Dagens Dobbel på mobiltelefon

Teknologier og problemstillinger ved design og utvikling av online betalingsspill på mobile enheter

Norsk Regnesentral
ANVENDT DATAFORSKNING
Norwegian Computing Center/Applied Research and Development

RAPPORT/REPORT

Rapport no 958

Ståle Heier

Juli 2000

Norsk Regnesentral
ANVENDT DATAFORSKNING

Rapport/Report

Tittel/Title: Dagens Dobbel på mobiltelefon.
Teknologier og problemstillinger ved design og utvikling av online betalingsspill på mobile enheter

Dato/Date: 13/7
År/Year: 2000
ISBN: 82-539-0462-2
Publikasjonsnr.: 958
Publication no.:

Forfatter/Author: Ståle Heier

Sammendrag/Abstract:

(Se eget avsnitt i rapporten)

Emneord/Keywords: Mobiltelefoni, WAP, Smartkort, Betalingsløsninger, Spill

Tilgjengelighet/Availability: Åpen

Prosjektnr./Project no.:

Satsningsfelt/Research field:

Antall sider/No. of pages: 119

Norsk Regnesentral / Norwegian Computing Center
Gaustadalléen 23, Postboks 114 Blindern, 0314 Oslo, Norway
Telefon 22 85 25 00, telefax 22 69 76 60

Forord

Denne oppgaven er levert til Cand. scient.-graden ved Institutt for Informatikk, Universitetet i Oslo, februar 2000.[1]

Jeg ønsker spesielt å takke min arbeidsgiver, Norsk Regnesentral ved Inger Vollstad og Riitta Hellman, som har latt meg gjøre denne oppgaven. Min veileder og inspirator har været forskningssjef Riitta Hellman. Internveileder ved IFI har vært Stein Gjessing. Takk skal dere ha alle sammen!

Flere personer har gitt av sin dyrebare tid og fortjener å bli nevnt, spesielt vil jeg takke Anund Lie, Thorstein Lunde og Torstein Strøm ved Norsk Regnesentral, Ingelin Drøpping og Stein Magne Sølna ved Telenor Mobil, Arild Enevoldsen og Roar Smidt ved Bull, Arnfinn Lindstad og Tore Holmberg ved Norsk Rikstoto, Eva Trasti ved Fellesdata, Stine Granviken ved Posten SDS og Do Van Thanh ved Ericsson.

”Hjemmefronten” fortjener også noen godord. Elisabeth har støttet og oppmuntret, og Hedda og Oda her virkelig anstrengt seg for å gi meg tid og ro. En stor takk til mine beste støttespillere!

Oslo, 1. februar 2000

Ståle Heier

[1] Det er foretatt mindre tilpasninger i denne NR-rapporten.

Sammendrag

I denne oppgaven har jeg sett på forutsetninger for bruk av mobile enheter i spill og betaling på Internett. Oppgaven har hatt et perspektiv på inntil to år frem i tid. Særlig betaling er viet oppmerksomhet, da enkle og sikre betalingstjenester er viktig for utbredelse og bruk av Internett-tjenester generelt, ikke bare spill. Oppgaven har tatt utgangspunkt i et spillescenario for å ha noe å relatere teknologier og tjenester til.

WAP-teknologien presenteres som ”limet” som vil muliggjøre betaling og spill-tjenester i nær fremtid. Per i dag er WAP-enheter bare såvidt nådd på markedet, og flere av standardene som er nødvendige for å realisere tjenestene er ennå ikke ferdig spesifisert. I dag realiseres WAP over GSMs linjesvitsjete datatjeneste, hvilket ikke er ideelt i forhold til WAPs pakkeorienterte natur. Pakketjenesten i GSM (SMS) er imidlertid beheftet med lange forsinkelser som gjør den uegnet som bærer for WAP. Nye bæretjenester spesifiseres i GSM fase 2+, og særlig GPRS vil tilfredsstille behovet for pakkesvitsjet kommunikasjon med båndbredde for begrenset multimedia en gang i år 2001.

Mobile enheter vil i denne oppgaven i praksis være mobiltelefoner, men behøver ikke være det. Mange andre enheter i forskjellige fasonger vil trolig være bedre egnet til spill enn den tradisjonelle mobiltelefonen. Forskjellige enheter presenteres og det argumenteres for at den tradisjonelle telefonen antakelig vil ha størst utbredelse på grunn av pris og allsidig funksjonalitet. En tjeneste som tenkes å nå ut til flest mulig bør fungere optimalt på denne enheten.

Smartkortfunksjonalitet er vesentlig for sikre betalings- og kommunikasjonsløs-ninger. Betalingsløsninger kan ikke realiseres uten smartkort. Med grunnlag i den sikkerheten som smartkort gir, kan man utvikle mobiltelefonen til et betalings-instrument for kredit-, debet- og småpengeløsninger. Oppgaven diskuterer fordeler og ulemper ved flere forskjellige betalingsmodeller i forhold til spill på Internett. Norsk lov vil trolig forhindre kredittløsninger, derfor synes særlig elektroniske kontanter og debetløsningen som interessante i spillsammenheng.

Handlingene rundt betaling ligger noe frem i tid, men handlingene er forsøkt beskre-vet og demonstrert i denne oppgaven. Båndbredden i dagens GSM-nett tillater ikke multimedia til mobile enheter, men oppgaven viser, ved empiriske studier, at animasjon ved hjelp av tegnbasert grafikk kan fungere tilfredsstillende. I mange til-feller kan tegnbasert grafikk antakelig være et godt alternativ til video.

Oppgaven diskuterer også flere forhold som en spilltilbyder må tenke igjennom, blant annet spill uten kundeforhold, autentisering og utbetaling av gevinst.

Innhold

1 Innledning

Dette kapittelet beskriver bakgrunnen for oppgaven. Problemstillingene klargjøres, og avgrensningene presenteres. Videre forklares den metodiske tilnærmingen som er brukt. For å kunne relatere stoffet i bakgrunnskapitlene (kapittel 2, 3, 4 og 5) til problemstillingene presenteres omrisset av et spillscenario. (Spillscenariet beskrives i detalj i kapittel 6). Til slutt presenteres oppgavens struktur. Leseren gis forhåpentligvis et godt utgangspunkt for å ta fatt på resten av oppgaven.

1.1 Bakgrunn

Da den digitale trådløse telekommunikasjonsstandarden GSM ble ”født” tidlig på 1990-tallet, ante man ikke at det skulle bli begynnelsen på en revolusjon innen bruk av trådløs teknologi. I dag kan man trygt si at utbredelsen av mobiltelefoni har overgått selv de mest optimistiske spådommer. Digitalisering av eteren, med det formål å skape en skalerbar standard for ”massene”, har hatt suksess, og utviklingen har fått en betydelig selvforsterkende massefart som ennå ikke viser svakhetstegn.

I dag, snart 10 år etter fødselen, knytter det seg fortsatt store forventninger til mulighetene som ligger i digital mobilteknologi. En rekke aktører, med mobiloperatørene og utstyrsleverandørene i spissen, kniver om å levere teknologi og tjenester i dette markedet. Ungdommen er en stor ny brukergruppe som har overrasket aktørene ved å være ivrige til å ta i bruk den nye teknologien.

Utviklingen og veksten innen mobilteknologi vil heretter ligge i utbygging av *datatjenester* – det vil si tjenester som ikke omfatter tale. På nettverkssiden har det i den senere tid vært usedvanlig mye ”oppstyr” rundt WAP, teknologien som skal gi ”Internett på mobiltelefonen”. WAP fremstilles nærmest ukritisk i pressen, og innholdsleverandører som ikke tilpasser seg WAP, levnes ikke mange sjanser.

Når WAP treffer markedet med full tyngde, trolig en gang i år 2000/2001, vil det kun være snakk om måneder før basisteknologien – transportmediet – for WAP er klart for utskiftning. Da kommer telekommunikasjonsaktørene med standarden GPRS som lover ti ganger høyere hastighet i eteren. På den trådløse horisont skimtes allerede UMTS som skal være en samlende standard med potensiale for multimedia levert til bærebare PC’er.

Uavhengig av utbredelsen av mobilteknologi skjer det en utbredelse av håndmaskiner, såkalte PDA’er, som også er overraskende. Håndmaskiner har eksistert i flere fasonger i mange år allerede, men det er først i den senere tid at håndmaskinen har fått et brukergrensesnitt som har gjort den praktisk anvendbar. Håndmaskinen får stadig kraftigere grafikk, og den har potensiale til å bli en liten personlig og ”uunnværlig” multimediaterminal.

De norske bankene har tradisjon for å beskytte sin posisjon, og bankene har vært lite villige til å åpne sin infrastruktur. En interessant utvikling er at det nå kommer nye krav og nye aktører inn i banknæringen, og bankene må tilpasse seg en ny (Internett-) virkelighet enten de vil eller ikke. Betaling av regninger over Internett har vist bankene at det ligger et enormt gevinstpotensiale i de nye mediene, og markedet har vist en villighet til å ta i bruk de nye mediene som langt har overgått bankenes forventninger. Markedet *betaler* til og med for tjenester som burde vært gratis!

Ved siden av utviklingen innen trådløs teknologi skjer det en mindre "synlig" utvikling innenfor smartkortteknologi. I smartkortteknologien finnes de teknologiske byggeklossene som kan realisere sikre løsninger i en "usikker" Internettverden. Digital signering, kryptering og banktjenester er naturlige applikasjoner for smartkort.

I krysningspunktet mellom en åpnere bankinfrastruktur, Internett-, mobilkommunikasjon-, håndmaskin- og smartkortteknologi ligger forholdene til rette for mange spennende nye tjenester. Noen tjenester aner vi konturene av i dag, andre tjenester vil utvikle seg når potensialet i de nye teknologiene virkelig forstås.

1.2 Om oppgaven

Denne oppgaven tar utgangspunkt i teknologi som enten er tatt i bruk i dag, som er under uttesting eller som ventes lansert i den nærmeste fremtid, og undersøker hvordan mobiltelefonen kan benyttes til spill- og betalingstjenester på Internett.

Transaksjonsdiagram benyttes for å analysere handlingene i et skissert scenario, og en demonstrator implementeres for å visualisere handlingene. Ved empiriske studier undersøker jeg om mobiltelefonen kan benyttes for å visualisere enkle animasjoner. Oppgaven er utført i Norsk Regnesentrals strategiske instituttprogram [ELCOM].

1.2.1 Formålet med oppgaven

I vitenskapelige arbeider i dag behandles gjerne teknologiene (mobilteknologi, brukerutstyr, Internett, smartkort, betaling) hver for seg slik at oversikten og problemene forbundet med sammensmelting av teknologiene ikke vies den samme oppmerksomhet. Det er et håp at denne oppgaven kan gi et lite bidrag til bedre forståelse for de problemene og muligheter som ligger i krysningspunktet mellom nye teknologier, og som teknologer arbeider med på mange fagfelt i dag.

1.2.2 Avgrensning

Oppgavens styrke og svakhet er at den favner bredt. Det har vært ønskelig å prioritere bredde fremfor dybde på grunn av helheten. Det har vært naturlig å avgrense oppgaven til kun å omfatte teknologisk relevante deler av scenariet, men det har likevel vært vanskelig å vektlegge stoffet slik at fokus blir representativt.

Oppgaven *beskriver* og *diskuterer* mobilkommunikasjon-, smartkort-, håndmaskin- og betalingsteknologi innenfor rammene av et gitt scenario. (Scenariet beskrives nedenfor). Et konkret scenario av *generell* interesse er valgt for å tilfredsstille grunnleggende krav til funksjonalitet som også vil være anvendbar i andre scenarier. Scenariet ligger fra 0 til cirka 2 år frem i tid; med andre ord teknologi og tjenester som i dag synes realiserbare.

For å visualisere hvordan scenariet kan virke for en mobiltelefonbruker har jeg programmert brukergrensesnittet i en demonstrator. Det er ikke meningen å demonstrere forskjellige muligheter i brukergrensesnittet, for så å vurdere disse opp mot hverandre. Demonstratoren gir eksempler på noen av de mulighetene som vil åpne seg med ny teknologi og illustrerer hvordan mobiltelefonen kan bli benyttet til nye tjenester i nær fremtid.

Juridiske, politiske, organisatoriske eller andre ikke-teknologiske problemstillinger nevnes kun unntaksvis.

For å gjøre oppgaven mer lesevennlig er begrepet *mobiltelefon* forsøkt benyttet istedenfor det mer generelle (og dekkende) begrepet *mobil enhet*. Bruk av begrepet *mobiltelefon* gir dessverre feilaktige assosiasjoner til tradisjonell bruk, det vil si tale-tjenesten. Tjenestene som beskrives i denne oppgaven gjør imidlertid ikke bruk av tale-funksjonalitet.

1.2.3 Metode

Metodegrunnlaget som er benyttet i denne oppgaven er:

- Litteraturstudier, papir og webbasert
- Intervjuer
- Scenario og transaksjonsmodell
- Demonstrator

Oppgavens formål setter klare krav til valg av metode. Litteraturstudier ligger bak teknologiene som beskrives. Mye informasjon er kun tilgjengelig ”på web” i dag. Webpublisering har også (som regel) fordel av å være tidligere ute, på grunn av mediets natur. En klar ulempe med web er at informasjonen er flyktig, og eksakte referanser mangler. Derfor foretrekkes referanser til papirbasert, publisert informasjon når det er mulig.

Fordi oppgaven beveger seg på fagfelt hvor utviklingen går i stort tempo, er det mye informasjon som enten ikke finnes publisert eller hvor publisert informasjon er utdatert. For å få ”fersk” informasjon har det derfor vært naturlig og nødvendig å intervjue teknologer, produktutviklere og andre. Intervjuene har hatt som formål å komplettere det teknologiske bildet.

I denne oppgaven har jeg brukt scenarieteknikken for å illustrere en tenkt spill-virkelighet innen mobiltelefoni. Scenariet er analysert ved hjelp av transaksjonskart. Dette beskriver handlingene i scenariet på en systematisk måte ved å avtegne interaksjonen mellom aktørene.

1.2.4 Scenariet i kortversjon

For å kunne relatere bakgrunnskapitlene til scenariets problemstillinger presenteres her de viktigste trekkene i scenariet. Etter bakgrunnskapitlene beskrives scenariet i detalj (i kapittel 6).

Scenariet beskriver spillet Dagens Dobbel som i korthet går ut på å tippe riktige vinnere i to hesteløp. Spillet finnes i manuell versjon i porteføljen til Norsk Rikstoto (spilltilbyderen). Brukeren trenger ikke ha et etablert kundeforhold til spilltilbyderen for å delta i spillet. Brukeren kobler seg opp til spilltilbyderen fra sin mobiltelefon, markerer to (eller flere) vinnerhester, signerer og betaler for tjenesten. Brukeren velger å se et hesteløp hvis han har vinnersjanser. Løpet overføres direkte til brukerens mobiltelefon. Etter løpet får brukeren beskjed om at han har vunnet en god slump penger og at pengene er overført og disponible. Brukeren blir gratulert og invitert til en navngitt veddeløpsbane som spilltilbyderen vet er nærmeste bane.

Scenariet kan synes enkelt, men som det skal vise seg, er det nok av problemstillinger å gripe fatt i.

1.2.5 Oppgavens struktur

Kapittel 2 *Sikkerhet* presenterer grunnleggende sikkerhetsaspekter.
Kapittel 3 *Trådløs kommunikasjon* presenterer og diskuterer mobilteknologi.
Kapittel 4 *Brukerutstyr* behandler utviklingen innen håndmaskiner.
Kapittel 5 *Smartkort* presenterer og diskuterer utviklingen innen smartkortteknologi.
Kapittel 6 *Scenario "hestespill"* presenterer hestespillet som danner utgangspunkt for valg av teknologier.
Kapittel 7 *Betalingsmodeller* diskuterer modeller for inn- og utbetaling i scenariet.
Kapittel 8 *Designaspekter* tegner en transaksjonsmodell og diskuterer problemstillinger fra scenariet.
Kapittel 9 *Demonstrator* skisserer en implementasjon av spillet og visualiserer brukergrensesnittet for betaling og animasjon.
Kapittel 10 *Oppsummering og konklusjon* gir oppsummerende konklusjoner

Vedlegg A gir forkortelser og forklaringer.
Vedlegg B lister noe av koden i demonstratoren.

2 Sikkerhet

Sikkerhet kommer igjen i flere kapitler og dette kapittelet vil presentere de viktigste begrepene og mekanismene for sikker kommunikasjon i åpne nett, inkludert nøkkel-kryptografi og elektroniske sertifikater.

2.1 Innledning

Sikkerhet har mange aspekter avhengig av innfallsvinkel. Sikkerhetstiltak må ta hensyn til hva som skal sikres og hvilke trusler som foreligger. Betaling ved hjelp av mobiltelefon er prinsipielt å sammenligne med betaling over Internett, det vil si transmisjon av betalingstransaksjoner over et usikret nett hvor kommunikasjonen kan avlyttes og - enda verre - innholdet manipuleres på vei mellom avsender og mottaker.

Graden av sikkerhet er ikke bare bestemt av teknologiske muligheter, men også av politiske føringer. Frankrike og USA kan tjene som eksempler: Frankrike har tradisjonelt vært restriktive i forhold til kryptering, og før 1996 måtte så og si all bruk av kryptografi deklareres på forhånd. USA har vært en sterk pådriver for å begrense "styrken" til krypteringsalgoritmer som tillates eksportert; det opplagte motiv er å sikre at myndighetene skal være i stand til å dekryptere meldinger. Norge, sammen med Frankrike, USA og mange andre land har forpliktet seg gjennom Wassenaar-samarbeidet [WAS] som regulerer eksport av konvensjonelle våpen og avansert teknologi.[2]

2.2 Grunnleggende begreper

Sikker kommunikasjon har følgende viktige aspekter [Ølnes97]:

- *Tilgjengelighet*. Tjenestene må være stabile og til stede for autoriserte brukere
- *Integritet.* Informasjonen som flyter mellom partene må ikke kunne endre innhold på veien uoppdaget.
- *Konfidensialitet.* Informasjon skal være konfidensiell for partene som kommuniserer. I det ligger at informasjonen ikke skal kunne avlyttes.
- *Sporbarhet*. Ved misbruk skal det være mulig å dokumentere det faktiske hendelsesforløpet og å identifisere den eller de ansvarlige.

[2] Siste nytt (13.1.2000): USA vil oppgi begrensningene på eksport av kryptografi [DIGI130100].

Et system for kryptografi kan adressere to av punktene ovenfor: integritet og konfidensialitet. Et kryptografisk system kan i tillegg ivareta følgende aspekter [Garfinkel97]:

? *Autentisering*. Partene som kommuniserer må være sikre på hverandres identitet.
? *Ikke-benekting.* Avsender må ikke senere kunne benekte å ha utført en handling eller sendt en melding.

2.3 Offentlig nøkkelkryptografi

Kryptografiske nøkler er sentralt i sikker kommunikasjon. Kryptografisk nøkler benyttes til autentisering, konfidensialitet og ikke-benekting, og vil i praksis også være nødvendig for å oppnå sporbarhet.

En såkalt *offentlig nøkkel – privat nøkkel*-struktur er en av byggesteinene i moderne kryptografi. Offentlig og privat nøkkel er to krypteringsnøkler med et iboende forhold til hverandre slik at meldinger som er kryptert med den ene nøkkelen bare kan dekrypteres med den andre. Forholdet mellom nøklene er slik at selv om den offentlige nøkkelen er kjent, er det ikke mulig å beregne den private nøkkelen. Som navnene antyder er den ene nøkkelen offentlig og tilgjengelig for alle og den andre strengt personlig.[Ford97]

Asymmetrisk kryptering åpner for interessante muligheter:
? *Signering*. Når meldinger krypteres med *avsenders* private nøkkel vil bare avsenders offentlige nøkkel kunne dekryptere meldingene.[3] Bare eieren av den private nøkkelen kan ha sendt meldingen. Dermed kan mottaker, ved å sjekke avsenders offentlige nøkkel, få bekreftet identiteten til avsender.
? *Kryptering.* Når meldinger krypteres med *mottakers* offentlige nøkkel, sikrer det at kun mottaker kan lese meldingen, da kun mottaker besitter den tilhørende private nøkkelen.
? *Kryptering og signering.* Meldinger krypteres med mottakers offentlige nøkkel og avsenders private nøkkel.

Angående signering: Det er vanlig ved signering at det ikke er selve meldingen som krypteres, men bare et matematisk sammendrag av melding. En såkalt enveis hash-algoritme kan generere en fast, begrenset kodelengde (hash) ut fra en stor data-mengde.[4]

Signering av en begrenset kodelengde er spesielt interessant i mobil sammenheng hvor det er ønskelig å begrense antall transmitterte bits. I de tilfellene hvor mottaker av en signert meldingen kjenner innholdet i meldingen allerede før mottak, vil det være tilstrekkelig at avsender heller transmitterer en signert hash av meldingen istedenfor hele meldingen.

[3]Meldingen kan eventuelt være i klartekst i følge med et *signert, matematisk "sammendrag"* av meldingen.
[4] På grunn av denne egenskapen er det vanlig å benytte hashfunksjoner for å garantere meldingenes *integritet*.

I spillesammenheng eller i forhold til andre tjenester på Internett, kan for eksempel avsender være en server som ber brukeren bekrefte (signere) de valgene han har gjort.

2.4 Elektroniske sertifikater

Såkalte *elektroniske sertifikater* er et standardisert hjelpemiddel til å utveksle offentlige nøkler og for å etablere tillit. De benyttes i sikker elektronisk kommunikasjon i åpne nett. Et elektronisk sertifikat kan sammenlignes med konvensjonell legitimasjon. I den ikke-elektroniske verden brukes flere typer legitimasjon avhengig av hvilken grad av sikkerhet som ansees nødvendig. Troverdigheten til legitimasjonen er avhengig av det vi kan kalle legitimasjonens kvalitet (bilde, underskrift, tiltak mot forfalskning, og så videre) og i hvilken grad en stoler på utsteder av legitimasjonen. Elektroniske sertifikater fungerer etter samme prinsipp i åpne nettverk. Et elektronisk sertifikat attesterer at et spesielt digitalt signatursystem tilhører en spesiell person eller organisasjon.

Et elektronisk sertifikat er ikke annet enn en attest i form av *signering* over en persons eller organisasjons offentlige nøkkel, i tillegg til annen relevant informasjon om personen eller organisasjonen. Et elektronisk sertifikat knytter med andre ord offentlige krypteringsnøkler til *identiteter*.

Den internasjonale standarden X.509 beskriver en infrastruktur (PKI – Public Key Infrastructure) for elektroniske sertifikater. X.509 beskriver formatet og felt i sertifikatet som navn, gyldighet, serienummer, utgiver, signaturalgoritmeidentifikator, offentlig nøkkel og annet. I tillegg beskrives rutiner for håndtering av sertifikatet, som registrering, initialisering, sertifisering, sikkerhetskopi og tilbakekallelse. I spesifikasjonene av X.509v3 og (først og fremst) i de såkalte profilene foretrekkes hashfunksjonen SHA-1 og signeringsalgoritmene RSA, DES eller Diffie-Hellman. [X.509]

2.5 Sikker kommunikasjon

Det er to tilnærminger til sikker kommunikasjon: *nettverkssikkerhet* som krypterer kanaler og *meldingssikkerhet* som krypterer meldinger. Tilnærmingene presenteres nedenfor.

2.5.1 Meldingssikkerhet

Meldingssikkerhet kan etableres ved hjelp av sertifikatsystemet som er beskrevet ovenfor. Meldingssikkerhet integrerer sikkerheten med dataene som kommuniseres, og meldingene selv inneholder alt som trengs for dekryptering og integritetssjekking. Hver melding kan mellomlagres og lagres konfidensielt i sender og mottakerutstyret. Meldingssikkerhet er nødvendig for å oppnå sporbarhet, da sporbarhet i praksis forutsetter signerte meldinger.

Meldingssikkerhet kan integreres med applikasjoner som epostprogrammer og tekstbehandlere. Praktisk utnyttelse av meldingssikkerhet krever bevissthet fra brukerens side, og har således en høyere bruksterskel enn *nettverkssikkerhet*

2.5.2 Nettverkssikkerhet

Nettverkssikkerhet etableres ved å opprette en ”privat”, virtuell kommunikasjonskanal mellom partene som kommuniserer. Nettverkssikkerhet oppnås i praksis ved at kommunikasjonsprotokollene mellom partene utvides med ett sikkerhetslag, som krypterer/ dekrypterer all data som transporteres mellom partene.

Nettverkssikkerhet kan tilbys transparent til brukere uten at det går særlig ut over ytelsen til systemet. Nettverkssikkerhet er også eneste praktiske tilnærming til sikring av strømmer som tale- og data-trafikk i dagens linjesvitsjete GSM-mobilnett.[5]

Nettverkssikkerhet gir kun en sikker kanal; dataene ligger ikke sikret i avsender- eller mottakerutstyret før eller etter at kommunikasjonen har funnet sted. Når meldinger om for eksempel pengetransaksjoner eller avtaler skal sikres, vil ikke nettverkssikkerhet oppfylle kravene til autentisering eller sporbarhet.

[5] For sikkerhet og autentisering i GSM-nettet, se avsnitt 3.1.7

3 Trådløs kommunikasjon

Dette kapittelet inneholder en diskusjon om infrastruktur og basistjenester i mobilnettet for realisering av scenariet. Eksisterende og kommende teknologier diskuteres. Det meste av teksten er direkte relatert til oppgaven. Noe av informasjonen har indirekte relevans, men er tatt med da det er viktig for å gi en helhetlig fremstilling.

GSM gis relativt bred (men ikke dyp) dekning, fordi GSM-teknologien også vil være viktig i de kommende faser av mobilteknologiutviklingen. Et poeng i fremstillingen av GSM er at dagens linje svitsjete GSM-nett ikke er godt egnet til overføring av datatrafikk. Når pakkesvitsjet nett kommer, vil det ha potensiale til å gi vesentlig bedre ytelse.

WAP-standarden vies også oppmerksomhet, da den kan realisere scenariet som er beskrevet i denne oppgaven, over små mobile enheter som mobiltelefoner.

3.1 GSM – Global System for Mobile communication

3.1.1 GSM historie[6]

Mobiltelefoni har hatt en enorm popularitet og utbredelse i Europa i 1990-årene. Standardisering, tilgjengelighet og pris har vært viktige suksesskriterier. Pris kan tjene som eksempel: På 1980-tallet kostet en mobiltelefon godt over kr. 20.000,-. Få år senere kunne man få telefoner til en brøkdel av prisen. På kort tid var det økonomisk mulig for alle å være trådløst tilgjengelig.

Allerede tidlig på 80-tallet var sentrale telekommunikasjonsaktører i Europa klar over skaleringsproblemene med datidens mobilnett. Det fantes visjoner om millioner av brukere, visjoner som ikke kunne realiseres med datidens mobilnettverk. Det var også klare kompatibilitetsproblemer mellom de ulike mobilsystemene. I Norden og Benelux-landene rådet NMT-systemet, i Storbritannia TACS, i Vest-Tyskland C-Netz, i Frankrike Radiocom 2000 osv. Hver av disse løsningene hadde høye forsknings- og utviklingskostnader, og løsningene var ikke kompatible. Det var økende forståelse for at lokale løsninger ikke var lønnsomt.

I 1982 nedsatte CEPT – datidens telekommunikasjonsforum i Europa – en arbeidsgruppe kalt Groupe Spéciale Mobile (GSM). Gruppens mandat var å utvikle spesifikasjonene for et pan-europeisk mobilkommunikasjonsnett beregnet for millioner av

[6] Historisk informasjon bygger hovedsakelig på [Kennedy97]. Annen informasjon om GSM i dette kapittelet bygger i hovedsak på [Walter95] og [Scourias98].

brukere. (Mange år senere ble akronymet GSM endret til å stå for *Global System for Mobile communication*.)

Arbeidsgruppens idé var at GSM-standarden skulle sikre god samhandling mellom komponenter i GSM-systemet, men likevel sikre konkurranse og innovasjon mellom leverandører. Dette ble gjort ved å utarbeide funksjons- og grensesnittspesifikasjoner for alle funksjonelle enheter i systemet. I dag omfatter GSM-spesifikasjonene over 8000 sider med dokumentasjon.

Digitale teknologier var ennå umodne tidlig på 1980-tallet, men arbeidsgruppen hadde tro på digitale fremskritt. Digitale nettverk har en attraktiv kombinasjon av høy ytelse og god spektral utnyttelse, og har i tillegg potensiale for kryptering og datakommunikasjon. Det digitale nettverket ville også komplettere ISDN, som telekommunikasjonsaktørene hadde under utvikling for et landbasert digitalt kommunikasjonssystem. Andre viktige krav til systemet var god talekvalitet og lave kostnader for terminaler og vedlikehold. 900Mhz-frekvensbåndet ble reservert for GSM.

Industrien måtte overbevises om at GSM var trygg satsning. I 1985 hadde telekommunikasjonsaktører i Europa forpliktet seg til å støtte GSM, og standarden fikk politiske støtte ved anbefaling fra EF i 1986.

1989 ble ansvaret for GSM-spesifikasjonene flyttet til nyetablerte ETSI. ETSI samlet interessene fra administrator-, operatør- og produktutviklerhold, hvilket ga utviklingen et kraftig puff. Fase 1 av GSM 900-spesifikasjonen ble publisert i 1990. For å øke eterkapasiteten spesifiserte ETSI parallelt en noe modifisert utgave av GSM, kalt DCS 1800 (senere kalt GSM 1800) for kommunikasjon i 1800MHz-båndet.

I 1992 var GSM ferdig testet og klar for markedet, og de første internasjonale roamingavtaler[7] ble tegnet. Ved slutten av 1993 hadde GSM én million brukere, ved utgangen av 1997 66 millioner og ved utgangen av 1998 130 millioner [ALC99].

Det første GSM 1800-nettet kom i produksjon i 1993. Så sent som i 1994 kom USA med i GSM-arbeidet da store blokker i 1900 MHz-frekvensbåndet ble auksjonert bort til mobiloperatører. 1900 MHz-båndet ble benyttet da 900 og 1800MHz-båndet allerede var i bruk. Nord-Amerika har derfor en GSM-variant som er skreddersydd for 1900 MHz-båndet. GSM har i dag en akselererende utbredelse på alle kontinenter, og bidrag til GSM-spesifikasjonene kommer ikke lenger utelukkende fra europeiske interesser selv om ETSI fortsatt er styringsorganet.

For ikke å utsette utrullingen av GSM ble utviklingen delt inn i faser etter grunn- og tilleggstjenester. Spesifikasjonen til fase 1 ble frosset i 1990 og la vekt på talетjenesten. I 1993 ble fase 2 lansert, med nye tjenester som data, faks og kortmeldinger (SMS). Utviklingen av GSM er i dag inne i *fase 2+* (startet i 1996),

[7] Administrative avtaler mellom teleoperatører om aksess i hverandres mobilnett. Se også vedlegg A for forkortelser og ordforklaringer.

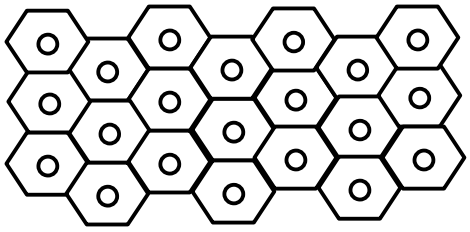
og GSM-nettet utvides gradvis med ny funksjonalitet og nye tjenester. Spesielt spennende er arbeidet med nye radiolinkprotokoller for linjesvitsjet (HSCSD) og pakkesvitsjet (GPRS) data, som vil mangedoble overføringskapasiteten i radionettet.

Det digitale GSM-nettet blir gjerne kalt *annengenerasjons*-mobilnett. NMT og lignende analoge mobilnett var første generasjon. Tredje generasjon vil representere en gjennomført integrasjon mellom mobilteknologi og data-Internett-teknologi.

3.1.2 Cellekonseptet

Cellekonseptet er den grunnleggende idéen for kapasitetsutnyttelse i trådløse nettverk. Istedenfor én kraftig, sentral sender/mottaker (basestasjon) vil en oppdeling i mindre geografiske områder (celler) med hver sin basestasjon gi muligheter for gjenbruk av frekvensområder. Dermed får nettet som helhet langt høyere kapasitet.

Cellestørrelse er avhengig av antall brukere og geografiske forhold. GSM-nettet benytter cellestørrelser fra ca 300 meter i tett befolkede områder, til ca. 35 km i grisgrendte. Celler illustreres gjerne med heksagonale mønstre som vist på Figur 1.



Figur 1. Cellekonseptet. Dekningsområde med én basestasjon per celle og gjenbruk av frekvensområder.

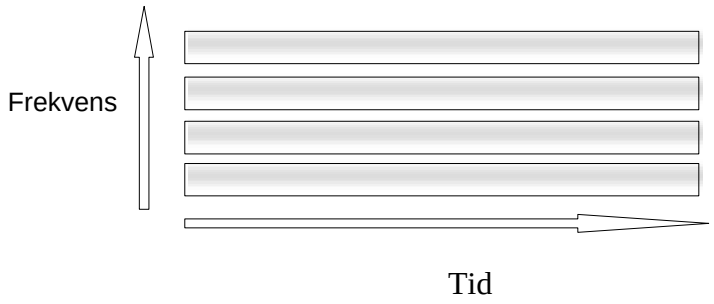
3.1.3 Radioteknologi

Radioteknologien er fundamentet for all mobil kommunikasjon. Radiobølger er elektromagnetiske felt som forplanter seg i ikke-ledende media. Det er to viktige begrensende faktorer i radiokommunikasjon [Walter95]:

- (batteri-) kapasitet
- frekvensspektrum

Ønskes utnyttelse av store deler av frekvensområdet for å oppnå høy båndbredde, koster det batterikapasitet. Batterikapasitet er en begrenset ressurs i mobile enheter.

Antenneteknologi tilsier at antennelengden er av samme orden som bærebølgelengden, hvilket i praksis begrenser aktuelle frekvensbånd for håndholdte apparater fra noen få MHz til noen få GHz. Frekvensspekteret som er tilgjengelig for mobil kommunikasjon er i tillegg gjenstand for nasjonal og internasjonal regulering.



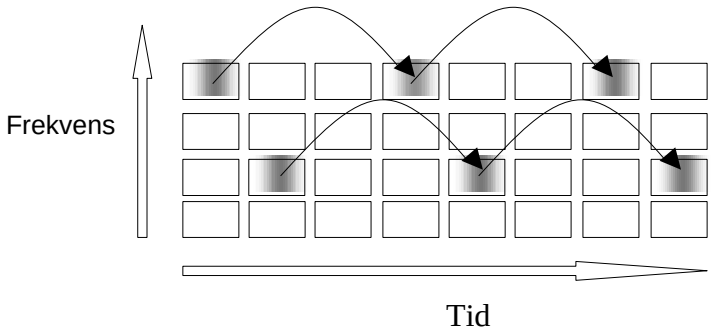
Figur 2. Prinsippet for frequency division multiple access (FDMA) benyttet i NMT-nettet. Hvert rektangel tilsvarer potensialet for én privat kommunikasjonskanal mellom basestasjon og mobil enhet. Hver kanal legger beslag på hele sitt frekvensbånd under hele sesjonen. Først når partene avslutter kommunikasjonen kan andre overta frekvensbåndet.

Signalene mellom basestasjon og mobil enhet forplanter seg ikke gjennom en perfekt eter. De kan utsettes for refleksjon, svekkelse og tidsforskyvninger (fading) på grunn av geografiske og værmessige forhold. Frekvensbåndene i MHz og GHz-områdene er i tillegg utsatt for ”fremmede” støykilder som for eksempel forbruker-elektronikk.

Prosessen med å transponere informasjonsdata til frekvensbånd kalles modulasjon. I førstegenerasjons-mobilnett NMT i Norge ble aksessteknikken FDMA brukt for å gi flere tilgang til frekvensbåndene, som vist på Figur 2. I GSM-nettet er TDMA valgt som aksessteknikk. Se Figur 3.

For å gjøre GSM *enda* mer robust mot fading og interferens er det i tillegg implementert et skjema for frekvenshopping, altså noe mer komplisert enn det som fremgår av Figur 3. Tidsblokkene som utgjør en kanal ligger derfor ikke sekvensielt i det samme frekvensbåndet, men er spredd ut over flere frekvensbånd etter et skjema som kringkastes i nettet. Frekvenshopping har gode egenskaper når det gjelder fading, og er i tillegg ikke så utsatt for interferens mellom frekvensbåndene. [Uddenfeldt98].

Tale og data kodes forskjellig som følge av forskjellige behov for protokoll-informasjon, som feilkorreksjon, synkronisering og så videre, hvilket gjør den effektive overføringshastigheten vesentlig lavere enn mediets hastighet på 33.9 kbits/s. Den effektive overføringshastigheten er 13 kbits/s for (såkalt ”full rate”) tale og 9 kbps/s for data.



Figur 3. Prinsippet for time division multiple access (TDMA) som GSM-nettet bygger på (illustrert i kombinasjon med FDMA). Flere kommunikasjonskanaler er tidsmultiplekset inn på det samme frekvensbåndet, her illustrert ved at hver tredje tidsblokk utgjør en kommunikasjonskanal mellom basestasjon og mobil enhet.[8]

3.1.4 Mobilnettets struktur og basistjenester

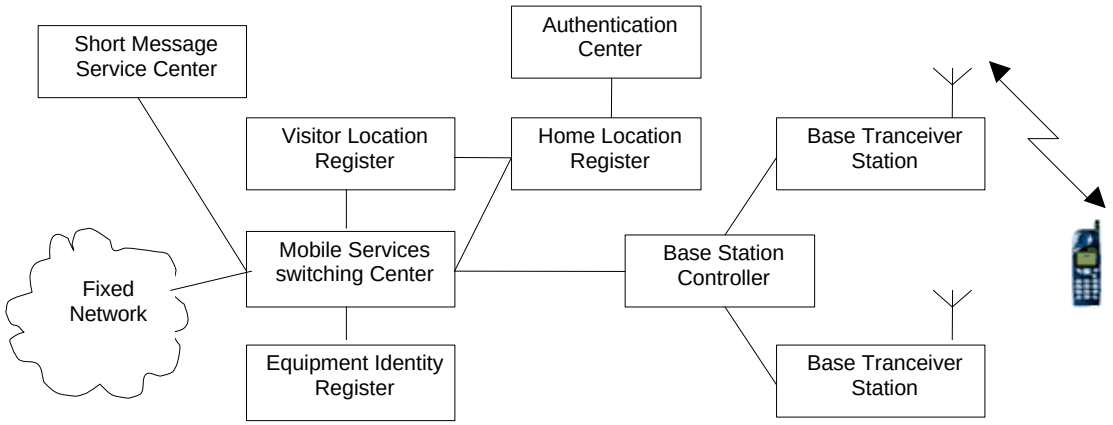
Mobilnettets grunnstruktur og kobling til fastlinjenettet er skissert i Figur 4. Det er verd å merke seg at kommunikasjon mellom to mobile enheter ikke nødvendigvis forutsetter bruk av fastlinjenettet. Foruten radiolinkaspekter har mobilnettet mobilitetsfunksjoner som gjør nettet vesentlig mer komplisert enn fastlinjenettet.

Følgende grunnleggende mobilitets- og administrative funksjoner skal ivaretas:

- *Paging* kalles problemet med å lokalisere en bestemt mobil enhet for å kommunisere med denne. I GSM-nettet er paging løst ved hjelp av to registere, *home register* og *visitor register*. Home register er en database med fast tilknytning i nettet, og home register peker til visitor register som holder rede på hvor den mobile enheten befinner seg fysisk.
- *Handover* kalles funksjonaliteten som flytter pågående kommunikasjon mellom basestasjon og mobil enhet til en annen basestasjon for å bedre mottakerforholdene. Handover er nødvendig når den mobile enheten forflytter seg ut av rekkevidden for en basestasjon. Den mobile enheten overvåker hele tiden mottakerforhold fra nærliggende basestasjoner (celler) og kommuniserer denne informasjonen til basestasjonen, som tar avgjørelsen om eventuell flytting av sesjonen.
- *Roaming*-avtaler mellom teleoperatører er nødvendig for å kunne benytte den mobile enheten i nettene til "fremmede" teleoperatører.
- *Betaling*. Et prinsipp innen tradisjonell telekommunikasjon har vært at den som initierer oppkoblingen betaler. Et annet prinsipp er at betaler skal ha mulighet til å kjenne til prisen på forhånd. Betalingsmodellen i GSM beholder sistnevnte prinsipp, men innfører prinsippet om at mottaker betaler for roaming utenfor lokal teleoperatørs operatørnett. Argumentet for denne praksisen er behovet for

[8] GSM implementerer egentlig 8 tidsblokker. GSM (900 MHz) benytter et 25 MHz bredt frekvensspektrum som holder 124 bærefrekvenser hver på 200 kHz båndbredde. Hver av de 124 bærefrekvensene har igjen 8 TDMA kanaler. GSM modulerer 271 kbits/s på et 200 kHz bredt bånd, hvilket gir en hastighet på 33.9 kbits/s for hver av de 8 tidsblokkene [Scourias98].

differensierte takster mellom lokal og internasjonal kommunikasjon uten å legge utgiftene på initierende part.



