottaker hadde fått avkodet den.

Implementeringen benytter seg av et forhåndsdefiner portnummer, 45454, i tekstmeldingen. Det er usannsynlig, men dersom en annen MIDlet installeres på telefonen som benytter samme portnummer vil den sist installerte MIDlet'en få forkjørsrett. Når man programmerer MIDlet'er har man et manifest som er en ren tekstfil. Det vil være mulig å dynamisk tildele et portnummer ved å bytte ut en variabel i manifestet ved installasjon dersom man har tilgang på Over The Air Provisioning (OTA). OTA vil si å installere MIDlet over telenettet.

Teleoperatører liker å installere programvare og forhåndskonfigurere nye mobiltelefoner. Dette er som regel en god ide, da oppsett av GPRS, MMS og epost kan være vanskelig. Dette er en god ide også med en NFC applikasjon, men også OTA vil være praktisk. Dette skjer uten at bruker trenger å sette opp parametere. Tilleggsfunksjonalitet kan installeres sømløst ved behov.

Mange flere funksjoner kan implementeres ved å utvide databasen:

- Forskjellige soner/gruppering av låser basert.
- Forskjellige brukere har forskjellige låser/soner og tidspunkt de kan gi gjester tilgang.
- Forskjellige profiler. For eksempel engangsbesøkende, tilbakevendende.
- Forskjellige brukergrupper: privatperson, hjemmehjelp, hotell, danskebåten, politi.
- Forskjellige sikkerhetspolitikk. Noen låser kan for eksempel kreve PIN i tillegg til eNøkkel. Forskjellige tjenester kan ha tilleggskrav til autentisering.
- Utveksle autentisert (PKI – telenor) personlig info, velg selv hvilke relevante (navn,adr,alder osv.) du vil gi fra deg ved hjelp av for eksempel en MIDlet.

For at implementeringen skal være fremtidsrettet må den kunne sameksistere med andre systemer som etablerer seg i markedet, for eksempel Sporveiens Flexuskort og MasterCard sitt PayPass. Disse kontaktløse smartkortene er av samme standard (ISO 14443). Minneområdet på SmartMx chipen kan deles opp og blir aktørene enige om en plattform for dynamisk tildeling kan man få mange funksjoner på samme mobiltelefon.

Philips har en mappestruktur kalt Application Directory (MAD) for MiFare. Starten av MiFare brikken blir holdt av til pekere for hvor applikasjoner og dataområder befinner seg. Dermed hentes data fra riktig mappe.

Dersom implementeringen opererer i et tjenertilknyttet scenario kan brukeren motta en tekstmelding når gjesten ankommer. Er det snakk om hjemmetilgang kan man for eksempel få beskjed om at rørleggeren har kommet og beskjed når han drar igjen.

Tekstmeldinger kan også brukes til å gi tilbakemeldinger dersom noe er galt i større grad enn i dag. Man kan også få beskjed dersom en gjest er registrert og akkurat har sveipet mobiltelefonen over NFC-låsen, men ikke har tilgang. En mulighet da er at man rett og slett skriver en melding med ja eller nei for å gi gjesten tilgang på direkten.

6.3 Skaleringsspørsmål og flaskehalser

Det er ingen flaskehalser som fort blir trange i systemet. På serversiden bruker vi en database- og webserviceserver med MySql som databasemotor og programvare fra Apache til webservices og html. Denne serveren er ikke avhengig av bredbånd med høy kapasitet, da den bare behandler webservices og databasetjenester når nye brukere legges inn, gis tilgang og så videre. Det vil tilsi at det er lite trafikk, i forhold til dagens prosessor- og linjekraft.

Det som imidlertid må utbedres før utrulling er databasestrukturen, som er relativt enkel i dag. Denne må støtte multiple administratorer (”tilgangsgivere”) og de forskjellige tilgangsgiverne må kunne ha forskjellige låser og områder de råder over.
Dermed må også flere, mer avanserte administreringsverktøy implementeres.

7 Drøfting

Vi valgte den mest mulig realistiske løsningen ut fra forutsetningene vi ble presentert.
For å belyse elektronisk nøkkel i mobiltelefonen har det vært hensiktsmessig å se på kontaktløs betaling og forskjellig bruk av smartkort. Disse funksjonene har vært markedet og har vært forsket på, setter vi de sammen kan vi trekke paralleller og konklusjoner om elektronisk nøkkel i mobiltelefonen.