Figur 4. GSM-nettets struktur. Figur fra [Walter95].[9]

3.1.5 GSM-data og SMS

Brukertjenester som implementeres på mobiltelefoner i dag må benytte enten GSM-data eller SMS som grunnleggende bæretjeneste[10]. Det undersøkes her hvor godt egnet de to bæretjenestene vil være i scenariet (uten å ta stilling til hvordan tjenestene på toppen av bæretjenesten skal implementeres).

[9] Det er generelt to typer utstyr i nettet: Basestasjoner som håndterer radiotransmisjon, og svitsjer som håndterer svitsjing og kontrollfunksjoner. En Base Station Controller kan kontrollere et ti-tall Base Tranceiver Stations som gir radioaksess til de mobile enhetene. Mobile Services switching Center (MSC) er "hjernen" og er ansvarlig for kommunikasjon fra mobil-til-mobil og mobil-til-fastlinjenett i sitt område. MSC er koblet til fastlinjenettet og kan være koblet til flere Base Station Controllers og flere andre MSCer. Visitor Location Register er en lokal database som inneholder alle relevante opplysninger om mobile enheter som befinner seg i MSC-kontrollert område. Home Location Register er en database for permanent lagring av alle abonnementsopplysninger. Hvert GSM-nett må ha minst en Home Location Register database. Denne holdes også konstant oppdatert med hensyn til mobilens omtrentlige posisjon. Home Location Register er også ansvarlig for håndtering av sikkerhetsparametere gjennom "sikkerhetsnoden" Authentication Center. Equipment Identity Register gir MSCen muligheter til å logge eller nekte kommunikasjon for gitte mobile enheter da alle enheter identifiseres av unike serienummere (IMEI/IMSI). **Short Message Service Center (SMSC)** betjener tekstmeldinger til og fra mobile enheter. Signaleringsprotokollene som benyttes er telekommunikasjonsstandarder som bygger på OSIs lagdelte referansemodell. Protokollene som benyttes i radiokommunikasjonen er nye, men inspirert av ISDN, og MAP-protokollen mellom MSC og Location Registerene (blant annet) er helt ny; ellers benyttes tilpasninger av ISDN-protokollen og standard signalering i fastlinjenettet, ITU Signaling System no 7 (SS7). [Scourias98]

[10] GSM spesifiserer fire bærere: GSM-CSD (Circuit Switched Data) som jeg har valgt å kalle GSM-data, GSM-SMS (Short Message Service), GSM-SS (Supplementary Service) og GSM-USSD (Unstructured Supplementary Service Data). De to sistnevnte er reservert for operatørbruk.

Tale er den klart viktigste tjenesten som tilbys i GSM-nettet. Datatjenesten i GSM har vist seg å ikke slå igjennom som ventet. Høye linjekostnader og lav overførings-hastighet er nok viktige grunner til at datatjenesten i GSM ikke har fått større omfang. I Norge har tekstmeldinger (SMS) vist seg å bli populært – særlig i yngre aldersgrupper. Relativt lave kostnader sammenlignet med taletjenesten og en viss nyhetsfaktor i ungdomsmiljøer kan være medvirkende årsaker til at SMS har slått an. Tekstmeldinger kan sammenlignes med e-post. Det er en mindre påtrengende form for kommunikasjon.

Som taletjenesten er datatjenesten i GSM linjesvitsjet. Man legger beslag på en 9 kbits/s kanal uansett om man har noe å kommunisere eller ikke i den tiden sesjonen varer. Oppkoblingstiden er relativt lang sammenlignet med ISDN, så på-sparket oppkoblinger er lite attraktivt. Bruk av datatjenesten er i dag priset ca. som taletjenesten.[11]

Datatjenesten i GSM synes ikke å være særlig godt egnet i spillscenariet av følgende grunner:

- *Kommunikasjonen prises etter antall minutter i bruk. Denne prismodellen passer dårlig da kommunikasjonen vil være preget av få og korte dataoverføringer og lange pauser mens brukeren fyller ut bong.*
- *Datatjenesten er linjesvitsjet, og kanalen står åpen så lenge kommunikasjonen varer. På grunn av den lange oppkoblingstiden er det ikke attraktivt å koble ned den tiden en ikke har noe å sende. Det er heller ikke sannsynlig at kommunikasjonsmodellen tillater på-sparket oppkoblinger som kan gjenoppta sesjonen etter et avbrudd.*
- *Overføringshastigheten på 9 kbits/s er tilstrekkelig ved tekstbasert informasjon, men blir alt for lav for overførsel av multimediainformasjon.*

I motsetning til datatjenesten i GSM er SMS-tjenesten i GSM pakkesvitsjet (SMS – Short Message Service). En SMS-melding får bestå av inntil 160 bytes og har samme overføringshastighet som GSM-data. GSM-standarden spesifiserer to typer SMS-meldinger: punkt-til-punkt og kringkasting. Kringkasting sendes til alle mobile enheter i en celle eller et område og kan for eksempel inneholde viktig informasjon fra teleoperatøren. Vanlige brukere vil normalt ikke ha mulighet til å kringkaste informasjon.

I punkt-til-punkt-modellen sendes en melding fra den mobile enheten til meldings-sentralen (Short Message Service Center, SMSC, se Figur 4 på side 14). Sentralen er meldingssystemets grensesnitt mot omverdenen og kan eventuelt mellomlagre meldinger inntil mottaker blir tilgjengelig for nedlasting. Meldingssentralen kan være gateway til andre tjenester som for eksempel elektronisk post, og atter nye tjenester kan utvikles på toppen av SMS-tjenesten (som WAP i avsnitt 3.4).

[11] Telenor tar fra kr 0,89 til kr 5,99 per minutt for GSM-data, avhengig av abonnementstype (4/8/99).

SMS-tjenesten er relativt dyr for forbrukere[12]. Nedenfor vises fordeler og ulemper med SMS-meldinger i forhold til GSM-datatjenesten:

? SMS bruker båndbredde kun når meldinger sendes og mottas, hvilket gir en vesentlig bedre ressursutnyttelse i nettet i forhold til datatjenesten.
? SMS har kort eller ingen oppkoblingstid.
? SMS har lange latenstider. En rundtripp fra mobiltelefon til SMSC og tilbake til mobiltelfonen kan ta 15 sekunder eller mer, som vist i avsnitt 9.4.1.
? Med SMS kan det også være nødvendig å stykke opp en melding for å tilfredsstille 160-tegnsgrensen som er maksimum meldingsstørrelse.

I scenariet betyr dette at:
? *Når innsatsen er lav kan utfyllingskostnadene ved SMS være en ikke ubetydelig del av kundens totalkostnad, avhengig av antallet SMS-meldinger som må sendes. Kostnaden er imidlertid konstant.*
? *På grunn av de lange latenstidene er det ikke attraktivt med tjenester som krever særlig interaksjon med brukeren. I scenariet betyr det at utfylling av bong antakelig kan implementeres over SMS, men visualisering av et løp er ikke mulig.*
? *Multimedia (selv i enkleste form) er utelukket på grunn av latenstidene og den lave båndbredden.*

Ut fra implikasjonene for GSM-data og SMS kan det synes som om de begge er egnet i scenariet, men på hver sin måte. SMS vil være godt egnet under utfyllingsfasen, hvor brukeren ikke må betale for den tiden han bruker på å bestemme seg for bong. Visualisering av et løp derimot er det bare GSM-data som kan håndtere, da det vil være nødvendig med en kontinuerlig strøm av data. Den lave båndbredden vil imidlertid sterkt påvirke kvaliteten på visualiseringen.

3.1.6 Lokalisering og posisjonering

Lokalisering av en mobil enhets posisjon er en tjeneste som tilbys i GSM. En applikasjon kan spørre den mobile enheten hvilken celle den betjenes av. Hvis cellen er liten, kan det gi god nok presisjon for enkelte applikasjoner. (Se også avsnitt 5.4.2 for realisering av denne tjenesten).

Det er generelt to tilnærminger til større presisjon [Taylor99]. En kan benytte radiokommunikasjon til å beregne hvor en enhet sender fra. Dette kan gjøres ved å beregne enhetens lokasjon i forhold til flere radiomottakere. Med tre eller flere stasjoner kan det oppnås ”gatenivå”-presisjon. Den andre tilnærmingen til posisjonsbestemmelse er bruk av et posisjonsredskap som Global Positioning System (GPS) på den mobile enheten. GPS benytter signaler fra et nettverk av satellitter for å bestemme posisjonen. For tiden har GPS presisjon ned til 100-150 meter, og helt ned til 1 meter for spesielle behov.

[12] Telenor priser tjenesten med kr 1,50 for sending av meldinger og kr 0 for mottak (4.8.99).

I scenariet ønsker tilbyderen å reklamere for et stevne. Lokasjonsinformasjonen som ligger i GSM er mer enn tilstrekkelig for dette behovet.

3.1.7 Sikkerhet og autentisering i GSM-nettet

Et GSM-abonnement er ikke knyttet til en fysisk mobiltelefon, men til SIM-smartkortet[13] som er installert i mobiltelefonen. Man kan flytte SIM-kortet til andre mobile enheter og dermed oppnå personlig mobilitet i forhold til GSM-utstyr.

SIM-smartkortet i en mobiltelefon inneholder tre viktige koder: Ett id-nummer som unikt identifiserer SIM-kortet, en krypteringsnøkkel som er unik for SIM-kortet, og en identifikasjon av krypteringsalgoritmen som skal benyttes. (Se også kapittel 5 om smartkort og 2 om sikkerhet)

For konfidensialitet benyttes *symmetrisk* kryptering i GSM-nettet. I symmetrisk kryptering benyttes samme nøkkel til både kryptering og dekryptering. Mottaker og avsender må begge ha kopi av nøkkelen. Det genereres unike kommunikasjons-nøkler for hver ny sesjon ut fra de hemmelige nøklene i SIM-kortet.[Nurkic97]. Alle bæretjenestene i GSM sikres konfidensialitet ved kryptering.

Symmetrisk kryptering har tradisjonelt vært vesentlig raskere enn asymmetrisk. Det er kanskje en av grunnene til at asymmetriske nøkler ikke er valgt i GSM-nettet. (Se avsnitt 2.3 for mer om kryptering). Som eksempel benytter SSL, den åpne sikkerhetsprotokollen som er utviklet av Netscape for sikker kommunikasjon på Internett, asymmetrisk kryptering kun til å utveksle symmetriske nøkler som så benyttes til kryptering av sesjonen [SSL].

Krypteringen som benyttes i GSM-nettet er ikke åpent tilgjengelig. Nettoperatørene hindrer innsyn i krypteringsteknologien. Det er usikkert hvor gode algoritmene er, men krypteringen antas å være moderat sikker.[14] Det er også usikkert hvor gode nettoperatørene er til å sikre sine nøkler. Det er opp til GSM-operatøren å bestemme hvilken algoritme som skal benyttes. Operatøren må dog ta hensyn til nasjonal lovgivning. [Nurkic97]

Det er verd å merke seg at kryptering i GSM-nettet kun gjelder mellom telefon og basestasjon. Fra basestasjon går kommunikasjonen ukryptert i teleoperatørenes lukkede nett. Det er også verd å legge merke til at det er *SIM-kortet, og ikke brukeren,* som autentiseres ved oppkobling i GSM-nettet.

Selv om bæretjenestene GSM-data og SMS vil være kryptert med standard GSM-kryptering vil det ikke være godt nok for bankapplikasjoner eller andre applikasjoner som trenger høy sikkerhet. Mangelen på ende-til-ende sikkerhet gjør i tillegg at konfidensialitet og integritet må adresseres på annen måte for å etablere en sikker tjeneste over GSM.

[13] SIM – Subscriber Identity Module. Se også avsnitt 5.4.1 for mer om SIM-kort.
[14] Siste nytt: Israelske forskere hevder å ha knekket GSM [DIGI071299].

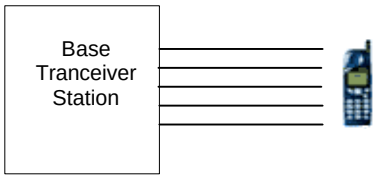
3.2 GSM Fase 2+: HSCSD og GPRS

HSCSD og GPRS er en videreutvikling av GSM-standarden (fase 2+ funksjonalitet) for raskere transport av henholdsvis linjesvitsjet og pakkesvitsjet data. I forhold til scenariet kan HSCSD- og GPRS-bæretjenestene, når de kommer, realisere multi-media til mobile enheter.

HSCSD, High Speed Circuit Switched Data, vil kunne gi opp til 64 kbits/s linjesvitsjet dataforbindelse. Det er samme hastighet som én ISDN-B-kanal, og vil være egnet for applikasjoner som trenger konstant overføringskapasitet – typisk lavkvalitets videoapplikasjoner. HSCSD kan sees på som en relativt enkel tilpasning til dagens GSM-teknologi, men krever tilpasning både på mobiltelefon- og basestasjonssiden. For å oppnå hele 64 kbits/s kreves mer effektiv modulasjon av radiobåndet enn vi har i dag. Innføring av HSCSD i den norske nettoperatøren NetCom's mobilnett vil for eksempel ikke bety mer enn dobling av hastigheten på sending (19.2 kbits/s), og tredobling på mottak (28,8 kbits/s) i forhold til dagens datahastighet. NetCom har da også annonsert at det ikke er aktuelt å implementere HSCSD, men heller vente på GPRS [IT050599]

Den andre protokollen, GPRS, General Packet Radio Service, vil kunne gi en pakke-orientert dataforbindelse med hastigheter fra 72 til 170 kbits/s avhengig av ønsket tjenestekvalitet. GPRS har potensiale til å erstatte både GSM-data- og SMS-tjenesten. Telenor forventer implementasjon av GPRS i år 2001.

Felles for HSCSD og GPRS er at begge kan utnytte flere enn én tidsluke under sending. Dagens datatjeneste (og taletjeneste) tidsmulitplekser et frekvensbånd slik at det gir åtte fysiske kanaler. Bare hver åttende tidsluke benyttes med andre ord i en logisk kanal i dagens GSM-nett. Et pakkesvitsjet nettverk kan (teoretisk) utnytte mange eller alle tidslukene til sending av data [David97]. Figur 5 illustrerer at flere kanaler er i bruk.



Figur 5. Flere fysiske kanaler (tidsluker) mellom mobil og basestasjon gir én logisk kanal, og dermed høyere ytelse for HSCSD og GPRS enn dagens GSM-datatjeneste. GPRS kan koble opp og ned tidsluker etter ønsket overføringshastighet og ønsket tjenestekvalitet. GPRS legger kun beslag på tidslukene under overføring av pakker, mens HSCSD reserverer tidslukene for hele sesjonen.

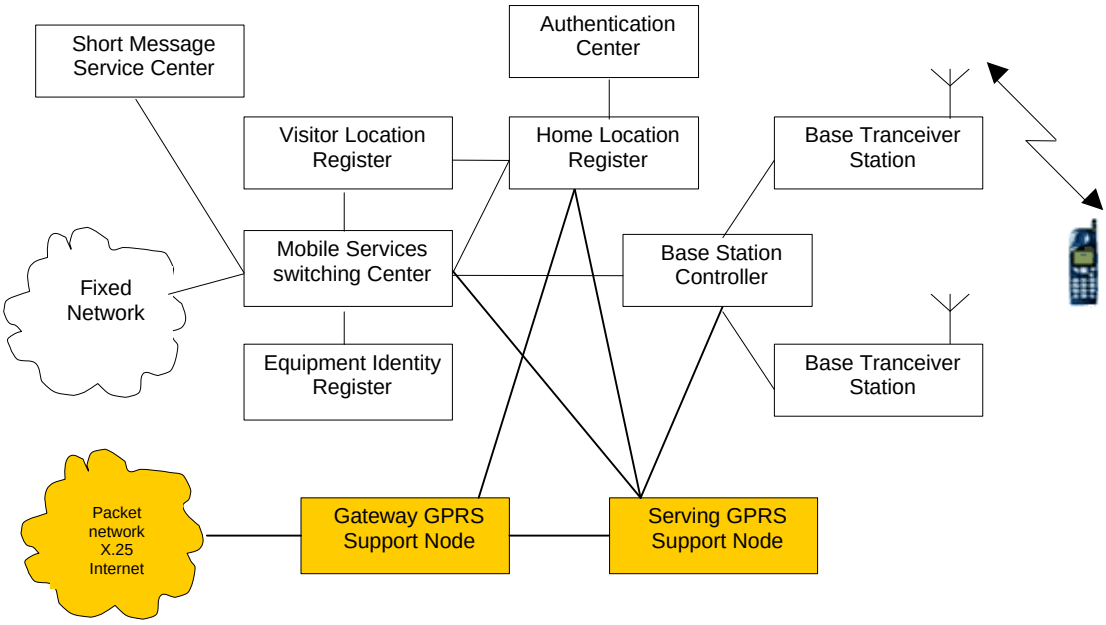
Datatrafikk, særlig trafikk som involverer menneske-respons, karakteriseres ved mye trafikk i korte perioder, og lange perioder med lite eller ingen trafikk. I disse tilfellene er pakkesvitsjete mekanismer kjent for å gi bedre utnyttelse av transmisjonsmediet enn linjesvitsjete [Brasche97]. Statistisk multipleksing gjør at flere kan dele mediet samtidig.

Funksjonelt vil GPRS være som GSM-datatjenesten, med den forskjellen at hastigheten vil være vesentlig høyere og det vil være *pakkebasert* IP helt ut til den mobile enheten. Med GPRS vil telenettoperatørene være i sterk posisjon til å gi Internettilgang, og de kan true dagens etablerte Internettilbyderene. Figur 6 viser GPRS-nettets struktur.

Med den siste utviklingen innen kompresjonsalgoritmer for audio og video (H.263 og MPEG-4) er til og med transmisjon av video realiserbart med GPRS [Brasche97].

Fordelene med GPRS i forhold til GSM-datatjenesten:

? Fra 7,5 til nærmere 18 ganger raskere – kan realisere medium kvalitet multi-media.
? Muliggjør betaling ”per bit” i stedet for ”per sekund”
? Kort eller ingen oppkoblingstid mot aksessnettet (ingen ”oppringingsfase”)
? Tale- og datatrafikk kan skje samtidig i den mobile enheten



Figur 6. GPRS-nettets infrastruktur. Figuren bygger på Figur 4 og [David97].[15]

[15] Foruten en GPRS-tilpasset Base Station Centroller er det definert to nye noder (uthevet) og nye grensesnitt for disse: Serving GPRS Support Node har ansvaret for å levere pakker til mobile enheter i sitt område. Home Location Register har utvidet funksjonalitet for å håndtere routing og GPRS abonnentinformasjon. Mellom GPRS mobile enheter (dvs mellom GPRS Support Noder) benyttes innkapsling av IP-meldinger (IP-tunneling). Gateway GPRS Support Node er grensesnittet mot fastlinje pakkenettverk eller Internett. Se også www.gsmword.com.

3.3 Tredje generasjons mobilnett

UMTS – Universal Mobile Telecommunication System – er ETSIs ambisiøse navn på satsningen på tredje generasjons mobilnett.[16]

Mens første generasjon mobilnett var analoge, og andre generasjon digitale, vil kjennetegnet for tredje generasjon være konvergensen som finner sted mellom tele- og datakommunikasjons-verdenen.

FN-organet ITU har gitt de overordnede krav til tredje generasjons mobilnett. Se Figur 7. ETSI og andre standardiseringskomiteer driver selve standardiseringsarbeidet. Fase 1 av UMTS ventes i år 2002, og full implementasjon av UMTS ventes først i år 2005.

IMT-2000 krav fra ITU

- Talekvalitet som fastlinje
- Sikkerhet som fastlinje
- Nasjonal og internasjonal roaming
- Support for flere offentlige og private operatorer
- Pakkesvitsjet og linjesvitsjet data
- Høy spektral effektivitet
- Support for flere cellelag
- Sameksistens og samhandling med satellittsystemer
- En fasetilnærming for datarater opp til 2 Mbit/s

Figur 7. Krav til tredje generasjons mobilnett fra International Telecommunication Union (Tredje generasjons mobilnett kalles IMT-2000 i ITU sammenheng) Figur fra [ER99]

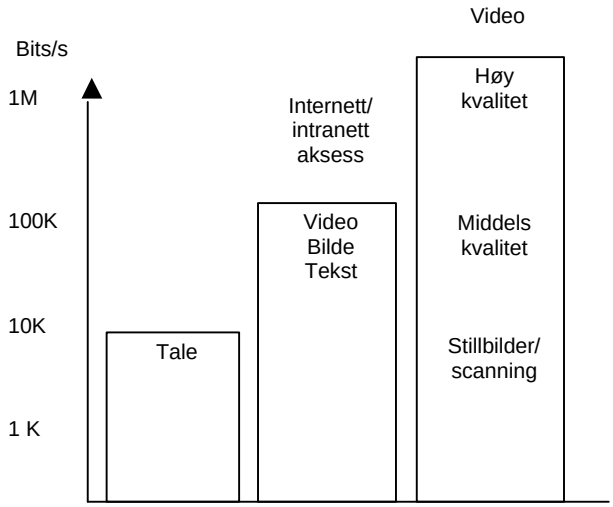
Det pågår for tiden aktivt harmoniserings- og standardiseringsarbeide. Nedenfor oppsummeres det som synes å være de viktigste konklusjonene i arbeidet med tredje generasjons mobilnett (3G):[17]

- 3G vil bygge på og komplementere eksisterende GSM Fase +2 nettverk. GPRS vil være en viktig del av 3G.
- 3G vil bygge på IP-teknologi.
- Ny modulasjon i radionettet vil gi GPRS i 3G en overføringsrate på opptil 384 kbits/s som vil være generelt tilgjengelig med mobilitetsfunksjoner som roaming og handover.
- Ny wideband modulasjonsteknologi vil kunne gi opp til 2 Mbits/s overføringsrate i begrensede områder, hvilket muliggjør høykvalitets video til bærbare PC'er.
- Det vil trolig bli flere rådende beslektede wideband modulasjonsteknologier
- 3G vil bruke frekvensspekter i 2 GHz-området, men det vil ikke lykkes å allokere det samme frekvensspekteret over hele verden.

[16] I andre deler av verden går denne satsningen under andre navn, f.eks Core-A i Japan. I ITU går arbeidet under betegnelsen IMT-2000.
[17] Se www.umts-forum.org

? Mobile enheter vil bli ”dual mode” ved å implementere 2G og 3G funksjonalitet
? Det kan bli mulig å være konstant online da betaling kan baseres på volum og ikke tid. Dette vil åpne for mange innovative produkter og løsninger.

3G er spennende i forhold til scenariet i denne oppgaven. 3G betyr i praksis først og fremst en vesentlig høyere overføringshastighet, noe som kan realisere mobile videotjenester som overføring av veddeløp på store (PC-) skjermer. Et utbygget GPRS nettverk vil trolig være mer enn godt nok til å drive selv avanserte videotjenester på mobile enheter med små skjermer. Se Figur 8.



Figur 8. Overføringskrav for forskjellige tjenester. Figur fra [ER99].

3.4 WAP – Wireless Application Protocol

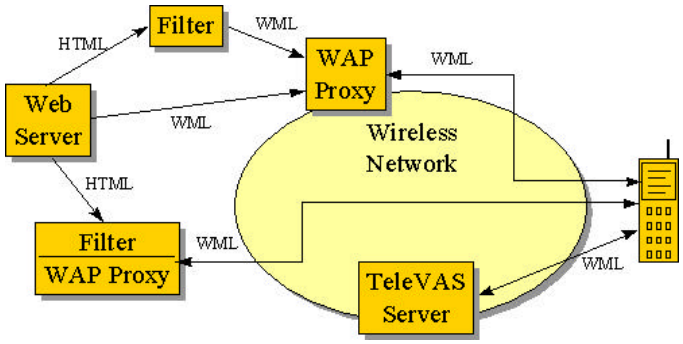
WAP-standarden er interessant fordi den gir teknologiske muligheter til å realisere scenariet som er beskrevet i denne oppgaven, over små mobile enheter.

Samarbeidet om WAP-standarden er motivert ut fra ønsket om å muliggjøre kommunikasjon mellom trådløse enheter, som mobiltelefonen, og TCP/IP-baserte nett. Særlig ønsket om å bruke mobiltelefonen ”på Internett” som klient til webservere har vært ønskelig (se Figur 9).

WAP-Forum er interesseorganisasjonen bak WAP-standarden. Initiativet til opprettelsen av WAP-Forum ble tatt av de sentrale mobiltelefonaktørene Ericsson, Nokia, Motorola og Unwired Planet i 1997. WAP-FORUM er ikke en standardiseringsorganisasjon, men gir input til og støtter andre standardiseringsorganisasjoner.[18] I dag er en lang rekke sentrale utstyrsprodusenter, nettoperatører, ISPer og innholdsleverandører med. Fra Norge er blant andre Telenor medlem.

[18] The World Wide Web Consortium (W3C), European Telecommunication Standards Institute (ETSI), Industry Association (TIA), Internet Engineering Task Force (IETF), European Computer Manufacturers' Association (ECMA). (November 1999).

WAP spesifiserer en rekke protokoller og grensesnitt. WAP spesifiserer nettverks-protokoller, smartkortgrensesnitt for sikkerhetsrelaterte funksjoner og grensesnitt til ”tradisjonelle” telefonfunksjoner. WAP inkluderer også en mikro-nettleser og et tag-språk (WML) optimalisert for begrensede ressurser i mobiltelefoner. WAP-spesifikasjonene er åpent tilgjengelig for alle. Spesifikasjonene og informasjon er tilgjengelige fra [WAP-Forum].



Figur 9. WAP Infrastruktur. Figur fra [WAP-Forum]

WAP-Forum begrunner utviklingen av nye protokoller i WAP med behovet for å optimalisere for det ”ekstreme” miljøet som de skal eksistere i. Dette miljøet kjennetegnes ved:

- lav båndbredde
- lange latenstider
- begrenset minne og prosessorkraft
- begrenset batterikapasitet
- liten skjerm
- begrensete inputmuligheter

WAP-protokollene er essensielt tilpasninger av Internett-baserte protokoller. Likheten til Internett-protokollene gjøre det lett å integrere WAP med IP-baserte nett. Mellom WAP-enheten og tjenester på Internett må det imidlertid være en gateway/proxy for å konvertere protokollene (se Figur 9). Et eksempel på gatewayens oppgave er oversetting av WML-kode i klartekst til binærkode før nedlasting til en WAP-enhet. WML er WAP’s svar på HTML (se nedenfor for presentasjon av WML og nettverksprotokollene).

WAP er i dag karakterbasert, men gir mulighet for bitmap-bilder. WAP gir ingen spesiell støtte til multimedia-applikasjoner i nåværende versjon (v. 1.2). Mulitmedia er neppe aktuelt med begrenset båndbredde og lange latenstider i dagens GSM-nett. Multimedia-applikasjoner på WAP-enheter er først aktuelt når GPRS blir bæretjensten for WAP.

3.4.1 Nettverksprotokollene i WAP

For å kompensere for lav båndbredde og lange latenstider i GSM-nettet[19] er protokollene optimalisert for å transmittere så få bits som overhodet mulig per transmisjon, og i tillegg begrense antall transmisjoner til et absolutt minimum. Protokollstakken i WAP er også designet for å ta hensyn til begrenset minne og batterikapasitet i mobile enheter.

WAP er en generell, lagdelt kommunikasjonsarkitektur hvor tjenester og utvidelser vil kunne implementeres på toppen av de spesifiserte protokollene. WAP spesifiserer ikke bæretjenester, men utnytter bæretjenester som allerede finnes. Figur 10 viser protokollstakken i WAP sammenlignet med Internett. Lagene i protokollen forklares nedenfor.

<table>
<tr><th>Internet</th><th colspan="2">Wireless Application Protocol (WAP)</th></tr>
<tr><td>HTML
JavaScript</td><td colspan="2">Wireless Application Environment (WAE)
WML / WML-Script</td></tr>
<tr><td rowspan="2">HTTP</td><td colspan="2">Wireless Session Protocol (WSP)</td></tr>
<tr><td colspan="2">Wireless Transaction Protocol (WTP)</td></tr>
<tr><td>TLS – SSL</td><td colspan="2">Wireless Transport Layer Security (WTLS)</td></tr>
<tr><td rowspan="2">TCP/IP
UDP/IP</td><td>Wireless Datagram Protocol (WDP)</td><td>User Datagram Protocol (UDP)</td></tr>
<tr><td colspan="2">CSD / SMS / USSD / GPRS / CDPD / ETC…</td></tr>
</table>

Figur 10. WAP-arkitekturen sammenlignet med Internett-arkitekturen. Figur fra [AUR99].

Wireless Application Environment (WAE) er det øverste nivået i WAP-stakken. WAE gir omgivelsene som er nødvendig for applikasjoner. De viktigste komponentene i WAE er Wireless Markup Language (WML) og skriptspråket WML-Script.

WML er et tagbasert presentasjonsspråk og ligner en forenklet utgave av HTML.[20] WML er basert på metaspråket [XML]. I WML brukes metaforene *deck* og *card* for å spesifisere en tjeneste. En deck kan bestå av flere cards. Deck er blokken som lastes ned til WAP-enheten. En card er en enhet med informasjon, typisk et skjermbilde. Manøvrering mellom cards i en deck vil være en lokal operasjon i brukerens WAP-enhet. Ideen er å redusere nettverksaksesser. Adressering gjøres med URL som i HTTP. WML har ellers egenskaper som tekstformatering, navigasjonskontroll, elementer av brukerinteraksjon (seleksjoner, input-felt osv), støtte for bilder og variable.

Skriftspråket WML-Script ligner Netscapes JavaScript.[21] WML-Script kan gjøre utregninger og utføre programlogikk. WML-Script kan benyttes til å validere brukerinput så en unngår en tidkrevende rundtur til serveren. Språket gir i tillegg

[19] WAP er uavhengig av bæretjenester. GSM (GSM-data) er bare en av mange mulige bæretjenester.
[20] Se [WML][HTML].
[21] Se [WML-Script] [NSJava].

tilgang til en rekke biblioteksfunksjoner. Sikkerhetsfunksjoner i smartkort og håndtering av adresseboken er eksempler på biblioteksfunksjonalitet. Biblioteks-konseptet gjør at fremtidig funksjonalitet kan legges til uten at basisspråket må endres. *WML-Script gir et programmeringsgrensesnitt til smartkort hvilket er nødvendig for de betalingsløsninger som skisseres senere i denne oppgaven.*

Wireless Session Protocol (WSP) er grensesnittet mellom WAE og resten av protokollstakken. WSP er i det vesentlige en binærversjon av HTTP med følgende tillegg: forhandlinger om egenskaper, caching av headere, støtte for lange sesjoner og push-egenskaper. WSP tilbyr forbindelsesløs eller forbindelsesorientert kommunikasjon til WAE. Hver av disse igjen kan tilbys med eller uten sikkerhet (autentisering, kryptering mm). WSP tilbyr dermed fire forskjellige kommunika-sjonstjenester.

Wireless Transaction Protocol (WTP) kontrollerer sending og mottak av meldinger. Funksjoner i WAP kan velge mellom tre meldingsklasser:

- Upålitelig sending uten svar-melding (mottaker sender ikke ack., ingen retransmisjon).
- Pålitelig sending uten svarmelding (retransmisjon hvis avsender ikke mottar ack.).
- Pålitelig sending med pålitelig svarmelding (treveiskommunikasjon hvor av-sender mottar svar og sender ack.).

WTP forsøker å redusere antall (re-) transmisjoner ved blant annet å slå sammen meldinger.

Brukerbetraktninger: WAP-teknologien er ny, og fra et brukersynspunkt er det en klar ulempe at dagens telefoner ikke er forberedt for WAP. De kan heller ikke oppgraderes. En annen ulempe idag er prispolitikken fra mobiloperatørene. WAP er idag implementert over GSM-data, og det betales fra sesjonsstart til sesjonsslutt. Det mønsteret harmonerer ikke med WAPs transaksjons-orienterte tilnærming til kommunikasjon. En sesjon med WAP vil typisk laste ned flere "sider" med informasjon i en transmisjon, og det kan gå lang tid til brukeren bestemmer seg til å laste ned neste blokk. Det er tydelig at GSM-nettet idag mangler en effektiv pakkebasert kommunikasjonsmodell. Med GPRS vil prispolitikken kunne endre seg fra prising på bakgrunn av tid til prising etter volum.

Wireless Transport Layer Security (WTLS) gir nettverkssikkerhet (se avsnitt 2.5.2) mellom WAP-klienten og WAP-gateway. WTLS gir altså ikke ende-til-ende-sikker-het i kommunikasjon mellom WAP-klient og en server på Internett. WAP-gate-wayen kan imidlertid sette opp en sikker forbindelse mellom gateway og server på Internett, men gatewaymaskinen må konvertere mellom protokollene. WTLS er basert på tilsvarende sikkerhetslag (TSL) over IP og tilbyr integritet ved hash-fuksjon, konfidensialitet ved kryptering, autentisering og ikke-benekting ved hjelp av digitale sertifikater. WTLS vil benytte WDP for både forbindelsesorientert og forbindelsesløs kommunikasjon. Se også avsnitt 5.4.3 for beskrivelse av den smart-kortbaserte modulen som muliggjør sikkerhetsfunksjonene i WTLS.

Wireless Datagram Protocol (WDP) tilbyr et konsistent datagramgrensesnitt for de øvre lag i protokollen mot de underliggende bæretjenestene. WAP-spesifikasjonene omfatter ikke bæretjenester. WDP benyttes ikke hvis bæretjenesten tilbyr datagram. Det betyr at WDP vil benyttes over GSM-SMS, men ikke over GSM-data. Bæretjenestens User Datagram Protocol (UDP) blir benyttet ved GSM-data som indikert i Figur 10.

Figur 11. Bluetooth-enheter skal kunne kommunisere trådløst med inntil åtte enheter i et selvkonfigurerende piconett.

3.5 Bluetooth

Bluetooth er teknologi under utvikling på initiativ fra telekommunikasjonsselskapet Ericsson og andre. Bluetooth er en digital radiostandard som muliggjør kommunikasjon over korte avstander (opp til 10 eller opp til 100 meter avhengig av strømforbruk). Bluetooth transmittere er designet for å bruke lite strøm (1 mW), kommuniserer i høyfrekvensbåndet 2.402 – 2.480 GHz med høye hastigheter (1 Mbits/s). Bluetooth kan supportere en synkron talekanal samtidig med asynkrone, asymmetriske datakanaler. (Mer informasjon om Bluetooth finnes på http://www.bluetooth.org)

Vesentlig i Bluetooth er konseptet om at Bluetooth-enheter automatisk kan sammenkobles i nettverk. Bluetooth gir visjoner om mange spennende bruksområder, som for eksempel:

- Automatisk sammenkobling av PC og mobiltelefon for oppkobling til Internett
- Bildeoverføring fra Bluetooth-kamera til mobiltelefon for lagring på ”nettet”
- Overflødiggjøre kabler: Automatisk sammenkobling og konfigurering av PC’er med periferenheter som printere, scannere, tastaturer osv.
- I betalingstransaksjoner: Overføring av digitale kontanter fra smartkortapplikasjoner i mobiltelefoner til kassaapparater

Bluetooth og lignende teknologier er interessante da de kan realisere betalingsløsninger hvor kundens mobiltelefon er smartkortterminal overfor et kassaapparat i en forretning for eksempel. En slik funksjonalitet ville gjøre mobiltelefonen anvendelig også i andre scenarier enn betaling av tjenester på Internett.

3.6 Oppsummering

Dette kapittelet har handlet om trådløs kommunikasjon i en mobil verden. GSM ble gitt bred dekning fordi GSM er, og vil være, sentral teknologi i mange år ennå for realisering av tjenester som ikke trenger høy båndbredde. De to aktuelle bæretjenestene i GSM-nettet, GSM-data og SMS, ble vist å ha vesensforskjellige egenskaper som gjør dem egnet på hver sin måte. GSM-data har ulempen med å være

linjesvitsjet slik at kunden må betale for tiden han er oppkoblet uansett om han kommuniserer eller ei. GSM-data har imidlertid fordelen av å tilby konstant båndbredde. SMS er pakkesvitsjet og kunden betaler per melding, men SMS har lange latenstider og kan egentlig ikke benyttes til annet enn å sende isolerte enkeltmeldinger. En serverbasert tjeneste som skal føre en dialog med brukeren, eller en tjeneste som skal vise en datastrøm til brukeren, vil kreve tålmodige brukere hvis tjenesten skal implementeres over SMS.

En annen ulempe med dagens bæretjenester i GSM-nettet er den lave båndbredden på bare 9600 bits/sek. Overføring av video eller grafiske animasjoner er for eksempel ikke mulig. Båndbredden er i praksis kun tilstrekkelig til overføring av tekstlig informasjon og stillbilder, hvilket WAP-standarden utnytter på beste måte med WML, WAPs svar på HTML. WAP i mobiltelefonen er interessant fordi WAP gir muligheter til å realisere kommunikasjon med tjenester på Internett.

Det er i dag spesielt to problemer med sikkerheten i GSM: GSM krypterer kun datastrømmen mellom mobil enhet og basestasjon, og denne krypteringen er kun moderat sikker. Det er derfor svært overraskende at disse problemene ikke er skikkelig adressert i WAP. Sikkerhetslaget i WAP (WTLS) som tilsvarer SSL/TSL i Internett-protokollstakken, kan tilby god sikkerhet, men ikke ende-til-ende. WAP-applikasjoner må selv besørge ende-til-ende-sikkerhet med maskiner på Internett.

GPRS ble presentert som kommende løsning på problemene med bæretjenestene SMS og GSM-data. GPRS vil også kunne gi den båndbredden som er nødvendig for multimediaapplikasjoner på WAP-enheter.

Radiostandarden Bluetooth ble nevnt å kunne realisere betalingsløsninger hvor kundens mobiltelefon er smartkortterminal overfor et kassaapparat i en forretning for eksempel.

4 Brukerutstyr

Dette kapittelet presenterer brukerutstyr som scenariet kan realiseres på i dag. Utstyr forsøkes kategoriseres etter deres egenskaper, og deres egnethet i scenariet vurderes. Brukerutstyr for visualisering av demonstratoren velges (mer om demonstratoren i kapittel 9).

Bildetekstene i dette kapittelet har med mange tekniske detaljer. Detaljene er ikke viktige for fremstillingen, men kan gi en idé om funksjonaliteten på utstyr anno år 2000.

Kapittelet avsluttes med en artikkel i Aftenpostens som beskriver *"fremtids-innretning"* som kan bli resultatet av konvergensen innen data og trådløs teknologi.

4.1 Kategorisering

Jeg tar her for meg enheter i håndstørrelse som har spillepotensiale, dvs enheter som er mindre enn en tradisjonell bærbar PC, men større enn for eksempel enheter på størrelse med et armbåndsur.

Det er ikke enkelt å kategorisere det utstyret som finnes, og i bransjen selv eksisterer det en viss begrepsforvirring. Et forsøk på kategorisering etter maskinutstyr kan være følgende inndeling – fra de minste mobile PC'er til de minste spesialiserte spillemaskiner:

- Miniatyr-PC'ene
- Håndmaskiner / Palmtops / PDA / Organizers
- WAP-telefoner
- Blandingsprodukter mellom håndmaskinen og mobiltelefonen
- Rene spillemaskiner

Teknologien kan også kategoriseres etter leverandørenes valg av operativsystem:

- Tradisjonelle operativsystemer
- Windows-CE fra Microsoft
- EPOC (fra Symbian som Psion, Ericsson, Nokia, Motorola og Matsubishita står bak)
- Palm-OS (fra Palm Computing som eies av 3COM)
- Operativsystemer fra andre leverandører

De ulike enhetene har forskjellige anvendelsesområder, og kategorisering etter applikasjoner og muligheter kan også være interessant. En meningsfull inndeling kan være følgende:

? Kontorapplikasjoner
? "Generelle" applikasjoner
? Epost
? Spill
? Grafiske muligheter / andre muligheter

Ytterligere en dimensjon kunne vært kategorisering etter enhetenes evne til kommunikasjon og integrasjon med andre enheter eller med omverdenen. I det følgende presenteres en maskinvareorientert tilnærming til enhetene, og hver klasse blir eksemplifisert med en typisk representant for klassen.

Figur 12 Eksempel på miniatyr-PC. Toshiba Libretto Modell 110CT har følgende spesifikasjoner: Ytre mål: 21 cm x 13 cm x 3,5 cm. Vekt: 1000 g. Operativsystem: Windows 98 eller Windows NT. Fargeskjerm: 7.1" aktiv matrise 800x600 punkter, 80 tasters tastatur med innebygget pekedevice ("mus") ved skjermen. Prosessor: 233MHz Intel Pentium MMX. Maksimum 64MB RAM, 4.3 GB disk. 16bit stereo lyd. 2.5 timers batterikapasitet. Ekstern diskettstasjon og andre eksterne tilkoblingsmuligheter gjennom påkobling av portreplikator. (Bilde og informasjon fra http://www.toshiba.com sept.1999)

4.2 Miniatyr-PC'ene

Miniatyr-PC'ene[22] er fullblods PC'er i miniatyr (se Figur 12). De har funksjonalitet og programvare som større modeller, men dekker et behov der portabilitet, vekt og størrelse har betydning. Miniatyr-PC'ene har QWERTY tastatur og farge-LCD-display. Det er en grense for hvor små en kan gjøre generelle datamaskiner med generell programvare før det går på bekostning av brukergrensesnittet. Miniatyr-PC'ene har antakelig passert denne grensen når det gjelder generell bruk; de er for små til å erstatte den tradisjonelle bærbare PC, men for stor og dyr til å erstatte de dedikerte håndmaskinene. En ulempene er at programvare ikke er tilpasset miniatyr-PC'ens minimalistiske skjerm og tastatur. Vekt, størrelse og pris taler også mot bruk av miniatyr-PC'en som spillemaskin.

Fordelene med miniatyr-PC'en er at den har kjent operativsystem og kjent programvare, og at den har integrasjonsmuligheter som en vanlig PC.

[22] Engelsk: Mini-notebooks

4.3 Håndmaskiner

Innenfor kategorien *håndmaskiner*[23] finnes det flere inkompatible, konkurrerende systemer. Håndmaskinene er mindre og lettere enn miniatyr-PC'ene. Felles for klassen er at maskinene lar seg holde eller bære i håndflaten. Et annet fellestrekk er at de har operativsystem og programvare tilpasset små enheter – i motsetning til miniatyr-PC'ene. Input-enheter i denne klassen er gjerne spesielt peke/skrive-utstyr og/eller tastatur.

En håndmaskin har funksjonalitet som gjør at den kan erstatte en papirutgave av en "syvende sans". Typiske applikasjoner er tidsplanlegger med alarm, adressebok, notatblokk, frihåndstegning og elektroniske visittkort. Leverandørene tilrettelegger for at andre skal kunne utvikle applikasjoner og utstyr. Det er derfor ikke uvanlig at det finnes en stor applikasjonsportefølje til maskinene. Spill er utbredt på denne plattformen. Posisjoneringssystemer koblet til GPS, med visning av maskinens posisjon på et kontinuerlig oppdatert kart, er et eksempel på en sofistikert applikasjon på håndmaskiner.

Det er en rekke forskjellige operativsystemer for håndmaskiner. Microsoft Systems har forsøkt å penetrere dette markedet med sitt plattformuavhengige operativsystem Windows-CE. De store mobiltelefonprodusentene har på sin side samlet seg om operativsystemet EPOC som de utvikler i fellesskap med Psion. Palm-OS er et annet utbredt operativsystem på modellene fra Palm Computing. Det finnes flere andre operativsystemer, men de nevnte systemene har størst utbredelse i markedet. Palm-OS har 68% av markedet ifølge [DIGI140999].

Håndmaskinene er gjerne godt utbygget med kommunikasjonsmuligheter. De har vanligvis trådløs, infrarød kommunikasjon til printer og PC, og synkronisering av data med standard PC-baserte applikasjoner. De mer avanserte maskinene har Internettilgang over innebygget TCP/IP kommunikasjonsprotokoll og infrarød kommunikasjon til mobiltelefon. Noen har sogar også bygget inn mobilaksess i håndmaskinen.[24]

Håndmaskinen faller naturlig i to klasser – med og uten tastatur.

4.3.1 Håndmaskiner med tastatur

Disse ligner på miniatyr-PC'ene ved at de begge har tastatur og liten skjerm. Håndmaskinene drar nytte av å være spesialdesignet, med tett kobling mellom applikasjoner og fysisk maskinutrustning. En fordel med denne typen maskiner er at tastaturet er en velkjent inputenhet. En ulempe er at et QWERTY-tastatur nødvendigvis vil gi enheten en viss fysisk størrelse.[25]

[23] På engelsk benyttes begrepene *handhelds, palmtops, PDA (personal digital assistant)* og *organizer* om hverandre

[24] Palm VII fra Palm Computing har innebygget aksess til mobilnettet. Dette er en proprietær løsning som ligner WAP, men er foreløpig bare tilgjengelig på utvalget steder i USA (www.palm.com, september 1999)

[25] Utbrettbare tastaturer kan hjelpe, men det finnes ennå ikke produkter som krymper til "akseptabel" størrelse sammenslått.

Figur 13. Håndmaskiner med tastatur. Her eksemplifisert med Psion Series 5MX. Maskinen har følgende spesifikasjoner: Ytre mål: 17 cm x 9 cm x 2,3 cm. Vekt: 350 g. Operativsystem: EPOC 32 bits multitasking. Skjerm: 640x240 punkter 16 gråtoner (100 tegn per linje, 26 linjer), 53 tasters tastatur, trykkfølsom skjerm og knapper på siden av skjermen for hurtigvalg av applikasjoner, pekeenhet (”mus”). Prosessor: 36MHz ARM710T RISC. Maksimum 16MB (intern) RAM, ingen disk. Innebygget høyttaler og mikrofon. Batterikapasitet: 30 dager. Innebygget funksjonalitet: Lydopptaks- og avspillingsmuligheter for opptil 1 time; Infrarød kommunikasjon til mobiltelefoner (som vist på bildet) for Internettilgang, PC’er, printere eller andre Psion håndmaskiner for utveksling av elektroniske visittkort eller annen informasjon. (Bilde og informasjon hentet fra http://www.psion.com)

4.3.2 Håndmaskiner uten tastatur

Det mest karakteristiske med denne kategorien er at gjenkjenning av håndskrift benyttes som inputmetode. Brukeren skriver med penn på den trykkfølsomme skjermen, og maskinen forsøker å tolke bokstav for bokstav. Forskjellige inputmodeller benyttes. Håndmaskinene fra Palm Computing har for eksempel et spesialalfabet som brukeren må lære. Andre modeller lar *brukeren* lære opp maskinen.

Håndmaskinene uten tastatur er mindre enn modellene med tastatur. Kapasitets-messig kan de være noe svakere. Håndmaskiner uten tastatur gir bedre muligheter til å jobbe stående eller i miljøer hvor det kan være vanskelig å finne en god tradisjonell arbeidsstilling. En ulempe er at brukeren må venne seg til et alfabet maskinen kan forstå, eller brukeren må lære opp maskinen.

Figur 14. Eksempel på håndmaskin uten tastatur. Palm Pilot V fra Palm Computing. Maskinen har følgende spesifikasjoner: Ytre mål: 11.4 cm x 7,9 cm x 1 cm. Vekt: 110 g. Operativsystem: Palm OS. Skjerm: 160x160 punkter, 16 gråtoner. Trykkfølsom skjerm og håndskriftgjennkjenning og/eller minitastatur på skjerm som betjenes av pekeredskap; knapper på siden av skjermen for hurtigvalg av applikasjoner. Prosessor 16MHz Motorola DragonBall EZ. 2 MB RAM, ingen disk. Beeper for akustiske beskjeder. Batterikapasitet: 30 dager. Innebygget funksjonalitet: Infrarød kommunikasjon til mobiltelefoner (Internettilgang) , printere, PC’er eller til andre Palm maskiner for utveksling av elektroniske visittkort eller annen informasjon. (Bilde og informasjon hentet fra http://www.palm.com)

I spillesammenheng er håndmaskinen uten tastatur godt egnet. Den er liten og relativt billig, og dens grafiske muligheter blir stadig bedre. Håndmaskinen kommer

nå også med innebygget aksess til Internett og WAP-nettleser.[26] *Med WAP på håndflaten og rask og enkel aksess til Internett kan håndmaskinen vise seg å bli en interessant mobil innretning – også i spillsammenheng.*

4.4 WAP-mobiltelefoner

Figur 15 er et eksempel på at det tradisjonelle brukergrensesnittet fra dagens mobiltelefoner er beholdt i nye WAP-telefoner. Til tross for at mobiltelefonens numeriske tastatur er lite egnet til tekstlig input, så integreres stadig mer av håndmaskinens funksjoner (se bildeteksten). Sammenlignet med håndmaskinen har WAP-telefonen liten skjerm. I sammenhenger (spill eller andre) hvor skjermens størrelse er viktig er ikke WAP-telefonene godt egnet.

I spillscenariet i denne oppgaven vil den tradisjonelle (WAP-) mobiltelefonen imidlertid være godt egnet fordi scenariet neppe stiller store krav til skjerm eller grafikk. Produsenter av WAP-telefoner annonserer at selv ordinære mobiltelefoner (billigmodeller) vil komme med WAP-funksjonalitet.[27] *Det betyr at disse telefonene vil ha et enormt markedspotensiale. En tjenesteleverandør (spilltilbyder eller andre) bør med andre ord implementere tjenester som kan fungere tilfredsstillende på denne type enheter. I demonstratoren i kapittel 9 er det valgt å visualisere spillet med et produkt fra denne kategorien.*

Figur 15. Siemens S25. Eksempel på dagens ordinære WAP-mobiltelefon. Telefonen har følgende funksjonalitet: Integrert WAP browser, 20 sek. taleopptak, kalkulator, datovisning og klokke med alarm, tidsplanlegger med alarm, valutakursomregner, elektronisk visittkort, 3 spill, integrert modem for data/fax transmisjon via grensesnitt, vibrator ringe-alarm, 40 ringelyder. Ytre mål: 11,7 cm x 4,7 cm x 2,4 cm. Vekt: 125 g. Fargeskjerm: 6 linjer á 16 tegn. (Bilde og informasjon fra http://www.siemens.de)

4.5 Mobiltelefoner med håndmaskinfunksjonalitet

Sammensmeltingen av teknologier er tydelig i produktene som kombinerer tradisjonelle mobiltelefontjenester med den håndholdte datamaskinens egenskaper. Disse hybride enhetene er mobiltelefoner med håndmaskinfunksjonalitet eller håndmaskiner med mobilfunksjonalitet – alt etter hvordan man ser det. Anvendelsesområdet er typisk trådløs tale, personlig assistent og trådløs Internettilgang.

[26] Se http://www.ausys.se/wap (4.1.00)
[27] Motorola annonserer at alle nye digitale telefoner vil ha implementert WAP-teknologi i år 2000 (Nettavisen 19.3.99, http://www.nettavisen.no). Nokia har senere meldt det samme.

I spillesammenheng er disse enhetene ideelle. De kombinerer den håndholdte maskinens egenskaper med integrert tilgang til Internett.

Figur 16. Mobiltlelefoner med håndmaskinfunksjonalitet kombinerer den håndholdte maskinens egenskaper med innebygget trådløs Internetttilgang – i tillegg til trådløs taletjeneste. Her eksemplifisert med Ericsson R380 (t.v.) Qualcomms pdQ 1900 og Nokias Communicator 9110. Ericssons modell lanseres våren 2000, vil implementere WAP og ha EPOC operativsystem fra Symbian. Qualcomm-modellen er bygget på teknologien fra Palm Computing. Nokias modell benytter GEOS operativsystem fra Geoworks (Bilder hentet fra http://www.ericsson.se, http://www.qualcomm.com og http://www.nokia.com)

4.6 Produktkonvergens

Mobiltelefonene, håndmaskinene og de rene spillemaskinene[28] er i full gang med å integrere teknologi fra hverandre. Fra et teknologisk synspunkt har disse produktene potensiale til å smelte sammen til ett produkt i nær fremtid. En annen ting er om en sammensmelting er klokt ut fra markedsmessige eller andre hensyn.

Aftenposten skriver følgende om konvergensen innen data og telefoni og de mulighetene det kan gi. Scenariene synes alle å være innenfor mulighetenes grenser:

> "… I løpet av de nærmeste par årene kan vi vente oss den nye universalinnretningen i salg. Industriens mål er at den skal gå inn som allemannseie, som en sentral for alle de tjenester man etterhvert kan bruke en datamaskin og en trådløs telefon til, og det er jo som kjent det meste. I det ytre vil den se ut som en mobiltelefon, der man kan åpne lokket og ha telefon på den ene siden, PC på den andre, tilkoblet fax og Internett med e-post. Innen kort tid kan vidunderet også brukes som radio og fjernsyn og med all slags underholdningselektronikk innlagt – en videreføring av data og teleteknologi flyter stadig tettere sammen med mediene.
>
> Samme lille tingest kan også brukes til telefonmøter og billedtelefon. Den vil selvsagt kunne fylle oppgaven som vekkerklokke, som regnskapsbok, adressebok, arkiv og elektronisk kalender. Forsøk har vist at den kan brukes som fjernkontroll til et uttall av tjenester. Den kan virke som nøkkel til hus og

[28] Dedikerte spillemaskiner som Gameboy fra Nintendo er ikke nevnt i denne oppgaven. Nintendo annonserer imidlertid at neste generasjon Gameboy vil ha muligheter for flerbrukerspill over Internett, e-post og annet. Se http://www.nintendo.com/corp/press/090199b.html (06.09.1999)

bil, den kan styre automater av alle slag, der en tallkode erstatter myntinnkast, og man vil kunne betjene bilvaskemaskinen med den uten å gå ut av bilen, om man skulle ha trang til dette. Snart vil den kunne betjene kjøkkenmaskiner i hjemmet så vel som kontormaskiner, avlese strømforbruket og slå strømmen av og på, brukes som uttakskort i kontantautomater, håndtere alt fra sikkerhetsalarmer til påfyll i brusautomater. Den vil ordne banktransaksjoner og innkjøp per elektronisk handel, bestille biletter og følge med i nyhetene, den vil hente opp værmeldinger og trafikkopplysninger og dertil alt det som i dag er informasjon på tekst-TV, den vil gi og motta meldinger av alle slag, skaffe oversikt over aksjekursene eller repertoaret på kino og teater, og betale bompenger. Selvsagt kan den brukes til spill, med eller uten penger som innsats. Den vil kunne gjøre nytten som «elektronisk fotlenke» til å sende ut signaler, slik at mine nærmeste kan holde følge med hvor jeg til en hver tid befinner meg, som om jeg var en ringmerket bjørn, og jeg kan holde følge med dem. Dette siste er blant de mer risikable bruksmåter. …" Aftenposten 5.1.99

Figur 17. Universalinnretningen slik Nokia tenker seg den. Bilde fra www.nokia.com

4.7 Oppsummering

Dette kapittelet har vist brukerutstyr, fra PC'er i miniatyrformat til håndholdte maskiner og avanserte mobiltelefoner. Utstyrets anvendbarhet i spillsammenheng i scenariet ble vurdert.

Håndmaskinen uten tastatur ble funnet godt egnet til spill. Den er liten og relativt billig, og dens grafiske muligheter blir stadig bedre. Den kommer nå også med innebygget WAP-nettleser og aksess til Internett.

Den tradisjonelle (WAP-) mobiltelefonen vil være særdeles godt egnet i scenariet som beskrives i denne oppgaven, fordi scenariet neppe stiller store krav til hverken skjerm eller grafikk. I nær fremtid vil selv ordinære billigtelefoner komme med WAP-funksjonalitet, og det gir denne kategorien telefoner et enormt markeds-potensiale. En tjenesteleverandør som er interessert i å nå ut til flest mulig, må derfor levere tjenester som fungerer optimalt på den ordinære WAP-mobiltelefonen. Demonstratoren i kapittel 9 visualiseres på en slik telefon.

5 Smartkort

Dette kapittelet gir en kortfattet bakgrunn om smartkort. Grunnleggende teknologier blir gjennomgått og aktuelle standarder blir presentert. Smartkortmodulene i mobiltelefoner gis spesiell oppmerksomhet. Smartkort er nødvendig for å ivareta sikkerhetsbehovene i en åpen og usikker Internett-verden. Smartkort kan benyttes i pengeapplikasjoner for eksempel, eller til generelle integritets-, autentiserings- og konfidensialitetsformål i mobil sammenheng.

5.1 Bakgrunn

Begrepet *smartkort* benyttes gjerne om en spesiell type integrerte kretskort (IC-kort) med prosesserings- og datalagringskapasitet. Et smartkort kan sammenlignes med en tradisjonell PC *uten* egen strømkilde eller PC'ens input/output-enheter. Kortet er helt avhengig av en kortleser for strøm og kommunikasjon med omverdenen.

Den grunnleggende ideen bak smartkort er idéen om en sikker og "tuklefri" enhet for bruk i en elektronisk verden. Smartkortets egenskaper gjør det egnet til å løse sikkerhetsrelaterte problemer. Beskyttelse av minnet i et smartkort er vesentlig; minnet vil kun være tilgjengelig gjennom prosessoren, som vil beskytte minnet mot forsøk på kompromittering.

Den første smartkortrelaterte patenten kom i 1968 da Jurgen Dethloff og Heilet Grotrupp patenterte ID-kort med integrerte kretser. Selve begrepet *smartkort* ble patentert av franskmannen Rolan Moreno. Moreno søkte patent på hele 47 smartkortrelaterte applikasjoner i tilsammen 11 land i perioden 1974-79. Det nye i Morenos patenter var en prosessor som kunne utføre enkle regneoperasjoner. [Høe99][Berge98].

Det var Bull som produserte det første kortet i 1975. Kortene var lenge for dyre, og det var først i 1984, da Fransk Telecom gjennomførte et vellykket pilotprosjekt, at de kom i alminnelig bruk.

I en periode på 80-tallet benyttet de norske forretningsbankene smartkort som debetkort, før magnetstripekortene overtok. Magnetstripekortene var billigere i produksjon. Først i disse dager kan smartkort være på vei inn igjen i det norske banksystemet, ved at BBS og de norske bankene vil satse på Proton for elektroniske kontanter [Proton].

Smartkort anvendes i dag i en rekke sammenhenger hvorav én aktuell anvendelse for denne oppgaven er som SIM-kort i mobiltelefoner. I dag finner vi smartkort som adgangskort, identitetskort, lojalitetskort, billettkort, småpengekort, osv. Norge ligger imidlertid langt etter resten av Europa med å ta i bruk smartkort [Berge98].

En signifikant utvikling i den senere tid er nye og enklere programmeringsmodeller som skjuler kompleksiteten rundt utvikling av applikasjoner på smartkort (Java for smartkort), og multiaplikasjonskortene som er generelle operativsystemer for administrasjon av applikasjoner på smartkotene. Sistnevnte omtales nedenfor.

Selv om sikkerheten i smartkort skal være godt ivaretatt, finnes det eksempler på angrep på smartkort, både fysiske angrep og logiske angrep [Husemann99].[29] Sikkerhet i smartkort er under konstant forbedring.

5.2 Basisteknologi

Smartkort er medlem av Integreated Circuit (IC) familien. Det finnes tre kategorier IC-kort:

? Minnekort
? Minnekort med sikkerhetslogikk
? Smartkort

Alle korttypene har minne i en eller annen form. De rene *minnekortene* er skrive- og lesbare og benyttes for lagring av informasjon. Minnekortene er ikke standardiserte, hverken på plassering eller størrelse av minnet, eller på protokollnivå i kommunikasjonen med kortleser. Minnekortene benyttes i dedikerte systemer hvor kort og kortleser er designet for å spille sammen. Et typisk eksempel kan være engangs telefonkort.

Minnekortene med sikkerhetslogikk er som minnekortene, men har i tillegg innebygget logikk i maskinvaren som en del av kortets grunnleggende egenskaper. Dette kan være aksessnøkler for autentisert aksess til minnet, eller logikk som for eksempel kun tillater å dekrementere minnet. En typisk anvendelse er kort som benyttes til forhåndsbetalte tjenester, hvor et ”beløp” trekkes fra kortet ved bruk. I dette tilfellet vil sikkerhetslogikken forhindre muligheten for å øke kortets beløp.

Den tredje klassen, *smartkortene*, har prosessor, RAM, ROM og EEPROM i tillegg til et enkelt I/O system og gjerne et avbruddssystem. Typiske smartkort har i dag bare 16KB EEPROM for persistent lagring av informasjon.

Figur 18. Parter i smartkortkommunikasjon. (Smartkort t.h.)

[29] Siste nytt: (31.1.00) Brudd på smartkortsikkerheten skaper panikk i det franske bankvesen [DIGI310100].

5.2.1 ISO 7816

Smartkort følger ISO 7816 spesifikasjonene fra standardiseringsorganisasjonen ISO [ISO7816]. Spesifikasjonene består av seks deler:

1. Fysiske karakteristika ved smartkort (ISO 7816-1).
2. Plassering av kontakter og dimensjoner (ISO 7816-2).
3. Elektriske signaler og lavnivå transport (ISO 7816-3).
4. Kommunikasjonsprotokollene *mellom smartkort og kortleser* (ISO 7816-4).[30]
5. Nummereringssystemer og applikasjonsidentifikatorer (ISO 7816-5).
6. Standardiserte dataelementer (ISO 7816-6).[31]

ISO 7816-4 har særlig interesse da den spesifiserer protokolldataenhetene, de såkalte Application Protocol Data Units (APDU), i kommunikasjonen. ISO 7816-4 spesifiserer i tillegg hvordan lagringssystemet på smartkortet kan organiseres som et filsystem. I tillegg adresseres metoder for ”sikre meldinger” (autentisering og konfidensialitet) og aksessmetoder til algoritmer i kortet.

En smartkortbasert *applikasjon* defineres i ISO-sammenheng som et sett med sikkerhetsmekanismer, filer, data og protokoller (ikke inkludert transmisjonsprotokollene).

Man kan si at en applikasjon er det grensesnittet som smartkortet tilbyr kortleser og vertsapplikasjonen (Figur 18). Man kan se på smartkortet som en tjener, og kortleser/vertsapplikasjon som en klient som gjør bruk av tjenestene.

Smartkortbaserte applikasjoner kan ikke fungere uten en vertsapplikasjon som kjenner dens filstrukturer og meldingsformater. I en mobiltelefon vil vertsapplikasjonen ligge i selve mobiltelefonen. Mobiltelefonen vil sende kommandoer (APDU) til kortleseren som styrer ISO7816-grensesnittet til smartkortet (SIM-kortet). Kortleser videresender APDU’ene til smartkortet. Respons formidles tilbake til vertsapplikasjonen omvendt vei. I andre systemer vil vertsapplikasjonen ligge i en PC eller i et kassaapparat for eksempel.

ISO 7816 må forstås som et rammeverk for smartkort. Standarden spesifiserer for mange opsjoner til at det er praktisk å implementere dem alle. Resultatet er at enheter som hevder å støtte standarden ikke nødvendigvis er kompatible.[Husemann99]

5.2.2 Andre standarder

Smartkortleverandørene har tradisjonelt bundet kundene til proprietære løsninger hvor hver leverandør har kontrollert alle ledd i kjeden: kort, kort-operativsystem og

[30] 18 kommandoer: select file, read binary, write binary, update binary, erase binary, read record, write record, log record, update record, get data, put data, verify, internal authenticate, external authenticate, get shallenge, get response, envelope.
[31] 4 dataelementer: name, address, PIN, expiration date.

kortleser, hvilket har ført til inkompabilitet i alle ledd mellom utstyr fra forskjellige leverandører.

Hvis det eksisterer usikkerhet rundt ISO 7816 for grensesnittet mellom smartkort og kortleser, så er usikkerheten til hvordan ISO 7816 skal tolkes ved implementasjonen av selve kortleseren enda større. Inkompatible kortleserer har vært et betydelig problem [Husemann99]. De siste årene er det imidlertid initiativ som forsøker å standardisere alle sider ved kortlesere, og i tillegg definere et programmerings-grensesnitt til selve kortleseren. To slike initiativ for *generelle* smartkortsystemer er:

? *OpenCard Framework* (OCF) fra OpenCard Consortium.[32]
? *PC/SC*. Microsoft-initiert (først og fremst for Windows 9X maskiner).[33]

OCF spesifiserer en lagdelt arkitektur og et veldefinert grensesnitt for applikasjons-programmereren. PC/SC kan benyttes som et lag under OCF i grensesnittet mot kortleseren på Windows-plattformen.

Det finnes også initiativ til å spesifisere smartkortsystemer for *spesielle* anvendelser. De store kredittselskapene har drevet frem spesifikasjoner for betalingssystemer[34]: [Berge98]
? EMV'96
? Visa ICC
? SET c.2.0
? Visa Open Technology Platform

Avsnitt 7.3.1 beskriver EMV, en aktuell debet/kreditt applikasjon i scenariet. Mens OCF og EMV spesifiserer grensesnitt mellom smartkort og vertsapplikasjon, skjer det en annen interessant utvikling med fokus på selve smartkortet. To trekk er fremtredende: Nye og enklere programmeringsmodeller (Java) skjuler kompleksiteten rundt utvikling av applikasjoner på smartkort, og smartkort er i ferd med å frigjøre seg fra leverandørkontrollerte operativsystemer på selve kortene. Sistnevnte utviklingstrekk presenteres i neste avsnitt.

5.3 Multifunksjonssmartkort

Multifunksjonskort er smartkort med mulighet til å holde flere enn én smartkort-applikasjon. ISO 7816 legger grunnlaget for å utnytte slik funksjonalitet ved å gi vertsapplikasjonen et sett med protokoller for å avgjøre hvilke applikasjoner som finnes i kortet, og hvilken applikasjon det skal sendes kommandoer til.

Tradisjonelt har smartkort vært fast programmerte. Kode og data i applikasjoner har vært lagt inn ved produksjonen eller den såkalte "personaliseringen" av kortene, og deretter kan programvaren i kortene ikke erstattes eller kompletteres.

[32] Se http://www.opencard.org (6.1.2000)
[33] Se http://www.smartcardsys.com (6.1.2000)
[34] Se http://www.vise.com og http://www.mastercard.com (6.1.2000)

Nyere standarder for multifunksjonskort går et skritt videre og tilbyr dynamisk sletting og lasting av applikasjoner på smartkortet. For denne funksjonaliteten må kortet ha et spesiell operativsystemstøtte. Det er tre aktuelle operativsystemer for såkalte *multiapplikasjonskort* for tiden:

? MULTOS
? JavaCard
? Smart Card for Windows (kun annonsert)

Vertsapplikasjonen vil forholde seg til grensesnittet, og det spiller derfor ingen rolle hvilken av standardene ovenfor som smartkortet er realisert på. Det spiller heller ingen rolle om vertsapplikasjonen kommuniserer med et smartkort med kun én applikasjon, eller om det er et smartkort med fast programmerte applikasjoner. Det spiller heller ingen rolle hvilket *programmeringsspråk* smartkortapplikasjonen er implementert i.

Utviklingsmiljøer for multiapplikasjonssmartkort (og smartkort generelt) lar brukeren utvikle og teste applikasjonen på en PC før nedlasting til kortet. For mulitapplikasjonskortene gjelder at en applikasjon som er utviklet for en bestemt plattform i utgangspunktet skal kunne kjøre på hvilket som helst kort med denne plattformen.

Smartkort-operativsystemene tilbyr i hovedtrekk: [Lie99]
? Administrasjon av applikasjoner, først og fremst nedlasting.
? Aktivering og kommunikasjon med applikasjoner (håndtering av kommunikasjonsprotokollen mellom kort og kortleser).
? Isolasjon mellom applikasjonene.
? Bibliotek av funksjonalitet av generell nytte, for eksempel kryptografi.
? Utviklingsverktøy for å programmere og teste ut applikasjoner.

Multiapplikasjonskortene er relativt nye, og det finnes flere interessante utfordringer og spørsmål [Husemann99]:
? Gjennomførbare løsninger for installasjon og deinstallasjon av applikasjoner mens kortene er i bruk må etableres.
? Hvem eier kortet? Er det kortholderen som bestemmer over innholdet eller er det organisasjonen som utstedte kortet? Hvem eier de private dataene?
? Ettersom vi blir mer avhengige av smartkort trenger vi ordentlig håndtering av hele kortets livssyklus: Et pålitelig backupsystem for tapte kort kan være nødvendig. Hvordan flytter vi applikasjoner fra ett kort til et annet?
? Kan vi stole på at sikkerheten er god nok?

Mulitapplikasjonskortene er interessante fordi de gir muligheter til å realisere betalingstjenester og elektroniske identitetstjenester på mobiltelefoner. Applikasjoner kan sam-eksistere og administreres hver for seg. Ved bruk av multiapplikasjonskortene, vil det (antakelig) være brukeren som bestemmer hvilke applikasjoner som skal ligge i kortet, og brukeren vil (antakelig) ikke måtte knytte seg til kun én leverandør.

5.4 Smartkort i GSM-mobiltelefoner

5.4.1 SIM

Svært mange personer bærer med seg et smartkort i dag uten å være klar over det. Smartkortet i GSM-telefoner (SIM-kortet - Subscriber Identity Module) sin viktigste oppgave er å gi basis sikkerhetsfunksjoner (autentisering og kryptering) i tillegg til eventuell mulighet for lagring av brukerdata (adressebok). Autentisering er nødvendig for identifisering av sesjonen og for fakturering. Grensesnittet til SIM-kortet er definert av ETSI [GSM11.11].[35] Typiske SIM-kort har fra 8 til 16KB EEPROM.

Viktige sikkerhetsrelaterte funksjoner i SIM-kortet er SIM-identitetsnummer (IMSI), krypteringsnøkkel og krypteringsalgoritmer. Ved påslag av telefonen avkreves brukeren en PIN-kode. PIN-koden er nødvendig for å aktivere GSM-applikasjonen i kortet. Nøklene som benyttes i autentiserings- og krypteringsalgoritmene forlater aldri SIM-kortet; SIM-kortet gjør nødvendig prosessering for mobiltelefonen. Kryptering i GSM-nettet skjer med den såkalte A5-algoritmen i telefonen. A5 benytter nøkler som er generert med A8-algoritmen. Nøkler genereres på nytt for hver sesjon. Krypteringen er symetrisk ved at den samme nøkkelen benyttes både til kryptering og dekryptering. For vanlige samtaler skal krypteringen være god nok. [Nurkic97]

5.4.2 SIM Application Toolkit

SIM Application Toolkit (SIM-Toolkit) er interessant, da teknologien kan gi både brukergrensesnittet og smartkortbasert sikkerhet på mobiltelefoner for scenariet.

SIM-Toolkit er smartkortfunksjonalitet spesifisert av ETSI [GSM11.14]. SIM-Toolkit tilbyr valgfri tilleggsfunksjonalitet for – i første rekke mobiloperatørene – slik at operatørene kan konkurrere på tilleggstjenester overfor forbrukerne. På samme måte som SIM-kortet eies av mobiloperatøren, vil også funksjonaliteten som operatørene tilbyr ved hjelp av SIM-Toolkit være eiet av operatørene. Fysisk vil SIM-Toolkit typisk være plassert på mobiltelefonens SIM-kort. Telefonen må være forberedt for SIM-Toolkit for å utnytte mulighetene.

SIM-Toolkit gir operatørene mulighet til å legge applikasjoner på SIM-kortet. Det finnes kommandoer for å integrere SIM-Toolkit-applikasjoner i telefonens menyer, slik at applikasjonene kan selekteres av brukeren. I forhold til et ordinært SIM-kort (GSM11.11), er SIM-Toolit såkalt proaktiv og kan selv initiere sending av kommandoer til mobiltelefonen. SIM-Toolkit-applikasjonen kan på den måten styre mobiltelefonens brukergrensesnittet. SIM-Toolkit-applikasjonen rår over kommandoer (APDU'er) for å vise tekst, lese input, spille av en melodi osv.

SIM-Toolkit-applikasjonen kan instruere mobiltelefonen om å sende SMS-meldinger, og mobiltelefonen kan sende (svar-) meldinger direkte til SIM-Toolkit-applikasjonen. Begge deler automatisk - uten å involvere brukeren. På denne måten

[35] ETSI-dokumenter ligger åpent tilgjengelig fra http://www.etsi.org

kan SIM-Toolkit-applikasjoner kommunisere med tjenester i det landbaserte telenettet eller på Internett.

For bæretjenesten SMS spesifiserer [GSM03.48] kryptering og digital signering av SIM-Toolkit-meldingene slik at sikker kommunikasjon mellom SIM-Toolkit-applikasjonen og SMS-senteret (SMSC – se Figur 4) er mulig. En svakhet er at kommunikasjonen kun er sikret mellom applikasjonen og SMSC. Applikasjoner som er opptatt av sikkerhet må implementere egen sikkerhet på toppen av GSM03.48.

En annen interessant egenskap er kommandoen ”Provide Local Information” hvor applikasjonen kan spørre mobiltelefonen om lokasjonsinformasjon. Kommandoen returnerer blant annet en identifikator for ”current serving cell” og identifikasjon av mobiltelefonen (IMEI). Førstnevnte egenskap er funksjonalitet som er ønsket i scenariet for å kunne avgjøre hvor brukeren befinner seg.

SIM-Toolkit har i tillegg kommandoer for å avgjøre om det finnes ekstra smartkort i mobiltelefonen, og å sende APDU’er til disse. Det er spesielt to grunner for å ha et smartkort i tillegg til SIM-kortet i mobiltelefonen: SIM-kortet er mobiloperatørens eiendom, og det er ikke sikkert at det er i operatørens, brukerens eller (eventuelt) bankens interesse å legge for eksempel en småpengeapplikasjon ned i SIM-kortet. Det andre grunnen til at det kan være interessant med et ekstra smartkort i dag, er SIM-kortets (foreløpige) begrensede lagringsressurser. Denne begrensningen kan forsvinne etterhvert som lagringsteknologien forbedres. Typiske SIM-Toolkit-kort har i dag kun 16 KB EEPROM.[36]

Mobiloperatørene kan fjernadministrere SIM-Toolkit-applikasjoner. Sletting av applikasjoner og nedlasting av nye applikasjoner kan skje ved ”cell broadcast” eller ”point-to-point” kommunikasjon.

SIM-Toolkit er relativt nytt på det norske markedet. Telenor benytter SIM-Toolkit i MobilHandel-løsningen som Telenor har implementert for FilmWeb. Denne tjenesten tillater kjøp av billetter hvor blant annet debitering av brukerens bankkonto er en av betalingsmodellene. (Beskrevet nærmere i avsnitt 7.6.)

SIM-Toolkit gir mye av den funksjonaliteten som er ønsket i scenariet. Integrasjon av spilletjenesten i mobiltelefonens menyer er elegant. Meldingssikkerheten er rimelig godt tatt vare på, selv om SMSC er et svakt punkt. Det er derfor viktig at applikasjoen selv ivaretar sine sikkerhetsbehov. I såkalte dual-slot-telefoner er det mulig å kommunisere med smartkortbaserte bankapplikasjoner; sikkerheten ved betalingstransaksjoner antas i så fall ivaretatt. I tillegg tilbyr SIM-Toolkit lokasjonsinformasjon som kan gjøre det mulig å bestemme innenfor hvilken celle mobiltelefonen befinner seg. Dette var ønskelig i spillscenariet.

[36] GSM 02.19 anbefaler minimum 24 KB ROM, 1 KB RAM og 16 KB EEPROM.

5.4.3 Wireless Identity Module i WAP

Sikker kommunikasjon i WAP er viktig når WAP-enheter skal benyttes til å foreta pengetransaksjoner og andre følsomme transaksjoner som overføring av spillebong i spillscenariet. Wireless Transport Layer Security (WTLS) tilbyr autentisering og kryptering, og er optimalisert for bruk i mobile omgivelser (se avsnittet 3.4.1).

Wireless Identity Module (WIM) i WAP er den smartkortbaserte sikkerhetsmodulen som muliggjør sikkerhetsfunksjonene i WTLS. WIM beskytter private nøkler; de vil aldri forlate WIM. For WTLS utfører WIM blant annet klient-autorisering (se [WAPWIM]). Fysisk vil WIM typisk være plassert i telefonens SIM-kort, men kan være plassert i eget smartkort i såkalte dual-slot telefoner. WIM-funksjonalitet forventes leveringsklart i tredje kvartal år 2000.

For applikasjoner tilbyr WIM en digital signeringsfunksjon som kan benyttes til meldingssikkerhet mellom mobiltelefonen og servere på Internett for eksempel. Signeringsfunksjonen kan signere et dokument eller bekrefte en transaksjon. En typisk ”bruker” i WAP vil være WML-Script. Funksjonen Crypto.signText som er definert i [WMLSCL], er grensesnittet til korteierens private signeringsnøkkel:[37]

signedString = Crypto.sign(stringToSign, options, keyIDType, keyID)

Input til Crypto.signText er klartekst som skal signeres, angivelse av signeringsnøkkel i tillegg til ønsket outputformat i MIME-standarden [MIME].

I spillscenariet skal (bør) bong signeres, og det er da hensiktsmessig å få returnert signedString som inkluderer både stringToSign og *brukerens sertifikat. Tilbyderen har da all informasjon han trenger; ved hjelp av resultatet signedString kan tilbyderen verifisere brukerens identitet, samtidig som han har brukerens bekreftelse på at bong er korrekt utfylt.*

I spesifikasjonen av Crypto.signText poengteres at implementasjonen *må* presentere den orginale teksten (*stringToSign*) for brukeren, og det *må* gjøres på en slik måte at det skiller seg fra tekst som er generert av WML eller WML-Script. Dette er relevant i forhold til diskusjonen rundt signeringsproblemet i avsnitt 8.2.2.

5.5 Oppsummering

Dette kapittelet har handlet om smartkort. En kortfattet bakgrunn er presentert, og de viktigste standardene er gjennomgått. Multiapplikasjonskort ble vist å ha potensiale til å realisere betalingsapplikasjoner og andre applikasjoner på smartkort i mobiltelefoner i nær fremtid.

SIM-kort og SIM-Application-Toolkit (Sim-Toolkit) ble gjennomgått, og det ble vist at SIM-Toolkit allerede i dag kan realisere sikre (betalings-) løsninger. SIM-Toolkit tilbyr også lokasjonsinformasjon slik det var ønskelig i scenariet. Integrasjon med mobiltelefonens øvrige applikasjoner er transparent for brukeren. Ulempen med

[37] Se avsnitt 2.4 om elektroniske sertifikater og ”signeringsproblemet” i avsnitt 8.2.2

SIM-Toolkit er at funksjonaliteten som tilbys vil være eiet og styrt av mobiloperatøren.

WAPs smartkortbaserte sikkerhetsmodul WIM vil muliggjøre nøkkelbasert sikkerhet. WIM har funksjonalitet til å opprette en konfidensiell kanal mellom mobiltelefon og mobiloperatørens gateway. I tillegg kan WIM ivareta meldingssikkerhet mellom mobiltelefonen og webservere på Internett.

Det henvises til avsnitt 7.7 for eksempler på småpengeapplikasjoner i smartkort, og til avsnitt 2.4 for bakgrunnsinformasjon om elektronisk signering.

6 Scenario ”hestespill”

Dette kapittelet beskriver et scenario for spill på hester. Hestespillet illustrerer flere av mulighetene som kan forventes med moderne mobiltelefoni.

Kapittelet gir først en kort presentasjon av Norsk Rikstoto, en tenkt spilltilbyder i vårt scenario. Selve spillet er en elektronisk versjon av ett av dagens spill. Det tas ikke stilling til om spillet er realiserbart i forhold til Norsk Rikstotos løsninger i dag.

Nye lover vil påvirke hva som er tillatt og hva som ikke et tillatt med hensyn til spill (og betaling) på Internett. Aktuelt lovverk presenteres.

Uttrykket *spilltilbyder,* eller bare *tilbyder,* benyttes istedenfor Norsk Rikstoto der det er mulig.

6.1 Om Norsk Rikstoto

Norsk Rikstoto er en frittstående, næringsdrivende stiftelse som er stiftet av Det norske Travselskapet og Norsk Jockeyklub. Norsk Rikstoto har som formål å ha overordnet ansvar med all totalisatorvirksomhet og overordnet ansvar for økonomiske styring av hestesporten i Norge. Landbruksdepartementet er regulerende fagdepartement. Norsk Rikstoto hadde i 1998 en totalomsetning på 2.1 milliarder kroner hvorav ca. 64% tilbakeføres spillere i form av gevinster, og ca. 10% gis i premier til hesteeiere [NR].