”Mobiltelefonen vil bli lommeboka, nøkkelknippet og identifikasjonen din,” sier Ron Hamma [15], Motorola

7.1 Med nøkkelen i mobilen

Det finnes flere fordeler ved å ha en nøkkel elektronisk lagret på en mobiltelefon. Noen ulemper finnes nok også, men mye gjøres for å redusere innvirkningen deres.

Å kunne ha med seg kun mobiltelefonen sin, uansett hva du skal hele dagen, må for mange være en lettelse. ”Folk er åpenbart knyttet til mobilen sin og har den med seg hele tida” [8]
Fra før har man kalender, notater, påminnelser, kamera og musikk integrert.
Snart vil også nøklene kunne ligge i mobiltelefonen, sammen med idkort, bankkort, trikkekort, bonuskort, medlemskort, kvitteringer, alt du har i lommeboken i dag.
”Mobilen vil sannsynligvis i nær fremtid bli vår ”personlige tillits-enhet” å foretrekke og en kraftig elektronisk lommebok.” [8]

7.2 Andre løsninger

Smartkort basert betaling

Første skritt i riktig retning for NFC skjer i disse dager. Smartkort skal ut til massene, driveren er bankene, med Europay, Mastercard og Visa (EMV) i spissen. Teknologien har

foreligget lenge (smartkort i stor skala siden 1990-tallet), men på grunn av de store kostnadene det medfører å innføre nye systemer tar slikt tid. Nå har imidlertid kortsvindelen nådd nye høyder og i 2005 ble norske kunder svindlet for 160 millioner kroner [19], noe som motiverer og påskynder betalingsaktørene.
Det er såkalt ”skimming,” som vil si avlesning av betalingskort i minibanker eller manuell avlesning, samt korttyveri som er de største årsakene.
Der det tradisjonelle magnetkortet kan leses rett av uten noen form for sikkerhetsforanstaltninger, støtter smartkortet flere [20]:

- Applikasjonene på smartkortet kan ta avgjørelser
- Kryptering: Triple-DES, SHA og RSA med nøkkellengde på 1024 og 1152 bit
- Public Key Infrastrukture
- PIN-koder (4 – 12 tegn) kan brukes både mot terminalen og smartkortet
- Signatur og biometriske data kan lagres i kortet

Dette kan gjøre betalingskortet i praksis uavlesbart og skimming blir umuliggjort, samtidig skal manuell belastning med signatur reduseres.

Betalingskortsvindel blir ofte knyttet til organisert kriminalitet [19]. I 2004 innførte Malaysia EMV som førte til en voldsom reduksjon i kortsvindel [21], som igjen fører til mindre erstatninger for bankene å punge ut.

Tester utført på McDonalds i Dallas og New York [15] med kontaktløskort betaling viste at betaling tok 6 sekunder mindre i forhold til betalingskort og 12 – 18 raskere enn med kontanter. Betaling er alltid tilgjengelig (hvis vi går ut fra at forbrukeren nesten alltid bærer mobiltelefonen med seg [8]), dette vil kunne øke salg for forhandlere.
Dette bør være gode motiver for å rulle ut smartkortbasert og mobilbasert handel.

Alle sikkerhetsfordelene på smartkort kommer også NFC-mobiltelefonen til gode, enten man bruker SIM-kortet eller en SmartMx brikke. Disse er fullverdige smartkort.

Avhengig av tjeneste vil man kunne bruke teleoperatøren over GSM eller banken, tjenestespesifikke partnere eller lignende over mobilens internettilkobling som en sikker tredjepart ved PKI-baserte transaksjoner. Mobilbetaling vil selvsagt også kunne benytte kredittkortselskapenes nett slik BBS og Visa gjør idag.

Her går bankene eller kortselskapene gode for identiteten, teleoperatøren blir unødvendig. Sikkerheten er dessuten bedre på lukkede nett enn mobilt internett.
All trafikk som benytter teleoperatørenes nett koster penger, derfor vil terminaler med nettilknytning være billigere. Alan Goode i Juniper Research er bekymret for at dette gjør mottagelsen av NFC-telefonen lunken blant teleoperatørene [9]. Det er imidlertid flere store teleoperatører blant medlemmene i NFC Forum, dermed fremstår de mer som drivere enn tilbakeholdne aktører.