Norsk Rikstoto forbereder seg på spill i nye medier, i første omgang Internett og TV/telefon, men mangler fortsatt tillatelse til å starte opp. Pengespill utenom etablerte kanaler, som spill på Internett, er ikke tillatt i Norge i dag. Nye lover ventes å gjøre Internett-spill lovlig. (Lovverket omtales i avsnitt 6.2)

Norsk Rikstoto har ca 1075 kommisjonærer (1.1.98) som står for ca 74% av omsetningen (1997). Inn- og utbetalinger skjer i dag hos kommisjonærer eller ved spillebanene. Systemspillere som leverer bonger på diskett hos kommisjonærene må være registrerte. Spillerens bankkonto benyttes i så fall til utbetalinger. Registrerte spillere autentiserer seg overfor kommisjonæren med et smartkort utstedt av Norsk Rikstoto. Ved siden av autentiseringfunksjonen benyttes kortet til signering av bongene. Signerte bonger overføres til Norsk Rikstoto, og en signert kopi legges tilbake på systemspillerens diskett. [Lin00]

6.2 Lovverket for spill og betalingstjenester

Både for betalingstjenester og Internett-spill er nye lover nært forestående, og det er derfor naturlig å ta utgangspunkt i lovforslagene ved vurdering av spill på Internett i

denne oppgaven. Aktuelle lovforslag er *Betalingssystemer m.v.* NOU 1996:24 [BS96] og *Odelstingsproposisjon nr 84 (1998-99) Om lov om lotterier m.v. og statens Lotteritilsyn (lotteriloven)* [OT99]. Mange av punktene nedenfor vil også legge føringer på valg av betalingsmodeller i neste kapittel.

Fra [BS96]: I Norge gis bare banker, og i visse tilfeller finansieringsforetak, rett til å etablere og drive betalingstjenester [BS96, §3-2 første ledd]. Andre institusjoner kan bare etablere og drive systemer for betalingstjenester etter konsesjon. Unntak fra bestemmelsen gjøres for forhåndsbetalte kort når det forhåndsbetalte beløp ikke overstiger kr 1000 eller et høyere beløp fastsatt av Kongen [BS96, §1-2 tredje ledd].

Det antas at bestemmelsene ovenfor også vil gjelde for beløp som deponeres hos en tilbyder som i avsnitt 7.6 på side 58. Dette betyr at tilbyderen kan starte en betalingstjeneste på egen hånd, forutsatt at han tar hensyn til de beløpsgrenser som gjelder. I dag praktiseres en grense på kr 1500 for forhåndsbetalte kort. Det er en grense satt av finansdepartementet [SG00].

Ny lotterilov vil regulere forhold rundt spillvirksomhet, inkludert totalisatorspill, i Norge. Forslaget til ny lov med høringsuttalelser og Justisdepartementets merknader foreligger som [OT99]. Forhold som kan påvirke gjennomføringen av totalisatorspill er:

? Spiller-registrering: Det vurderes å kreve registrering av spillere for deltagelse i totalisatorspill [OT99, punkt 10.1.2]. Norsk Rikstoto har frivillig spiller-registrering i dag. Departementets begrunnelse er ønsket om å forhindre hvitvasking av penger. Departementet vil vurdere å gi Lotteritilsynet innsyn i databaser [OT99, punkt 7.3.4].
? Internett-spill: Det vurderes å gjøre pengespill over Internett (såkalte *hjemme-spill*) lovlig [OT99, punkt 7.3.4]. Totalisatorspill (og andre spill som omfattes av lotteriloven) over Internett er i dag ikke lovlig. I merknadene fra Justis-departementet står det at spill på Internett må vurderes nærmere for blant annet å sikre at spill kan foregå i trygge former; forhold som skal vurderes er aldersgrense, betalingsformer og sikring mot kriminell virksomhet.
? Kreditt: Det vurderes å gjøre spilling på kreditt ulovlig [OT99, punkt 7.3.4]. Ifølge dagens lovverk kan det ikke heftes for gjeld som følge av spill. Spilltilbyderen kan med andre ord tillate spill på kreditt etter dagens lovverk, men han kan ikke bruke lovverket til å inndrive eventuell gjeld. Norsk Rikstoto har avtale med sine kommisjonærer om kun å tillate spill mot kontant betaling [LIN00].
? Inn- og utbetalinger: Det vurderes å kreve at spilltilbyder kun kan ta imot innskudd fra borgere bosatt i Norge, og som i tillegg har bankforbindelse i Norge. En eventuell gevinst utbetales til bankforbindelsen. Annet utbetalingskonsept kan vurderes hvis sikkerheten er tilfredsstillende [OT99, punkt 7.3.4].

6.3 Om hestespillet

I hestespillet er idéen å benytte moderne teknologi til å erstatte delvis papirbaserte og manuelle rutiner. Selve spillet skal være velkjent for hestesportspillere; bare mediet skal være nytt i denne sammenheng. Det er flere fordeler ved å ta utgangspunkt i et spill som allerede er etablert:

? Spillet har en lav introduksjonsterskel. I og med at dette er en ny måte å spille et velkjent spill, vil ikke terskelen for å bruke og forstå spillet være høy.
? Mobiltelefonen slik vi kjenner den i dag, har begrensede input/output-muligheter. Brukerdialogen bør derfor være begrenset til kun det aller nødvendigste for å ”utføre jobben”.
? Lav introduksjonsterskel og enkel betjening er trolig vesentlig for utbredelse og popularitet til det mye mediet til å begynne med.

6.3.1 Hestespillets regler

Det valgte spillet er en elektronisk utgave av Norsk Rikstotos spill ”Dagens Dobbel”. Spillet består i å plukke ut vinnere i to forskjellige hesteløp. Baner og hester annonseres av Norsk Rikstoto. For at en bong skal være korrekt utfylt skal den inneholde markering av vinnere og spilleinnsats. Utbetaling i det virkelige spillet skjer kun mot gyldig stemplet bong hvor tilsvarende kopi finnes i Norsk Rikstotos datasystem. Spillereglementet er fastsatt av Norsk Rikstoto og godkjent av Landbruksdepartementet [LD95]. Dagen Dobbel omsatte for kr. 121 millioner i 1997.

6.4 Hestespillscenariet

Nedenfor presenteres scenariet i kortversjon, slik det ble beskrevet i kapittel 1; deretter gis en detaljert beskrivelse av hvordan spiller og spilltilbyder opplever scenariet.

Kortversjon: Brukeren kobler seg opp til spilltilbyderen fra sin mobiltelefon, markerer to (eller flere) vinnerhester, signerer og betaler for tjenesten. Brukeren velger å se det siste hesteløpet hvis han har vinnersjanser. Løpet overføres direkte til brukerens mobiltelefon. Etter løpet får brukeren beskjed om at han har vunnet en god slump penger og at pengene er overført og disponible. Brukeren blir gratulert og invitert til en navngitt veddeløpsbane som spilltilbyderen vet er nærmeste bane.

6.4.1 Scenariet slik spilleren ser det

I det følgende beskrives scenariet slik det oppfattes av spilleren.

1. Spilleren initierer oppkobling fra sin personlige mobiltelefon. Det er første gangen spilleren prøver spillet. Han taster inn URL’en til hestespilltilbyderen.[38]

[38] Han kan eventuelt finne URL under kategorien *Spill* i mobiloperatørens wap-portal. Talegjenkjenning er ikke aktuell teknologi i dette scenariet.

Neste gang han ønsker å spille vil URL’en være lagret i telefonen. Oppkoblingen skjer umiddelbart og uten ventetid for spilleren.

2. Spillet lastes ned umiddelbart. Spilleren kjenner spillet. Han er vant til utfylling av bong på papir og levering til kommisjonæren. Spilleren ser fram til å slippe den lange turen for å levere spillebongen. Brukerdialogen er godt tilpasset den lille skjermen slik at spilleren kan starte spillingen uten unødvendig trykking på det lille tastaturet. Selv om spilleren ikke hadde kjent spillet hadde han kommet fort i gang takket være den interaktive hjelpedialogen (et menneskehode som veileder i spillets regler og virkemåte).
3. Spilleren bruker tastaturet til å pile seg opp og ned og krysse av eller taste inn tall i feltene. Mobiltelefontastaturet er ikke godt egnet til å skrive tekst, men numerisk input fungerer greit. Spilleren kan velge tilleggstjenester som å se hvilke hester som er med i bestemte løp, eller få annen informasjon som spilltilbyderen har gjort tilgjengelig. Han velger å få melding om hestenes sluttplassering i løpene. Han velger også å få overført levende bilder fra det siste løpet dersom han har vinnersjanser. Når spilleren har bestemt seg for spillerekker og tjenester, trykker han OK.
4. Spilleren får umiddelbart opp et nytt skjermbilde som viser pris. Spillerens mobiltelefon viser til enhver tid disponibelt beløp på spillerens bankkonto, så spilleren har god kontroll på sin økonomi. (Mobiltelefonen kan selvfølgelig også benyttes i andre betalingssammenhenger istedenfor kontanter, og i kjøp over Internett.) Spilleren bekrefter spillets pris, og applikasjonen ber han signere meldingen ved å taste inn sin PIN-kode. Spillet og betalingsinformasjon overføres spilltilbyderen (dette er avhengig av betalingsmodell; se kapittel 7). Spillerens bong lagres i telefonen slik at han ikke trenger papirkopi hvis han ønsker å se på bongen senere. Bong er uansett mindre viktig fordi spilleren vil få tekstbeskjed til telefonen samtidig med gevinstutbetaling til konto hvis han er så heldig å vinne.
5. Underveis i hesteveddeløpet får spilleren tekstbeskjed til sin mobiltelefon om at hans førstevalg har gått inn i første løp. Han kan samtidig få annen interessant informasjon, som for eksempel hans potensielle vinnersjanser.
6. Før siste løp får spilleren beskjed om at han har vinnersjanser, og han får se siste løp direkte overført på mobiltelefonen. For dette beregner *nettoperatøren* seg et lite beløp per minutt da overføringen er meget kapasitetskrevende. Spilleren godtar forhåndsbetaling til nettoperatøren for denne tjenesten.
7. Etter siste løp får han beskjed til mobiltelefonen at han har vunnet en god slump penger og at pengene allerede er overført og disponible for spilleren.
8. Spilleren får i tillegg en gratulasjonsmelding fra spilltilbyderen hvor spilleren inviteres til VIP-tribunen på Leangen travbane for å overvære helgens veddeløp. Spilleren synes tilbudet er interessant, og han bestemmer seg for å bli med. Leangen er nærmeste travbane.

6.4.2 Hestespillscenariet slik spilltilbyderen ser det

Det samme scenariet fra avsnittet ovenfor:

1. Tilbyderen mottar oppkobling til spilletjenesten fra spillerens mobiltelefon. For tilbyderen betyr aksess fra mobiltelefoner visualisering av en kraftig nedskalert versjon av det samme informasjonsinnholdet som tilbyderen har på sine regulære

Internett-sider. Tilbyderen slår opp spillerens identifikasjon fra metainformasjon som medfølger sesjonen, og tilbyderen finner at spilleren ikke har spilt før. Spilleren får en meny med tilbud om å velge blant de mest populære spillene til tilbyderen. Neste gang spilleren besøker tilbyderens tjenester vil organiseringen av innholdet som presenteres være basert på spillerens tidligere menyvalg. En slik organisering vil hjelpe spilleren til å manøvrere raskere.

2. Spilleren velger å spille ”Dagens Dobbel”. Dette er et enkelt spill som ble lastet ned i mobiltelefonen som en del av det initielle brukergrensesnittet. Det er altså ikke nødvendig med ytterligere nettaksess for å fortsette spillingen. Sammen med spillet lastes annen informasjon slik at spillets pris og verifikasjon av input kan gjøres lokalt i mobiltelefonen.
3. Tilbyderen mottar ferdig utfylt bong og eventuelle ønskede tilleggstjenester sammen med betalingen for spill og tjenester. Tilbyderen har nok informasjon til sikker identifikasjon (autentisering, se avsnitt 2.2) av spiller og hans bankkonto for eventuell utbetaling av gevinst. (Merk at dette er avhengig av betalingsmodell; se kapitel 7)
   Da hestespillsport har et historisk ”frynsete” rykte i Norge, og for å hindre at spillet skal kunne brukes i kriminell virksomhet (hvitvasking av penger), vil norske myndigheter legge sterke føringer på tilbyderens virksomhet. Autentisering av spillere kan derfor bli et krav for å tillate elektroniske versjoner av tilbyderens spill (se avsnitt 6.2).
4. Spillet, betalingsinformasjon, ønskete tjenester og autentiseringsinformasjon registreres i tilbyderens databaser.
5. Tilbyderen realiserer spillerens betaling for deltagelse i spillet, og beløpene krediteres tilbyderens ”fysiske” bankkonto. (Det er flere måter å gjøre dette på, avhengig av betalingsmodell)
6. Tilbyderen venter til det fysiske hesteveddeløpet starter.
7. Tilbyderen leverer ønskede tjenester og informerer spilleren ved hjelp av tekstmeldinger om delresultater i spillet.
8. Tilbyderen streamer levende bilder av siste løpet til spillerens mobiltelefon.
9. Etter spillet utbetaler tilbyderen pengepremien til spilleren slik at beløpet blir umiddelbart disponibelt. Det gis samtidig en tekstmelding til mobiltelefonen om at beløpet er overført.
10. Tilbyderen ønsker å premiere spilleren ekstra i håp om at noe av gevinsten tilbakeføres i nye spill. Tilbyderen inviterer spilleren til å overvære et virkelig veddeløp på en travban som ligger i nærheten av spilleren.

6.5 Utfordringer i scenariet

Mobiltelefonens bruk i betalingssammenheng er en viktig del av scenariet. Denne anvendelsen skiller seg vesentlig fra mobiltelefonens tradisjonelle tjeneste i dag – taletjensten.

Under arbeidet med denne oppgaven har flere aktører i det norske markedet lansert betalingstjenester over mobiltelefonen. Telenor har lansert produktet [MobilHandel] som er en generell betalingsløsning (MobilHandel beskrives i avsnitt 7.6). Banker kommer med løsninger for kontohold og betaling av regninger ved hjelp av mobiltelefon etter noen års erfaring med tilsvarende tjeneste over Internett. Kapittel 7 går i dybden på betalingsmodeller.

Betalingsutfordringene ved dette scenariet synes å være relatert til følgende:
? Direkte betaling for tjenester ved hjelp av mobiltelefonen.
? Synkronisering av saldoopplysninger mellom spillerens/brukerens bankkonto og mobiltelefon.
? Betaling av transportkapasitet i radionettet til nettoperatøren samtidig med faktisk bruk.
? Pengeoverføring til mobiltelefonen.
? Sikkerhetsaspekter, herunder sikker kommunikasjon og autentisering av partene.

Andre utfordringer i scenariet er:
? Teknologi for brukerdialog og brukergrensesnitt på mobiltelefonen
? Overføring av tale og video av passende kvalitet
? Geografisk posisjonering gjort tilgjengelig.

Tidligere kapitler har gitt nødvendig bakgrunn. De påfølgende kapitler diskuterer problemstillingene ovenfor.

6.6 Aktører i scenariet

Spilleren og *spilltilbyderen* er to aktører i spillet. Det kan være at spilltilbyderen ikke er identisk med spill*eieren* – spilleieren er i vårt scenario Norsk Rikstoto. Hestespill over Internett og hestespill på Tekst-TV er eksempler på spill som vil drives av to aktører med kommisjonærstatus overfor Norsk Rikstoto. *Spilleieren* kan derfor bli en tredje aktør i spillet.

Kommisjonærene er viktige aktører i *tradisjonell* totalisatorspilling. Da spillets administrative organisering er av mindre betydning i denne oppgaven antas det for enkelthets skyld at spill*eier* og spill*tilbyder* er en og samme aktør. Spilleren forholder seg direkte til spilltilbyderen. De tradisjonelle kommisjonærene har med andre ord ingen rolle i dette mobiltelefonspillet.

En eller flere aktører må i tillegg håndtere betaling. Det er flere måter å løse ”betalingsproblemet” på, og aktører er avhengig av valg av løsning. En kan for eksempel tenke seg at innbetaling for å få spille skjer over telefonregningen. Spillerens mobiloperatør kan med andre ord bli en aktør. Utbetaling av eventuell gevinst til spillerens mobiltelefon eller hans bankkonto krever igjen andre aktører. I kapittel 7 diskuteres betalingsproblemet nærmere.

Spillerens mobiloperatør er i det minste indirekte en aktør ved at han bidrar med teknologien som muliggjør trådløs kommunikasjon. Når mobiloperatøren tar seg direkte betalt for båndbredde i scenariet, blir han å anse som en tjenesteleverandør på linje med spilltilbyderen. Kapittel 8 diskutere denne problemstillingen nærmere.

7 Betalingsmodeller

En av grunnene til at handel på Internett ennå ikke har tatt av, er mangelen på enkle og sikre betalingsverktøy. Mobiltelefonen har potensiale til å løse betalingsproblemene.

Dette kapittelet handler om problemstillinger rundt elektronisk betaling. Med bakgrunn i spillscenariet fra kapittel 6, diskuterer jeg mulighetene som finnes for å *betale* for å delta i spillet, og for eventuell *utbetaling* av gevinst. Aktuelt lovverk, som kan påvirke valg av betalingsmodeller, er blitt presentert i foregående kapittel, i avsnitt 6.2.

Ved å stille opp syv forskjellige kriterier, forsøkes det å finne den beste egnede betalingsmodellen for scenariet. Kapittelet beskriver også smartkortimplementasjoner av de aktuelle betalingsmodellene.

7.1 Innledning

I spillscenariet kan ulike modeller for nettbasert betaling anvendes. I det følgende tas det utgangspunkt i relevante betalingsmodeller for spillscenariet, og det forsøkes å finne frem til den beste egnede modellen. De fleste av modellene er tradisjonelle og godt kjent (kredit, debet, telefonregning) , mens andre eksisterer som en følge av mulighetene som finnes i en digital infrastruktur (”konto”, elektroniske kontanter).

Kredittmodellen og telefonregningmodellen er lite attraktive i spillsammenheng da de ikke tar forhåndsbetaling. Forslaget til ny lotterilov vil trolig forby disse betalingsmodellene. Vår spilltilbyder (Norsk Rikstoto) tillater ikke sine kommisjonærer å gi kreditt, selv om dette ikke er forbudt ved lov i dag (se avsnitt 6.2). Selv om kreditt- og telefonregningsmodellen neppe er aktuelle i dette spillet vurderes likevel modellene da de kan være interessante i andre betalingssituasjoner på Internett.

Sikker identifikasjon av spillere er et krav norske myndigheter kan sette for spillvirksomhet (se avsnitt 6.2). Hvis *betalingsmodellen* kan autentisere spilleren er det et ekstra pluss.

Utbetaling av eventuell gevinst representerer et problem. Det vurderes derfor også om modellen som spilleren benytter til innbetaling kan ”reverseres” og benyttes av tilbyderen for utbetaling av gevinst. Hvis det ikke kan la seg gjøre, må tilbyderen fremskaffe informasjon om utbetalingskonto på annen måte.

For tilbyderen vil den tradisjonelle løsningen på autentiseringsproblemet og gevinstutbetalingsproblemet være å registrere spilleren i en separat handling før deltagelse i spillet tillates. Hvis betalingsmodellene gjør at en kan unngå en (manuell?)

registreringsfase vil det være interessant, da det antakelig vil senke terskelen for deltagelse i spillet betydelig. En skal imidlertid ikke se bort fra at tilbyderen kan ha sine motiver (markedsføring og annet) for å etablere et kundeforhold til spilleren ved registrering. I denne oppgaven antas imidlertid at registrering ikke er ønskelig.

Betalingsmodellen som skal velges i spillscenariet bør tilfredsstille følgende krav:
1. *Enkel bruk*. Det må være mulig å betjene hele scenariet fra mobiltelefonen.
2. *Betaling av innsats*. Modellen må kunne betjene innbetaling av små (under kr 10.-) og store (over kr 1000.-) spilleinnsatser online.
3. *Autentisering*. Modellen bør kunne autentisere spilleren overfor tilbyder.
4. *Gevinstutbetaling*. Det er et pluss om modellen som spilleren benytter for *inn*betaling også kan brukes av tilbyderen til å *ut*betale eventuell gevinst. Modellen må i så fall kunne betjene utbetaling av større og mindre gevinster.
5. *Ikke kundeforhold*. Modellen bør *ikke* forutsette at det er etablert et kundeforhold for å kunne betale for deltagelse i spill.
6. *Sikkerhet og tillit*. Modellen må være, *og* oppfattes, som god nok for alle parter.
7. *Lave transaksjonskostnader*. Modellen må ikke være dyr for spiller eller tilbyder.

Angående sikkerhet: Det forutsettes at de betalingsmodellene som ikke har iboende nettverkssikkerhet i protokollene, kan opprette en sikker kommunikasjonskanal mellom aktørene. Når nettverkssikkerhet blir tilgjengelig i WAP for eksempel, vil opprettelse av en sikker kommunikasjonskanal kunne skje transparent for brukeren, analogt med tilsvarende nettverkssikkerhet på Internett (SSL/TSL)[39].

Modellene vurderes opp mot kravene ovenfor. Tabellen på side 66 oppsummerer alle modellene. I fremstillingen av betalingsmodellene på påfølgende sider benyttes noen ganger de mer generelle betegnelsene *selger* og *kunde* istedenfor *spilletilbyder* og *spiller*. Bruk av betegnelsen *kunde* må forstås som *kjøper* der annet ikke fremgår av sammenhengen; betegnelsen *kunde* impliserer ikke nødvendigvis at det foreligger et kundeforhold til spilltilbyderen. Figurene av betalingsmodellene i avsnittene nedenfor er basert på intervju med [ET99].

7.2 Kreditt

Handel ved hjelp av kredittkort er blitt den ”tradisjonelle” elektroniske metoden for oppgjør mellom parter på Internett eller over telefon – i mangel av noen bedre fungerende modell. Modellen er enkel, og man har lang erfaring for at den virker. Kjøp på kreditt vil i denne sammenhengen bety levering av varer eller tjenester hvor oppgjør finner sted i etterhånd.[40] Et typisk bruksscenario er følgende: (En forutsetning er at kunden må besitte et kredittkort; beskrevet i de første to punktene).

? Kunden (spilleren) søker til sin bank eller annen finansinstitusjon om å få utstedt personlig kredittkonto.

[39] Secure Socket Layer, Transport Layer Security

[40] For kortbruker kan det kanskje oppfattes som om oppgjør finner sted før varen er levert ved kjøp over Internett og levering av varen per post.

? Utsteder sjekker kunden, og utsteder kort i tiltro til at kunden vil holde seg til avtalte regler. Utsteder fungerer som en tiltrodd tredjepart, som går god for kundens identitet, og er også en rimelig god garantist for kundens grad av seriøsitet fordi utsteder kan tape penger på å utstede kort til useriøse personer.
? Kunden betaler ved å oppgi sitt kredittkortnummer. Dette nummeret, kanskje sammen en enkel validitetskontroll på kortets utløpsdato, er alt selger krever for å godta handelen (se Figur 19)

Som nevnt ovenfor blir spill på kreditt antakelig ikke tillatt i Norge. Kredittmodellen er likevel med for å gi en samlet vurdering av tilgjengelige modeller. Vurderingen nedenfor vil gjelde i andre betalingsscenarier enn spillscenariet.

Følgende er positive sider ved kreditt som oppgjørsform i forhold til scenariet:
1. Enkelt, innarbeidet og kjent av kunden.
2. Modellen håndterer betaling av små og store beløp.
3. Utbetaling til kredittkonto er mulig (forutsetter at selger registrerer kontonummer i betalingstransaksjonen).
4. Kunden holdes skadefri ved eventuelt misbruk fra selgerens side såfremt kunden oppdager uautoriserte transaksjoner.
5. Ikke nødvendig med kundeforhold for å betale.

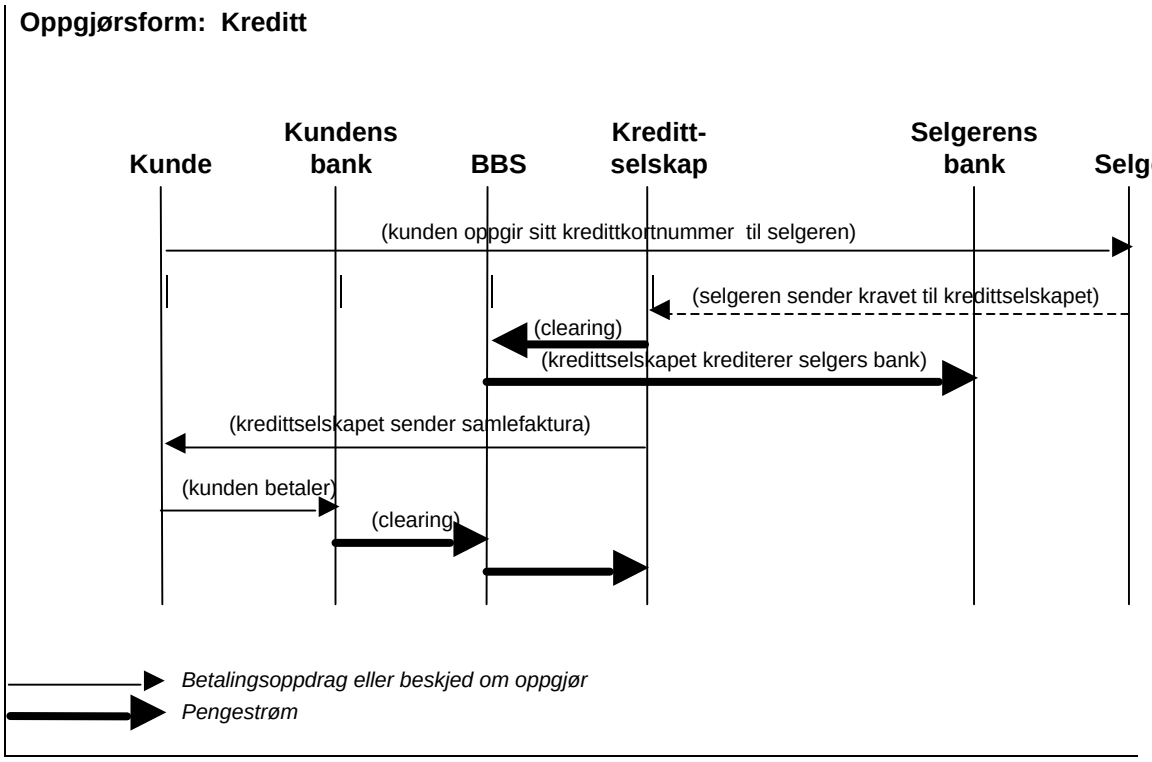
Nedenfor listes negative sider ved kreditt som oppgjørsform i forhold til scenariet:
1. Selgeren påtar seg en risiko. Kunden har ikke fysisk signert bestillingen. Selgeren er innforstått med at han kan tape en tvistesak hvis kunden ikke vil vedkjenne seg bestillingen.
2. Kunden gir fra seg kredittkortnummeret, og utsetter seg således for misbruk.
3. Transaksjonskostnadene er høye da de inkluderer flere ledd i betalingskjeden.
4. Selgeren kan ikke være sikker på kundens identitet. Kunden autentiseres ikke.

Kreditt som oppgjørsform kan være tiltalende fordi modellen er enkel, og fordi selger påtar seg en stor del av risikoen. Men det knytter seg usikkerhet til om kjøper vil føle at sikkerheten er god nok. Da kommunikasjon i mobilnettet er kryptert[41] vil bare selger (og mobiloperatørene, i teorien) ha tilgang til kundens kredittkort-nummer.

En alvorlig innvending mot kreditt er kostnadene. I mange scenarier må det være regningssvarende å betale lave innsatser. Transaksjonskostnadene kan fort beløpe seg til mer enn innsatsen.

Kostnadene ved transaksjoner kan reduseres ved oppsamling av transaksjoner før belastning. Qpass [QPASS] tilbyr en slik tjeneste hvor Qpass er betalingsformidler mellom registrerte nettsteder og registrerte kunder. Kunden registrerer seg hos Qpass med kredittkortnummer og andre personopplysninger. Når kunden handler på nettsteder som støtter betaling med Qpasstjenesten, registreres kontobelastningen hos Qpass. Qpass belaster kundens kredittkonto kun én gang per måned.

[41] Krypteringen er bare av moderat styrke, og det krypteres bare mellom mobiltelefon og basestasjon. Se avsnitt 3.1



Figur 19. Kreditt. Konseptuell skisse av meldingsveier og penge-strømmer med kreditt som oppgjørsform. (Gjelder også for "Kreditt med SET")

I Figur 19 sender selger pengekravet til kredittselskapet, som krediterer selgers bank og debiterer kunden. Kunden får samlefaktura fra kredittselskapet (han kan eventuelt betale på annen måte). Inter-banktransaksjoner må via clearing hos BBS. Den stiplede linjen indikerer at tilbyder ikke må være online med kredittselskapet (i praksis vil han trolig være det, for validitetssjekk av kredittkortnummer). Som det fremgår er det mye kommunikasjon involvert i kredittmodellen. Det synes klart at modellen ikke er egnet til småpengetransaksjoner.

7.3 Kreditt med SET

7.3.1 EMV

EMV er EuroPay, MasterCard og Visas standard for bruk av smartkort i kreditt- og debet-transaksjoner (se også avsnitt 5.2.2 i kapittelet om smartkort). EMV spesifiserer tekniske, fysiske, logiske og transaksjonsflyt-sider ved bruk av smartkort. Versjon '96 er siste versjon (spesifikasjonene kan lastes ned fra www.setco.com). Sentralt i EMV er SET-protokollen.

SET, Secure Electronic Transaction, er en standard for sikker overføring av betalings-*informasjon* i åpne nett. I Norge promoterer BBS og sentrale banker SET-standarden for å få fart på handel over Internett.[42]

SET-standarden prøver å etterligne de fysiske handlingene i konvensjonelle kreditt-transaksjoner (derfor er transaksjonene identisk med figuren i forrige avsnitt, Figur 19). Det er tre parter med i en SET transaksjon, kunden, selger og kredittselskap, og alle besitter digitale sertifikater for å sikre autentisering, sporbarhet, konfidensialitet og integritet.

En transaksjon skjer ved at en todelt melding går fra kunde til selger. Én del inneholder opplysninger om kredittkortnummer med mer, som er nødvendig for kredittselskapet. Den andre delen inneholder opplysninger om varen. SET-standarden sikrer kunden stor grad av konfidensialitet ved at opplysningene som er beregnet for kredittselskapet bare kan dekrypteres av kredittselskapet, og opplysninger som er beregnet for selger kun er tilgjengelig for selger. Selger får ikke kjennskap til kundens kortnummer, og kredittselskapet får ikke vite hva kunden har handlet.[43]

Installasjon og bruk av personlige PC-baserte SET-tjenester har vist seg tungvint da tjenestene mangler et standardisert grensesnitt mot nettlesere [AL00]. Dette problemet vil ikke eksistere med SET-tjenester i mobiltelefoner da kunden ikke involveres i installasjon og konfigurasjon.

EMV-standarden for kredit og debet kan implementers som en applikasjon i mobil-telefon.

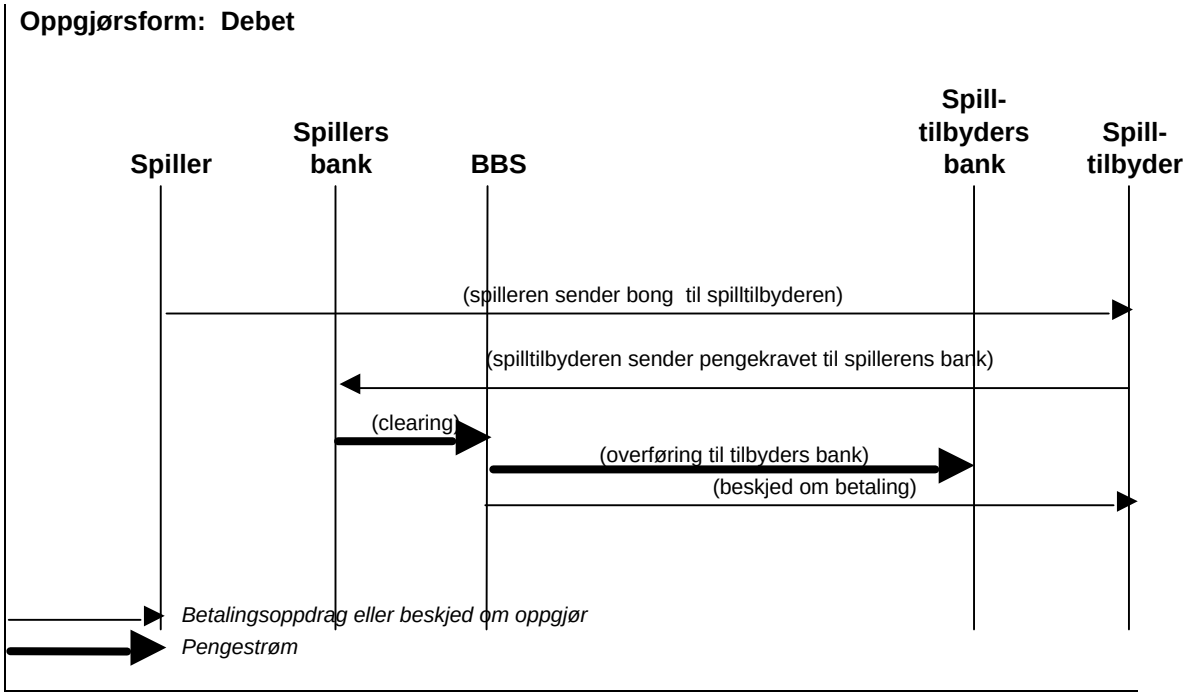
7.3.2 SET i scenariet (kreditt)

Nedenfor oppsummeres positive sider ved SET:
1. Enkelt for kunden.
2. Store og små innsatser er mulig.
3. Krever ikke kundeforhold.
4. God sikkerhet for kunde, selger og kredittselskap.
5. Kunden autentiseres av SET-protokollen.

Nedenfor listes negative sider ved SET:
1. Høye transaksjonskostnader. Involverer online kommunikasjon mellom kunde, selger og kredittselskap.
2. Løser ikke problemet med utbetaling av gevinst. SET-standarden skal jo sikre at selger ikke har tilgang til kontonummer.

De høye transaksjonskostnadene taler mot bruk av SET. Bortsett fra ”utbetalings-problemet” tilfredsstiller denne kreditt-modellen betalingskravene i spillscenariet.

[42] Mer SET-informasjon her: [SET], [VISA], [MCARD], [BBS], [Solberg96]
[43] Kredittselskapet kan med andre ord ikke spesifisere hva kunden har handlet på fakturaen. Det kan oppfattes negativt av kunden at kortselskapet ikke kan yte denne servicen lenger.



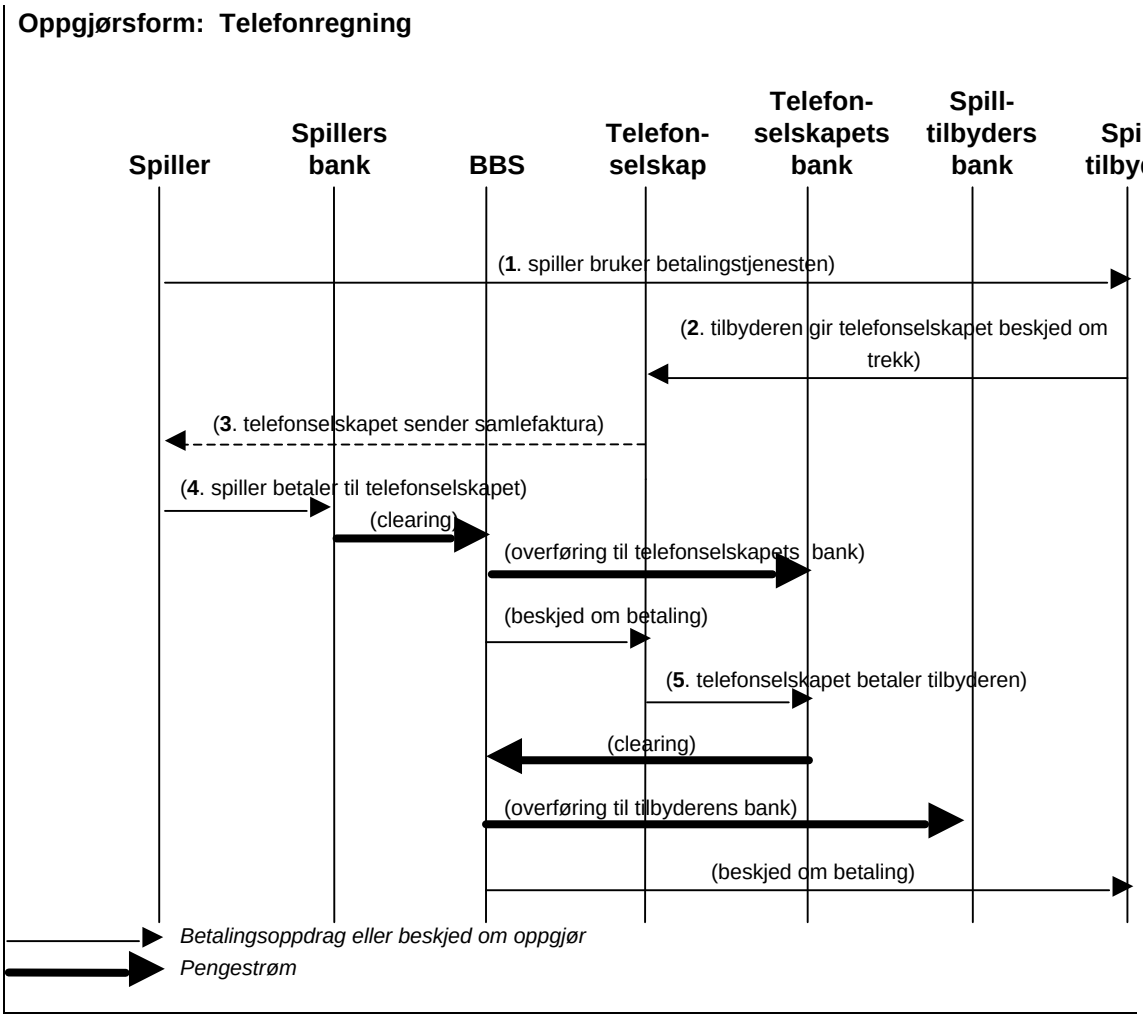
Figur 20 Debet. Selger debiterer kundens bankkonto ved hjelp av SET-protokollen.

7.4 Debet

Debetkort har langt på vei erstattet kontanter i Norge og kan benyttes som betalingsmiddel ved nær sagt alle handelssteder landet over. Et debetkort inneholder identifikasjon av kunde og konto. Ved betaling i butikk drar kunden kortet gjennom en dedikert kortleser, taster en identifikasjonskode (PIN) og transaksjonen overføres til BankAccept/BBS som foretar en avregning mellom konti i bankene en gang i døgnet (se Figur 20). Kombinasjon av kort og kode autentiserer brukeren, og konfidensialitet er sikret ved at overføring skjer i bankens lukkede nett.

Debetløsninger hvor selger mottar beløp og kontonummer fra kunden og selv initierer debitering, tillates ikke i det norske banklovverket i dag ifølge [ET99] [DNB97].

SET-protokollen fra avsnittet ovenfor blir imidlertid spesifisert for debetløsninger i tillegg. Det jobbes også med å tilpasse SET til mobiltelefoner (se [SET]). Mobiltelefonen vil dermed kunne fungere som en vanlige BankAccept betalings-terminal. Debetløsningen vil ha nøyaktig de samme egenskapene som SET-løsningen i avsnittet ovenfor, og de gjentas ikke her. Transaksjonene vil imidlertid bli som i Figur 20.



Figur 21. Konseptuell skisse av oppgjør over telefonregningen. Selger gir telefonselskapet beskjed om trekk (2) . Kunden mottar regning over ordinær faktura (3 – stiplet for å markere tidsforsinkelsen). Kunden betaler via sin bank (4), og selger får oppgjør fra telefonselskapets bank (5).

7.5 Oppgjør over telefonregningen

Mobiloperatørene har gode forutsetninger for å være tiltrodde tredjeparter i handel som benytter mobiltelefoner som betalingsterminal. Operatørene har allerede nødvendig betalings-infrastruktur på plass: Det eksisterer et kundeforhold, og betalingsrutiner finnes.

Israelske Trivnet tilbyr en betalingstjeneste med oppgjør over telefonregningen. Løsningen kalles WISP[44] og markedsføres overfor Internettilbydere. Tjenesten er rettet mot småpengetransaksjoner. Når kunden handler på Internett sendes trans-

[44] For mer informasjon om WISP, se [Comp99], [TRIVNET]

aksjonen tilbake til kundens Internettilbyder, som så belaster kunden ved en samlefaktura sammen med vanlig telefonregning.