Alle funksjoner man måtte ha på betalingskortene til EMV er mulig å implementere i SIM-kortet på en mobiltelefon, men man trenger bare en sikker måte å overføre dataene kontaktløst til terminalpunktene. Her vil det være naturlig å benytte seg av NFC. MasterCard og Visa som er driverne for smartkort er også de største sponsorene i NFC Forum. NFC-mobilen kan også dra nytte av den godt etablerte smartkort infrastrukturen (Sony alene har solgt 52 millioner smartkort på verdensbasis). Alt som trengs er å implementere NFC-funksjonalitet i terminalene.

Elektronisk lommebok på mobilen

Det finnes allerede løsninger for betaling med mobilen. De fleste av disse løsningene er ganske upraktiske og dermed ikke blitt tatt i bruk i noen større skala. Å betale for cola i få, utvalgte brusautomater med SMS og å kjøpe flybillett over WAP/GPRS er to eksempler på hva Telenor Mobilhandel gjør deg i stand til. Du vil da enten bli trukket fra en ladekonto knyttet til mobilabonnementet, belastet Visa-kortet eller få summen ført opp på mobilregningen (denne muligheten er avsluttet). Disse betalingsløsningene er for så vidt greie. Det er selv handelen som er treg, dyr og lite intuitiv.

Å surfe på internett og ”shoppe” med mobiltelefon kan være en ugrei affære med liten skrift, små bilder, vanskelig navigering og treg overføring, i tillegg til at det koster en del å være oppkoblet. Dette bekrefter Hanne Sjursen, direktør for Mobile Commerce hos Telenor, i en artikkel på digi.no [17]. Hun sier imidlertid hun at hun har tro på ”tjenester som dekker behov i situasjoner hvor man ikke sitter foran en PC.”

Den andre løsningen for lommebok på mobilen, ”SMS-handel,” foregår eksempelvis ved at man ser en brusautomat og lar seg friste. For å utføre handlene sender man en SMS ”cola123” til 20554. Brusen faller ut når meldingen er behandlet og godkjent. Dette vil sannsynligvis ta like lang eller lengre tid enn å kjøpe brus i en kiosk, dersom det ikke er kø, i tillegg at du må betale for tekstmeldingen.
Av dette kan man trekke slutninger som at mobilhandel ikke kan erstatte netthandel, men kan være nyttig når forbrukeren er mobil, travel eller har gått fra lommeboka.
Mobilhandel blir i dag brukt nesten utelukkende til å fylle på kontantkort.

NFC integrert på SIM-kortet.

Fra tjenestetilbyderes synspunkt vil problemer og ulemper løses ved å bygge NFC og SmartMx (eller kompatibel funksjonalitet) inn i SIM-kortet. SIM-kortet er rett og slett et smartkort som teleoperatøren har full kontroll over. Det inneholder et unikt identifikasjonsnummer som er direkte knyttet til bruker. Telefoneieren får inntrykk av at han eier SIM-kortet og informasjonen på det, spesielt kanskje siden teleoperatørene gir kundene adgang til å lagre kontaktinformasjon, telefonnumre og meldinger. Det er imidlertid teleoperatørene som sitter med full tilgang til kortet (over GSM-nettet). De kan legge til, endre og slette informasjon og applikasjoner. Dette kan gjøres uten å hefte forbruker når han ber om tilleggsfunksjonalitet.
Her er imidlertid tredjeparts aktører som tilbyr tjenester avhengig av å samarbeide med teleoperatørene, enten må de få tilgangskoder til områder på SIM-kortet eller mer sannsynlig la teleoperatørene legge inn applikasjonene for dem.
Sømløs autentisering via IMSI av teleoperatøren vil være grunnlaget for mange av tjenestene. At kun teleoperatøren har tilgang til dataene hindrer menigmann fra å slette, endre eller ødelegge sensitive data.
Når dataene ligger i SIM-kortet vil det være enkelt å sperre tilgangen til tjenestene dersom telefonen blir stjålet. Har man sperret SIM-kortet er alle tjenestene sperret.

SIM-kortet er langt fra fullt utnyttet i telefonen, og det finnes også mye større SIM-kort enn de vanlige som er i bruk. SIM-kort med kapasitet på 512MB (MegaSim, mot 64KB som er vanlig) finnes allerede, dessuten har kortet kommunikasjonspinner som ikke er tatt i bruk. Disse pinnene kunne vært brukt til en NFC-antenne.

SIM-kortet forskes på av store aktører i både Europa, Asia og Amerika. Et firma i Asia tilbyr allerede et såkalt MegaSim og NFC, men per i dag er de fortsatt ikke kombinert i samme komponent.

SIM-kortet vil også kunne være en god frittstående identitetstilbyder for PDA, PC og en hvilken som helst elektronisk enhet. Teleoperatør er en sikker identitetstilbyder og kan autentisere uansett hvor man er, stasjonær eller mobil.

7.3 Sikkerhet

Sikkerhetstrusler mot NFC-mobilen har blitt diskutert tidligere i dette kapitlet og kapittel 3 og 4. Robin Simpson, Gartner's directør for mobilforskning [13] sier at sikkerheten må være i høysetet i prosjekter som involverer NFC teknologi. Flerfaktors autentifisering bør alltid være til stedet i applikasjoner.
I avsnittet som omhandler betaling med smartkort vises at kryptering av data, PIN-kode og PKI gir sikkerhet god nok for aktører som Visa og MasterCard.

Avlytting av radiobølger vil alltid kunne være en trussel mot NFC-kommunikasjon. Radiobølger er sensitive for avlytting. Man sender radiobølger gjennom lufta og dermed er det fritt for alle i nærheten av sender å avlytte disse uten at sender og mottaker vet om det og hvem som gjør det. Det er relativt enkelt og kan gjøres over store avstander (avhengig av bølgelengde og signalstyrke). Sensitiv informasjon kan komme på avveie uten at man i det hele tatt vet om det. Dette har ført til at RFID har fått et litt frynsete rykte. Frykten gjelder spesielt der RFID blir tatt i bruk i pass, på ID-kort og lignende hvor personlig informasjon er lagret eller gjør det mulig å stjele identitet, overvåke eller forfølge personen. Et eksempel på dette er det nye amerikanske passet med en RFID-brikke med personlig og biometrisk informasjon: fullt navn, personnummer og bilde. Dette var mulig å avlese på 10 meters avstand. Passet skulle vært tatt i bruk i mars 2005, men ble utsatt til en ny utgreiing er gjennomført. De vil fortsatt bruke RFID-brikker i passene, men nå snakker man om flere former for "anti-avlytting". Selv om RFID-brikker lar seg kryptere og informasjonen tilsynelatende er uleselig, er sannsynligheten til stedet for at noen kan klare å bryte denne.

Når det gjelder NFC er dette sikret mot avlytting først og frem ved en maksimal operasjonsdistanse på 10 cm. Implementeringen viste at denne i praksis var 0 – 4 cm. I tillegg kommer de vanlige sikkerhetsmekanismer til smartkortet: kryptering, samt lese- og skrivenøkler. Dersom noen skulle få lest noe av radiotrafikken, vil det være helt uleselig.

En tilleggstrussel, dersom ikke passet hadde blitt gjort noe med, er muligheten for terrorister å gjenkjenne vestlige lands statsborgere. Det er Amerika og Vesten som planlegger å ta i bruk RFID-pass i første omgang, dermed er det for ekstreme motstandere av disse landene rett og slett bare å skanne kafeer, hoteller og lignende etter RFID-pass generelt og de kan finne mål for sine handlinger. De trenger ikke bry seg om å knekke krypteringen på passene.

Folk liker ikke å føle seg overvåket. Gillette gjorde et forsøk med å legge RFID-brikker i barberbladpakningene og RFID-lesere ved kassene. I noen butikker var det i tillegg installert kameraer som tok bilde av kundene både når de forsynte seg i hylla og når de betalte i kassa og automatisk sjekket hvem som betalte for seg. Bildene ble overført til en PC i butikken og de ansatte kunne sjekke bildene. Her har konsumentene ingen kontroll over hvor RFID-lesere er skjult og hvordan bildene blir brukt. Det er mulig å overvåke en person ved hjelp av RFID-lesere koblet opp mot en tjener eller et nettverk, eller med en håndholdt RFID-leser. Dette forsøket førte til store protester.