Netcom var tidlig ute med å lansere kjøp av Cola ved hjelp av mobiltelefonen. Ved å ringe til automaten kan kunden få slukket tørsten og betale varen som ringetid over telefonregningen. Et annet aktuelt eksempel er betaling av piggdekkavgiften i Oslo [DIGI021299].

Se Figur 21 for betalingsveier. Nedenfor listes fordeler med betaling over telefonregningen:
1. Enkelt, lettfattelig konsept.
2. Betalingsinfrastruktur allerede på plass.
3. Lave transaksjonskostnader – selger kan samle opp transaksjoner før videresending.
4. Godt egnet for småpengetransaksjoner.
5. Kunden mottar samlefaktura fra teleoperatøren.
6. Kundens identitet er kjent.

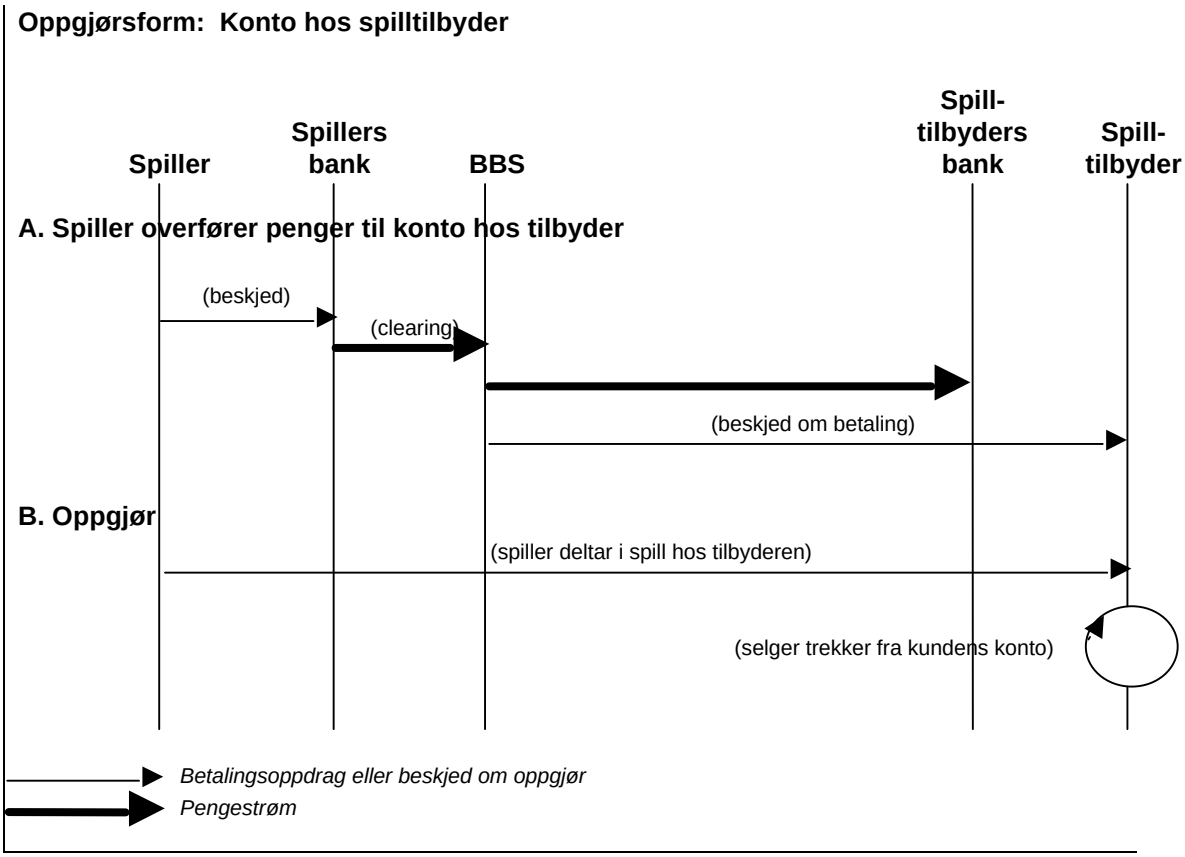
Følgende punkter taler mot betaling over telefonregningen:
1. Neppe god nok sikkerhet for selger ved store beløp.
2. Løser ikke problemet med *utbetaling* av gevinst .
3. Høye administrasjonskostnader legges på teleoperatørene.
4. Kundeforhold antakelig nødvendig for å få spillerens aksept på fakturering over telefonregningen.
5. Usikkert om teleoperatørene vil påta seg ansvaret som garantist overfor selgere.

Oppgjør over telefonregningen er en mer hensiktsmessig variant av å sende regning. Det er ikke noe i veien for at selger kan sende regning selv, men det er klare logistikkfordeler ved å la teleoperatørene gjøre det. Selger vil ikke få oppgjør før kunden har betalt regningen, og denne oppgjørsformen egner seg ikke hvis selger ikke vil innrømme kunden kreditt. Som nevnt ovenfor, er det sannsynlig at denne ”kredittmodellen” ikke vil tillates i spill i Norge.

7.6 Konto hos tilbyderen

Mange av dagens handelsløsninger på Internett forutsetter at det er opprettet et tillitsforhold mellom selger og kjøper som gjør at selger kan sende regning eller belaste kundens kredittkonto eller annen oppgjørsform som partene har avtalt. Kredittkonto har vi behandlet ovenfor, og å sende regning er uaktuelt i spillscenariet.

En løsning som er innrettet mot småpengetransaksjoner hvor det er etablert et tillitsforhold, er ordningen der kunden deponerer penger ”på konto” hos selgeren. Ved hvert salg vil selgeren trekke penger fra kundens konto. Eksempler på slike løsninger finnes ved det svenske travselskapet AB Trav och Galopp [ATG], Hong Kong Jockey Club [HKJC] og FilmWebs billettbestilling [FW].



Figur 22. Konto som oppgjørsform.

I Figur 22 deponerer spilleren kontanter hos tilbyderen (del A). Spilleren overfører i dette tilfellet kontanter ved en vanlig banktransaksjon. Tilbyder har kontroll med spillerens saldo (del B); ingen kommunikasjon med andre er nødvendig ved betaling for deltagelse i spill.

Nedenfor listes fordeler med konto-løsningen:
1. Enkel, lett forståelig.
2. Godt egnet for småpengetransaksjoner.
3. Meget lave transaksjonskostnader.
4. God sikkerhet for tilbyder.
5. Spiller er autentisert på forhånd.
6. Gevinstutbetaling er mulig.

Følgende er ulemper med konto-løsningen:
1. Administrasjonskostnader for tilbyder.
2. Også egnet for meget høye beløp hvis spilleren er komfortabel med å stole på tilbyderen. Myndighetene setter imidlertid begrensninger på denne typen konti; for tiden på kr. 1000. Dette er etter dispensasjon fra gjeldende lovverk [SS00].
3. Ikke god sikkerhet for spilleren.
4. Konto må fylles opp av spilleren.

5. Spilleren binder penger hos tilbyderen.
6. Bruk av kontoen knyttes kun til én bestemt selger/tilbyder.
7. Det må eksistere et kundeforhold for at løsningen skal fungere.

Kontomodellen er implementert i flere land i hestespillsammenheng. Norsk Rikstoto vurderer det norske markedet som for lite til at denne løsningen forsvarer administrasjonskostnadene. [TH99]

7.6.1 Telenors kontoløsning MobilHandel

Man kan få en mer generell variant av kontomodellen når andre enn selgeren, for eksempel *mobiloperatøren*, administrerer kundens konto. Kontoen blir dermed ikke knyttet til bare én selger, men kan benyttes overfor alle selgere som støtter systemet. Norske FilmWeb[45] var tidlig ute i Norge med å etablere en såkalt skyggekonto-løsning for kjøp av kinobilletter over Internett. Løsningen bygger på Telenors MobilHandel og beskrives nedenfor (se også [MobilHandel]).

MobilHandel-løsningen krever at kunden inngår en avtale med Telenor. Administrator (Telenor) må ha informasjon om bankkontonummer, mobiltelefon og personopplysninger for å etablere tjenesten. Teknisk forutsetter tjenesten funksjoner i SIM-Toolkit, hvorav kryptering[46] av SMS-meldinger er en nødvendig egenskap for å ivareta sikkerheten. (SIM-Toolkit er beskrevet i avsnitt 5.4.2). Kunden må derfor ha en nyere mobiltelefon som er tilpasset SIM-Toolkit. Opplysningene kunden gir i avtalen vil gi ham et nytt SIM-kort med nødvendig funksjonalitet.

Lading av mobilkontoen kan skje fra brukerens bankkonto eller hans kredittkonto. Kontoadministrator (Telenor) kjenner kontonumrene fra registreringsfasen; konto-numrene transporteres ikke til mobiltelefon. Sikkerheten ved lading er ivaretatt ved kryptering av SMS-meldingene. Dette er imidlertid en løsning som bare krypterer mellom mobiltelefonen og kortmeldingssenteret (SMSC – se Figur 4 på side 14). I tillegg til SMS-kryptering må kunden benytte engangspassord. Hver melding må bekreftes med en unik PIN-kode fra en liste som kunden mottar fra sin bank. Det antas ellers at transport av meldingene fra SMSC til endesystemene hos Telenor eller bank går med Internett-baserte sikkerhetsløsninger. Etter lading mottar kunden en SMS-kvittering.

Betaling i MobilHandel kan skje med kundens debetkonto, kredittkonto eller ved å benytte mobilkontoen. Kundens spesielle SIM-Toolkit-kort gjør at menyene til FilmWebs billettbestillingssystem er integrert med telefonens andre menyer. Kunden vil normalt gjøre ett søk etter aktuell film før betaling. Ved betaling bekrefter kunden bestillingen med et engangspassord (ved debet eller kreditt-løsningene), eller med mobiltelefonens påloggings-PIN-kode ved bruk av mobilkonto. En kryptert SMS-melding sendes kontoadministratoren som viderefor-midler transaksjonen. Det gis til slutt en kvittering i form av et referansenummer tilbake til kunden.

[45] Se FilmWeb, http://billettluka.filmweb.no (1.2.00)
[46] Det er også mulig med digital signering, men det antas at kryptering er brukt i MobilHandel.

For å få ned transaksjonskostnadene må en unngå clearing gjennom BBS hver gang kunden betaler med mobilkontoen. Selger (i eksempelet over er det FilmWeb) må derfor også ha konto hos kontoadministratoren. Betaling blir da en intern overføring mellom konti hos administratoren. I dette tilfellet er det kontoadministratoren som foretar clearing istedenfor BBS. Det er ikke sikkert det blir billigere for kunden, men det åpner for konkurranse rundt clearingfunksjonen. Overføring av kontanter fra kontoen hos administratoren til det virkelige banksystemet gjøres ved vanlige banktransaksjoner med vanlige transaksjonskostnader, og vil normalt bare være aktuelt for selger når selger ønsker å realisere midlene fra salgene. Det kan for eksempel være aktuelt for selgeren å realisere én gang per dag.

Nedenfor gis noen kritiske bemerkninger til MobilHandel og en sammenligning med WAP:

? Løsningen realiseres med SIM-Toolkit. Denne teknologien er proprietær og knytter løsningen til kundens mobiloperatør. Dette vil endre seg når sikkerheten i WAP-teknologien er på plass (se WTLS i avsnitt 3.4.1). Mobiloperatørene vil da ikke lenger ha denne fordelen av sitt forhold til kunden.
? Inkludering av betalingsløsninger for andre salgssteder er tungvint da SIM-Toolkit er statisk. WAP-teknologi vil gjøre det dynamisk og enkelt.
? Betaling ved hjelp av mobiltelefonen er en dyr løsning for kunden i dag. Det vil trolig endre seg med flere konkurrerende løsninger med WAP-teknologi.

7.7 Elektroniske kontanter

Elektroniske kontanter er pengereprensentasjoner i elektronisk form. En elektronisk lommebok, fysisk representert i et smartkort, fylles opp ved at konvensjonelle penger veksles i elektroniske kontanter. De elektroniske kontantene er digitalt signert av utsteder, og pengerepresentasjonene kan bare veksles til konvensjonelle penger igjen hos utsteder. Digitale signaturer garanterer pengenes ekthet. Elektroniske kontanter kan benyttes som andre fysiske penger i handel, og i ”ekte” systemer gå fra person til person uten å løses inn. Transaksjonskostnadene er lave. Det er ikke noe krav for selger å være online. En svakhet kan være at det er lett å starte eget ”seddeltrykkeri” ved å kopiere penger. Løsningen for elektroniske kontanter (småpengeløsningene) skiller seg fra hverandre blant annet i måten de håndterer dette problemet. (Se Mondex og Proton nedenfor. Se ellers [MONDEX], [DIGIC] og [VISAC] for andre eksempler).

Elektroniske kontanter har egenskaper som svarer til kontanter: [Lie99]

? Verdien er lagret i kortet (evt. i en annen informasjonsbærer), analogt til mynter og sedler som ligger i en lommebok, og kortet gir ikke adgang til noe annet enn å disponere over innholdet.
? Verdien er disponibel for ihendehaver (men kan være beskyttet ved en PIN-kode eller lignende).
? Elektroniske kontanter er anonyme og kan ikke spores tilbake til bruker.
? Kostnadene per transaksjon er marginale.
? Sett fra korthaverens side er verdi som er lagret i kort ikke samtidig til stede på noen bankkonto, og gir ikke noen renteinntekter.

? Tapt kort betyr tapte midler.

Beløpsgrensen i kortet setter en absolutt grense for hvilket tap et bortkommet kort innebærer.

7.7.1 Mondex

Mondex-systemet har disse spesielle egenskapene[47]: [Lie99]

? Fullstendig smartkortbasert. Forfalskning forhindres ved at smartkortene er fiklefrie, ihendehaver kan i praksis ikke komme til eller påvirke kortets saldo på noen måte.
? Når en bruker mottar Mondex-kontanter som betaling, kan disse fritt brukes for betaling videre. (Det er altså ikke nødvendig å løse dem inn, som for noen andre systemer.)
? Betalingstransaksjonene går direkte (kort til kort) mellom kjøper og selger, ikke via bank eller clearing-sentral.
? Overføring av midler kan skje over nett. (Internett, telefonlinje etc.)

7.7.2 Proton

I Norge vil BBS og bankene vil går for Proton som småpengeløsning[BBSP]. Proton er en internasjonal standard for elektronisk lommebok, og promoteres av Proton World (se [PROTON]). Proton-kontanter er sterkt knyttet til bankenes konto-systemer. Proton-kontanter kan ikke benyttes til videre kjøp og salg, men må løses inn etter at de er brukt én gang.

En Proton-småpengeapplikasjon vil være knyttet til brukerens bankkonto. Lading av Proton-kontanter kan kun skje fra denne kontoen. Ved lading vil penger trekkes fra brukerens konto over til en såkalt float-konto. Lading kan skje fra minibankauto-mater, dual-slot mobiltelefoner eller annet.

Ved bruk går elektroniske kontanter fra brukerens smartkort til selgerens smartkort. Selger må løse inn kontantene ved å sende dem til banken. Kontantene kan ikke omsettes på annen måte. Innløsning kan gjøres satsvis, per dag, per uke eller når det er ønskelig. Når kontantene innløses vil de bli avstemt mot float-kontoen. Renter fra float-kontoen vil tilfalle banken.

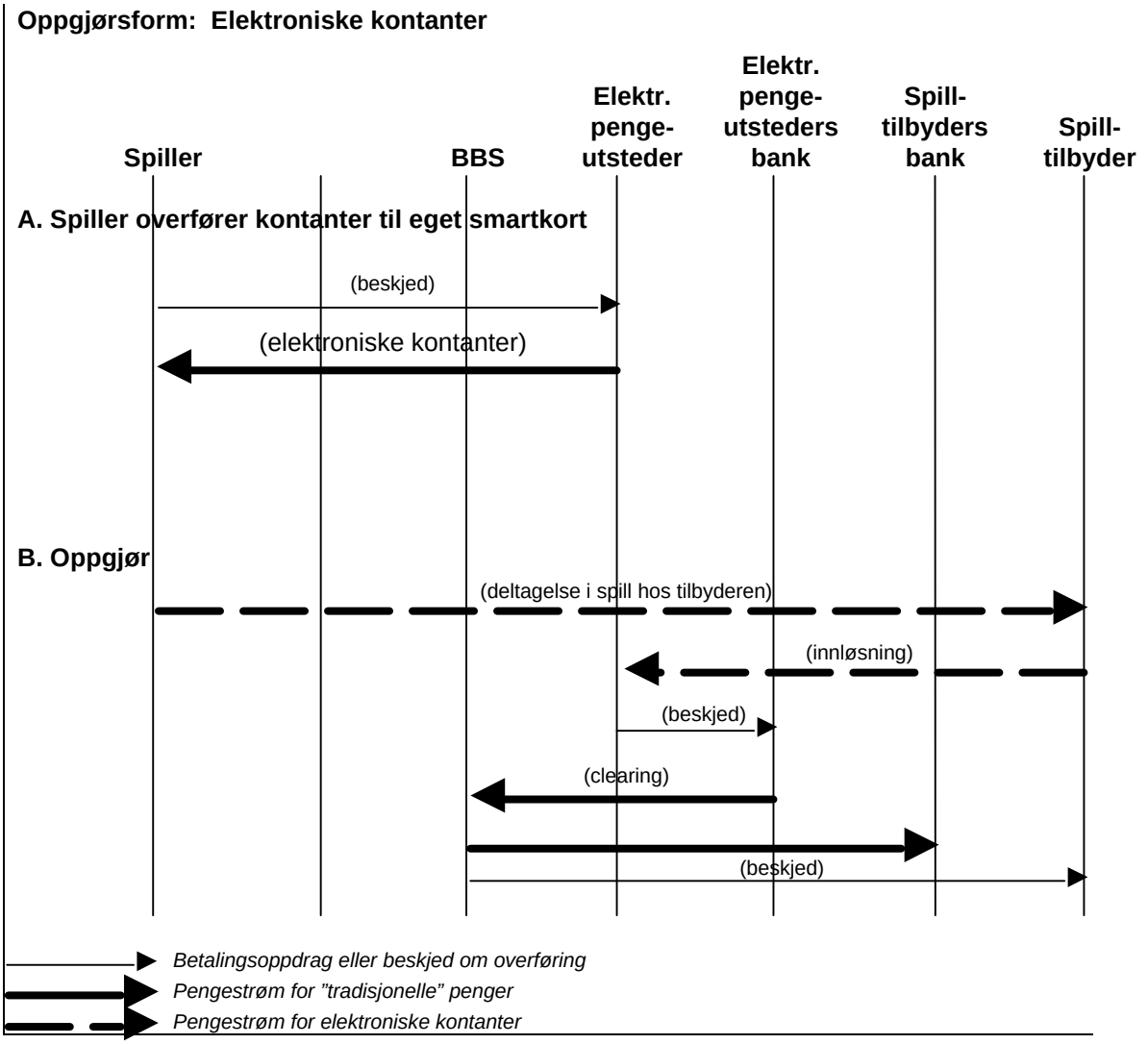
Proton tenkes implementert på flere typer smartkort. Per i dag er smartkortløsninger med Proton og EMV vist på Mulitapplikasjonskort av type JavaCard[48] men vil også bli implementert på Multos og Smart Card for Windows.

[47] Mer informasjon om Mondex finnes på http://www.mondexnorge.no og http://www.mondex.com Norsk representant for Mondex er Posten SDS.
[48] Se http://www.protonworld.com/systems/javacard.htm, http://www.protonworld.com/press/releases/press38.htm (6.1.2000)

Proton tenkes å fungere på ”alle” plattformer: I forhold til Internett vil Proton kunne aksesseres fra PC’er, smart-telefoner, web-telefoner, Internett-kiosker og mobiltelefoner.

I forhold til Mondex har Proton to klare ulemper:

? Proton-kontanter er potensielt mindre anonyme enn Mondex; midlene kan spores. (Dette kan også være en fordel, avhengig av hvordan man ser det.)
? Proton kan ikke gå fra kunde til kunde og bryter derfor med analogien til konvensjonelle kontanter.



Figur 23. Elektroniske kontanter. Kunde må først lade kortet (del A). Pengeutsterder er spillerens bank. Oppgjøret skjer så med elektroniske kontanter. Selger kan vente med å realisere kontantene (den stiplede linjen).

7.7.3 Elektroniske kontanter i scenariet

Modellen for elektroniske kontanter i scenariet velger Proton-systemet, som er beskrevet ovenfor. Lading av kontanter antas derfor å skje fra brukerens egen bank.

Nedenfor listes fordeler med elektroniske kontanter i spillscenariet:
1. Enkel bruk.
2. Godt egnet for små innsatser.
3. Lave transaksjonskostnader.
4. God sikkerhet.
5. Noen systemer kan håndtere utbetaling av mindre gevinster.

Følgende er ulemper med elektroniske kontanter i spillscenariet:
1. Ikke egnet for store innsatser på grunn av beløpsgrensen (se avsnitt 6.2).
2. Løser ikke problemet med utbetaling av større gevinster.
3. Som fysiske kontanter er elektroniske kontanter tapt hvis brukeren mister eller ødelegger den elektroniske ”lommeboken”. Noen systemer, som Proton, sporer transaksjoner slik at tapte kontanter kan rekonstrueres [AL00].
4. Elektroniske kontanter er (i prinsippet) anonyme. Brukeren kan (i prinsippet) ikke autentiseres av betalingshandlingen.

7.8 Oppsummering og konklusjon

Tabellen på side 66 oppsummerer betalingsmodellene med utgangspunkt i kravene som ble fremsatt i avsnitt 7 på side 51.

Som nevnt innledningsvis i dette kapittelet er kreditt- og telefonregningsmodellen mindre interessante i spillescenariet da de begge er modeller som trolig ikke vil tillates i fremtiden. Modellene er med i oppsummeringstabellen, men de er ikke med i diskusjonen nedenfor. Gjenstående betalingsmodeller er da debetmodellen (med SET), modellen for elektroniske kontanter og konto-hos-tilbyder-modellen (konto-modellen). Kolonnen *Ønskede egenskaper* i tabellen på side 66 er referansemodellen som tilfredsstiller alle krav.

Som det fremgår av tabellen på side 66 er det ingen av betalingsmodellene som gir alle de ønskede egenskaper:

Det forutsettes at alle modellene er enkle i bruk.. I det ligger at modellene skal kunne betjenes i en enkel dialog med spilletjenesten ved hjelp av tastaturet på mobil-telefonen.

Autentisering av spilleren kan bli et lovpålagt krav, og det er derfor et poeng for spilltilbyderen i scenariet. Hvis betalingsmodellen kan autentisere spilleren overfor tilbyderen vil det gjøre det enkelt for tilbyderen. Av de aktuelle modellene er det bare modellen for elektroniske kontanter som er helt anonym. Tilbyderen kan i prinsippet plukke opp autentiseringsinformasjon fra både debet- og kontomodellen, men det forutsetter at implementasjonen av betalingsmodellene har gjort det mulig. Det synes derfor å være høyst usikkert å basere seg på at *betalingsmodellen* skal tilby ønsket autentisering. Av prinsipielle grunner bør antakelig betalingshandlingen skilles fra spillehandlingen, og handlingene bør ha hver sine sikkerhetsløsninger.

Alle modellene betjener videre betaling av innsats, men bare debetmodellen kan håndtere store innsatser over kr 1000. Debetmodellen som håndterer store innsatser har også høyest transaksjonskostnader.

Det er bare kontomodellen som klarer å håndtere gevinstutbetaling. Utbetaling av gevinst krever i min fremstilling at selger allerede har, eller kan, tilegne seg kunnskaper om kundens kontonummer fra, for eksempel, spillerens *innbetaling*. I kontomodellen er det ikke nødvendig da tilbyderen allerede disponerer spillerens

	Ønskede egen-skaper	**Debet med SET**	**Elektr. kon-tanter**	**Konto hos tilbyder**	**Kreditt**[?]	**Telefon-regning**[?]
Enkel bruk?	*Ja*	Ja	Ja	Ja	Ja	Ja
Autentiserer modellen spiller?	*Ja*	Ja	Nei	Ja	Nei	Ja
Håndterer modellen betaling av innsats?	*Ja*	Ja	Kun små-beløp	Kun små-beløp	Ja	Kun små-beløp
Transaksjonskostnad ved innsats < 10 Kr	*Rimelig*	Dyrt	Rimelig	Rimelig	Dyrt	Rimelig
Trans. kost. ved innsats > 1000 Kr	*Rimelig*	Relativt rimelig	--	--	Relativt rimelig	--
Gevinstutbetaling mulig?	*Ja*	Nei	Nei	Ja	Ja	Nei
Utbet. < 10 Kr	*Rimelig*	--	--	Rimelig	Dyrt	--
Utbet. > 1000 Kr	*Rimelig*	--	--	Ikke lovlig	Relativt rimelig	--
Krever kundeforhold til selger/ tilbyder for bet. av innsats?	*Nei*	Nei	Nei	Ja	Nei	Ja
Akseptabel sikkerhet for kjøper/spiller?	*Ja*	Ja	Ja	Ja?	Nei?	Ja?
Akseptabel sikkerhet for selger/tilbyder?	*Ja*	Ja	Ja	Ja	Nei?	Neppe ved store beløp

Tabell 1. Sammenligning av betalingsmodellene. Kolonnen for *Kreditt med SET* er utelatt da den er identisk med *Debet med SET*.

konto. Kontomodellen er imidlertid den eneste som krever at det er etablert et kundeforhold før deltagelse i spillet. Det er naturlig at tilbyderen spør spilleren om bankkontonummeret ved opprettelse av kundeforholdet. Tilbyderen vil da også kunne håndtere utbetaling av store beløp.

Angående sikkerhet: Tabellen har to rader for sikkerhet – en for kunde og en for selger. Radene gir i stor grad uttrykk for hvordan sikkerheten *oppfattes* av aktørene. Overføring av for eksempel kredittopplysninger over mobilnettet forutsettes sikkert (ved bruk av nettverkssikkerhet, se avsnitt 2.5.2), men kunden må stole på at selgeren ikke misbruker opplysningene (hvilket kan være et generelt problem, men trolig ikke er særlig sannsynlig i akkurat dette tilfellet). Kontomodellen er sikkerhetsmessig skjev, ved at spilleren er den klart svakeste part ved brudd på tilliten. Det er bare debetmodellen og modellen for elektroniske kontanter som har god sikkerhet for alle parter.

[?] Betalingsmodellen vil antakelig bli ulovlig i spillsammenheng (se avsnitt 6.2).

En konklusjon er at en løsning som involverer innsatser over kr 1000 må inkludere debetmodellen da debetmodellen er den eneste som kan håndtere dette. Debetmodellen bør kombineres med modellen for elektroniske kontanter eller kontomodellen, for å gi rimelige transaksjonskostnader. Gevinstutbetalingsproblemet må imidlertid løses.

Ulempen med kontomodellen er at den krever at det er opprettet et kundeforhold før deltagelse i spill. Sikkerheten er heller ikke tilfredsstillende for spilleren. Kontomodellen må også kombineres med en annen modell for utbetaling av høye gevinster.

Ulempen med modellen for elektroniske kontanter er at den – i likhet med debetmodellen – må løse utbetalingsproblemet for store gevinster. Ellers er modellen for elektroniske kontanter godt egnet da den løser sikkerhetsproblemene og i tillegg ikke krever kundeforhold.

Angående utbetalingsproblemet: En praktisk tilnærming er å avkreve spilleren bankkontonummeret som en del av brukerdialogen i spillet. Tilbyderen kan eventuelt registrere kontonummeret i sin database for senere bruk.

Det er grunn til å tro at modellen for elektroniske kontanter har lavere administrasjonskostnader enn kontomodellen. I modellen for elektroniske kontanter er tilbyderen ikke "bank" for spilleren, og tilbyderen trenger heller ikke å gjøre det administrative rundt registrering av spillere. Modellen for elektroniske kontanter har også potensiale til å bli brukt offline, det vil si i direkte kontakt mellom kunde til selger over disk – uten å benytte mobilnettet. Dette kan realiseres ved Bluetooth-teknologi for trådløs kommunikasjon over korte avstander (se avsnitt 3.5). Brukt offline vil elektroniske kontanter (nesten) ikke ha transaksjonskostnader, og i tillegg synes brukspotensialet å være mye større enn med kontomodellen. Som beskrevet i avsnitt 7.7, synes Proton å være den mest realistiske implementasjonen av elektroniske kontanter i Norge i nærmeste fremtid.

En konklusjon blir derfor at kombinasjon av modellen for elektroniske kontanter og debetmodellen vil være godt egnet i spillscenariet.

8 Designaspekter ved spilltjenesten

Dette kapittelet diskuterer problemstillinger med utgangspunkt i scenariebeskrivelsen i kapittel 6. Kapittelet diskuterer overordnede problemstillinger som en hvilken som helst spilltilbyder må tenke igjennom før tjenester som blant annet omfatter inn- og utbetalinger kan implementeres. Det er tatt utgangspunkt i de to betalingsmodellene (fra kapittel 7) som ble funnet best egnet for denne typen Internett-spill på mobiltelefon – modellen for elektroniske kontanter og debetmodellen.

En overordnet transaksjonsmodell for scenariet tegnes i neste avsnitt. Det avdekkes seks faser i spillet. Kapittelet organiserer problemstillingene etter disse seks fasene.

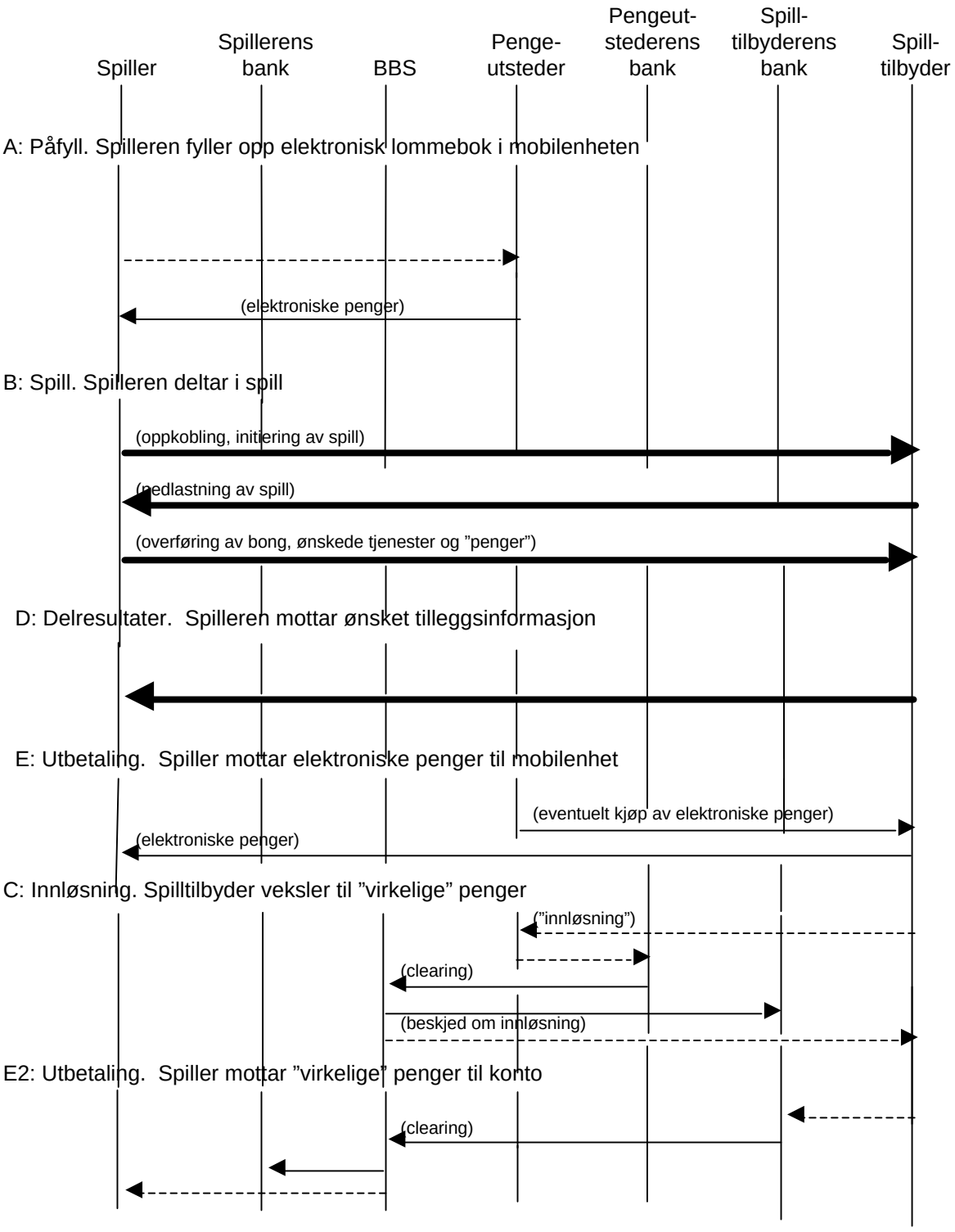
8.1 Transaksjonsmodell for elektroniske kontanter

Fra avsnitt 7.8 på side 64 ble det konkludert med at elektroniske kontanter var best egnet som småpengeløsning i scenariet. En overordnet transaksjonsmodell for alle spillets faser med elektroniske kontanter som betalingsmodell er tegnet i Figur 24. (Debetmodellen er egnet for store innsatser, men den tegnes ikke da den ikke bringer noe vesentlig nytt.)

Figur 24 avdekker seks faser i spillet:

1. *Påfyllfasen*: I denne fasen er spilleren koblet opp til utsteder av elektroniske penger for påfyll av den elektroniske lommeboken i mobiltelefonen. Denne fasen er uavhengig av de andre fasene i spillet.
2. *Spillefasen*: I denne fasen har spilleren midler til å delta i spillet. Han knytter seg opp mot tjenesten til tilbyderen, deltar i spillet og betaler.
3. *Delresultatfasen*: I denne fasen leverer tilbyderen ønskede delresultater i spillet til spillerens mobiltelefon.
4. *Utbetalingsfasen*: I denne fasen utbetaler tilbyderen gevinst til konto eller til mobiltelefonen for de heldige vinnerne.
5. *Innløsningsfasen*: I denne fasen løser tilbyderen inn elektroniske kontanter hos pengeutsteder.
6. *"Hyggelig-meldingsfasen"*: I denne fasen forsøker tilbyderen å bygge relasjoner ved å invitere spilleren til nærmeste travbane.

Modellen for elektroniske kontanter



Figur 24. Transaksjonsmodell for elektroniske penger som betalingsmodell.

8.2 Påfyllfasen

I påfyllfasen er brukeren koblet opp mot sin bank for overføring av et beløp fra sin bankkonto til smartkortet i mobiltelefonen. Denne fasen i transaksjonsmodellen er uavhengig av de andre fasene i spillet, og gjør mobiltelefonen til et generelt ”betalingsinstrument” med et bruksområde som ikke bare er knyttet til spillscenariet.

Det er ikke noe i veien for at brukeren kan handle elektroniske kontanter andre steder enn i sin bank, men det forenkler modellen hvis brukerens bank og utsteder av elektroniske kontanter er én og samme aktør. Administrasjon av brukerens konto blir da en intern handling hos banken, og en unngår den tidkrevende og dyre veien om clearing hos BBS. Skal denne modellen fungere må bankene påta seg rollen som utsteder av elektroniske kontanter, noe som bankene er på vei til å gjøre ved oppslutningen om Proton. Demonstratorens brukerdialog i Figur 28 på side 87 forutsetter at spilleren forholder seg kun til én aktør og at kontantene overføres umiddelbart.

8.2.1 Sikkerhet for banken

Løsningen har innebygget sikkerhet på flere nivåer. For å ta tjenesten i bruk vil banken forutsette at det er tegnet en avtale som gir brukeren tilgang til bankens tjenester på mobiltelefon for brukerens konti. Småpengeapplikasjonen i smartkortet i mobiltelefonen vil være implementert og eiet av banken og vil ivareta bankens sikkerhetsbehov. Det er viktig for banken at småpengeløsningens sikkerhet ikke kan trekkes i tvil, det vil si at forhold rundt konfidensialitet, integritet og autentisering er ivaretatt. Videre er kravet til ikke-benekting viktig. Brukeren må ikke senere kunne nekte for at han har utført handlingen. (Dette er sikkerhetsaspekter som er behandlet i kapittel 2). Brukeren må derfor avkreves en positiv bekreftelse på at transaksjonen skal finne sted, på samme måte som det gjøres med PIN-koder i dagens Bank-Accept-løsning. Man kan si at PIN-koden brukes til signering av meldingen som går til banken. Teknisk sett låser PIN-koden opp for bruk av signeringsnøkkelen i smartkortet. (Se også avsnitt 5.4.3 om signering ved hjelp av smartkort.)

8.2.2 Sikkerhet for brukeren - signeringsproblemet

Brukerens bekymring i kontakt med banken bør være om korrekt beløp er trukket fra hans konto, og om beløpet er trygt overført og disponibelt i hans mobiltelefon. Brukeren har ikke annet valg enn å stole på banken. Brukerens aktive handling i denne transaksjonen består kun av signering ved hjelp av PIN-koden. Det sentrale spørsmålet blir derfor hvordan brukeren kan være sikker på hva han egentlig signerer? [49]

Usikkerhet rundt signering av meldinger fremkommer fordi brukeren ikke har god nok kontroll over situasjonen. Når en applikasjon selv ”sier” at den signerer en

[49] Bruk av PIN-kode i minibanker har mange fellestrekk med problemstillingene her. I en minibank har imidlertid banken full kontroll over brukergrensesnitt og infrastruktur, hvilket ikke er tilfellet ved bruk av mobiltelefon.

melding, har brukeren bare begrenset mulighet til å verifisere at riktig tekst signeres, eller at signering i det hele tatt faktisk skjer.

WAP-applikasjoner, det vil si potensielt fiendtlige applikasjoner som lastes ned over Internett, vil representere en betydelig risiko når de er i interaksjon med applikasjoner i smartkort i mobiltelefoner. Risikoen er størst hvis WAP-applikasjoner får styre kommunikasjonen mellom smartkortapplikasjoner og eksterne (serverbaserte) applikasjoner og i tillegg være alene om å håndtere dialogen med brukeren. *Det* må ikke skje, da sikkerheten i så fall vil ligge i selve WAP-applikasjonen og i praksis gjøre signering verdiløs.

Bruk av smartkort til signering krever at alle ledd som er involvert, det vil si smartkort, kortleser, skjerm, tastatur og vertsapplikasjonen på mobiltelefonen samspiller for å gjøre hele signeringsoperasjonen sikker. En WAP-applikasjon må ikke tillates å kontrollere noen av disse leddene, i hvert fall ikke under signeringsprosessen.

Signering fra en WAP-applikasjonen vil skje med biblioteksfunksjonen *Crypto.signText* i WML-Script [WMLSCL]. Kontroll av alle aspekter ved signeringen vil med andre ord besørges av biblioteket og ikke av WAP-applikasjonen selv. Dermed ivaretas sikkerheten ved signering, men en står fortsatt overfor et administrativt problem: Hvordan vet brukeren at han faktisk er i en ekte dialog, og ikke en falsk dialog hvor han lures til å avgi PIN-koden sin? En falsk dialog kan være en WAP-applikasjon med fiendtlige hensikter.

Fra spesifikasjonen står kun at den originale teksten må presenteres på en måte som er distinkt fra tekst som genereres av applikasjoner som benytter WML eller WML-Script [WMLSCL, s.16]. En slik tilnærming er mulig i en WAP-setting hvor det er sterkt begrenset hvilket visuelt uttrykk en applikasjon kan ha. I en nettleser på Internett kan en tilstandsindikator gjøre samme nytten, som vist i Figur 25. Det er uansett opp til mobiltelefonprodusenten hvordan dialogen faktisk blir utformet.

Figur 25. Tilstandsindikatorer i nettleseren Netscape Navigator. Et hengelåsikon indikerer at sesjonen er kryptert mellom klient og tjener. Ikonet ved siden av indikerer at forbindelsen mellom klient og tjener er operativ. (Eksempelet er hentet fra Kreditkassens tjeneste for betaling av regninger, http://www.kbank.no).

8.2.3 Modell for sanntid saldovisning

Fra scenariebeskrivelsen i kapittel 6 er det gitt at mobiltelefonen alltid har oppdatert visning av innestående beløp på brukerens bankkonto. Denne tjenesten vil bidra til å

gi brukeren bedre kontroll over egen økonomi. Fordelen med sanntid saldovisning vil være at brukeren slipper å vente på oppkobling og eventuell bruk av engangspassord for å få tilgang til tjenesten. Tjenesten må ytes av spillerens bankforbindelse. For å realisere sanntid saldovisning må banken varsle brukeren ved alle kontotransaksjoner.