Timo Arnall [7] sier i et intervju til Digi.no at NFC er RFID uten RFID sine problemer. Videre forteller han at NFC skal gi RFID uten personvernproblemer og reklame som ikke kan trenge seg på deg. NFC er nemlig veldig sikkert med hensyn på avlytting, man må for det første helt inntil enheten man skal kommunisere med. Det virker fort mistenkelig når noen er i umiddelbar nærhet av noe de ikke skal. Man ser også personen det dreier seg om fordi han eller hun må være fysisk tilstedet. Dette hadde ikke vært slik dersom NFC på bærbare PC'er, pda'er og mobiler ikke kunne skrues av og på. Da ville man vært sårbar også for lesere som var montert og ikke kunne sees. NFC-brukere kan velge når og hvor de vil være tilgjenglige, er man usikker deaktiverer man rett og slett NFC.

Når man sammenligner NFC betalingstjenester med andre konvensjonelle betalingsmetoder er det betalingskortet NFC først vil erstatte. Når du bruker en minibank og tar ut penger, trenger du både det håndfaste kortet og en personlig kode, mens betaler du varer på internett trenger du kun kortinfoen. Midt i mellom disse har du såkalt manuell betaling med kort, hvor kortets

sifre trykkes over på en kvittering. Ved bruk av NFC vil man kunne minske faren for misbruk og tyveri i hvert fall i to av tilfellene. I det siste tilfellet, manuell betaling med kort, vil man, når man bruker NFC, ikke trenge å gi fra seg noe fysisk (Visa, Mastercard etc.) som kan skrives av og misbrukes. I tillegg kan det implementeres at man må taste inn beløp og pin-kode for å godkjenne betalingen. Å kjøpe varer på nett, bruke nettbank og lignende kan sikres ved at man må holde mobilen sin opp mot terminalen for godkjenning. Dette gjør de to siste betalingsscenarioene like sikre som minibanken, du må ha en fysisk enhet som beviser hvem du er, pin-kode kan implementeres, du slipper å stole på at andre (ukjente) er ærlige og identitet, konto og lignende kan sjekkes mot en database.

Informasjonen på NFC-telefonen eller NFC-enheten beholdes i enheten og kun det som er nødvendig å sende blir sendt. Informasjonen vil bli lagret på sikre områder, som i en secure chip eller i SIM-kortet. I tillegg vil informasjonen som blir sendt være kryptert, slik at den er uleselig for andre enn den tiltenkte mottakeren. Dette er de tunge, grunnleggende sikkerhetstiltakene.
Det er også, som nevnt tidligere, mulighet for pinkode. Den typiske pinkoden med fire siffer har 10 000 muligheter, mens på mobilen trenger ikke koden å bestå kun av tall. Passord kan være av variabel lengde, bestående av tall og små og store bokstaver, eller til og med engangspassord. Dette gir tilnærmet uendelige passord muligheter.

7.4 Suksessgrunnlag

For at mobil betaling og mobil nøkkel skal bli en suksess holder det ikke at det finnes og er tilgjengelig. Det må bli akseptert og føles praktisk av forbrukerne. Akseptanse fremmes gjennom brukervennlighet, kostnad, anvendelighet, tillit, mobilitet og uttrykksfullhet/uttrykksmulighet påstår Zmijewska [25]. Videre sier hun at det er brukeren som bestemmer om et nytt betalingssystem blir tatt i bruk eller ikke, derfor kan ikke ny løsninger bli evaluert kun på bakgrunn av tekniske spesifikasjoner. Uttrykksmuligheter gjelder i mindre grad m-betaling/nøkkel, da dette går på muligheten for å uttrykk sin personlighet, mote og å tilpasse applikasjonen/enheten.

David Chamberlain (analytiker i InStat, market research firm) sier at forbrukerne må støtte teknologien og funksjonene som fremmes [9]. Fremmed teknologi er avskrekkende.

At mange oppfatter NFC som RFID kan få negativ innvirkning. RFID har hos noen et frynsete rykte. Dersom ”vanlige” enheter som mobiltelefon, TV, PC og lignende får NFC muligheter vil det være en driver for teknologien.
Med NFC og smartkort på telefonen har du ikke bare et trådløst smartkort, men kan kombinere det med funksjonaliteten som finnes på telefonen (GSM, internett, inntastings- og skjermsvisningsgrensesnitt) i tillegg til det smartkortspesifikke. Dette gir muligheter som å vise kontosaldo, kjøpshistorie, når den elektroniske nøkkelen er gyldig og så videre. Mobilen er en veldig personlig enhet man føler seg komfortabel med.

Under er en oversikt hvor fornuftig forskjellige trådløse teknologier er å bruke i transaksjoner som betaling, som kollektivbillettsystem og lignende [25].

GSM	GSM er for tregt. Man må ringe opp, bli ringt opp, eller benytte SMS for å forta transaksjoner. Brukers betalingsinformasjon må være forhåndsregistrert. Nytteverdien kommer av at man ikke trenger å ha med penger og kort, kun mobil (denne fordelen gjelder for øvrig alle teknologivalgene).
Infrarød	Infrarød ble blant andre prøvd av Visa. Infrarød overføring er mindre praktisk enn NFC siden man må peke rett mot terminalen. Infrarød er imidlertid finnes på så godt som alle mobiltelefoner. Gir tillit på grunn av den korte rekkevidde.
Blåtann	Blåtann er mer avansert og tungt å bruke enn NFC, infrarød og GSM. Blåtann er heller ikke kjent for tillit (Blåtann-jacking er et kjent fenomen). Blåtann bruker mye batteri hvis slått på. Terminalene er dyre. En fordel er at Blåtann har lenger rekkevidde og kan gå gjennom vegger. Dette er imidlertid et tveegget sverd, da å kunne se terminalen og vite at overføringen ikke kan avlyttes skaper tillit.
NFC	NFC er den enkleste i bruk (like lett som berøring) Sikkerheten er meget godt ivaretatt. Et forsøk med PayPass konkluderte med at å betale med en NFC mobiltelefon er gjennomsnittlig 6 sekunder raskere enn med kort [26]. NFC-terminaler er billige i forhold til Blåtann.

Det er NFC som blir dratt frem som allsidig mest brukervennlig, anvendelig, tillitsvekkende, mobil og kostnadseffektiv.

8 Konklusjon

NFC er en kontaktløs protokoll, bygget med tanke på brukervennlighet og sikkerhet. Denne kontaktløse kommunikasjonsteknologien åpner for forenkling, fleksibilitet og mobilitet i hverdagen der vi vanligvis ville benyttet fysiske media som magnetkort og nøkler. NFC vil også kunne starte opp andre kommunikasjonsprotokoller, som Blåtann og Wi-Fi, mellom enheter uten noen form for oppsett.

Brukervennlighet, praktisk verdi og sikkerhet er blant de viktigste kriteriene for at nyvinninger av dette slaget skal bli godtatt av allmennheten.
Gjennom å studere andres forskning og prototypen mener jeg å vise at dette er innfridd.

Prototypen er unik i det at den mottar en elektronisk nøkkel gjennom tekstmelding. Å bruke smartkort (både kontaktløst og med fysisk grensesnitt) som nøkkel er innført og regnet for sikkert, men her må kort og kode lagres på forhånd. Sikkerheten til prototypen er ivaretatt på tjener, sending og mobiltelefonen, samtidig som du har denne fleksibiliteten. Man kan på direkten gi eller frata gjester tilgang til huset/kontoret sitt eller få sperret betalingsmuligheter og lignende.

Det er mobiltelefonen som ventes å bli den største driveren for NFC. Stadig mer får plass i den lille mobiltelefonen vi alltid har med oss. Funksjonalitet som elektronisk nøkkel (over SMS eller GSM), betalingskort og identifikasjon krever alle grundig sikkerhet, men allerede begynner dette å bli tatt i bruk av seriøse aktører. Gartner og Det spås av om 3 – 4 år vil 33 – 50% av alle nye mobiltelefoner leveres med NFC.

ABI Research tror at kontaktløs betaling blir en suksess, den største utfordringen ligger i at svært få telefoner har NFC og smartkort implementert i dag.
Så fort flere kommer på banen med NFC telefoner og flere applikasjoner tas i bruk, er det mye som taler for suksess.

9 Kilde henvisninger

[1] NFC whitepaper

http://www.ecma-international.org/activities/Communications/2004tg19-001.pdf

[2] ABIresearch

http://www.abiresearch.com/home.jsp

[3] "Nokia, Philips and German Public Transport Network Operator RMV trial NFC for ticketing", November 02, 2004

http://press.nokia.com/PR/200411/966921_5.html

[4] "Personal Area Networks: near-field intrabody communication - MIT Media Lab"

Sept-Dec, 1996, Thomas G. Zimmerman

http://www.findarticles.com/p/articles/mi_m0ISJ/is_n3-4_v35/ai_18891266

[5] "NFC Gets Closer", Suzanne Deffree, *Electronic News*, 3/18/2005

http://www.reed-electronics.com/electronicnews/article/CA511172.html

[6] RFID

Wikipedia

http://en.wikipedia.org/wiki/Rfid

[7] "NFC: Kreativ RFID for folk flest", Jonas Blich Bakken, 01.09.2005

http://www.digi.no/php/art.php?id=264040

[8] "Personal Trust Space and Devices: Geography will not be history"

C. Adams and P. Millard, 2003

[9] "Is Near-Field Communication Close to Success?"