Det er i dag tre mulige implementasjoner for sanntid saldovisning:

1. Regulære tekstmeldinger. Ulempen med regulære tekstmeldinger er at de er lette å forfalske da hvem som helst kan sende tekstmeldinger til mobiltelefoner (SMS, avsnitt 3.1.5). Hvis det kan aksepteres at sikkerhetsnivået ikke må være 100%, kan tekstmeldinger likevel være en god implementasjon. Tekstmeldingen kan identifisere kontonummer i tillegg til saldo, hvilket kan være akseptabel sikkerhet. Enklere kan det i hvert fall ikke implementeres.

2. Tekstmeldinger til applikasjon i SIM-Toolkit (se avsnitt 5.4.2). Denne løsningen kan lages sikker med signering og kryptering hvis ønskelig. En annen fordel er at denne implementasjonen vil være transparent for brukeren. SIM-Toolkit-applikasjonen vil selv håndtere mottak av meldinger uten at brukeren er klar over at kommunikasjon finner sted. Saldo kan i tillegg integreres i telefonens menyer ved hjelp av funksjonalitet i SIM-Toolkit. Ulempen med SIM-Toolkit er at det krever at mobilleverandørene har gjort tjenesten tilgjengelig i SIM-kortet i mobiltelefonen.

3. Manuell saldo. Alternativet til alltid å ha oppdatert informasjon om saldo er å la brukeren selv hente denne informasjon fra bankens webtjeneste slik det gjøres i dag.

Det vil påløpe en ekstra kostnad for tekstmeldinger knyttet til hver transaksjon ved sanntid saldovisning. Hvis denne kostnaden er høy vil sanntid saldovisning være lite attraktivt. Hvis manuell saldo kan implementeres slik at det er enkelt å bruke (med GPRS beskrevet i avsnitt 3.2, vil oppkobling skje raskt), kan det være uaktuelt å implementere annet enn en ”manuell” tjeneste.

8.3 Spillefasen

I spillefasen er spilleren knyttet opp til tilbyderen og tjenestene hans. Spilleren har alt ordnet seg slik at han kan betale for tjenesten. Spilleren besøker tilbyderens webtjeneste. Han fyller ut en bong ved å tippe vinnere i to hesteløp, han betaler for tjenesten og mottar kvittering.

8.3.1 Forutsetninger for spill uten kundeforhold

I tjenester som omfatter innbetalinger og utbetalinger er det naturlig at det er etablert et kundeforhold på forhånd. I scenariet vil det være naturlig å ha en registreringsfase forut for bruk av tjenesten. Fra beskrivelsen av lovverket i avsnitt 6.2 er det rimelig at registrering av identitet vil bli krevet av myndighetene for deltagelse i spill. Registrering av spillerens bankkonto er en praktisk måte å løse utbetalingsproblemet på for tjenesteleverandøren.

Registrering er imidlertid en ”unødvendig” handling som kan være en terskel for å delta i spillet – i hvert fall for tilfeldige spillere. Registrering slik det foregår i dag innebærer fysisk underskrift ved fremmøte hos kommisjonær. I vårt scenario er alternativet til papirbasert registrering, registrering over mobiltelefonen. En kan eventuelt tenke seg at selve spillesesjonen inneholder nok informasjon til at spilltilbyderen kan foreta sikker identifikasjon av spiller og spillerens konto, og dermed unngå eksplisitt registrering. I det følgende antas det at myndighetenes krav ikke er registrering i seg selv, men muligheter for identifikasjon av spillere, det vil si muligheten for å knytte identifikasjon til bong.

Autentiseringsproblemet
For mobiloperatørene er autentisering av *mobiltelefonen* (det vil si telefonens SIM-kort) godt nok med hensyn til fakturering, men autentisering av *brukeren* av mobil-telefonen krever en eksplisitt autentiseringshandling (PIN-kode eller lignende) som en del av dialogen med tjenesten.

Kapittel 5 introduserte smartkort som en løsning på autentiseringsproblemet. Autentisering av brukeren overfor tilbyderen fordrer at telefonen inneholder en smartkortbasert autentiseringsapplikasjon og at det transporteres nok informasjon over til tilbyderen slik at han er i stand til å verifisere brukerens identitet. Autentisering må være en grunnleggende egenskap i mobiltelefonen (på samme måte som betalingsapplikasjonene) og *det* forutsetter at andre aktører enn tilbyderen har gjort autentiseringstjenesten mulig. Autentisering ved hjelp av mobiltelefon vil da kunne benyttes i alle scenarier hvor autentisering er påkrevd.

I scenariet vil autentisering av brukeren ligge implisitt i signering av bong. Brukeren vil signere bongen før sending. Tilbyderen kan verifisere signaturen ved å hente frem brukerens offentlige nøkkel fra brukerens identitetssertifikat. Dermed er brukerens identitet gitt. (Mer om sertifikater i avsnitt 2.4).

Bankkontoproblemet
I forslaget til ny lotterilov (se avsnitt 6.2) vurderes det å kreve at utbetalinger ved spill må skje til bankkonto. Det er flere mulige løsninger for tilbyderen på problemet med å få kjennskap til spillerens bankkontonummer for utbetaling av eventuell gevinst. Hvis en forutsetter at spilleren ikke er registrert hos tilbyderen, må tilbyderen få kontonummeret i løpet av kommunikasjonen med brukeren. Skal dette skje automatisk må mobiltelefonen inneholde denne informasjonen, og informasjonen må være tilgjengelig for tilbyderen.

Det mest nærliggende er i så fall at kontonummeret kan ligge som en del av brukerens elektroniske identitetssertifikat. X509v3 tillater for eksempel utvidelser som kunne bli brukt til dette formålet (se avsnitt 2.4). Kontonummer ville dermed være lett tilgjengelig for tilbyderen. Det er en imidlertid ikke naturlig å ha bankkontonummeret i identitetssertifikatet. Et sertifikat som dette vil være, er et offentlig tilgjengelig ”dokument”, og av sikkerhetsgrunner bør kontonummeret derfor *ikke* ligge i sertifikatet.

En annen løsning er å gi mobiltelefonens smartkort en egen banknummerapplikasjon som kan aktiveres som en del av brukerdialogen i spillesesjonen. Tidligere i dette kapittelet ble det argumentert med at tjenestene i mobiltelefonen (eksempelvis elektronisk identitetsapplikasjon og elektronisk lommebok) måtte være en integrert del av mobiltelefonen for at de skulle være enkle å ta i bruk. Applikasjonene som skal legges ned i mobiltelefonens smartkort fra "tidenes morgen" må være så alminnelige at de vil være av interesse for alle. Det er vanskelig å tenke seg at en banknummerapplikasjon vil være generell nok til å fortjene en slik status, og denne løsningen synes derfor ikke å være realistisk.

Nok en løsning kunne være å snappe opp bankkontonummeret fra småpenge- eller debet-applikasjonen i mobiltelefonens smartkort, men det ville være betenkelig med hensyn til sikkerheten om applikasjonene tilbød denne muligheten.[50]

Det synes som om den eneste realistiske måten å få tak i kontonummeret vil være å spørre brukeren om dette som en del av brukerdialogen. Tilbyderen kan lagre kontonummeret knyttet til identitet og tilbyderen kan presentere siste oppgitte kontonummer som standardverdi ved senere besøk. Brukeren får dermed kun en kontrollerende oppgave.

8.3.2 Er det fordeler *med* et etablert kundeforhold?

Hvis brukeren er registrert hos tilbyderen kan det forenkle deler av kommunikasjonen. Registrering vil kunne gjøre en identitetsapplikasjon i mobiltelefonen overflødig da tilbyderen i så fall er kjent med brukerens identitet. Han vil også kjenne kontonummeret til brukeren.

Med et etablert kundeforhold kan autentisering av brukeren for eksempel skje ved at brukeren logger seg på hos tilbyderen med sin egen PIN-kode eller passord.

Det er imidlertid argumenter for å beholde identitetsapplikasjonen for signering av meldinger selv med et etablert kundeforhold: Uten sikkerheten som ligger i signering av meldinger utsetter tilbyderen seg for ikke-benektingsproblemet; brukeren kan i ettertid nekte for å ha utført handlinger, og tilbyderen mangler mekanismer for å motbevise det. Med mindre myndighetene faktiske vil kreve kunderegistrering kan jeg ikke se andre fordeler med kunderegistrering i forhold til selve spillet, enn at tilbyderen får kjennskap til brukerens kontonummer.

En skal imidlertid ikke se bort fra at tilbyderen kan ha gode motiver (markedsføring og annet) for å etablere et kundeforhold til spilleren.

[50] Hverken Mondex, Proton eller EMV har grensesnitt for å gi ut informasjon om kontonummer ifølge [SG00][RS00].

8.3.3 Håndtering av innbetaling

Fra avsnitt 7 om betalingsmodeller ble det konkludert med at elektroniske kontanter er godt egnet som betalingsløsning så lenge beløpet er lite. Ved større beløp (over kr 1000.-) må den direkte debetmodellen benyttes.

Betalingsløsninger med bruk av elektroniske kontanter over mobiltelefon finnes ikke i Norge i dag. Telenor har imidlertid implementert en debetløsning på mobiltelefon i MobilHandel-konseptet (se avsnitt 7.6). Ved bruk av debetløsningen i MobilHandel må kunden bekrefte beløp med å taste inn et engangspassord fra en liste som brukeren får av sin bank. Hvis mobiltelefonen hadde hatt en generell signeringsapplikasjon antas det at engangspassord hadde vært overflødig.

Det kan synes som om Proton og EMV er de mest aktuelle systemene for å realisere betalingsløsninger for henholdsvis elektroniske kontanter og debitering (se kapittel 7). Det forutsettes at de begge er enkle å betjene, det vil si at kundens handling begrenser seg til å bekrefte transaksjonen med bruk av PIN-kode.

Begge systemene vil kreve installasjon av bankprogramvare hos tilbyderen. Det vil være bankene som setter premissene for datasystemene hos tilbydere.

8.3.4 Brukerdialogen

Spillet ”Dagens Dobbel” er i utgangspunktet et meget enkelt spill, og det er ikke mange mulighetene til å være kreativ i brukergrensesnittet. Brukeren skal plukke ut vinnerhester, og kreativiteten begrenser seg stort sett til presentasjon av hestene. Det naturlige vil nok være å presentere hestene etter startnummer, nummerert fra 1 til 15. Et annet alternativ er presentasjon etter odds, hvilket igjen kan virke selvforsterkende på oddsen. Et tredje alternativ er ”Amazon.com”-metoden: ”Spillere som har tippet på hest nr 3 har også tippet på hest nr 7”.[51] En annen mulighet er presentasjon av hestene ut fra spillerens tidligere interesse for de startende hestene.

Scenariet i kapittel 6 antydet en hjelpfunksjon som var et syntetisk generert menneskehode som er i stand til audio-visuell kommunikasjon med brukeren. Denne tilsynelatende beskjedne funksjonen kan vanskelig gjennomføres med dagens båndbredde i GSM-nettet. Audio-visuelle hjelpefunksjoner av denne typen må først og fremst være enkle og billige å tilpasse i brukerdialogen. Et typisk karakterbasert spill som ”Dagens Dobbel” er neppe en god kandidat til å spesialutvikle en avansert tilleggsfunksjon som neppe gir særlig forbedret funksjonalitet.

8.3.5 Spillefasen *uten* bruk av smartkortfunksjonalitet

Denne oppgaven har skissert mobiltelefonspillet med aktiv bruk av applikasjoner i mobiltelefonens smartkort. Smartkort har muliggjort flere av de tjenesten som er beskrevet, først og fremst den elektroniske lommeboken og debetløsningen for

[51] Amazon.com-metoden vil nok oppfattes som useriøs i denne sammenheng.

betaling, men også identitets/signeringsapplikasjonen var nødvendig for å unngå kunderegistrering og for å imøtekomme ikke-benektingsproblemet.

Er det mulig å tenke seg en implementasjon av spillet uten bruk av ovennevnte applikasjoner og uten smartkortfunksjonalitet i det hele tatt? Nedenfor følger en diskusjon av alternativer med hensyn til implementasjon:

1. *Autentisering*: Registrering av spilleren forut for deltagelse i spillet vil være nødvendig uten bruk av smartkortbasert autentisering. Kunden må logge seg på med passord på tilbyderens websider.

2. *Signering*:[52] Uten signerte meldinger mistes den tryggheten dette gir for problemet med ikke-benekting. Tilbyderen kan få problemer med å dokumentere de faktiske forhold hvis spilleren nekter for å ha sendt en melding. Det vil være en avveiningssak hvorvidt tilbyderen er komfortabel med sikkerheten uten signering. En tvist angående sikkerhet vil kunne være ødeleggende for tilbyderen, og omdømmet til tilbyderen er antakelig det viktigste som blir ivaretatt ved en signeringsapplikasjon.

3. *Elektronisk lommebokapplikasjon*: ”Internett-konto” peker seg ut som alternativ småpengebetalingsmetode (se avsnitt 7.6). I avsnitt 7.8 ble det konkludert med at en elektronisk lommebok har større potensielt bruksområde enn Internett-konto-løsningen, ved at den også kan benyttes offline i andre sammenhenger (for eksempel betaling i vanlige butikker) og dermed også gi lavere transaksjons-kostnader. I spillscenariet må begge modellene være online, og det vil neppe være stor differanse i transaksjonskostader i dette tilfellet. Som beskrevet benyttes kontoløsningen i MobilHandel-konseptet til Telenor. Denne løsningen er imidlertid avhengig av en smartkortapplikasjon i SIM-Toolkit for konfidensialitet, integritet og autentisering da SMS-bæretjenesten alene ikke er sikker nok. Selv i en WAP-implementasjon vil ikke sikkerhetslaget WTLS tilby ende-til-ende-sikkerhet; det må med andre ord være et lag over WTLS som tilbyr ende-til-ende-sikkerhet, og det er vanskelig å se hvordan dette kan gjøres uten funksjonaliteten som ligger i smartkort.

4. Debetløsning: Debetløsninger som EMV vil forutsette smartkortsikkerhet.

Konklusjon er klar: Ingen av betalingsløsningene vil bli sikre nok uten bruk av smartkort. Også i forhold til tilbyderen er smartkortfunksjonalitet nærmest en forutsetning i forhold til ikke-benektingsproblemet. Helt uten smartkortfunksjonalitet kan man uansett ikke klare seg. Grunnleggende nettverkssikkerhet som konfidensialitet og integritet baserer seg aktivt på sikkerhetsmodulene som ligger i smartkort.

[52] Merk at en signeringsapplikasjon og en identitetsapplikasjon vil være en og samme applikasjon/funksjon.

8.4 Delresultatfasen

I denne fasen er spilleren ferdig med den aktive fasen av spillet. Spilleren venter på eventuelle delresultater som følge av de valgene han har gjort i spillefasen. Spilleren har valgt å få tekstmelding om resultatet fra det første løpet, og audio-visuell visning til mobiltelefonen av hele det andre løpet hvis han har tippet riktig vinner i første løp.

8.4.1 Tekstmeldinger til mobiltelefonen

I GSM-nettet betjenes tekstmeldinger av kortmeldingssenteret (SMSC – se Figur 4 på side 14). Mobiloperatørene har integrert kortmeldingssenteret med Internett-teknologi slik at sending av tekstmeldinger til mobiltelefoner kan skje med elektronisk post hvor mobiltelefonnummeret er en del av e-postadressen. Levering av tekstmeldinger til spilleren reduseres dermed til å fange opp spillerens mobil-telefonnummer i spillerfasen. Det byr imidlertid ikke på problemer. Identifikasjon av telefonnummer er standard funksjonalitet i GSM.

8.4.2 Video til mobiltelefonen

Som beskrevet i kapittel 3 ligger levering av video til mobile enheter noe fram i tid. Selv om radioaksessnettet blir dimensjonert for å levere båndbredden som video krever (GPRS eller UMTS), er det likevel begrenset hvor mange parallelle videostrømmer som kan sendes ut innenfor dekningsområdet til en basestasjon samtidig. I scenariet vil video av et sanntids hesteløp bli å anse som kringkasting, og en kan tenke seg at mobiloperatøren kan kringkaste (det vil si multicaste) til alle interesserte kunder.

Suksessen for videotjenesten antas derfor å være avhengig av at mobiloperatøren tilbyr multicastfunksjonalitet i radionettet. Mulitcast-streaming av video på Internett er kjent teknologi [Casner94] og vil antakelig være like godt egnet for implementa-sjon i mobiloperatørenes nett også.

8.4.3 Animering av hesteløpet

Videovisning av hesteløpet er ressurskrevende og vil kreve teknologi som ikke eksisterer i dag. Visning av hesteløpet kan imidlertid realiseres også i dag i en primitiv variant ved å animere hestene. Animering kan for eksempel implementeres ved å la tekstsymboler representere hestene. Visuelt kan denne teknikken sammenlignes med å gå fra dagens videorealistiske dataspill *tilbake til* dataspillene med tegnbasert grafikk (!)

Animering har meget beskjedne båndbreddekrav da bare tekstsymboler som repre-senterer hestene beslaglegger båndbredde. En klar ulempe er selvfølgelig at animering ved hjelp av tekstsymboler kan oppleves som visuelt kjedelig i forhold til video. Hvis en bare ser på informasjonsinnholdet kan animering trolig gi et klarere bilde av hestenes innbyrdes posisjoner enn det er mulig å få til på en liten videoskjerm.

I demonstratorkapittelet (neste kapittel) beskrives forsøket på å implementere en enkel animasjon av hesteløpet med dagens teknologi.

8.4.4 Direkte betaling for båndbredde

I scenariet betaler spilleren for båndbredde direkte til mobiloperatøren i forbindelse med overføring av video av hesteløpet. En slik direktebetalingsmodell kan sammenlignes med telefonkiosker med myntinnkast hvor myntene betaler for ringetid underveis i samtalen.

Hvis operatørene implementerer denne betalingsmodellen er det lite trolig at de vil nøye seg med å benytte den kun til å ta seg betalt for video. Modellen har klart et potensiale til å erstatte dagens kontantkort. Sammen med en elektronisk lommebok-applikasjon er dette en ideell situasjon for en mobiloperatør til å ta seg direkte betalt av kunden. Mobiloperatøren vil helt slippe fakturering og administrasjon.

Det gjenstår å se om en direktebetalingsmodell lar seg gjennomføre. Telenor har for eksempel ikke planer om å realisere en slik modell i forhold til MobilKonto-løsningen i MobilHandel-konseptet [SS00].

8.5 Utbetalingsfasen

I denne fasen står tilbyderen overfor problemet med gevinstutbetaling til kunden. I scenariet vil spillere som har vunnet i spillet komme til utbetalingsfasen.

8.5.1 Utbetaling til bankkonto

Fra diskusjonen om betalingsmodeller i avsnitt 7 er det gitt at store utbetalinger kan bare skje til konto. Forslaget til ny lotterilov kan i tillegg komme til å *forutsette* utbetaling til konto for deltagelse i spill over Internett.

I avsnitt 8.3.1 ble det diskutert forskjellige modeller for å få tak i spillerens kontonummer. Det ble konkludert med at det var to måter å gjøre dette på. Den første og mest nærliggende er en registreringsfase forut for deltagelse i spill, hvor tilbyderen kan få all relevant informasjon om spilleren. Den andre modellen forutsetter at spilleren oppgir kontonummeret som en del av brukerdialogen i selve spillet. Utbetaling til bankkonto vil gå som en vanlig banktransaksjon.

8.5.2 Utbetaling til mobiltelefonen

En kan tenke seg at utbetaling kan skje til den elektroniske lommeboken i mobiltelefonen. Tilbyderens motiv for utbetaling til mobiltelefon kan for eksempel være å få pengene fort inn i omløp igjen. Det er imidlertid to sider som denne utbetalingsmodellen må håndtere:

? Full lommebok: Overføring må ikke medføre at beløpsgrensene i lommeboken overskrides.
? Ingen kommunikasjon: Mobiltelefonen kan være utenfor dekningsområdet eller avslått.

Problemene ovenfor kan løses med utbetaling til konto. Da utbetalingsmodellen uansett må håndtere utbetaling til konto vil det redusere kompleksiteten å ikke tilby utbetaling til mobiltelefonen.

Det er et godt prinsipp ved tradisjonelle (ikke-elektroniske) lommebøker at eieren har full kontroll over innholdet. Eieren vil miste noe av kontrollen hvis andre skal få lov til å "tukle" med innholdet. Konsistensen mellom den fysiske og den elektroniske lommebokmodellen blir brutt hvis tilbyderen skal tillates å fylle opp den elektroniske lommeboken. Det er heller ikke sikkert at lommebokapplikasjonen tillater "utenforstående" aksess på denne måten. Proton vil for eksempel ikke tillate lasting av kontanter fra andre kilder enn bankkontoen som Proton er knyttet til.[RS00]

Ut fra ovenstående betraktninger synes ikke direkte utbetaling til mobiltelefonen å være en god idé.

8.6 Innløsningsfasen

Ved kjøp og salg med elektroniske penger vil selgeren sitte igjen med elektroniske kontanter som han ønsker å realisere. Hvis selgeren hadde sittet med Mondex-kontanter kunne kontantene vært benyttet for videre kjøp og salg. Hvis selgeren sitter med Proton-kontanter *må* han løse dem inn. Innløsning kan skje så ofte selgeren ønsker. Innløsning for Proton kan gjøres i en batch-jobb mot selgers bank. Pengene godskrives selgers konto.

8.7 "Hyggelig-meldingsfasen"

Etter at spillet er gjennomført sender tilbyderen en melding hvor han inviterer spilleren til å overvære et hesteveddeløp på nærmeste travbane. Tilbyderen navngir banen fordi han besitter informasjon om hvor spilleren befinner seg i øyeblikket. Teknologiene som gjør denne tjenesten mulig er beskrevet i avsnitt 3.1.6

Implementasjon av "posisjonsavsløring" må være en tjeneste i mobilnettet, det vil si en tjeneste som tilbys av mobiloperatørene. Fra et personvernsynspunkt er det ikke vanskelig å se betenkelige sider ved en slik tjeneste, og det er ikke utenkelig at en implementasjon av tjenesten vil måtte omfatte en prosedyre hvor brukeren aktivt godtar at tjenesteleverandøren får innhente denne opplysningen.[53]

8.8 Oppsummering

Dette kapittelet har diskutert problemstillinger rundt gjennomføringen av tjenestene i scenariet. Diskusjonene har tatt utgangspunkt i scenariet, betalingsmodellene og teknologiene som er beskrevet tidligere i denne oppgaven.

[53] Jeg foretar ingen vurdering av gjeldende lovverk om det er nødvendig eller tilstrekkelig med brukerens aksept for å tilby denne tjenesten.

Det ble avdekket seks faser i scenariet, og kapittelet ble organisert etter disse fasene: Påfyll-, spill-, delresultat-, utbetaling-, innløsning- og ”hyggelig meldings”-fasen. Fire av fasene omhandlet betaling (påfyll, spill, utbetaling og innløsning).

I påfyllfasen ble sikkerheten for banken og for brukeren i betalingssammenheng tatt opp. Særlig signering er et problem. Hvordan kan brukeren være sikker på hva han egentlig signerer? WAP vil tilby biblioteksfunksjoner for signering, og mobilprodusentene må implementere dialogen slik at det er tydelig for brukeren at han er i en virkelig signeringssituasjon.

I spillefasen ble det blant annet vurdert om det er mulig å delta i spill uten et etablert kundeforhold på forhånd. To problemer må i så fall løses: Autentiseringsproblemet og problemet med å få tak i brukerens kontonummer for utbetaling av eventuell gevinst. Det ble argumentert for at autentiseringsproblemet kan løses med signering av meldinger, mens bankkontoproblemet må håndteres i brukerdialogen med tjenesten. Det ble også konstatert at spillet (og særlig betalingstjenestene) er helt avhengig av sikkerheten som smartkort tilbyr.

I delresutatfasen ble det blant annet argumentert for at med dagens teknologi kan animering av hesteløpet ved tegnsymboler være et realistisk alternativ til video-visning.

I utbetalingsfasen ble det konstatert at utbetaling til bankkonto *må* håndteres, og det ble argumentert for at utbetaling til den elektroniske lommeboken i mobiltelefonen antakelig ikke er en god idé.

De andre fasene ble bare kort nevnt. I ”hyggelig-meldingsfasen” ble det stilt spørsmålstegn ved lovligheten av å kunne lokalisere, eller avsløre posisjonen, til brukeren av en mobiltelefon.

9 Demonstrator

I dette kapittelet implementeres relevante deler av mobiltelefonspillet i en *demonstrator*. Demonstratoren implementerer interessante deler av *brukergrense-snittet* og noen av bakgrunnsprosessene. Nødvendige handlinger og infrastruktur hos spilltilbyderen beskrives for de relevante fasene i spillet, men fordi viktige teknologiske byggesteiner ikke er tilgjengelige (som smartkortapplikasjoner og WAP-funksjonalitet) forsøkes det ikke å spesifisere grensesnitt eller datastrukturer. Slike detaljer er heller ikke interessante i denne sammenhengen.

Visualisering av spillet implementeres ved hjelp av tegnbasert animering av hestene; en teknologi som kan realiseres ved hjelp av WAP i dag. Det argumenteres for hvorfor animasjon kan være en ”attraktiv” visualiseringsform. Videre utføres det empiriske studier av båndbredden i dagens mobilnett for å bekrefte at båndbredden er tilstrekkelig for animasjon.

9.1 Demonstrator på WAP-plattform

Som nevnt i kapittel 1 er formålet med min implementasjon av mobiltelefonspillet å visualisere handlinger som er knyttet til spill og betaling i scenariet. Det er flere grunner til at det ikke implementeres en full versjon av spillet. En viktig grunn er at en full implementasjon vil være et særdeles omfattende arbeid, og vil ligge langt utenfor rammene av en hovedoppgave. En annen og like viktig grunn er at byggeklossene som kan realisere spillet ikke finnes ennå; det pågår fortsatt arbeid med spesifikasjoner. Mobiltelefon mangler fremdeles muligheten til å kunne fungere som en integrert nettleser og smartkortleser, og det er spesielt aksess til smartkort-applikasjoner i mobiltelefonen som gjør det umulig å realisere spillet i dag (i det minste med de teknologiene som denne oppgaven ønsker å benytte). Det er også klart at spilltilbyderen ikke kan implementere slik smartkortfunksjonalitet selv. Han er helt avhengig av at teknologileverandører gjør teknologiene tilgjengelig og legger premissene for bruk.

Spillet tenkes implementert på en *mobil enhet* (som i denne oppgaven er kalt *mobil-telefon* for enkelthets skyld). Det er i utgangspunktet kun to teknologier som har potensiale til å realisere spillscenariet på tradisjonelle mobiltelefoner i dag og i nær fremtid: WAP og SIM-Toolkit (beskrevet henholdsvis i avsnitt 3.4 og 5.4.2).

Som beskrevet i avsnitt 5.4.2 har SIM-Toolkit en smartkortfokusert tilnærming til applikasjoner i mobiltelefonen. Skal spillet realiseres med SIM-Toolkit må spillerens mobiloperatør ha lagt spilleapplikasjonen på telefonens SIM-kort ved utstedelse av kortet, eller applikasjonen må lastes ned til SIM-kortet og installeres etter at kortet er tatt i bruk. Applikasjonen vil eies (eller i det minste kontrolleres og godkjennes) av mobiloperatøren.

Terskelen for å utvikle SIM-Toolkit-applikasjoner vil være svært høy i forhold til WML/ WML-Script i WAP da det vil kreve inngående kunnskaper om programmering av smartkort. Begrenset minne i smartkort er en utfordring, og selv protokollen for utveksling av data mellom tilbyderens server og SIM-Toolkit-applikasjonen vil måtte defineres av tilbyderen. Funksjoner som kryptering og signering kan ivaretas av funksjonalitet i SIM-Toolkit, men vil egentlig ikke være godt nok da det bare vil gjelde mellom applikasjonen og mobiloperatørens kortmeldingssenter (SMSC). Av ovenstående grunner blir implementasjon i SIM-Toolkit tungvint, og løsningen blir halvproprietær, men det synes å være mulig hvis man kompletterer den innebygde sikkerheten (dvs. komplettere [GSM03.48]).

WAP-teknologien har de byggesteiner som er nødvendig, selv om ikke alle er implementert ennå; spesielt smartkortfunksjonalitet og ende-til-ende-kryptering i nettverket finnes bare som spesifikasjoner i dag (funksjonalitet i [WTLS]). WAP-modellen har også fordel av å være nettverkssentrisk og bygge på Internett-teknologi som ligner HTTP og HTML. Det gjør det enkelt å utvikle applikasjoner og tjenester for WAP. Det har derfor vært naturlig å la demonstratoren bygge på og demonstrere muligheter med WAP-teknologi.

Figur 26. Spillet på mobiltelefon med WAP-funksjonalitet. Her: Brukeren kobler seg opp til (en tenkt) utsteder av elektroniske kontanter i påfyllfasen av scenariet.

9.1.1 WAP-Toolkit

Verktøy fra Nokia er benyttet for å visualisere demonstratoren på en PC. Nokia WAP-Toolkit [NWT] simulerer selve mobiltelefonen, slik den er vist i Figur 26. WAP-gateway er også levert av Nokia og har som oppgave å oversette WAP-protokollene til Internettprotokoller (se beskrivelsen av WAP i avsnitt 3.4; WAP-gateway er betegnet WAP-proxy i Figur 9 på side 22). WAP-gateway er installert på samme maskin for å gjøre det enkelt, men den kan installeres på vilkårlig maskin.

Nokia WAP-Toolkit forenkler arbeidet med utvikling av WML og WML-script-applikasjoner for WAP ved å gi muligheter for hurtig og kontrollert testing. Ved utprøving på en virkelig WAP-telefon er det bare PC-simulatoren som byttes ut. En virkelig WAP-telefon kan benytte den samme gateway som simulatoren, eller en WAP-gateway på en vilkårlig maskin på Internett. Det er imidlertid naturlig å se på WAP-gateway som funksjonalitet i mobilnettet og da heller benytte mobiloperatørenes gatewaytjeneste med virkelige WAP-telefoner.

WML-filene og programmene som utgjør demonstratoren i denne oppgaven er lagt til en standard webserver, i dette tilfellet webserveren til Norsk Regnesentral (www.nr.no).

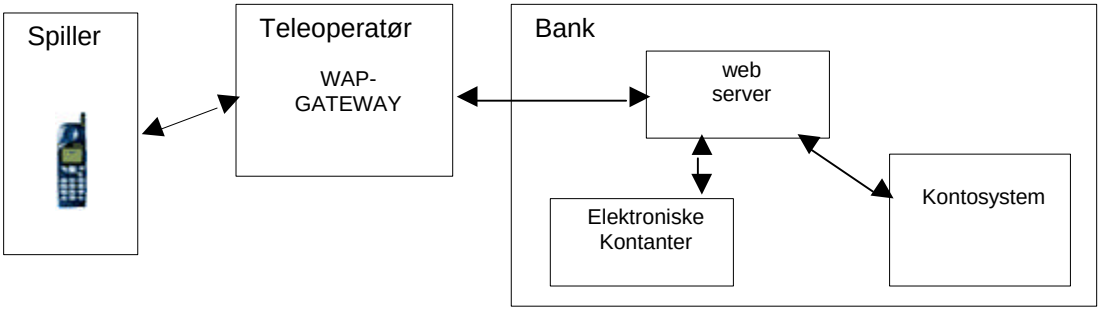
Mobiltelefondemonstratoren illustrerer ett brukergrensesnitt på en type telefon. Da WAP ikke er detaljstyrende for enhetenes utseende, vil brukergrensesnittet kunne se anderledes ut på andre enheter. På samme måte som en nettleser på Internett må mobiltelefonen imidlertid tilby et minimum av funksjonalitet for manøvrering og input. Demonstratoren i dette eksempelet tilbyr to kontekstavhengige taster i underkant av skjermen, én på venstre og én på høyre side. Tastefunksjonaliteten indikeres av ledetekster på skjermen. WML-språket tilbyr eksplisitt programmering av tekstene for de enhetene som støtter denne muligheten. For enheter som ikke støtter ledetekster må brukerdialogen utformes på annen måte enn det som vises i figurene i dette kapittelet.

9.2 Påfyllfasen

I denne fasen fyller brukeren opp sin mobile lommebok. Det er i dag sannsynlig at BBS og bankene vil gå for Proton småpengeløsning [BBSP]. Påfyll, eller lasting, av kontanter antas derfor være en handling hvor kun brukeren og hans bank er aktører. Etter påfyll vil den mobile lommeboken kunne benyttes som et generelt betalingsinstrument i handel over Internett; spillescenariet er bare ett av mange scenarier hvor betaling via en mobil lommebok vil bli mulig. Merk at påfyll ikke er aktuelt for *debet* betalingsløsninger.

Bankens WAP-tjeneste tilbyr kunden kontohold fra mobiltelefonen. Foruten vanlige funksjoner som saldo og overføring mellom konti tilbyr banken kjøp av elektroniske kontanter. Påfyllfasen forutsetter følgende infrastruktur på tilbydersiden, det vil si banken (se Figur 27):

- Operativ webtjener for å betjene kunden.
- Rutiner for autentisering, konfidensialitet og sporbarhet.
- Kommunikasjon med bankens kontosystem.
- Banktjeneste for utstedelse av elektroniske kontanter.
- Sikker kommunikasjon, herunder meldingsbekreftelse (signering) fra avsender, med elektronisk-lommebok-applikasjonen i kundens WAP-telefon ved overføring av elektroniske kontanter.



Figur 27. Infrastruktur i påfyllfasen.

Påfyllfasen forutsetter bruk av WAPs programmeringsgrensesnitt (API) for WML/ WML-Script slik at det er mulig å få aksess til smartkortfunksjonaliteten i

mobiltelefonen. I påfyllfasen må bankens småpengeapplikasjon eksistere i et smartkort i mobiltelefonen.

I avsnitt 7.7 ble det argumentert for at automatisk påfyll av brukerens mobile lommebok ikke var noen god ide. Påfyll av lommebok må gjøres med brukerens aktive medvirkning. I det følgende presenteres stegene i påfyllfasen slik det også er vist i demonstratoren (i figur Figur 28):

1. Brukeren (spilleren) kobler seg opp til utstederens webtjeneste for overføring av elektroniske kontanter. Det forutsettes at kommunikasjonen i denne tjenesten vil være ende-til-ende-kryptert med småpengeapplikasjonens sikkerhetsmekanismer i tillegg til standard WTLS sikkerhetssprotokoller i WAP (se avsnitt 3.4.1). Det forutsettes også at brukerens medvirkning til å sette opp sikker kommunikasjon ved hjelp av WTLS blir transparent på samme måte som med tilsvarende protokoll (SSL/TSL) på Internett.
2. Brukeren går i interaksjon med betalingsapplikasjonen. Avsnitt 8.2 beskrev problemstillinger knyttet til påfyllfasen, spesielt bankens behov for sikkerhet, og at brukerens bør bekymre seg for hva han egentlig signerer. Banken er ansvarlig for betalingsapplikasjonen som lastes ned i mobiltelefonen. Det antas her at applikasjonen vil være skrevet i WML/WML-Script, og at den vil kommunisere med småpengeapplikasjonen i mobiltelefonens smartkort gjennom et standard WML-Script-API. Brukeren må i denne fasen stole på at banken håndterer transaksjonene sikkert og riktig. Proton eller Mondex småpengeapplikasjonene er begge knyttet til en konto. Brukerens input begrenser seg derfor til å angi beløp og bekrefte med PIN-kode. På grunn av myndighetenes begrensninger på beløpsstørrelser må det også kunne settes et tak på overføringen.
3. Brukeren bekrefter beløpet med sin private PIN-kode, som ”låser opp” for signeringsnøkkelen som signerer meldingen (se avsnitt 2.3). Eksakt hva som skjer i denne fasen er opp til bankapplikasjonen i telefonens smartkort. Applikasjoner i *SIM-Toolkit* har for eksempel mulighet til å ”overta” tastatur og skjerm på mobiltelefonen slik at PIN ikke blir eksponert utenfor SIM-Toolkit.[54] I WAP vil aktivering av applikasjoner i smartkort skje ved kall på en WML-Script-biblioteksfunksjon. Håndtering av en smartkortleser vil skje i biblioteket, og PIN vil derfor aldri kunne tilkomme WML eller WML-Script. Som beskrevet i avsnitt 8.2.2 har brukeren ikke mulighet til egentlig å vite hva han signerer i denne operasjonen. Brukeren er imidlertid nødt til å stole på noen, og applikasjonene i mobiltelefonens smartkort må forventes å være sikre. WAP-applikasjoner som lastes ned over Internett har han ingen grunn til å stole på. Signering av meldingen vil samtidig autentisere brukeren overfor banken.
4. Den signerte meldingen sendes til banken som debiterer kundens konto og overfører elektroniske kontanter tilbake til smartkortapplikasjonen i mobiltelefonen. De elektroniske midlene blir umiddelbart disponible etter nedlasting.

[54] SIM-kommandoene DISPLAY_TEXT og GET_TEXT [GSM11.14] instruerer kortleseren i mobiltelefonen om å fremvise tekst og returnere input fra tastaturet.

9.2.1 Påfyll implementert i demonstratoren

Demonstratoren visualiserer hvordan brukerdialogen for påfyll kan kunne se ut på en WAP-telefon. Da smartkortaksess ikke kan simuleres i demonstratorverktøyet vises kun brukergrensesnittet slik det vil arte seg for bankkunden. Figur 28 viser resultatet av denne fasen implementert i WML. Alle skjermbildene som utgjør dialogen kan overføres i en transmisjon. Brukerdialogen manøvrerer mellom de forskjellige skjermbildene som alle er lastet ned samtidig og ligger lokalt i mobiltelefonen.

Figur 28. Dialogen i påfyllfasen i modellen for elektroniske kontanter.

9.3 Spillefasen

I spillefasen besøker brukeren tilbyderens WAP-tjeneste, fyller ut og sender over spillet (bong), betaling, identifikasjon og gevinstkontonummer til tilbyderen. Elementene i det virkelige spillet er vist i Figur 28. I denne fasen forutsettes det ikke at tilbyderen besitter kunnskaper om kunden, det vil si at det ikke er nødvendig med et kundeforhold mellom brukeren og tilbyderen før deltagelse i spillet.

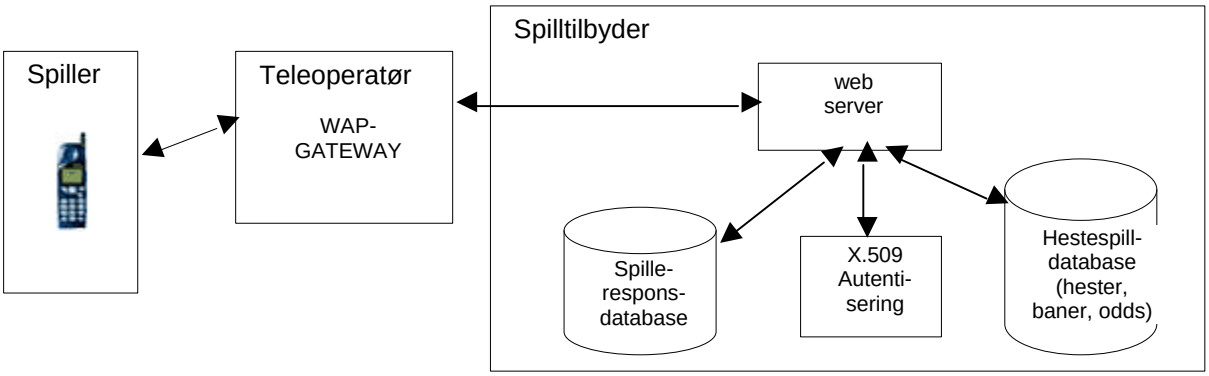
Tilbyder må ha infrastruktur for tjenestene han ønsker å tilby. Her forutsetter spillet følgende:

? Operativ webtjener for spillet.
? Oppdatert informasjon om spillet (baneinformasjon, deltagende hester, odds og eventuelt annen informasjon).

? Infrastruktur for identifikasjon av spiller.
? Infrastruktur for å håndtere spillerespons, lagring og sikring av denne.
? Håndtering av ulike betalingsmodeller avhengig av innsatsens størrelse.

Spillerens mobiltelefon må på sin side være utstyrt med smartkort med småpenge-applikasjon, debetapplikasjon og identitetsapplikasjon.

Spillet lastes fra tilbyderens webserver. Informasjonen om baner, hester, odds og så videre er dynamisk. Tilbyderen må derfor lese denne informasjonen fra en oppdatert database som vist i Figur 29. En server-applet eller et cgi-bin-skript på tilbyderens webserver presenterer spillet på spillerens mobiltelefon. På grunn av de lange latenstidene i mobilnettet (se avsnitt 9.4.1) er det viktig at kommunikasjonen mellom tilbyder og spiller involverer så få transmisjoner som overhode mulig. I WAP brukes WML-språket til å forsøke å overkomme mobilnettets begrensninger ved å overføre flere logiske web-sider i samme transmisjon og ved å gjøre bruk av WML-Script til å utføre lokale beregninger (se avsnitt 3.4). Denne funksjonaliteten må utnyttes fullt ut.