Sixto Ortiz Jr., for the IEEE Computer Society.

[10] "Analysis of Using Java Card for DRM Master Key Security"

J. Buford, R. Kumar, IEEE Communications Society, 2005

[11] "Using Smart Cards as a Secure Storgage for Digitally Signed Documents"

M. Trampus, M. Ciglaric, m.fl., IEEE, 2003

[12] "Using Smart Phones to Access Site-Specific Services"

E. Toye, R. Sharp m.fl., 2005, www.computer.org/pervasive

[13] "Taipei commuters to make secure payments"

Vivian Yeo, juli 2005

http://www.zdnetasia.com/news/communications/0,39044192,39243420,00.htm

[14] "Mye mer lagringsplass i SIM-kortet"

http://www.digi.no/php/art.php?id=292720

[15] ” Motorola Tests M-Commerce “

Ed Dodds, oktober 2004

http://www.oasis-open.org/archives/ihc/200410/msg00017.html

[16] Telefonintervju med Trioving

Haakon Eikenes, juni 2006

[17] ”Suksess og fiasko for mobilhandel”

Einar Ryvarden, mai 2005

http://www.digi.no/php/art.php?id=114651

[18] NFC for payment and ticketing,

http://www.nokia.com

[19] ”Bankene satser på nytt kort”

Dagbladet 20 juli 2006, side 25 – 27.

[20] ”Smart card for payment systems”

Thales

http://www.thales-esecurity.com/Whitepapers/documents/Smart_cards_for_payment_systems.pdf

[21] Smart card

http://www.wikipedia.org

[22] “Close encounter of the magnetic kind”

mai 2005, Christine Evans-Pughe

[23] “An Architecture for the Management of Smart Cards by Mobile Devices Using Java Technologies”, T. K. Apostolopoulos, I. S. Kapetanakis, G. Oikonomou, IEEE CEC ’05, 2005

[24] “Security Issues of Emerging Smart Cards Fare Collection Application in Mass Transit”, N. O. Attoh-Okine, L. D. Shen, IEEE, 1995

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

[26] “Motorola and MasterCard to Trial Contactless Mobile Payments”

Finextra, 2005

http://www.finextra.com/fullstory.asp?id?12684

10 Appendiks

A. Hvordan bruke implementeringen og SMS design

1. Registrere ny bruker
    a. Send SMS ”RFID REG THOMAS 92427222” til 2034
2. Opprett en tilgang for brukeren
    a. Send SMS “RFID 92427222 L1 120606 1200”
3. Hold mobiltelefonen foran NFC-terminalen på døra og gå inn

RFID er kodeordet 2034 eller PATS trenger for å bestemme at det er en RFID-key SMS.
REG er et kodeord for at UniK-serveren skal legge til en ny bruker i databasen.
Brukere blir gjenkjent av UniK-serveren både på brukernavn og telefonnr.
L1 … Lm er identifikasjonen på de forskjellige låsene. Dermed er det mulig å bruke en server på flere bygninger eller lage soner innenfor en bestemt bygning.

De forskjellige tilgangsmønstrene:

1. Tilgang fra dato og klokkeslett.
    a. Gir tilgang en time fra gitte klokkeslett på gitt dag.
2. Tilgang fra dato og klokkeslett til dato og klokkeslett.
3. Tilgang en spesifikk dato.
    a. Gir tilgang et helt døgn
4. Generell tilgang
    a. Gir tilgang et år
5. Ukedagbasert tilgang
    a. Gir tilgang bestemte dager og på gitte tidspunkt, for eksempel mandag – fredag 08:00 til 16:00.

De fleste av disse gir gjesten tilgang 5 minutter før det egentlige tidspunktet, dette for å neglisjere unøyaktige klokker og for at man skal være på plass på for eksempel møter i det de starter og ikke komme 2-3 minutter for sent.