Figur 29. Infrastruktur i spillefasen.

Når spillet lastes ned i mobiltelefonen bør det lastes så mye av dialogen i WML og WML-Script at spillet kan fullføres i én transaksjon. Kompleksiteten rundt implementasjon av utfylling av bong over WAP er å sammenligne med tilsvarende utfylling over HTTP. Pris for bong er avhengig av antall markerte hester og innsatsen. Totalprisen kan presenteres for spilleren ved hjelp av WML-Script ved at utregningen skjer lokalt i mobiltelefonen. Alle variable (antall markeringer, pris per rekke) suppleres av brukeren. Verifisering av input og utregning av totalpris kan derfor skje lokalt ved hjelp av WML-Script. I WML-Script kan det programmeres slik at programkode utføres på brukerens input før aktivering av nye skjermbilder i dialogen med brukeren.

I det følgende skisseres en mulig algoritme for eksekvering i mobiltelefonen. Det forutsettes at WML/WML-Script lastes ned i telefonen fra tilbyderens webserver:

1. Dialogen avbrytes eller det gis en feilmelding hvis det ved hjelp av WML-Script ikke kan fastslås om mobiltelefonen støtter elektronisk betaling eller signering. Disse funksjonene ansees som kritiske for tjenesten.
2. Brukerdialogen fører brukeren gjennom utfylling av bong, og kan regne ut pris lokalt i telefonen.
3. Tilbyderen trenger bankkontonummer for utbetaling av eventuell gevinst. Fra WML-Script forsøkes det å snappe opp kontonummer fra debet-applikasjonen

eller fra småpengeapplikasjonen. (Det vil sannsynligvis være mislykket; se avsnitt 8.3.1) Hvis dette ikke lykkes, vil det i WML eksplisitt bli spurt etter kontonummer. All prosessering i dette punktet kan foregå lokalt.

4. Betaling for spillet skjer ved at den lokale betalingsapplikasjonen i telefonens smartkort aktiveres fra WML-Script. Brukergrensesnittet og handlingene ved betaling vil være bestemt av betalingsapplikasjonen. Brukeren bekrefter (signerer) beløpet. På dette tidspunktet er det viktig at brukeren vet hva han bekrefter; se diskusjonen i avsnitt 8.2.2. Resultatet av betalingshandlingen vil være en signert melding som inneholder elektroniske kontanter. I WML-Script vil dette sannsynligvis bli implementert med at meldingen skrives inn i en variabel som kan håndteres i WML.[55] I begge småpengapplikasjonene som er diskutert i avsnitt 7.7 (Mondex og Proton), overføres elektroniske kontanter kun mellom smartkort. WML-koden får således rollen som ”transportør” av kontantene mellom tilbyderens smartkort og smartkortet i mobiltelefonen.
5. Utfylt bong vil representeres i nok en variabel, og det ble argumentert (blant annet) i avsnitt 8.3.5 at tilbyderen bør få spilleren til å signere bong og kontonummer. Dette kan gjøres i én operasjon med brukerens egen identitets-applikasjon og vil avkreve brukeren nok en PIN-bekreftelse. WML-Script vil kalle funksjonen Crypto.signText for signering (se avsnitt 5.4.3). Brukerens sertifikat vil typisk følge med i den signerte meldingen, hvilket gjør det enkelt for tilbyderen å verifisere hans identitet.
6. Meldingen sendes til tilbyderens webserver. All prosessering har til nå vært gjort lokalt i mobiltelefonen. Det er (i prinsippet) to signerte meldinger som over-sendes tilbyderen: elektroniske kontanter og bong pluss kontonummer.[56]

Tilbyderen har nå all den informasjon som han trenger for å la spilleren delta i spillet. Tilbyderens naturlige behandling av meldingene bør være følgende: (Tilbyderens handlinger kan relateres til Figur 29).

1. Lagring av meldingene. Persistent lagring av elektroniske kontanter forutsettes å være en del av småpengeløsningens protokoll; det ligger utenfor tilbyderens kontroll. Bong kan imidlertid gå tapt hvis tilbyderens webtjeneste ”går ned” etter at meldingen er mottatt, men før den er persistent lagret.
2. Sjekking av identiteter. Særlig viktig er det å fastslå de digitale kontantenes ekthet. Denne jobben trenger ikke tilbyderen bry seg med; det vil være en del av småpengeløsningens protokoll. Sjekking av spillerens identitet vil imidlertid tilbyderen måtte gjøre. Det til være en lokal operasjon da hans sertifikat følger med ved den signerte bongen. Det vil være naturlig at partene i scenariet følger X.509 PKI (se avsnitt 2.4).
3. Oppdatering av oddsdatabasen (se Figur 29). Oddsen endrer seg helt frem til løpsstart og er avhengig av størrelsen på innsatsen og hestene det er satset på.
4. Spilleren gis kvittering. Det må være et referansenummer som identifiserer bong og betaling ved eventuell reklamasjon.

[55] Dette er en mulig implementasjon. Den er imidlertid er bygget antagelser som ikke har latt seg bekrefte (ingen jobber med dette i Norge). Det er mulig at kommunikasjonen vil bli implementert på annen måte.

[56] Merk at betalingskommunikasjonen trolig må foregå adskilt fra annen kommunikasjon for å oppnå god nok sikkerhet, og at det derfor er sannsynlig at kompleksiteten er større enn skissert her.

Figur 30. Spillefasen implementert i WML. Initiering av spillet.

Figur 31. Spillevalg i første løp i dagens dobbel

Figur 32. Spilleren angir innsats

Figur 33. Sending av bong som siste del av brukerdialogen i spillefasen

Det er ellers verd å merke seg at tilbyderen ikke har behov for å lagre informasjon om spilleren mellom spill. Hver gang spilleren ønsker å spille vil alle data overføres til tilbyderen på nytt.

9.3.1 Implementasjon av spillefasen i demonstratoren

Demonstratoren er bygd over infrastrukturen i spillefasen slik den er vist i Figur 29. I det virkelige spillet må dynamisk informasjon om veddeløpsbaner, hester, og spesielt odds hentes fra en løpende oppdatert database. Oddsen vil endre seg dynamisk frem til løpsstart, og vil være avhengig av beløpene som satses på hestene. I demonstratoren har det ingen hensikt å implementere denne dynamikken da det gir lite eller intet med hensyn til formålet til demonstratoren, nemlig å visualisere handlinger som er knyttet til spill og betaling. I demonstratoren implementeres derfor databasen som en statisk fil, slik at det blir statiske websider som sendes til WAP-telefonen. WML og WML-Script-koden som oversendes inneholder imidlertid nok informasjon til å simulere brukergrensesnittet nøyaktig slik det vil oppleves i en virkelig spillesituasjon. Figur 30 til og med Figur 33 viser demonstratoren i spillefasen fra initiering av spillet til betaling og sending av bong. webserveren lagrer spillerresponsen i sin ”database”; i demonstratoren forenkles det til å opprette en fil med linjer inneholdende bong, betaling og kontonummer. Det gjøres ikke noe forsøk på å identifisere spilleren da signeringsmekanismene mangler i demonstratoren. Spillerresponsen brukes siden til å informere spilleren om utfallet av spillet.

9.4 Delresultatfasen ved hjelp av animasjon

I delresultatfasen vises hesteløpet på spillerens mobiltelefon. I scenariet har spilleren valgt å få se det siste løpet i Dagens Dobbel, fordi han har vinnersjanser. Problemet i denne fasen er hvordan løpet skal visualiseres for spilleren.

Videovisning av løpet har til hensikt å gi spilleren kontinuerlig visuell informasjon (det vil si informasjon om hestenes innbyrdes posisjoner) underveis i det virkelige hesteløpet. Det visuelle understreker i tillegg spenningsmomentet. Som vi har sett i kapittel 3, er ikke dagens mobilnett egnet for overføring av video på grunn av lav båndbredde. Det er et spørsmål om det er mulig å gjenskape det samme informasjonsinnholdet og den samme spenningen uten bruk av video. Det er interessant å undersøke om animasjon av løpet med dagens teknologi, det vil si med alfanumeriske tegnkarakterer og/eller enkle bitmaps, kan klare dette. Det er flere fordeler med animasjon av hesteløpet i forhold til video:

- Animasjon stiller beskjedne krav til nettverkets båndbredde; det vil trolig virke med dagens båndbredde.
- Animasjon krever ikke grafiske muligheter på mobiltelefon. Dagens alfanumeriske egenskaper eller enkle bitmaps i WAP-telefoner er tilstrekkelig.
- Animasjon kan faktisk være å foretrekke fordi det kan være vanskelig å skille hestene fra hverandre på små skjermer med videovisning.

GPRS-nettet vil etterhvert tilby båndbredde som tilfredsstiller båndbreddebehovene for video, men animasjon er likevel interessant fordi det kan kjøres på billige terminaler/mobiltelefoner som ikke har videomuligheter. I tillegg kan animasjon

visualiseres på SIM-Toolkit-telefoner som ikke er tilpasset for WAP. Transmisjonskostnadene kan trolig også vise seg å være rimeligere enn for video, på grunn av de beskjedne båndbreddebehovene.

For å undersøke om animasjon er en god idé er det nødvendig å studere den faktiske overføringshastigheten i dagens GSM-nett for å se om denne er tilfredsstillende. I tillegg er det nødvendig å se på visualiseringen av animasjonen; visualiseringen må ikke ligge langt tilbake for det man får til med video. Begge disse faktorene er kritiske med hensyn til suksessfull implementasjon av animasjon. Faktorene diskuteres nedenfor.

9.4.1 Empirisk studie av oppfriskningsraten i dagens mobilnett

Animering stiller minstekrav til *oppfriskningsrate* av mobiltelefonens skjerm. En WAP-telefon som Nokia 7110 har for eksempel 4 linjer á 20 tegn[57]. Maksimalt 80 tegn må altså overføres kontinuerlig (eller med korte intervaller) og fremvises på skjermen. Dagens GSM-nett har en overføringshastighet på 9600 bits/sek som gir en teoretisk oppfriskningsrate på rundt 10 skjermbilder i sekundet. Dette tallet er naturligvis alt for høyt. Det er mange faktorer som begrenser oppfriskningsraten. Ved siden av nettets båndbredde vil operativsystemer, kommunikasjonsform (”push” eller ”pull”), nettverksprotokoller, prosessorhastigheter, skjermenes egenskaper med mere være begrensende faktorer.

For å undersøke den reelle overføringshastigheten har jeg undersøkt tiden på overføringer av forskjellige pakkestørrelser for forskjellige protokoller. Undersøkelsen er gjennomført på de trådløse plattformene WAP, GSM-data og SMS for å kunne sammenligne effektiviteten på disse plattformene, som alle er tuftet på en bæretjeneste på 9600 bits/sek.

Forskjellige pakkestørrelser er undersøkt for å se om det påvirker oppfriskningraten. Målingene er foretatt flere ganger for hver kombinasjon av protokoll og pakkestørrelse. Gjennomsnittet presenteres for hver kombinasjon. Alle testene er foretatt på samme tidspunkt flere påfølgende dager for å forsøke å nøytralisere eventuelle trafikale variasjoner.

SMS

Som beskrevet i avsnitt 3.4 definerer ikke WAP-standardene bæretjenester, men utnytter de bærerne som finnes. I praksis er det bæretjenestene SMS eller GSM-data som kan være aktuelle for WAP. Av tabellen nedenfor fremkommer hvorfor WAP ikke er implementert over SMS. SMS har uforholdsmessig lang latenstid.

SMS ble testet ved å overføre forskjellige blokkstørrelser fra mobiltelefonen tilbake til den samme mobiltelefonen. Testen ble gjennomført på en mobiltelefon av typen Ericsson GF 388. Telefonens innebygde grensesnitt ble benyttet for sending og mottak av meldinger. Da SMS bare tillater opp til 160 tegn begrenset testen seg til to

[57] Avhengig av modus. Spesifikasjonene vil variere mellom mobile enheter, men en oppløsning på 4x20 tegnposisjoner antas tilstrekkelig for animering i eksempelet med hesteløp.

forskjellige blokkstørrelser. Tiden ble startet ved sending og stoppet ved mottak for én og én melding. For å ta høyde for eventuelle belastninger i nettet og gjøre målingene mest mulig sammenlignbare, ble korte meldinger og lange meldinger sendt annen hver gang. Pakkene ble sendt med ett minutts mellomrom på et tidspunkt på dagen (en ukedag fra kl. 14) hvor det antas "normal" belastning i GSM-nettet. Prosedyren ble gjentatt 10 ganger. Tabellen nedenfor gjengir målingene i sekunder for 1 og 160 bytes meldinger.

SMS 1 Byte	14	15	15	14	12	13	7	16	8	14	Snitt 12.8
SMS 160 Bytes	15	19	16	18	18	20	18	15	15	18	Snitt 17.2

Tabell 2. SMS-meldinger. Rundtur målt i sekunder.

Målingene av SMS-meldinger viser i dette eksempelet at en rundtur kan ta fra 7 til 20 sekunder. Korte meldinger viser også en tendens til å ha mindre latenstid enn større meldinger.

TCP/IP over GSM-data

GSM-data er bæretjeneste for dagens WAP-protokoller, og målinger av TCP/IP over GSM-data bør derfor gi en god idé om egenskapene i WAP. Målinger av TCP/IP over GSM-data er også enklere å gjennomføre da de kan utføres på en vanlig PC. Testen av TCP/IP over GSM-data ble foretatt på en middels rask stasjonær PC tilkoblet mobiltelefon til GSM-nettet.[58] GSM-telefonen brukte oppringt samband til en isdn-aksessrouter i lokalnettet til Norsk Regnesentral. Det ble testet mot aksessrouteren og mot maskiner i NRs lokalnett. Som vi skal se, ble programmene ping og ftp testet for se på "best-case"-tilfeller av latenstider og båndbredde, og HTTP-protokollen ble benyttet på grunn av likheten til WAP (det vil si WSP).

PING og FTP

Programmet *ping* ble benyttet for å se på "best case" oppfriskningrate som en kan forvente. Ping benytter ikke IP, men en egen kontroll-protokoll (ICMP). Ping ble brukt til å teste rundturen fra PC'en til aksessrouteren og tilbake til PC'en. Målingene ble kjørt 10 ganger for én-bytes meldinger og presenteres i sekunder i tabellen nedenfor. Resultatene er rapportert av programmet.

PING 1 Byte	0.66	0.66	0.67	0.67	0.70	0.69	0.65	0.66	0.67	0.66	Snitt 0.67

Tabell 3. Ping over GSM. Rundtur målt i sekunder.

Som det fremgår viser målingene et snitt på godt under ett sekund på rundturen til aksessrouteren. Det vil med andre ord uansett ikke være mulig å få til en oppfriskningsrate på mer enn én til to bilder i sekundet over GSM-data med såkalt pull-metode (hvor klienten ber om hver ny side). Som ventet er latenstidene med GSM-data bare en brøkdel av latenstidene med SMS.

Programmet *ftp* ble brukt til testing av "best case" båndbredde. Ifølge GSM-spesifikasjonene har GSM-data båndbredde på 9600 bits/sek. For å teste den

[58] 233MHz Windows NT tilkoblet Ericsson GF388

praktiske båndbredden ble tiden målt på overføring av en større fil ved hjelp av fil-overføringsprotokollen FTP. Denne testen var kun ment som en indikator på forventet båndbredde i GSM-nettet, og derfor ble ikke testen kjørt flere ganger. Målingen presenteres nedenfor.

FTP 101541 bytes	108 sek.	7520 bits/sek.

Tabell 4. FTP. Effektiv båndbredde i GSM ved overføring av en stor fil.

Overføringen viser i dette tilfellet en effektiv båndbredde på 7520 bits/sek., hvilket synes å være bra. Målingene viser riktignok ikke 9600 bits/sek., men det er ikke noe poeng å jakte på de forsvunnede bit'ene i denne sammenheng. Det interessante med testen er at den gir et tall på båndbredden i GSM-nettet, som garantert er mulig.

HTTP

For å gjøre sammenligningen med WAP så lik som mulig ble protokollen HTTP valgt for dataoverføring over TCP/IP. HTTP tilsvarer protokollen WSP i WAP (se avsnitt 3.4.1). Det var også nødvendig å velge en overføringsmetode som aktivt vil hente ned nye sider fra webserveren (pull-metode). Pull-metoden vil kreve en rundtur til serveren for hvert nytt skjermbilde, men per i dag kan det ikke program-meres på annen måte i WAP. (Push-metoden, hvor serveren sender kontinuerlig, er ferdig spesifisert, men ikke implementert i WAP-enheter ennå [WAPP]).

Testen ble utført ved at websider av gitte størrelser ble lastet 30 ganger, før tiden ble notert. HTML-sidene som ble lastet hadde et lite program i JavaScript, som førte til at nedlasting av nye sider umiddelbart ble aktivert. Det var visning av én linje tekst til skjerm under denne testen, men altså ingen ventetid før ny nedlasting ble aktivert. En pakkestørrelse på 160 bytes (HTML-kode) vise seg å være tilnærmet minste praktiske pakkestørrelse på grunn av syntaks-kravene i HTML. Større pakker ble generert ved å inkludere tekst mellom HTMLs kommentar-tagger. Merk at det ikke er samsvar i antall sendte byte og antall mottatte bytes. Kommandoen GET i HTTP som vil igangsette selve nedlastingen av websiden vil inneholde konstant antall bytes (URL-adressen). Resultatet av målingene er vist nedenfor:

HTTP	160 bytes	500 bytes	1000 bytes	2000 bytes	5000 bytes
30 pakker	48 sek.	59 sek.	73 sek.	132 sek.	225 sek.
Sek./pakke	1.6 sek.	2.0 sek.	2.4 sek.	4.4 sek.	7.5 sek.
Pakker/sek. (oppfrisk.rate)	0.65	0.5	0.42	0.23	0.13

Tabell 5. HTTP. Forsinkelse og oppfriskningsrate ved HTTP over GSM

Resultatene viser at rundturen til webserveren tar noe over ett og et halvt sekund for 160 bytes pakker og opp til 7.5 sekunder for 5KB pakker. En interessant observasjon er at tre ganger økning i pakkestørrelse fra 160 bytes til 500 bytes ikke betyr mer enn 1,25 ganger økning i transmisjonstid (fra 1.6 sek. til 2.0 sek). Overføring av 500 bytes vil med HTTP gi en oppfriskningsrate på et halvt bilde i sekundet, hvilket vil være svært akseptabel oppfriskningsrate for visualiseringen.

WAP
Det gjenstår å se om tallene ovenfor harmonerer med de faktiske resultatene ved bruk av WAP. WAP ble testet ved å laste ned binære versjoner av WML-sider av forskjellige størrelser fra webserveren i NRs lokalnett. WAP-enheter kan bare lese kompilert WML (se avsnitt 3.4.1). Hvis ukompilerte WML-sider forsøkes lastet så vil WAP-gatewayen kompilere dem på veien til WAP-enheten. Merk at binær-versjonene kan potensielt inneholde mer informasjon enn tilsvarende HTML-filer. I mine forsøk observerte jeg at koden kunne bli halvert ved kompilering. Ved inspeksjon av de ferdigkompilerte filene fremkommer det at WML-teksten som skal skrives til skjerm, ikke er gjenstand for komprimering (den ligger i klartekst), mens taggene er binært representert.

Testingen av en pakkestørrelse ble gjort ved å starte stoppeklokken når URL sendes fra mobiltelefonen. Denne URL transporterte en fil av gitt størrelse til mobil-telefonen. Idet WML-siden ble lastet ned til telefonen, ble det utført WML-Script som forårsaket umiddelbar nedlasting av en ny WML-side av samme størrelse (ny URL-aksess). Dette ble gjentatt 30 ganger på tilsvarende måte som HTTP ble testet. WAP ble testet med telefonen Nokia 7110. Resultatene presenteres nedenfor.

WAP – WSP	160 bytes	500 bytes	1000 bytes	2000 bytes	5000 bytes
30 pakker	40 sek.	51 sek.	70 sek.	–	–
Sek./pakke	1.3 sek.	1.7 sek.	2.3 sek.	–	–
Pakker/sek. (oppfrisk.rate)	0.77	0.59	0.43	–	–

Tabell 6. WAP. Forsinkelse og oppfriskningrate i WAP.

Som det fremgår av tabellen ovenfor ble det ikke resultater for de største overføringene. Målingene av 2KB og 5KB filer ble avbrutt under lasting. Målingene ble gjentatt med ett sekund venting før ny nedlasting, men igjen ble de store overføringene avbrutt på samme måte. 2KB og 5KB viste heller ikke tekst til skjerm mellom nedlastingene. Problemene med de store overføringene kan skyldes feil i WAP-implementasjonen. Problemene ble ikke forfulgt videre, da jeg hadde gode tall fra de andre målingene.

Resultatene for 160, 500 og 1000 bytes viser sammenlignbare tall med målingen for HTTP. Resultatene viser at WAP faktisk er noe raskere på alle tre pakkestørrelsene. Størst er forskjellen for de minste pakkene. WAP bruker gjennomsnittlig 1.3 sek. på rundturen til serveren mot 1.6 sekunder for HTTP for 160 bytes pakker. De tilsvarende tallene er 1.7 sek. mot 2.0 sek. for 500 bytes pakker.

Tolkning av resultatene
For det første viser resultatene at SMS er helt uegnet som bærer for WAP, i hvert fall slik SMS er implementert i mobiloperatørenenes nett i dag. SMS har også en alvorlig ulempe ved at maksimum pakkestørrelse bare er 160 bytes.

Et annet resultat er at WAP over GSM-data viser seg å være vel så effektivt som HTTP over GSM-data. Ved kommunikasjon med pull-metoden vil en kunne forvente en oppfriskningsrate på 0,77 bilder i sekundet med skjermbilder med begrenset informasjon (160 bytes). Pakker med 160 bytes er nok til å fylle en

skjermside med tekst. Kontinuerlig pull av 160-bytes pakker kan skje med bare 1,3 sekunder mellom oppfriskningene.

I forhold til animasjon av et hesteløp vil ett nytt bilde hvert 1,3 sek, det vil si en oppfriskningrate på 0.75, være mer enn godt nok. Det spørs om ikke ett bilde ca. hvert 3. sekund også ville være godt nok i akkurat dette tilfellet. I andre situasjoner vil imidlertid 1,3 sekunder være helt uakseptabelt.

Tallene i tabellene ovenfor gir også holdepunkter for å kunne si noe om mulighetene for å benytte bitmaps istedenfor tegnbasert animasjon. Ved bruk av pull-metoden kan bitmaps på 500 bytes vises kontinuerlig med 1,7 sekunders forsinkelse. På en WAP-telefon av typen Nokia 7110 vil dette være tilstrekkelig for å overføre sort/hvitt-bitmaps som tilsvarer hele skjermen.

Angående push-metoden: Ovenfor har vi sett på pull-metoden for overføring av data fordi push-metoden ikke har vært tilgjengelig for testing. Ved animasjoner vil det imidlertid være naturlig å benytte push-metoden. Rundturen til serveren for å hente en ny webside eller et nytt bitmap er helt unødvendig. Det naturlige vil være at klienten kun er involvert i initiering og stopping av overføringen. Hvis vi legger til grunn den målte båndbredden for ftp ovenfor, så vil en push-protokoll antakelig kunne overføre omlag 940 bytes kontinuerlig fra server til klienten. Med en bitmapstørrelse på omlag 500 bytes vil det tilsvare to fulle skjermbilder i sekundet på en Nokia 7110.

Figur 34. Nokia 7110. Nokias første WAP-telefon.

I mange tilfeller vil to skjermbilder i sekundet være godt nok til å vise primitiv video. I tilfellet med et hesteløp vil to skjermbilder i sekundet antakelig kunne gi et akseptabelt visuelt inntrykk av spillet. Som vi ser er det vi langt igjen til oppfriskningsraten på 30 bilder i sekundet for fjernsyn.

9.4.2 Animering av hesteløp

Animering ved hjelp av karaktersymboler ble presentert som et alternativ til videovisning i avsnitt 8.4.3 på side 78. I det følgende diskuteres implementasjonen av animeringen og hvordan dette er simulert i demonstratoren.

Det er et hesteløp som skal animeres i dette tilfellet, men problemstillingen er generell: I sanntid skal animasjonen forsøke å etterligne objekters oppførsel i den virkelige verden. Det vil være to kritiske oppgaver: Lokalisering av objektenes posisjon i den virkelige verden, og generering og presentasjon av de syntetiske objektene. Lokalisering og presentasjon diskuteres nedenfor.

Lokalisering av hestenes posisjoner

En klar ulempe ved animasjon i forhold til videovisning er behovet for nøyaktig posisjonsangivelser av hestene under løpet. Tilbyderen trenger et system for å omgjøre hestenes posisjoner til elektronisk informasjon, som kan brukes i

presentasjonen. I sin enkleste form kan en tenke seg *manuell* registrering underveis i løpet. En person må i så fall observere hestene i løpet og foreta registreringer når hestenes innbyrdes posisjoner endrer seg. *Automatisk* registrering kan for eksempel skje ved videotracking og mønstergjenkjenning. Posisjonsbestemmelse ved hjelp av GPS eller mobiltelefonteknologi vil ikke gi tilfredsstillende nøyaktighet.

I det virkelige spillet må tilbyderen løse posisjonsproblemet, men når det er gjort, er det enkelt å presentere resultatene ved hjelp av WAP-teknologi. I demonstratoren visualiseres animasjonen slik det kan bli presentert i et virkelig system. Posisjoneringsproblemet er løst ved å implementere posisjonering som en egen prosess som simulerer et hesteløp. Det er viktig at hesteløpet simuleres slik at det oppleves som et ekte hesteløp. Et dårlig simulert hesteløp vil virke negativt på demonstratorens troverdighet.

Nedenfor skisseres forutsetninger og posisjoneringsalgoritmene som forsøker å etterligne valgene en kusk/jockey må foreta underveis i løpet:

1. Antall hester, odds, startposisjoner og banens lengde (i sekunder) er gitt på forhånd i tilbyderens database.
2. Avstanden fra ledende hest til nummer to i løpet skal aldri være flere enn tre hestelengder. Det skal bevare spenningen.
3. Antall spor settes til 4 (konfigurerbart).
4. Sporbytte er bare tillatt hvis det er en stor nok luke i nabosporet, og hvis hesten har større fart en foranliggende hest. Unntaket er en galopperende hest som vil forflytte seg til ytterste spor (sport 4+1) for ikke å ødelegge for de andre hestene.
5. Sporbytte foretrekkes fra ytre til indre spor (kortere vei rundt banen).
6. Sporbytte foretas bare hvis det forbedrer hestens posisjon, det vil si at det er færre hester i bedre posisjon i nabosporet.
7. Ytre spor gir lengre vei i svingene. Hvert spor har ekstra ”vekt” i svingene.

Implementasjon i tilbyderens webløsning og i demonstratoren

I et virkelig system vil et posisjonssystem ha til hensikt å holde en database over hestene løpende oppdatert om hestenes posisjoner. En WEB/WAP-løsning for visualiseringen av hestenes posisjoner vil hente grunnlagsdata fra databasen og generere et passende format som er egnet for fremvisning. Det vil altså være en klar todeling mellom posisjonering og visualisering i et virkelig system. Visualiseringsprosessen i et virkelig system må også være effektivt implementert og integrert i et websystem på grunn av stor belastning under et hesteløp.

Demonstratoren har ikke de samme kravene til optimal integrasjon for visualiseringsprosessen. I demonstratoren er hestenes posisjoner i tillegg kun simulert. Todelingen mellom posisjonering og visualisering har derfor vært naturlig å implementere innenfor rammene av posisjonseringprosessen alene. Implementasjonen av demonstratoren fungerer slik at aksess til en gitt URL igangsetter simuleringen av hesteløpet. Posisjoneringsprosessen regner så ut hestenes posisjoner *og* utfører samtidig visualiseringen. Resultatet av visualiseringen skrives deretter ut i WML-kode til filer på webserveren. Posisjoneringsprosessen lever videre og genererer nye ”bilder” med korte intervaller. Visualiseringen på mobiltelefonen i demonstratoren skjer ved nedlasting av filene etter tur. WML-koden inneholder selv instruksjoner som identifiserer neste bilde i sekvensen.

Simuleringen er delt opp i et antall diskrete steg som tilsvarer oppfriskningsraten som spillet krever. Den reelle lengden på spillet (i sekunder) er gitt på forhånd, og simuleringsprosessen ”sover” en tidsenhet som er gitt av spillets lengde og oppfriskningsraten mellom hvert diskrete steg. I hvert steg beregnes hestenes nye posisjoner uavhengig av hverandre i henhold til algoritmene ovenfor, og hestenes posisjoner justeres slik at to hester i samme spor ikke kan bytte plass.

Simuleringen gjør ikke forsøk på å legge opp strategier eller taktiske disposisjoner for hestene. Simuleringen mangler derfor vesentlige elementer i forhold til et virkelig løp. Det var naturlig å ikke legge mer i simuleringen enn nødvendig for å illustrere ideen om tegnbasert animering.

Visualisering av animasjonen
Man kan tenke seg flere alternative visualiseringer i nett med begrenset båndbredde:
? ”Radiomodellen”: Tekstlig fremstilling av hesteløpet, det vil si en slags ”sanntids tekst-radio” hvor løpet beskrives med tekst istedenfor lyd.
? Stillbilder som genereres av web-kamera eller fremstilles fra videofilming av løpet. Oppfriskningsraten begrenses av båndbredden i nettet.
? Kunstige stillbilder som konstrueres ut fra posisjoneringssystemet som er beskrevet ovenfor.
? Tegnbasert visning, hvor ett alfanumerisk tegn tilsvarer én hest. Dette krever også et posisjoneringssystem.
? En kombinasjon av stillbilde og tegnbasert visualisering.

Radiomodellen ansees som uaktuell. Da spillet tenkes implementert på en mobiltelefon ville det være mer naturlig om telefonen ble brukt på tradisjonell måte. Spilleren kunne ringe et nummer og få lytte til løpets kommentator.

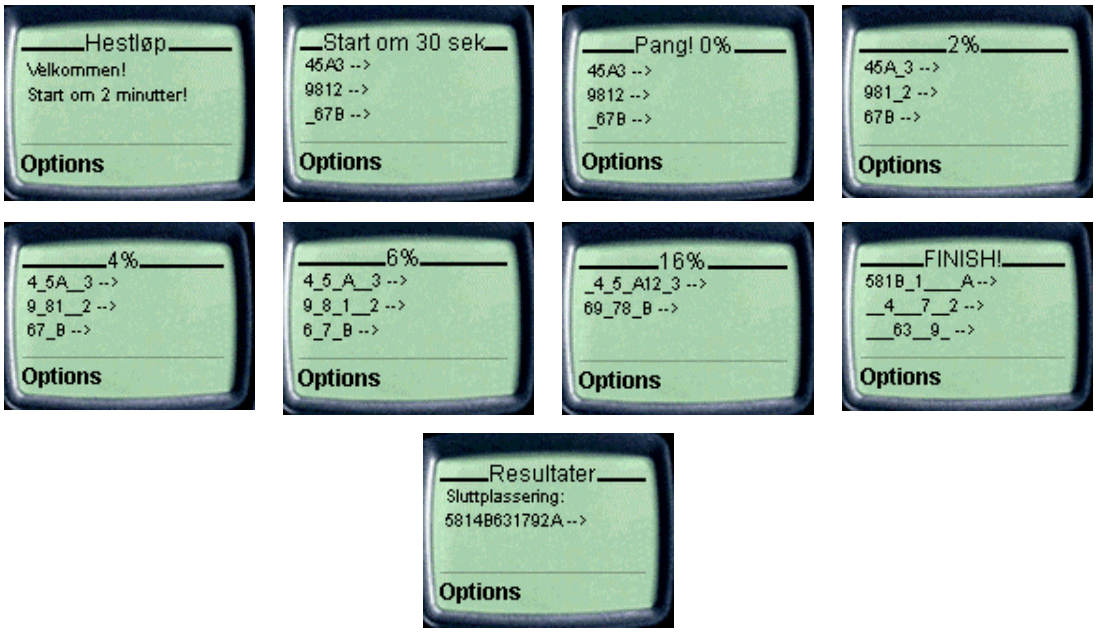
Angående stillbilder: Fra mine empiriske undersøkelser ovenfor ble det vist at sort/hvitt bitmaps ikke er vesentlig mer ressurskrevende å overføre enn tekst. En tekstside vil typisk kreve nedlasting av ca. 160 bytes, og et sort/hvitt-bitmap vil kreve ca. 500 bytes. Ved pull-metoden var det liten forskjell i forsinkelse ved lasting 160 bytes og 500 bytes (1,3 mot 1,7 sek.). I visualiseringen av et hesteløp antas det også å være mer enn tilstrekkelig med forsinkelsen som ble målt for 500 bytes pakker, det vil si ett nytt bilde hvert 1,7 sek. Hvis en antar push-modellen for overføring av data, vil en kunne oppleve en oppfriskningsrate på ca. to bilder i sekundet for denne type bitmaps. Et annet spørsmål er om den lille skjermen kan gjengi et informativt bilde av løpet. På grunn av liten skjerm vil antakelig kunstig genererte stillbilder gi best inntrykk av løpets gang. Ulempen ved den kunstige animerte modellen er igjen at den krever et posisjoneringssystem.

Tegnbasert animasjon har fordel av å være lite kapasitetskrevende og kan ha en høyere oppfriskningsrate enn stillbildemodellene. I sammenligningen ovenfor vil en full tekstskjerm ha ca. en tredjedel av størrelsen til bitmaps, noe som skulle gi ca. 6 skjermbiler i sekundet ved push-modellen. Fordelen med høyere oppfriskningsrate oppveies imidlertid av ulempene med faste karakterposisjoner på skjermen. I eksempelet fra hesteløp vil hestenes relative forflytninger neppe skje så raskt at det vil være noe poeng med hele 6 bilder i sekundet – i hvert fall ikke med tegnbasert

visning. Det *er* imidlertid et poeng at informasjons*innholdet* kan pakkes tettere slik at det er mulig å få et godt bilde av hele hestefeltet under løpet. Ulempene er at tegnbasert animasjon krever et posisjonerings-system, og det kan være visuelt kjedelig. Programmeringsteknisk er den ”kunstige” stillbildemodellen og den tegnbaserte modellen temmelig like, selv om det er noe mer komplisert å generere et bitmap.

Det er i denne oppgaven valgt å implementere tegnbasert visualisering, fordi dette er noe enklere å realisere enn stillbildemodellen og fordi denne modellen har egenskaper som gjør den interessant også som brukergrensesnitt. I denne oppgaven gjøres det imidlertid ikke noe forsøk på å vurdere hvordan spillere opplever tegnbasert visualisering i forhold til de andre visualiseringsmodellene. Problemstillingen er interessant, men det er dessverre ikke rom for å studere brukergrensesnittaspekter i denne oppgaven.

Ved tegnbasert animasjon må inntil 15 hester visualiseres i en 4x20 tegns matrise. Antall rader på skjermen passer bra med antall spor på en travbane, og det er derfor naturlig å velge ”horisontal” visning av løpet hvor én rad tilsvarer ett spor. Det er videre naturlig å velge tall som identifiserer hestenes startnummer til å representere hestene visuelt. Startnumrene 1 til 9 er uproblematisk, og numrene 10 til 15 kan for eksempel visualiseres med bokstavene A til F slik at også startnummer over 10 bare legger beslag på en tegnposisjon på skjermen. En kan også tenke seg at hestene som spilleren har satset på markeres spesielt med utheving, understrek, alternativ farge, eller annet som tilbys i programmeringsspråket. Resultatet av tegnbasert animasjon, slik det er implementert i demonstratoren, er vist i Figur 35.



Figur 35. Tegnbasert animering av hesteløpet.

Kritikk av animasjonen
Visualiseringen av hesteløpet med tegnene 0 til 9 og A til F viste seg å fungere relativt bra. Jeg synes også at spenningen ble godt tatt vare på. Visualiseringen kan leseren bedømme selv (Figur 35). ”Hestene” hadde imidlertid en tendens til å klumpe seg sammen, så noe mer arbeid kunne vært lagt i posisjoneringsprosessen.[59]

Det viste seg også at markering, utheving eller lignende av enkelte tegn på en linje ikke var mulig å få til WML-språket (i det minste i verktøyet fra Nokia). Derfor kunne ikke hestene som spilleren er interessert i markeres spesielt.

Det ble lagt inn en forsinkelse på 3 sekunder mellom hver ny nedlastning av skjermsider. I simulatoren til Nokia ga det glidende overganger slik at nedlasting av et nytt skjermbilde foregikk i bakgrunnen mens det forrige bildet ble vist på skjermen. Ved uttesting av løsningen på en virkelig WAP-telefon (Nokia 7110) var det derfor en stor overraskelse at WAP-telefonen tok over hele skjermbildet med timeglass og en ventebeskjed ved hver ny nedlasting. WAP-telefonens iver etter å informere brukeren om at nedlastning kan ta tid ødelegger rett og slett for denne måten å implementere simuleringen i en virkelig WAP-telefon!

Selv om simuleringen slik den er implementert ikke fungerer tilfredsstillende på en virkelig WAP-telefon, vil idéene og brukergrensesnittet kunne utprøves i det verktøyet som er benyttet. Implementasjon i en virkelig WAP-telefon må angripe presentasjonsformen på en annen måte. Jeg kan tenke meg flere måter det kan gjøres på:

? WML-Script-funksjon for å slå av venteinformasjonen til brukeren ved nedlasting. Det må være en skript-funksjon som slår av funksjonaliteten; det holder ikke at brukeren eventuelt kan gjøre det fra telefonmenyene. Jeg kan imidlertid ikke se at WML-Script tilbyr styring av den siden av brukergrensesnittet.
? Hele visualiseringen kan implementeres i WML-Script slik at WML-Script-applikasjonen selv henter ned nye oppdateringer av hestenes posisjoner. Dette kan utføres av WML-Scripts biblioteksfunksjon *URL.loadString*. Denne funksjonen returnerer innholdet av en URL til en variabel, og det antas at denne funksjonen ikke vil ha bivirkningene som er beskrevet overfor. WML.Script kan så formatere og presentere skjermbilder.
? Hele eller store deler av hesteløpet kan lastes ned til mobiltelefonen samtidig, og løpet kan så simuleres i WML-Script eller WML. Animasjonen vil da ikke skje i sanntid, men kanskje opp til ett eller to minutter etter at det faktiske løpet har startet.

Det siste av forslagene ovenfor vil redusere antall nedlastinger og dermed antall ganger ventebeskjeden fremvises. Det vil redusere plagen, men ikke fjerne den helt med mindre hele løpet lastes ned samtidig. Bruk av WML-Script-funksjonene *URL.loadString* vil sannsynligvis fjerne ventebeskjeden (dette ble ikke testet), men

[59] Posisjoneringsprosessen fungerte relativt dårlig. Jeg måtte håndkode alle bildene i en sekvens for å få et godt inntrykk av objektene i bevegelse.

vil til gjengjeld kreve noe programmering i WML-Script, i motsetning til den statiske fremvisningen som det opprinnelig var lagt opp til. Da alternative metoder for implementasjon på en virkelig WAP-telefon synes å eksistere, og da idéene om karakterbasert visualisering lar seg teste uten problemer i verktøyet som er benyttet, anså jeg det ikke som interessant å forfølge teknikkene for å få det til å fungere tilfredsstillende på en virkelig WAP-telefon. Det antas være en mindre jobb å implementere de manglende bitene hvis det senere blir aktuelt å demonstrere simulatoren på en virkelig WAP-telefon.

9.5 De andre fasene

Som det fremkommer nedenfor i dette avsnittet er innløsningsfasen, utbetalingsfasen og ”hyggelig melding”-fasen i spillet relativt greit håndterbare for scenariets spill-tilbyder. Fasene har begrenset interesse i en demonstrator hvor bare brukergrense-snittet er synlig.

I innløsningsfasen overføres spillerens signerte elektroniske kontanter fra tilbyderen til pengeutsteder for godskriving av tilbyderens konto. Denne fasen inkluderer ikke spilleren. Premissene og prosedyrene for innløsning vil være lagt av utsteder av elektroniske kontanter.

Gevinstutbetalingsfasen vil på samme måte være en handling som heller ikke omfatter spilleren, men vil være en handling mellom tilbyderen og spillerens bank. I avsnitt 8.5 ble det argumentert med at utbetaling av elektroniske kontanter til mobiltelefonen ikke er en god idé, og spillerens rolle i denne fasen blir ikke annet enn en tekstmelding med informasjon om forestående utbetaling. Utbetaling vil gå som en vanlig banktransaksjon.

”Hyggelig-melding”-fasen vil, for den heldige spilleren, resultere i en tekstmelding til hans mobiltelefon. Avsnitt 8.7 beskrev betenkelige sider ved å plukke opp spillerens geografiske posisjon, selv om mobilnettet har denne funksjonaliteten. I en teknisk realisering av denne fasen må også tilbyderen gjøre om en identifikator for mobiltelefonens basestasjon til fysisk stedsangivelse. Mobiloperatørene må være tilretteleggere.

9.6 Oppsummering

Dette kapittelet har beskrevet mobiltelefonen i praktisk bruk mot en enkel spilletjeneste. Handlingene i påfyll av den mobile lommeboken ble beskrevet, og brukergrensesnittet ble vist. Spillefasen, hvor brukeren fyller ut bong og betaler, ble gitt samme oppmerksomhet. Dette kapittelet har lagt spesiell vekt på delresultatfasen. I denne fasen får brukeren se spillet visualisert på sin mobiltelefon. Det ble regnet på overføringshastigheter i GSM-nettet, og det ble konstatert at båndbredde og forsinkelse var innenfor akseptable grenser. Forskjellige protokoller ble sammenlignet og det ble vist at WAP-protokollene er vel så effektive som HTTP.

Simulering og tegnbasert animering ble beskrevet. Animasjonen fungerte tilfredsstillende på demonstratorverktøyet under uttestingen, men i en virkelig WAP-telefon viste implementasjonen seg mindre attraktiv. Det ble argumentert med hvordan implementasjonen kunne vært utført for å omgå problemene.

10 Oppsummering og konklusjon

I denne oppgaven har jeg undersøkt hvordan mobiltelefonen kan benyttes til spill- og betalingstjenester på Internett. Jeg har eksemplifisert tjenestene i en enkel demonstrator. Oppgaven har hatt et perspektiv på inntil to år frem i tid. Særlig betaling er viet oppmerksomhet, da enkle og sikre betalingstjenester er viktig for utbredelse og bruk av Internett-tjenester. Oppgaven har tatt utgangspunkt i et spillescenario for å ha noe å relatere teknologier og tjenester til.

I diskusjonen av bæretjenester ble det konstatert at hverken dagens linjesvitsjete eller dagens pakkesvitsjete datatjenester i GSM-nettet er ideelle. De utnytter kapasiteten i eteren dårlig. Dagens tjenester er først og fremst begrenset av lav båndbredde, noe som utelukker selv lavkvalitet multimedia. Også prising av tjenesten per tidsenhet som i dag, i motsetning til prising etter volum, vil ikke alltid passe i scenarier med mye brukerinteraksjon. Den kommende pakkesvitsjete bæretjenesten GPRS synes å ha de savnede egenskapene: rask oppkobling til aksessnettet, liten forsinkelse og båndbredde for begrenset multimedia. GPRS forventes en gang i år 2001.

WAP – Wireless Application Protocoll – er viet spesiell oppmerksomhet i flere kapitler, og det vises at WAP har muligheter til å kunne realisere betalingstjenester og enkle spill over Internett levert til mobile enheter. Studier av WAP-protokollene viser, noe overraskende, at sikkerhetsprotokollen i WAP (WTLS) ikke vil gi ende-til-ende-sikkerhet mellom den mobile enheten og tjenester på Internett. Skal ende-til-ende-sikkerhet bygges må WAP-applikasjonene besørge det selv.

Mobile enheter er ikke nødvendigvis ensbetydende med den tradisjonelle mobiltelefonen. Mange andre mobile enheter i forskjellige fasonger vil ha større skjerm og raskere grafikk, og vil være bedre egnet til spill enn den tradisjonelle mobiltelefonen. Ut fra utviklingstrekkene som er presentert i denne oppgaven, kan det synes som om de forskjellige enhetene vil smelte sammen til én universalinnretning – en multimediaterminal i lommestørrelse. Det konkluderes imidlertid med at den tradisjonelle telefonen vil ha størst markedspotensiale i umiddelbar fremtid på grunn av pris og allsidig funksjonalitet. En tjeneste som tenkes å nå ut til flest mulig brukere bør fungere optimalt på denne enheten.

Sikkerhetsfunksjonaliteten som smartkort gir er en forutsetning for realisering av mobiltelefonen i betalingssammenheng, enten det er snakk om debet-, kreditt- eller småpengeløsninger. Smartkort er en sikker og ”tuklefri” enhet for bruk i en åpen og usikker Internett-verden. Det argumenteres for at heller ikke handlingene i spillet, som utfylling av bong, vil være godt nok sikret uten bruk av smartkort til signering.

Digital signering ved hjelp av mobiltelefonen kan komme til å bli en interessant tjeneste på linje med betaling over mobiltelefonen. Det vises at WAPs biblioteks-

funksjoner vil gi nettopp den autentiseringsfunksjonaliteten som ofte er ønsket i interaksjon med tjenester på Internett.

Generelle smartkortoperativsystemer hvor flere applikasjoner kan administreres på ett kort, er i ferd med å komme på markedet. Denne fysiske forutsetningen kan være med på å virkeliggjøre visjonene om mobiltelefonen som et universelt betalingsinstrument.

Pengespill over Internett er ikke tillatt i dag. I lovutkast ligger det an til lovendring som gjør spill over Internett lovlig, forutsatt at tjenestene kan sikres mot kriminell virksomhet og at trygge betalingsformer kan etableres. En annen interessant observasjon er at spill på kreditt faktisk ikke er forbudt i dag. Det heter seg imidlertid at ingen hefter ved spillegjeld, slik at spillegjeld ikke kan inndrives med loven i hånd. I nye lovforslag vurderes det å gjøre spill på kreditt forbudt.

Oppgaven vurderer flere mulige betalingsmodeller, blant andre også Telenors MobilHandel og oppgjør over telefonregningen. Det konkluderes med at en debetløsning kombinert med elektroniske kontanter vil være ideelt for betaling på Internett, da løsningene er generelle, gir god sikkerhet, gir potensielt rimelige transaksjoner og modellene håndterer til sammen små og store transaksjoner.

Oppgaven diskuterer spill uten en forutgående registreringsfase. Registrering er en ”unødvendig” handling og kan være en terskel for å delta i spill eller andre tjenester på Internett. Det konkluderes med at en signeringsapplikasjon (i mobiltelefonens smartkort) i mange tilfeller kan gi nok informasjon til at en registreringsfase kan unngås. På den annen side later det ikke til at det finnes gode og generelle mekanismer for utbetaling av små og store gevinster i spill. Utbetaling til mobiltelefonen hadde vært ideelt. En spilltilbyder er i praksis henvist til å be spilleren om utbetalingskonto.

GSM-nettet har ikke båndbredde til å realisere video til mobile enheter i dag. Siste versjon av WAP (1.2) spesifiserer push-funksjonalitet hvor den mobile enheten mottar en kontinuerlig strøm av data, men push er ikke implementert i dagens nett og kan derfor ikke testes. Jeg har i denne oppgaven uført empiriske studier av oppfriskningsraten i WAP ved å benytte ”pull”-modellen hvor den mobile enheten aktivt henter ned nye websider. Undersøkelsene viste at det vil være mulig å laste ned ett nytt skjermbilde med tekstlig informasjonsinnhold hvert 1,3 sek., og inntil ett nytt bitmap hvert 1,7 sek. Denne takten vil være tilstrekkelig for å gi et godt inntrykk av et hesteløp for eksempel, men vil være helt uakseptabelt i andre sammenhenger. Ved push-modellen ble det beregnet – ved å sammenligne med filoverføring på TCP/IP over GSM – at det vil være mulig å laste ned inntil to bitmaps i sekundet.

Animering ved hjelp av karaktersymboler ble studert nærmere, og det ble implementert en enkel simulator som visualiserte en hesteløp. Det ble vist at tekstbasert visualisering på mobiltelefonen kan gi et akseptabelt inntrykk av enkle objekter i bevegelse hvis det ikke stilles for store krav til plassering av objektene på skjerm. Karakterbasert animasjon vil være begrenset av symboler av fast utstrekning og faste posisjoner på den mobile enhetens skjerm. Slik teknikken er i dag er dette en

primitiv måte å animere et spill innen de begrensningene som eksisterer. Dagens systemer må da også sees på som kun en mellomstasjon før teknologien raser videre. Innen kort tid vil push-teknologi over dagens bærer, GSM-data, gi noe bedre kvalitet. Push-teknologi over morgensdagens bærer, GPRS, vil kunne realisere lavkvalitet mulitmedia til mobile enheter i år 2001, mens UMTS vil være ”den endelige løsningen”, tidligst i år 2002.

I listeform kan oppgavens konklusjon sammenfattes som følger:

? **Ang. lovverket:** Lovverket er foreløpig til hinder for spill på Internett, men det vil trolig endre seg når nye lovforslag vedtas (se avsnitt 6.2). Lovforslagene vil antakelig kreve at det etableres sikre rutiner for identifisering av spillere for å unngå hvitvasking av penger og unngå misbruk fra mindreårige. Betaling for spill vil antakelig kun bli tillatt mot kontant betaling (forhåndsbetaling, elektronisk kontanter eller debetløsninger), og utbetaling vil trolig i praksis måtte gå til spillerens bankkonto for å tilfredsstille kravet om sikker utbetaling av gevinst. Mobiltelefonen er meget godt egnet til å imøtekomme forventede krav i de nye lovene. Mobiltelefonen har et klart fortrinn fremfor tradisjonelle nettleser-løsninger på Internett ved at mobiltelefonen har smartkortbasert sikkerhet som iboende funksjonalitet. Forhold som autentisering, konfidensialitet og integritet vil kunne fungere ende-til-ende på en svært enkel og integrert måte. Noe arbeide gjenstår dog før dette er på plass i WAP.

? **Ang. betaling:** Igjen gir smartkortet i mobiltelefoner mulighet for å implementere tilfredsstillende sikkerhet for betalingsløsninger. Særlig i kombinasjon med Bluetooth (se avsnitt 3.5) har mobiltelfonen potensiale til å bli en universell personlig betalingsterminal. Bankene sitter med de fleste kortene på hånden, og det vil antakelig være bankene som avgjør om vi får gode betalingsløsninger som er tilpasset mobilteknologien og er tjenlig for brukerne.

? **Ang. device-teknologi:** Dagens WAP-skjermer er stort sett for små til å holde informasjon av noe ”størrelse”. Produsentene står i dag overfor valget mellom å lage mobiltelefoner med WAP-funksjonalitet eller WAP-enheter med tale-funksjonalitet. Det er rimelig å tro at WAP-telefonene utvikler seg i retning av små multimediaterminaler med langt bedre brukergrensesnitt enn dagens utstyr.

? **Ang. visualisering:** Visualisering av informasjon på WAP-enheter er i dag begrenset til karakterbasert informasjon og enkle bitmaps. Mulighetene for å implementere ”interessante” spill er begrenset, som vist i denne oppgaven. Det er et åpent spørsmål om mobiltelefonprodusentene vil åpne sine systemer for f.eks. nedlasting av Java-applets og eksekvering i mobiltelefonen.

? **Ang. kommunikasjonssikkerhet:** Kommende versjoner av WAP vil adressere problemene med kommunikasjonssikkerhet. Det er imidlertid uheldig at transportlagssikkerhet i WAP ikke vil fungerer ende-til-ende. Mobiloperatørene vil konkurrere om å tilby tilleggstjenester på toppen av WAP som gir ende-til-ende-sikkerhet. Hva dette betyr for forbrukere er usikkert, men det bør uansett ikke gå ut over interoperabilitet.

? **Ang. bæretjenester:** Dagens GSM-bæretjenester er beheftet med lange latenstider og lav båndbredde. Det er først når GPRS-nettet er på plass at vi vil få en WAP-tjeneste som har potensiale til å gi brukervennlige responstider samt et mer interessant brukergrensesnitt.

Mobiltelefonen har alle forutsetninger for å bli en universell enhet for kommunikasjon, spill og betaling, som har vært denne oppgavens fokus. *Teknologiske muligheter* betyr imidlertid ikke at alle teknologier realiseres eller at tjenestene vil få gjennomslagskraft i markedet. Det blir uansett spennende å følge med i den videre utviklingen i tiden som kommer.

Referanser

[AL00] Intervju med Anund Lie, sjefsforsker ved Norsk Regnesentr. Jan. 2000

[ALC99] *The future beyond GSM.* Compagnie Financière Alcatel France. 1999. http://www.alcatel.com/telecom/mcd/keytech/gsm/page_5.htm

[ATG] AB Trav och Galopp. http://www.atg.se (22.3.99)

[AUR99] AU-System Radio AB. *WAP White Paper*. Februar 1999. http://www.wapguide.com/wapguide/Auwap.pdf (21.1.00)

[Berge98] Nils Harald Berge og Joachim Lous. *Smartkort: teknologi og anvendelser*. ELCOM-seminar. 13. novenber 1998. http://www.nr.no/gem/elcom/seminar/tekn-sem.html

[Brasche97] Götz Brasche og Bernhard Walke, *Concepts, Services, and Protocols of the New GSM Phase 2+ General Packet Radio Service*, IEEE Communications Magazine, august 1997

[BBS] Bankenes Betalingssentral AS. http://www.bbsas.no (23.3.99)

[BBSP] *Proton in the World – Norway*. Protonworld Information (1.2.00), http://www.protonworld.com/world/countries/norway.htm

[BS96] Finansdepartementet. *Betalingssystemer m.v.* NOU 1996:24. Statens Forvaltningstjeneste. 11.november 1996. http://www.odin.dep.no/nou/1996-24/index.htm

[Cai97] Jian Cai og David J. Goodman, *General Packet Radio Service in GSM*, IEEE Communications Magazine, oktober 1997

[Comp99] Trivnet. *Piggybacking on ISPs with a payment system that couldn't be simpler*. ComputerLetter Vol 15 No 16, May 17, 1999, http://www.trivnet.com/html/article9.html (9.6.99)

[David97] Klaus David, *Network evolution aspects toward a third generation mobile system*, ITG-Fachbericht, vol 145, 1997

[Husemann99] David Husemann. *The Smart Card: Don't Leave Home Without It.* IEEE Concurrency. April-June 1999.

[DIGI041298] *Norge innfører lisensplikt på krypteringseksport.* Artikkel i digi.no 4.12.98

[DIGI140999] Øystein Kviestad, *3Com skiller ut Palm.* Artikkel i digi.no 14.9.99

[DIGI021299] Fride Eriksen. *Telenor stenger for betaling av piggdekkavgift.* Artikkel i digi.no 2.12.99. http://www.digi.no/digi98.nsf/pub/te19991202153200fse1709773404

[DIGI071299 Harald Blombach. *GSM-kryptering angivelig knekket*. Artikkel i digi.no 7.12.99. http://www.digi.no/digi98.nsf/pub/te19991207145000hab7154039826

[DIGI130100] Einar Ryvarden. *Nå blir datasikkerheten bedre*. Artikkel i digi.no 13.1.00. http://www.digi.no/digi98.nsf/pub/dd20000113115800er3576562142

[DIGI310100] Eirik Rossen. *Panikk i det franske bankvesen*. Artikkel i digi.no 31.1.00. http://www.digi.no/digi98.nsf/pub/dd20000131162600ero6650644694

[DIGIC] DigiCach Inc, http://www.digicash.com (26.3.99) [Konkurs 4. nov. 1998, (regnes som oppfinneren av digitale kontanter)]

[DNB97] *Avtale- og regleverksamling for innenlandsk betalingsformidling.* Den Norske Bankforening. November 1997.

[Eberspächer99] Jörg Eberspächer og Hans-Jörg Vögel. *GSM Switching, Services and Protocols*. John Wiley & Sons, 1999

[ELCOM] ELCOM-programmet, Norsk Regnesentral, http://www.nr.no/gem/elcom (27.12.99)

[ER99] Ericcson. *Welcome to the third generation,* Ericsson Radio Systems AB, AE/LZT 123 4351, 1999

[ET99] Intervju med Eva Trasti, markedssjef Fellesdata AS. Juni 1999

[Ford97] Warwick Ford og Michael S. Baum. *Secure electronic commerce.* Prentice Hall PTR. 1997

[Garfinkel97] Simon Garfinkel og Gene Spafford. *Web Security & Commerce.* O'Reilly & Associates, juni 1997.

[GEM] GEM – Gruppe for Elektronisk Markedsplass og virksomhetsutvikling, Norsk Regnesentral, http://www.nr.no/gem (22.3.99)

[GSMASS] GSM Association, http://www.gsmwolrd.com (8.6.99) [Internasjonal organisasjon av teleoperatører.]

[GSM] ETSI. [Alle spesifikasjonene ligger online] http://www.etsi.org 16.1.00.

[GSM 03.48] ETSI. *Digital cellular telecommunication system (Phase 2+); Security Mechanisms for the SIM Application Toolkit; Stage 2.* ETSI 1999-07. http://www.etsi.org (16.1.00)

[GSM 11.11] ETSI. *Digital cellular telecommunication system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface.* ETSI 1998-01. http://www.etsi.org (16.1.00)

[GSM 11.14] ETSI. *Digital cellular telecommunication system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface.* ETSI 1999-07. http://www.etsi.org (16.1.00)

[GWD98] Gemplus Wireless Division. *Boosting Value Added Services with SIM Application Toolkit – White Paper.* Gemplus 8. oktober 1998. http://www.gemplus.com/app/wireless/technology/sim_toolkit.html (28.12.99)

[HKJC] Hong Kong Jockey Club, http://ww.hkjockeyclub.com (22.3.99)

[Holms96] Peter Holms og Frode Løbersli og Yngve Lindsjørn og Joachim Lous, *Scenarios for IMiS.* NR notat 30.10.96. http://www.nr.no/imis/imis-p/SCENARIO.html (17.8.99)

[Høe99] Christian Høe. *Smartkort som betalingsmiddel. Hvordan fungerer teknologien og hvordan implementerer man løsninger som tar den i bruk?* Hovedfagsoppgave IfI UiO. 3. mai 1999

[ISO7816] ISO. *ISO 7816: Identification cards, integrated circuit vards with contacts.* International Standards Organization. 1999

[IT050599] Jørgen Berner Ross, *Utsetter raskere mobil, NetCom vil ikke tilby HSCSD*. Artikkel i www.itavisen.no 5.5.99. http://www.itavisen.no/mobil/?id=1287117

[Kennedy97] Richard Kennedy. *The history of GSM*. Mobile Communications International. 1997. http://www.gsmworld.com/history

[LD95] *Spillereglement for totalisatorspill.* Godkjent av Det Kgl. Landbruksdepartement oktober 1995. http://195.18.195.56/spill_info/spilleregler_2.html (25.11.99)

[LDAP] W. Yeong og T. Howes og S. Kille. *Lightweight Directory Access Protocoll.* Internet Engeneering Task Force RFC 1777. 1995 Se http://www.ietf.org/rfc/rfc1777.txt , http://www.ieft.org/rfc/rfc2251.txt

[Lie99] Anund Lie. *Bilagsapplikasjon i smartkort.* GEM Rapport 2/99, Norsk Regnesentral. Desember 1999

[Lin00] Intervju med Arnfinn Lindstad, utvikl.sjef Norsk Rikstoto. Jan. 2000

[NR] Norsk Rikstoto. http://www.rikstoto.no (1.2.00)

[Casner94] Steve Casner, *Frequently Asked Questions on the Multicast Backbone*. 7.11.94 http://www-ks.rus.uni-stuttgart.de/mbone/faq.html (1.2.00)

[McClure98] Stuart McClure. *SSL makes headway as an encryption standard.* Netscape Communications. http://www.ne-dev.com/ned-01-1998/ned-01-security.html

[MCARD] MasterCard Inc. http://www.mastercard.com (23.3.99) betalingsformidling, SET

[MIME] Borenstein, et al. *MIME (Multipurpose Internet Mail Extensions), Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies*. RFC 1521. September 1993. http://ftp.isi.edu/in-notes/rfc1521.txt (16.1.00)

[MobilHandel] MobilHandel, Telenor 5.11.1999. http://www.privat.telenor.no/Produkter/MobilHandel.asp (18.11.99)

[MONDEX] Mondex Inc. http://www.mondex.com (26.3.99), elektroniske kontanter

[Nurkic97] Ilhana Nurkic. *Mobile Communication Security: Current Status and Future Trends*. Global Communication Interactive 1997.

[NWT] Nokia Wap Toolkit, versjon 1.1, http://www.forum.nokia.com/developers/wap/wap.html (02.11.99)

[NSJava] Netscape. http://www.netscape.com (1.2.00)

[OT99] Justis og politidepartementet. *Odelstingsprepisosjon nr 84 (1998-99) Om lov om lotterier m.v. og statens Lotterisyn (lotteriloven).* ODIN. 11. juni 1999. http://odin.dep.no/repub/98-99/otprp/84/ (8.1.00)

[Proton] Proton World. http://www.protonworld.com (6.1.00)

[QPASS] Qpass Inc, http://www.qpass.com, (23.3.99), elektronisk betaling

[RS00] Intervju med Roar Smidt, Bull. Januar 2000

[Scourias98] John Scourias. *Overview of the Global System for Mobile Communication.* Nov. 1998. http://www.shoshin.uwaterloo.ca/~jscouria/GSM/gsmreport.html (1.2.00)

[SET] http://www.setco.org (6.5.99) Informasjon om Secure Electronic Transaction protokollen.

[SG00] Intervju med Stine Granviken, seniorkonsulent. Posten SDS. Jan. 2000

[Solberg96] Knut Solberg, *Secure Electronic Transaction (SET) – En gjennomgang*. Notat GEM 3/96. http://www.nr.no/gem/elcom/publikasjoner/set (19.8.99)

[SSL] Netscape. *Secure Socket Layer Protocol.* http://www.netscape.com

[SS00] Intervju med Stein Magne Sølna, konsulent. Telenor Mobil. Jan. 2000

[Taylor99] Ian Taylor et al. *Wireless Communication, Portables Devices and Use.* Notat. 08/99 IMEDIA. Norsk Regnesentral. Desember 1999.

[TELEK] http://privat.telenor.no/Produkter/TeleKort.asp (22.3.99) Telenors TeleKort

[TH99] Intervju av Tore Holmberg. IT-sjef Norsk Rikstoto. Januar 1999

[TRIVNET] Trivnet Inc, http://www.trivnet.com (9.6.99), elektronisk betaling

[Uddenfeldt98] Jan Uddenfeldt. *Digital Cellular –its roots and its ruture.* Proceedings of the IEEE. Vol.86 No 7. July 1998.

[VISA] Visa Inc. http://www.visa.com (23.3.99) betalingsformidling, SET

[VISAC] http://www.visa.com/cgi-bin/vee/pd/cash/main.html?2+0 (26.3.99) Visa Cash, elektroniske penger, fra Visa Inc.

[WAP] *Wireless Application Protocol Architecture Specification.* Wireless Application Protocol Forum, Ltd. Versjon 30. april 1998. http://www.wapforum.org (29.01.99)

[WAE] *Wireless Application Protocol Wireless Application Environment Overview.* Wireless Application Protocol Forum, Ltd. Versjon 30. april 1998. http://www.wapforum.org (29.01.99)

[Walter95] Knyt Erik Walter og Per Hjalmar Lehne, *The basics of mobile communications*. Telektronikk, nr 4 1995

[WAP-Forum] Wireless Application Forum.. http://www.wapforum.org

[WAPP] WAP-Forum. *WAP Push Message*. Wireless Application Protocol Forum, Ltd. Version 16-August-1999. http://www.wapforum.org

[WAPWIM] WAP-Forum. *Wireless Aplication Protocol Identity Module Specification. Part: Security*. Wireless Application Protocol Forum, Ltd. Proposed Version 05-Nov 1999. http://www.wapforum.org

[WAS] Wassenaar-samarbeidet. http://www.wassenaar.org (23.3.99) [Samarbeidsorgan (33 land) om kontroll av sensitiv teknologi.]

[WML] WAP-Forum. *Wireless Application Protocol Wireless Markup Language Specification.* Wireless Application Protocol Forum, Ltd. Versjon 30. april 1998. http://www.wapforum.org

[WMLSCL] WAP-Forum. *Wireless Application Protocol WMLScript Crypto Library Specification.* Wireless Application Protocol Forum, Ltd. Proposed Version 05-Nov-1999. http://www.wapforum.org

[WTLS] WAP-Forum. *Wireless Application Protocol Wireless Transport Layer Security Specification.* Wireless Application Protocol Forum, Ltd. Versjon 30. april 1998. http://www.wapforum.org

[X500] ISO/IEC/ITU. *Information Technology – Open Systems Interconnection – the Directory.* ISO/IEC 9594. ITU-T X.500 serien. 1993. http://www.itu.ch

[X509] ISO/IEC/ITU. *Information Technology – Open Systems Interconnection – the Directory: Authentication Framework.* ISO/IEC 9594-8 og ITU-T X.509. April 1996. http://www.itu.ch

[XML] Extensible Markup Language

[Ølnes97] Jon Ølnes, *Infrastruktur for sikker kommunikasjon – TTP-tjenester og offentlig engasjement.* Norsk Regnesentral, NR Notat OMNI/01/97 1997. http://www.nr.no/publications/omni_01_97.ps

Vedlegg A. Forkortelser og forklaringer

1G	Første generasjons mobilnett. Eksempelvis analoge NMT i Norden.
2G	Andre generasjons mobilnett. Dagens digitale GSM-nett.
3G	Tredje generasjons mobilnett. Kommende sammensmelting av tele- og datakommunikasjon
Alfanumerisk	Tegnsymboler (som f.eks. kan genereres på et ordinært PC-tastatur)
APDU	Application Protocol Data Unit.
API	Application Programming Interface
Applet	*Standardisert utvidelse av WEB-servere og eller klienter (se cgi-bin)*
Applikasjon	(I smartkort:) Et sett med sikkerhetsmekanismer, filer, data og protokoller
Asymmetrisk kryptering	Kryptering ved hjelp av et nøkkelpar. Kryptering skjer med den ene nøkkelen, dekryptering med den andre.
Autentisering	Handling for å fastslå ektheten til en identitet. Den klassiske autentiseringsmetoden er bruk av passord.
BBS	Bankenes Betalingssentral
Bong	Spillerekke i hestespillsport
Bookmarkliste	Brukerens liste av URL'er i nettleseren (muligens i en mobiltelefon)
Browser	Se nettleser
Båndbredde	Overføringskapasitet i transportmedium.
C-Netz	Analog mobiltelekommunikasjonsstandard i (Vest-) Tyskland
CEPT	Conférence des Administrations Européenes des Postes et Télécommunications. Samarbeidsorgan bestående av et tjuetalls europeiske telekommunikasjons-administrasjoner. Nå nedlagt; rollen overtatt av ETSI
cgi-bin-skript	Standardisert utvidelse av WEB-servere for behandling av data sendt fra nettleser; ineffektivt fordi prosess må startes/stoppes for hver transaksjon
Clearing	Pengeoverføringer mellom banker i Norge gjennomføres av BBS i en prosess kalt *clearing*
Datagram	Melding som ikke bekreftes av mottaker
EEPROM	Electrical Erasable Programmable Read Only Memory.
Elektronisk sertifikat	Elektronisk legitimasjon som knytter offentlige krypteringsnøkler til *identiteter*.
ETSI	Europeean Telecommunication Standardization Institutt
FN	Forente Nasjoner
Handover	Mobilitetsfunksjon for mobile enheter som gir transparent overføring av pågående sesjoner mellom tilknytningpunkter i mobilnettet
HTML	HyperText Markup Language. Standardisert presentasjonsspråk i WWW
HTTP	HyperText Transport Protocol
GSM	Global System for Mobile communications
GSM-data	GSM linjesvitsjet data (GSM Circuit-Switched Data) protokoll
GPRS	Global Packet Radio Service. Pakkesvitsjet datakommunikasjon i GSM
GPS	Global Position System. Satellittbasert navigasjonssystem

IC	Integreted Circuit
IMEI	International Mobile Equipment Identity. Kode for identifikasjon av *mobiltelefonen.*
IMSI	International Mobile Subscriber Identity. Kode for identifikasjon av mobiltelefonens SIM-kort.
IP	Internet Protocol. Standard nettverksprotokoll på Internett.
ISDN	Integrated Services Digital Network. Landbasert (i motsetning til eterbasert) internasjonalt digitalt telekommunikasjonsnettverk.
ISO	International Standards Organization.
ISP	Internett Service Provider. Internettleverandør. Aktører som leverer aksesstilgang til Internett og tjenester knyttet til Internett.
Interferens	”Støy” i radiokommunikasjon som skyldes bruk av overlappende frekvensbånd, hvor radiobølger ukontrollert forsterker eller utsletter hverandre.
ITU-T	International Telecommunication Union. Underlagt FN
Latens	Forsinkelse. Den tiden det tar å overføre én og samme bit fra sender til mottaker.
Nettleser	Klient-programvare for fremvisning ”WWW-informasjon” (webklient)
NMT	Nordic Mobile Telecom. Første generasjons analoge mobiltelekommunikasjonssystem i Norge og Norden.
MAP	Mobile Application Part. Høynivå telekommunikasjonsprotokoll som implementerer mobilitetsfunksjoner i GSM-nettet.
OSI	Open System Interconnect. Referansemodell for kommunikasjons-protokoller. Spesifisert av ISO.
PCMCIA	Personal Computer Memory Card International Association. Innstikkskort til bærbare Pcer.
PCS 1900	Det amerikanske GSM-nettet på 1900 MHz, nå kalt GSM 1900.
PDA	Personal Digital Assistant. Håndholdt datamaskin
PIN	Personal Identification Number
PKI	Public Key Infrastructure
ROM	Read Only Memory
QWERTY	Betegnelse på standard tastaturlayout
Roaming	Administrative avtaler mellom teleoperatører om aksess i hverandres mobilnett.
SET	Secure Electronic Transaction. Åpen industristandard-protokoll for sikker overføring av betalingsinformasjon over Internett og andre elektroniske nett. Utviklet av MasterCard, Visa med flere.
SIM	Subscriber Identity Module. Smartkort som benyttes i mobiltelefoner. Inneholder bla. identitetsnummer, krypteringsnøkkel og krypterings-algoritme.
Smartkort	Chip-kort med prosessor og minne
SMS	Short Message Service. Toveis tjeneste i GSM nettet for sending av alfanummeriske meldinger på inntil 160 tegn
SSL	Secure Socket Layer. Åpen standard, utviklet av Netscape Communications Company, for sikker kommunikasjon ved hjelp av elektroniske sertifikater i åpne nett.
Symmetrisk kryptering	Kryptering med en nøkkel. Kryptering og dekryptering skjer med en og samme nøkkel. Se også asymmetrisk kryptering
Synkron	Overføring av bits i takt med klokkepulsen (i kommunikasjonsprotokoll)

TACS	Total Access Communication Service. Analog mobiltelekommunikasjonsstandard i Storbritannia
TCP/IP	Transport Communication Protocoll / Internet Protocoll
Tiltrodd tredjepart	Se TTP
Totalisator	Et apparat for kontroll av innsatsene og fordelingen av gevinstene ved hesteveddeløp og andre konkurranser
TTP	Tiltrodd TredjePart. En aktør eller megler som begge parter i en handel har tillit til; eksempelvis en eiendomsmegler
URL	Uniform Resource Locator. Adresse for WWW-informasjon
USSD	Unstructured Supplementary Service Data. Bæreprotokoll i GSM-nettet.
WAP	Wireless Application Protocol. Protokoll designet for å levere Internett-tjenester og avansert telefonitjenester til digitale telefoner og tråløse terminaler
WAP-Forum	Rådgivende industri-samarbeidsforum for WAP standarden.
WML	Wireless Markup Language. HTML-lignende presentasjonsspråk optimalisert for bruk i trådløse telekommunikasjon. WML er implementert innenfor rammen av XML.
XML	eXtended Markup Language. Rammeverk for å lage struktureringsspråk for tekst
WEB	Se WWW
WTLS	Wireless Transport Layer Security. Sikkerhetsprotokollen i WAP som tilsvarer SSL/TSL på Internett.
WWW	World Wide Web. ”Informasjonsverden” på Internett

Vedlegg B. Kode

Deler av koden for betalings-brukergrensesnittet i WAP-demonstratoren

```
/*
 * Hestespill - Dagens dobbel
 *
 * Sjekk av input og initialisering av antall rekker og pris
 * @param returncard -- returnerer til dette card
 */

extern function ddkalk(returncard)
{
  var calc=1,dd1r=0,dd2r=0;
  var dd1=WMLBrowser.getVar("dd1");
  var dd2=WMLBrowser.getVar("dd2");
  var krprrekke=WMLBrowser.getVar("krprrekke");

  if (String.isEmpty(dd1))
    dd1r=0;
  else
    dd1r = String.elements(dd1,";");

  if (String.isEmpty(dd2))
    dd2r=0;
  else
    dd2r = String.elements(dd2,";");

  WMLBrowser.setVar("dd1r", dd1r);
  WMLBrowser.setVar("dd2r", dd2r);
  WMLBrowser.setVar("ddr", dd1r * dd2r);

  if (String.isEmpty(krprrekke)) {
    WMLBrowser.setVar("krprrekke", "?");
    calc=0;
  }

  if (calc==0 || dd1r==0 || dd2r==0) {
    WMLBrowser.setVar("ddpris", "?");
  }
  else {
    WMLBrowser.setVar("ddpris", dd1r * dd2r * krprrekke);
  }

// WMLBrowser.refresh();
// WMLBrowser.go("#ddkalk");
  WMLBrowser.go(returncard);
}


extern function ddsend(feilUrl, okUrl) {
```

```
// Sjekk at variabelene finnes og er initialisert
// og hopp til et av input-kortene
// Kunne ev. sende med en ev. feilmelding i en variabel

  var returl;
  var dd1=WMLBrowser.getVar("dd1");
  var dd2=WMLBrowser.getVar("dd2");
  var krprrekke=WMLBrowser.getVar("krprrekke");


 returl=okUrl;
  if (String.isEmpty(dd1) || String.isEmpty(dd2) ||
String.isEmpty(krprrekke))
    returl=feilUrl;

  WMLBrowser.go(returl);
}



<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">

<wml>

  <template>
   <!-- Sett på back label på alle kort per default -->
   <do type="prev" name="back" label="Back">
    <prev/>
   </do>
  </template>

      <card id="card1" title="Hestespill" newcontext="true">
   <!-- Override template -->
    <do type="prev" name="back" label="Back">
      <noop/>
    </do>

           <p align="center">
                 <!-- H O V E D V I N D U -->

            <img src="hestlogo.gif" alt="(Logo ikke tilgj)"/>
      <br/> <br/>
      Norsk<br/> Spillegalskap<br/> presenterer<br/>...

      <do type="accept" label="Dagens dobbel">
         <go href="#dobbel"/>
      </do>
      <do type="accept" label="V5">
         <go href="#ikkeimpl"/>
      </do>
      <do type="accept" label="Forhåndsutfylt">
         <go href="#ikkeimpl"/>
      </do>

     <do type="accept" label="Se på bong">
         <go href="#ikkeimpl"/>
      </do>
```

```
      <do type="reset" label="Veiledning">
         <go href="hestehjelp.wml"/>
      </do>

            </p>
      </card>

  <card id="dobbel" title="Dagens Dobbel">
  <p align="center">
     <br/>
    <b>Dagens løp</b>
  </p>
    <do type="accept" label="DD1 Bjerke">
       <go href="#dd1"/>
    </do>
    <do type="accept" label="DD2 Leangen">
       <go href="#dd2"/>
    </do>
    <do type="accept" label="Beløp pr rekke">
       <go href="#ddbelop"/>
    </do>
    <do type="accept" label="Send bong">
       <!-- Sjekk om inputfelt er fylt ut før vi havner på kortet
ddsend -->
       <go href="hestdd.wmls#ddsend('#ddsendfeil','#ddsend')"/>
    </do>
    <do type="accept" label="Tjenester">
       <go href="#ddtjen"/>
    </do>
    <do type="accept" label="Veiledning">
       <go href="#ikkeimpl"/>
    </do>
  </card>


  <card id="ddtjen" title="Dagens Dobbel">
  <p align="center">
     <br/><b>Velg tjeneste</b>

    <do type="accept" label="Kalkuler pris">
       <!-- <go href="#ddkalk"/>
        Kommer til #ddkalk fra WML-skript funk under -->
       <go href="hestdd.wmls#ddkalk('#ddkalk')"/>
    </do>
    <do type="accept" label="Sjekk odds">
       <go href="#ikkeimpl"/>
    </do>
    <do type="accept" label="Resultater">
       <go href="#ikkeimpl"/>
    </do>
  </p>
  </card>

  <card id="ikkeimpl" title="Beklager!">
  <p align="center">
    <b> Funksjon ikke implementert </b>
  </p>
  </card>

  <card id="dd1" title="Dagens Dobbel 1">
```

```
  <p align="center">
     <small> Marker vinner(e) i
         DD1 på Bjerke i dag<br/>
     </small>
            <select name="dd1" multiple="true">
            <option value="1"> 1 Mirka</option>
            <option value="2"> 2 Trø Knetken</option>
            <option value="3"> 3 Muttok</option>
            <option value="4"> 4 Julie Snerta</option>
            <option value="5"> 5 Troll Jonas</option>
            <option value="6"> 6 Lynge Prins</option>
            <option value="7"> 7 </option>
            <option value="8"> 8 </option>
            <option value="9"> 9 </option>
            <option value="10"> 10 </option>
            <option value="11"> 11 </option>
            <option value="12"> 12 </option>f
            <option value="13"> 13 </option>
            <option value="14"> 14 </option>
            <option value="15"> 15 </option>
            </select>
  </p>
  </card>

  <card id="dd2" title="Dagens Dobbel 2">
  <p align="center">
     <small> Marker vinner(e) i
         DD2 på Leangen i dag<br/>
     </small>
            <select name="dd2" multiple="true">
            <option value="1"> 1 Dream</option>
            <option value="2"> 2 Arigel</option>
            <option value="3"> 3 Hjelset Grim</option>
            <option value="4"> 4 Kling Hamra</option>
            <option value="5"> 5 Minijakken</option>
            <option value="6"> 6 </option>
            <option value="7"> 7 </option>
            <option value="8"> 8 </option>
            <option value="9"> 9 </option>
            <option value="10"> 10 </option>
            <option value="11"> 11 </option>
            <option value="12"> 12 </option>
            <option value="13"> 13 </option>
            <option value="14"> 14 </option>
            <option value="15"> 15 </option>
            </select>
  </p>
  </card>

  <card id="ddbelop" title="Dagens Dobbel">
  <p>
   Angi kr. per rekke
   <input name="krprrekke" value="10" format="*N" emptyok="false"
title="Kr per rekke" size="4" maxlength="4"/>
  <br/>
  </p>
  </card>

  <card id="ddkalk" title="Dagens Dobbel">
  <p>
```

```
    <table columns="2" align="LR">
    <tr> <td>Rekker i DD1</td> <td> $(dd1r) </td> </tr>
    <tr> <td>Rekker i DD2</td> <td> $dd2r </td> </tr>
    <tr> <td>Rekker tils</td> <td> $ddr </td> </tr>
    <tr> <td>Rekkepris</td> <td> $krprrekke </td> </tr>
    <tr> <td><b>Pris tils kr.</b></td> <td><b> $ddpris
</b></td></tr>
    </table>
  </p>
  </card>


  <card id="ddsendfeil" title="Feil!">
  <p><b><i>
     OBS: Du må fylle ut DD-1 og DD-2 og
     Beløp per rekke!
  </i></b>
  </p>
  </card>


  <card id="ddsend" title="Dagens Dobbel">
  <p>
     <small>
     Innsats kr. $ddpris <br/>
     Velg betalingsmåte:
     </small>
   <select name="betalingsmaate">
   <option value="El.kont"> El. kontanter </option>
   <option value="Debet"> Debet </option>
     </select>
     <small>Gi PIN-kode: </small>
     <input name="pin" type="password" format="*N" emptyok="false"
title="PIN-kode" size="4" maxlength="4"/>
     <small>og send</small>
 </p>
    <do type="accept" label="Send bong">
       <go href="#ddsend2"/>
    </do>
  </card>


  <card id="ddsend2" title="Dagens Dobbel">
  <onevent type="onenterforward">
    <go method=”post” href="http://www.nr.no/~staale/bong.cgi">
      <postfield name=”pin” value=$pin/>
      <postfield name=”El.kont” value=$Elkont/>
      <postfield name=”Debet” value=$debet/>
      <postfield name=”dd1” value=$dd1/>
      <postfield name=”dd2” value=$dd2/>
      <postfield name=”krprrekke” value=$krprrekke/>
    </go>
  </onevent>
  <p align="center">
     <big>... bong er sendt
  </big>
  </p>
  </card>

</wml>
```